Separating Variables in Bivariate Polynomial Ideals

Manfred Buchacher*, Manuel Kauers†, Gleb Pogudin‡

Abstract

We present an algorithm which for any given ideal $I \subseteq \mathbb{K}[x, y]$ finds all elements of I that have the form $f(x) - g(y)$, i.e., all elements in which no monomial is a multiple of xy.

1 Introduction

One of the fundamental problems in computer algebra and applied algebraic geometry is the problem of elimination. Here, we are given a polynomial ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and the task is to compute generators of the ideal $I \cap \mathbb{K}[x_1, \ldots, x_n]$. The resulting ideal of $\mathbb{K}[x_1, \ldots, x_n]$ consists of all elements of I that do not contain any terms that are a multiple of any of the variables y_i. It is well-known that this problem can be solved by computing a Gröbner basis with respect to an elimination order that assigns higher weight to terms involving $y_1, \ldots, y_m$ than to terms not involving these variables.

It is less clear how to use Gröbner bases (or any other standard elimination techniques) for finding ideal elements that do not contain any terms which are a multiple of certain prescribed terms rather than certain prescribed variables. The problem considered in this paper is an elimination problem of this kind. Here, given an ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$, we are interested in all elements of I that do not involve any terms which are multiples of any of the terms $x_i y_j$ ($i = 1, \ldots, n$, $j = 1, \ldots, m$). Note that, these are precisely the elements of I which can be written as the sum of a polynomial in $x_1, \ldots, x_n$ only and a polynomial in $y_1, \ldots, y_m$ only, so the problem under consideration is as follows.

Problem 1.1 (Separation)**.**

Input *An ideal* $I \subseteq \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$*;*

Output *Description of all* $f - g \in I$ *such that*

$$f \in \mathbb{K}[x_1, \ldots, x_n] \text{ and } g \in \mathbb{K}[y_1, \ldots, y_m].$$

At first glance, it may seem that there should be a simple way to solve this problem with Gröbner bases, similarly as for the classical elimination problem. However, we were not able to come up with such an algorithm. The obstruction seems to be that there is no term order that ranks the term xy higher than both x^2 and y^2.

We ran into the need for such an algorithm when we tried to automatize an interesting non-standard elimination step which appears in Bousquet-Mélou's "elementary" solution of Gessel's walks [9]. Dealing with certain power series, say $u \in \mathbb{K}[x][[t]]$ and $v \in \mathbb{K}[x^{-1}][[t]]$, she finds polynomials f, g such that $f(u) - g(v) = 0$, and then concludes that $f(u)$ and $g(v)$ must in fact belong to $\mathbb{K}[[t]]$. Deriving a pair (f, g) automatically from known relations among u, v amounts to the problem under consideration.

The problem also arises when one wants to compute the intersection of two $\mathbb{K}$-algebras. For example, suppose that for given $u, v \in \mathbb{K}[t_1, \ldots, t_n]$ one wants to compute $\mathbb{K}[u] \cap \mathbb{K}[v]$. This can be done by finding all pairs (f, g) such that $f(u) = g(v)$, i.e., all pairs (f, g) with $f(x) - g(y) \in \langle x - u, y - v\rangle \cap \mathbb{K}[x, y]$. See [3, 13] for a discussion of this and similar problems.

Definition 1.2. *Let* $p \in \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$*.*

1. p *is called* separated *if there exist* $f \in \mathbb{K}[x_1, \ldots, x_n]$ *and* $g \in \mathbb{K}[y_1, \ldots, y_m]$ *such that* $p = f - g$*.*
2. p *is called* separable *if there is a* $q \in \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ *such that* qp *is separated.*

*manfred.buchacher@jku.at, Institute for Algebra, Johannes Kepler University, Linz, Austria
†manuel.kauers@jku.at, Institute for Algebra, Johannes Kepler University, Linz, Austria
‡gleb.pogudin@polytechnique.edu, Department of Computer Science, Higher School of Economics, Moscow, Russia and LIX, CNRS, École Polytechnique, Institut Polytechnique de Paris, France

Proposition 1.3. *Let I be an ideal in $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m]$. Then*

$$A(I) := \{ (f, g) \in \mathbb{K}[x_1, \dots, x_n] \times \mathbb{K}[y_1, \dots, y_m] : f - g \in I \}$$

is a unital $\mathbb{K}$-algebra with respect to component-wise addition and multiplication and component-wise multiplication by elements of $\mathbb{K}$. We refer to $A(I)$ as the algebra of separated polynomials *of I.*

Proof. We just note that $A(I)$ is clearly a $\mathbb{K}$-vector space, and that it is closed under component-wise multiplication, as for any $(f, g), (f', g') \in A(I)$ we have $f - g \in I$ and $f' - g' \in I$, so $(f - g)f' + g(f' - g') = ff' - gg' \in I$. It is unital, because we always have $(1, 1) \in A(I)$. ☐

Given ideal generators of I, we want to determine $\mathbb{K}$-algebra generators of $A(I)$. This is in general too much to be asked for, because, as shown in Example 5.1, $A(I)$ may not be finitely generated. On the positive side, it is known that $A(I)$ is finitely generated if I is a principal ideal in the ring of bivariate polynomials (see [15]).

The main result of the paper is Algorithm 4.3 for computing generators of the algebra $A(I)$ for a given bivariate ideal $I \subseteq \mathbb{K}[x, y]$. In particular, it implies that such an algebra is always finitely generated and yields an algorithm to compute a minimal separated multiple of a bivariate polynomial [15, Definition 4.1]. An implementation of the algorithm in Mathematica can be found on the website of the second author.

The general structure of the algorithm is the following. Every bivariate ideal is the intersection of a zero-dimensional ideal and a principal ideal. We solve the separation problem for the zero-dimensional case (Section 2) and for the principal case (Section 3) separately. Then we show how to compute the intersection of the resulting algebras in Section 4. We conclude with discussing the case of more than two variables in Section 5.

In the context of separated polynomials, many deep results have been obtained for some kind of "inverse problem" to the problem considered here, i.e., the study of the shape of factors of polynomials of the form $f(x) - g(y)$, see [6, 7, 10, 11, 12, 14, 15] and references therein. We use techniques developed in [10] in our proofs (see Section 3).

We assume throughout that the ground field $\mathbb{K}$ has characteristic zero and that for a given element of an algebraic extension of $\mathbb{K}$ we can decide whether it is a root of unity. This is true, for example, for every number field (see Section 3.3).

It is an open question whether the assumption on the characteristic of $\mathbb{K}$ can be eliminated. In positive characteristic, additional phenomena have to be taken into account. For example, separable polynomials need not be squarefree, as the example $(x + y)^2 \in \mathbb{Z}_3[x, y]$ shows, which is separable because $(x + y)(x + y)^2 = (x + y)^3 = x^3 + y^3$.

2 Zero-Dimensional Ideals

When $I \subseteq \mathbb{K}[x, y]$ has dimension zero, it is easy to separate variables. In this case, there are nonzero polynomials p, q with $I \cap \mathbb{K}[x] = \langle p \rangle$ and $I \cap \mathbb{K}[y] = \langle q \rangle$. Clearly, these univariate polynomials p and q are separated. Also all $\mathbb{K}[x]$-multiples of p and all $\mathbb{K}[y]$-multiples of q are separated elements of I.

An arbitrary pair $(f, g) \in \mathbb{K}[x] \times \mathbb{K}[y]$ belongs to $A(I)$ if and only if $(f + up, g + vq)$ belongs to $A(I)$ for all $u \in \mathbb{K}[x]$ and $v \in \mathbb{K}[y]$. In particular, we have $(f, g) \in A(I) \iff (\operatorname{rem}_x(f, p), \operatorname{rem}_y(g, q)) \in A(I)$. It is therefore sufficient to find all pairs $(f, g) \in A(I)$ with $\deg_x f < \deg_x p$ and $\deg_y g < \deg_y q$. These pairs can be found with linear algebra.

Algorithm 2.1. *Input: $I \subseteq \mathbb{K}[x, y]$ of dimension zero.*
Output: generators of the $\mathbb{K}$-algebra $A(I) \subseteq \mathbb{K}[x] \times \mathbb{K}[y]$

1 *if $I = \langle 1 \rangle$, return $\{(1, 0), (x, 0), (0, 1), (0, y)\}$.*
2 *compute $p \in \mathbb{K}[x]$ and $q \in \mathbb{K}[y]$ such that*

$$I \cap \mathbb{K}[x] = \langle p \rangle \quad \text{and} \quad I \cap \mathbb{K}[y] = \langle q \rangle.$$

3 *make an ansatz $h = \sum_{i=0}^{\deg_x p - 1} a_i x^i - \sum_{j=0}^{\deg_y q - 1} b_j y^j$ with undetermined coefficients a_i, b_j.*
4 *compute the normal form of h with respect to a Gröbner basis of I and equate its coefficients to zero.*
5 *solve the resulting linear system over $\mathbb{K}$ for the unknowns a_i, b_j and let $(f_1, g_1), \dots, (f_d, g_d)$ be the pairs of polynomials corresponding to a basis of the solution space.*
6 *return $(f_1, g_1), \dots, (f_d, g_d), (p, 0), \dots, (x^{\deg_x p - 1} p, 0)$, $(0, q), \dots, (0, y^{\deg_y q - 1} q)$.*

Proposition 2.2. *Algorithm 2.1 is correct.*

Proof. It is clear by construction that all returned elements belong to $A(I)$. It remains to show that they generate $A(I)$ as $\mathbb{K}$-algebra. This is clear if $I = \langle 1\rangle$, because then $A(I) = \mathbb{K}[x] \times \mathbb{K}[y]$. Now suppose that $I \neq \langle 1\rangle$ and let $(f, g) \in A(I)$. Because of $I \neq \langle 1\rangle$, we have $\deg_x p, \deg_y q > 0$. Then $\langle p\rangle \subseteq \mathbb{K}[x]$ is generated as a $\mathbb{K}$-algebra by $p, xp, \ldots, x^{\deg_x p-1}p$. To see this, we just note that, by performing repeatedly division by p on a polynomial and the resulting quotients, any $u \in \langle p\rangle$ can be written

$$u = \sum_{i=1}^{k} r_i p^i$$

where r_i are polynomials with $\deg r_i < \deg p$. Hence, $\langle p\rangle$ is a subset of the algebra generated by $p, xp, \ldots, x^{\deg_x p-1}p$, and clearly, the reverse inclusion holds as well. For the same reason, $\langle q\rangle$ is generated as $\mathbb{K}$-algebra by $q, xq, \ldots, x^{\deg_x q-1}q$.

Hence (f, g) can be expressed in terms of the given generators if and only if $(\mathrm{rem}_x(f, p), \mathrm{rem}_y(g, q))$ can be expressed in terms of the given generators. Because of $\deg_x(\mathrm{rem}_x(f, p)) < \deg_x(p)$ and $\deg_y(\mathrm{rem}_y(g, q)) < \deg_y(q)$, the pair $(\mathrm{rem}_x(f, p), \mathrm{rem}_y(g, q))$ is a $\mathbb{K}$-linear combination of $(f_1, g_1), \ldots, (f_d, g_d)$, as required. □

Example 2.3. *Consider the* 0*-dimensional ideal* $I = \langle x^2y^2 - 1, y^5 + y^3 + xy^2 + x\rangle$. *We have*

$$I \cap \mathbb{K}[x] = \langle x^{10} + x^8 - x^2 - 1\rangle \text{ and } I \cap \mathbb{K}[y] = \langle y^{10} + y^8 - y^2 - 1\rangle.$$

Every separated polynomial of I *therefore has the form*

$$f(x) + u(x)(x^{10} + x^8 - x^2 - 1) - g(y) - v(y)(y^{10} + y^8 - y^2 - 1)$$

for certain $f(x), g(y)$ *of degree less than* 10 *and some* $u(x), v(y)$. *To find the pairs* (f, g), *compute the normal form of* $h = \sum_{i=0}^{9} a_i x^i - \sum_{i=0}^{9} b_j y^j$ *with respect to a Gröbner basis of* I. *Taking a degrevlex Gröbner basis, this gives*

$$(a_0 + a_8 - b_0) + (a_6 - b_2)y^2 + (a_7 + b_5)xy^2 + \cdots .$$

Equate the coefficients with respect to x, y *to zero and solve the resulting linear system for the unknowns* $a_0, \ldots, a_9, b_0, \ldots, b_9$. *The following pairs of polynomials* (f, g) *correspond to a basis of the solution space:*

$$\begin{aligned}
&(1, 1),\ (x - x^9, y^9 - y),\ (x^2, y^8 + y^6 - 1),\ (x^9 + x^3, -y^9 - y^3)\\
&(x^4, -y^8 + y^4 + 1),\ (x^5 - x^9, y^3 - y^7),\ (x^6, y^8 + y^2 - 1)\\
&(x^9 + x^7, -y^5 - y^3),\ (x^8, 2 - y^8).
\end{aligned}$$

These pairs together with the pairs $(x^i(x^{10} + x^8 - x^2 - 1), 0)$ *and* $(0, y^i(y^{10} + y^8 - y^2 - 1))$ *for* $i = 0, \ldots, 9$ *form a set of generators of* $A(I)$.

For an ideal $I \subseteq \mathbb{K}[x, y]$ to be zero-dimensional means that its codimension as $\mathbb{K}$-subspace of $\mathbb{K}[x, y]$ is finite. Note that, in this case, also $A(I)$ has finite codimension as $\mathbb{K}$-subspace of $\mathbb{K}[x] \times \mathbb{K}[y]$. Since we will need this feature later, let us record it as a lemma.

Lemma 2.4. *If* $I \subseteq \mathbb{K}[x, y]$ *has dimension zero, then there is a finite-dimensional* $\mathbb{K}$*-subspace* V *of* $\mathbb{K}[x] \times \mathbb{K}[y]$ *such that the direct sum* $V \oplus A(I)$ *is equal to* $\mathbb{K}[x] \times \mathbb{K}[y]$. *Moreover, we can compute a basis of such a* V, *and for every* $(f, g) \in \mathbb{K}[x] \times \mathbb{K}[y]$ *we can compute a* $(\tilde{f}, \tilde{g}) \in V$ *such that* $(f, g) - (\tilde{f}, \tilde{g}) \in A(I)$.

Proof. Let $p, q, (f_1, g_1), \ldots, (f_d, g_d)$ be as in Algorithm 2.1. Note that, as a $\mathbb{K}$-vector space, $A(I)$ has the basis

$$\{(f_1, g_1), \ldots, (f_d, g_d)\} \cup \{(x^k p, 0) : k \in \mathbb{N}\} \cup \{(0, y^k q) : k \in \mathbb{N}\}.$$

Using row-reduction, it can be arranged that the f_i have pairwise distinct degrees. Note that, all f_i are nonzero by the choice of q. Let V be the $\mathbb{K}$-subspace of $\mathbb{K}[x] \times \mathbb{K}[y]$ generated by the pairs $(x^k, 0)$ for all $k < \deg_x(p)$ which are not the degree of some f_i and the pairs $(0, y^k)$ for all $k < \deg_y(q)$. We have $V \oplus A(I) = \mathbb{K}[x] \times \mathbb{K}[y]$.

Given $(f, g) \in \mathbb{K}[x] \times \mathbb{K}[y]$, we compute $(\mathrm{rem}_x(f, p), \mathrm{rem}_y(g, q))$, and then eliminate all terms from the first component whose exponent is the degree of an f_i. The resulting pair $(\tilde{f}, \tilde{g})$ is an element of V with $(f, g) - (\tilde{f}, \tilde{g}) \in A(I)$. □

3 Principal Ideals

We now consider the case where $I = \langle p \rangle$ is a principal ideal of $\mathbb{K}[x, y]$. If $p \in \mathbb{K}[x] \cup \mathbb{K}[y]$, the algebra $A(I)$ of separated polynomials is finitely generated, as we have seen in the proof of Proposition 2.2. It was shown in [15, Theorem 4.2] that, if p is separable, there is a separated multiple $f(x) - g(y)$ of p that divides any other separated multiple of it. We refer to $f(x) - g(y)$ as *the minimal separated multiple* of p. Moreover, [15, Theorem 2.3] implies that if $p \notin \mathbb{K}[x] \cup \mathbb{K}[y]$, then (f, g) is an algebra generator for $A(I)$. We note that, [15, Theorem 2.3] was reproven in [8], and generalized further in [1, 19]. The proof of [15, Theorem 4.2] was not constructive. In the following we provide a criterion that allows to decide if p is separable, and if it is, to compute its minimal separated multiple.

Our criterion is based on considering the highest graded component of the polynomial with respect to a certain grading. The separability of the highest component is a necessary but not a sufficient condition for the separability of a polynomial itself. Surprisingly, there is a weaker converse, that is, the minimal separated multiple of the highest component is equal to the highest component of the minimal separated multiple of p *if the latter exists* (see Theorem 3.5). This allows us to reduce the problem for a general not necessarily homogeneous polynomial to the same problem for a homogeneous polynomial (which is solved in Section 3.1) and solving a linear system. The resulting algorithm is presented in Section 3.3.

Since the case $p \in \mathbb{K}[x] \cup \mathbb{K}[y]$ is trivial, for the rest of the section, we assume that $p \in \mathbb{K}[x, y] \setminus (\mathbb{K}[x] \cup \mathbb{K}[y])$.

3.1 Homogeneous case

Definition 3.1.

1. *A function ω from the set of monomials in x and y to $\mathbb{R}$ is called a* weight function *if there exist $\omega_x, \omega_y \in \mathbb{Z}_{>0}$ such that $\omega(x^i y^j) = \omega_x i + \omega_y j$ for every $i, j \in \mathbb{Z}_{\geq 0}$.*
2. *Two weight functions are considered to be* equivalent *if they differ by a constant non-zero factor.*
3. *For a weight function ω and a nonzero polynomial $p \in \mathbb{K}[x, y]$, $\omega(p)$ is defined to be the maximum of the weights of the monomials of p.*
4. *For a weight function ω and a polynomial $p \in \mathbb{K}[x, y]$, we define* the ω-leading part of p *(denoted by $\operatorname{lp}_\omega(p)$) as the sum of the terms of p of weight $\omega(p)$.*

In this subsection, we consider the case of p being homogeneous with respect to some weight function ω, that is, $\operatorname{lp}_\omega(p) = p$.

Proposition 3.2. *Let ω be a weight function, and let $p \in \mathbb{K}[x, y] \setminus (\mathbb{K}[x] \cup \mathbb{K}[y])$ satisfy $\operatorname{lp}_\omega(p) = p$. Then p is separable if and only if*

1. *p involves a monomial only in x, and*
2. *all the roots of $p(x, 1)$ in the algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$ are distinct and the ratio of every two of them is a root of unity.*

Moreover, if p is separable and N is the minimal number such that the ratio of every pair of roots of $p(x, 1)$ is an N-th root of unity, then the weight of the minimal separated multiple of p is $N\omega_x$.

Proof. Assume that p is separable, and let P be a separated multiple. Replacing P with $\operatorname{lp}_\omega(P)$ if necessary, we will further assume that $P = \operatorname{lp}_\omega(P)$. Since $P \notin \mathbb{K}[x] \cup \mathbb{K}[y]$ and is separated, P involves a monomial in x only, and hence, so does p.

Since P is ω-homogeneous and separated, it is of the form $ax^m - by^n$ for some $a, b \in \mathbb{K} \setminus \{0\}$, so $p(x, 1) \mid ax^m - b$. All roots of the latter are distinct and the ratio of each of them is an m-th root of unity. Hence, the same is true for $p(x, 1)$. This proves the only-if part of the proposition.

To prove the remaining part of the proposition, let N be as in the statement of the proposition, and $\gamma \in \overline{\mathbb{K}}$ be a root of $p(x, 1)$. Consider the ω-homogeneous Puiseux polynomial

$$P := x^N - \gamma^N y^{N\omega_x/\omega_y}.$$

We perform Euclidean division of P by p over the field F of Puiseux series in y over $\overline{\mathbb{K}}$. This will yield a representation $P = qp + r$, where q and r are also ω-homogeneous. Since $P(x, 1)$ is divisible by $p(x, 1)$, we see that $r(x, 1) = 0$. However, the ω-homogeneity of r implies that each of its coefficients with respect to x is a Puiseux monomial in y. Thus, $r = 0$. Next, assume that $N\omega_x/\omega_y$ is not an integer. Then there is an automorphism σ of the Galois group of F over $\overline{\mathbb{K}}(y)$ that moves $y^{N\omega_x/\omega_y}$. Then

$$p \mid P - \sigma(P) \in F,$$

which is impossible. Therefore, P is a separated polynomial divisible by p of weight $N\omega_x$. □

Of course, because of symmetry, the statements of Proposition 3.2 also hold for y instead of x.

3.2 Reduction to the homogeneous case

We will start with a necessary condition for p being separable.

Lemma 3.3. *Let $p \in \mathbb{K}[x, y] \setminus (\mathbb{K}[x] \cup \mathbb{K}[y])$ be separable.*

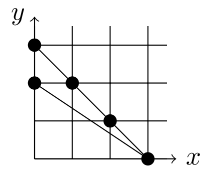
1. *There exists a unique (up to a constant factor) weight function ω such that $\operatorname{lp}_\omega(p)$ involves at least two monomials.*
2. *The polynomial $\operatorname{lp}_\omega(p)$ is separable.*

Proof. Let $q \in \mathbb{K}[x, y] \setminus \{0\}$ be such that qp is separated. Let $\deg_x qp = m$ and $\deg_y qp = n$. Define $\omega(x^i y^j) = ni + mj$. If $\operatorname{lp}_\omega(p)$ contains only one monomial, then every monomial in $\operatorname{lp}_\omega(qp)$ is divisible by it. This is impossible since $\operatorname{lp}_\omega(qp)$ involves both x^m and y^n.

To prove the uniqueness, assume that there are two nonequivalent weight functions ω_1 and ω_2 with this property. Since $\operatorname{lp}_{\omega_i}(qp) = \operatorname{lp}_{\omega_i}(q) \operatorname{lp}_{\omega_i}(p)$ for $i = 1, 2$, we have that both $\operatorname{lp}_{\omega_1}(qp)$ and $\operatorname{lp}_{\omega_2}(qp)$ contain at least two monomials. However, the only monomials of qp that can appear in the leading part are x^m and y^n, and there is a unique weight function so that they have the same weight.

The second claim of the lemma follows from $\operatorname{lp}_\omega(q) \operatorname{lp}_\omega(p) = \operatorname{lp}_\omega(qp)$. □

There is an analogous version of Lemma 3.3 with the lowest homogeneous part in place of the leading homogeneous part. However, even when both the lowest and the leading homogeneous part are separable, the whole polynomial need not be separable, as the following example shows.



Example 3.4. *For $p = (x^3 + x^2y + xy^2 + y^3) + y^2 \in \mathbb{Q}[x, y]$, the relevant weight function for the leading homogeneous part as in Lemma 3.3 is given by $\omega_x = \omega_y = 1$. It leads to the leading homogeneous part $x^3 + x^2y + xy^2 + y^3$. Analogously, the relevant weight function for the lowest homogeneous part is given by $\omega_x = 2, \omega_y = 3$. It leads to the lowest homogeneous part $x^3 + y^2$. Both the leading and the lowest homogeneous part are separable. We claim that p is not separable.*

Let ω be the weight function defined by $\omega(x^i y^j) = 2i + 3j$, so that the lowest homogeneous part of p is $x^3 + y^2$ (weight 6), and the next-to-lowest part is x^2y (weight 7). With respect to ω, any separated polynomial involving both variables only consists of homogeneous parts $ax^n + by^m$ whose weight $2n = 3m$ is a multiple of 6.

Assume that p is separable and let $q \in \mathbb{Q}[x, y] \setminus \{0\}$ be such that qp is separated. Write $q = q_0 + q_1 + \cdots$, where $q_0, q_1, \ldots$ are the lowest, the next-to-lowest, etc. homogeneous parts of q with respect to ω. The lowest homogeneous part of pq is then $q_0(x^3+y^2)$, and since it must be separated and involve both variables, we have $\omega(q_0) = 0 \bmod 6$.

Because of $\omega(q_0x^2y) = \omega(q_0(x^3 + y^2)) + 1 = 1 \bmod 6$, none of the terms of q_0x^2y can appear in qp, so they must all be canceled by something. We must therefore have $\omega(q_1) = \omega(q_0)+1$ and $q_0x^2y+q_1(x^3+y^2) = 0$. This implies that $x^3 + y^2$ divides q_0, which in turn implies that the lowest homogeneous part $q_0(x^3 + y^2)$ of pq has a multiple factor. On the other hand, $q_0(x^3 + y^2) = ax^n + by^m$ for some $a, b \neq 0$, and every such polynomial is squarefree. This is a contradiction.

The main result of the section is the following "partial converse" of Lemma 3.3.

Theorem 3.5. *Let $p \in \mathbb{K}[x, y] \setminus (\mathbb{K}[x] \cup \mathbb{K}[y])$ be a separable polynomial. Let ω be the weight function given by Lemma 3.3, and let P be the minimal separated multiple of p. Then $\operatorname{lp}_\omega(P)$ is the minimal separated multiple of $\operatorname{lp}_\omega(p)$.*

Before proving the theorem, we will establish some combinatorial tools for dealing with divisors of separated polynomials extending the results of Cassels [10].

Notation 3.6. *Consider a separated polynomial $f(x) - g(y)$ with $\deg_x f = m$ and $\deg_y g = n$, where $m, n > 0$, and a weight function $\omega(x^i y^j) = in + jm$. We introduce a new variable t and consider two auxiliary equations*

$$f(x) = t \quad \text{and} \quad g(y) = t.$$

We solve these equations with respect to x and y in $\overline{\mathbb{K}(t)}$, the algebraic closure of $\mathbb{K}(t)$. Let the solutions be $\alpha_0, \dots, \alpha_{m-1}$ and $\beta_0, \dots, \beta_{n-1}$, respectively. Then every element π of $\mathrm{Gal}(\overline{\mathbb{K}(t)}/\mathbb{K}(t))$, the Galois group of $\overline{\mathbb{K}(t)}$ over $\mathbb{K}(t)$, acts on $\mathbb{Z}_m \times \mathbb{Z}_n$ by

$$\pi(i, j) := (i', j') \iff (\pi(\alpha_i), \pi(\beta_j)) = (\alpha_{i'}, \beta_{j'}).$$

Let $G \subseteq \mathbf{S}_m \times \mathbf{S}_n$ be the group of permutations induced on $\mathbb{Z}_m \times \mathbb{Z}_n$ by this action.

Notation 3.7. *For a subset $T \subseteq \mathbb{Z}_m \times \mathbb{Z}_n$, and $(i, j) \in \mathbb{Z}_m \times \mathbb{Z}_n$, we introduce*

$$T_{i,*} := \{k \mid (i, k) \in T\} \text{ and } T_{*,j} := \{k \mid (k, j) \in T\}.$$

Lemma 3.8. *Let $T \subseteq \mathbb{Z}_m \times \mathbb{Z}_n$ be a G-invariant subset. Then $|T_{0,*}| = |T_{1,*}| = \ldots = |T_{m-1,*}|$ and $|T_{*,0}| = |T_{*,1}| = \ldots = |T_{*,n-1}|$.*

Proof. We show that $|T_{0,*}| = |T_{1,*}|$, the rest is analogous. First, we observe that $f(x) - t$ is irreducible over $\mathbb{K}(t)$. If it was not, it would be reducible over $\mathbb{K}[t]$ due to Gauss's lemma. The latter is impossible because $f(x) - t$ is linear in t and does not have factors in $\mathbb{K}[x]$. The irreducibility of $f(x) - t$ implies that its Galois group acts transitively on the roots. In particular, there exists $\pi \in \mathrm{Gal}(\overline{\mathbb{K}(t)}/\mathbb{K}(t))$ such that $\pi(\alpha_0) = \alpha_1$. Hence, π maps $T_{0,*}$ to $T_{1,*}$, and we have $|T_{0,*}| \leqslant |T_{1,*}|$. The reverse inequality is analogous. ◻

Lemma 3.9 (cf. [10, p. 9-10])**.** *Let $T \subseteq \mathbb{Z}_m \times \mathbb{Z}_n$ be a G-invariant subset. There exists a divisor p of $f(x) - g(y)$, unique up to a multiplicative constant, such that*

$$T = \{(i, j) \in \mathbb{Z}_m \times \mathbb{Z}_n \mid p(\alpha_i, \beta_j) = 0\}. \tag{1}$$

Proof. Existence. Let $T_{0,*} = \{j_1, \dots, j_s\}$. Since $f(\alpha_0) = t$, we have $\mathbb{K}(\alpha_0) \supseteq \mathbb{K}(t)$, so every element of $\mathrm{Gal}(\overline{\mathbb{K}(t)}/\mathbb{K}(\alpha_0))$ leaves T invariant. If α_0 is fixed, then $\beta_{j_1}, \dots, \beta_{j_s}$ are permuted. Therefore, the polynomial $(y - \beta_{j_1})(y - \beta_{j_2}) \dots (y - \beta_{j_s})$ is invariant under the action of $\mathrm{Gal}(\overline{\mathbb{K}(t)}/\mathbb{K}(\alpha_0))$. Hence, by the fundamental theorem of Galois theory, it is a polynomial in $\mathbb{K}(\alpha_0)[y]$. Since, by construction, it divides $f(\alpha_0) - g(y)$ over $\mathbb{K}(\alpha_0)$, and α_0 and y are algebraically independent, it in fact belongs to $\mathbb{K}[\alpha_0, y]$. Replacing α_0 by x, we find a polynomial $p \in \mathbb{K}[x, y]$, which divides $f(x) - g(y)$ in $\mathbb{K}[x, y]$.

Let $(i, j) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Since $\mathrm{Gal}(\overline{\mathbb{K}(t)}/\mathbb{K}(t))$ acts transitively on the roots of $f(x) - t$ (see the proof of Lemma 3.8), there is an automorphism π with $\pi(\alpha_i) = \alpha_0$. Let $\beta_{j'} = \pi(\beta_j)$. We then have

$$p(\alpha_i, \beta_j) = 0 \iff p(\alpha_0, \beta_{j'}) = 0 \iff j' \in T_{0,*} \iff (i, j) \in T.$$

Uniqueness. It remains to prove that p is unique up to a multiplicative constant. Assume that $\tilde{p}$ is another divisor of $f(x) - g(y)$ such that $\tilde{p}(\alpha_i, \beta_j) = 0$ for all $(i, j) \in T$. The same argument which proved that p is a divisor of $f(x) - g(y)$ applies to show that p is a divisor of $\tilde{p}$ in $\mathbb{K}[x, y]$, and vice versa. Hence, they only differ by a multiplicative constant. ◻

Lemma 3.10. *Let $T \subseteq \mathbb{Z}_m \times \mathbb{Z}_n$ be a G-invariant subset. The unique factor p corresponding to $T \subseteq \mathbb{Z}_m \times \mathbb{Z}_n$ (see Lemma 3.9) is separated if and only if*

$$\forall\, i, j \in \mathbb{Z}_m : (T_{i,*} \cap T_{j,*} = \varnothing) \text{ or } (T_{i,*} = T_{j,*}) \tag{2}$$

Proof. Assume that T satisfies (2), and let $T_{0,*} = \{j_1, \dots, j_s\}$. Consider the corresponding polynomial p constructed in the proof of Lemma 3.9, which is of the form

$$p(x, y) = y^s + a_{s-1}(x) y^{s-1} + \dots + a_0(x),$$

where, for every $0 \leqslant i < s$ and $0 \leqslant j < m$, $a_i(\alpha_j)$ is (up to sign) the $s - i$-th elementary symmetric polynomial in $\{\beta_k \mid k \in T_{j,*}\}$.

Since $p \mid f(x) - g(y)$, we have $\mathrm{lp}_\omega(p) \mid \mathrm{lp}_\omega(f(x) - g(y)) = ax^m - by^n$, with $a, b \in \mathbb{K} \setminus \{0\}$. Hence, y^s belongs to $\mathrm{lp}_\omega(p)$, and so $\omega(a_i(x) y^i) \leqslant \omega(y^s) = ms$ for all $i \in \{0, \dots, s-1\}$, This implies

$$\deg_x a_i(x) \leqslant \frac{ms - mi}{n} = (s - i)\frac{m}{n}.$$

1 separated | $x^2 + y^2 + 1$ separated | $x^2 - y^2 - 1$ separated | $x^4 - (y^2 + 1)^2$ separated

Figure 1: The factors of $x^4 - (y^2 + 1)^2$ in $\mathbb{Q}[x, y]$ and the sets $T \subseteq \mathbb{Z}_4^2$ corresponding to them.

Since T is the disjoint union of the $T_{i,*}$'s and of the $T_{*,j}$'s, respectively, whose cardinality, by Lemma 3.8, does not depend on i and j, and $T_{0,*}$, by definition, consists of s elements, we find that $ms = |T| = n|T_{*,j_1}|$, in particular $\ell := |T_{*,j_1}| = \frac{ms}{n}$. Hence there exist $0 = i_1 < i_2 < \ldots < i_\ell < m$ such that $j_1 \in T_{i_1,*} \cap \ldots \cap T_{i_\ell,*}$ and so, by (2), $T_{i_1,*} = \ldots = T_{i_\ell,*}$. This shows that the polynomial $a_j(x) - a_j(\alpha_0)$ has at least ℓ pairwise distinct roots, $\alpha_{i_1}, \ldots, \alpha_{i_\ell}$, while it has degree less than ℓ for $0 < j < s$. Hence, it is the zero polynomial, and $a_j(x)$ is a constant (which we denote by a_j). Therefore, p is separated and of the form $p(x, y) = f_0(x) - g_0(y)$ with $f_0(x) = a_0(x)$ and $g_0(y) = -(y^s + a_{s-1}y^{s-1} + \cdots + a_1 y)$.

To prove the other implication, let $p(x, y) = f_0(x) - g_0(y)$ be a separated factor of $f(x) - g(y)$. It is sufficient to show that

$$(i, j),\ (i', j),\ (i, j') \in T \implies (i', j') \in T.$$

Indeed, $(i, j),\ (i', j) \in T$ implies that $f_0(\alpha_i) = f_0(\alpha_{i'})$, so that $f_0(\alpha_i) - g_0(\beta_{j'}) = 0$ implies that $f_0(\alpha_{i'}) - g_0(\beta_{j'}) = 0$, i.e. $(i', j') \in T$. □

Lemma 3.10 motivates the following definition.

Definition 3.11. *1. A subset $T \subseteq \mathbb{Z}_m \times \mathbb{Z}_n$ is called* separated *if it satisfies* (2)*, that is*

$$\forall\ i, j \in \mathbb{Z}_m : (T_{i,*} \cap T_{j,*} = \varnothing) \text{ or } (T_{i,*} = T_{j,*}).$$

2. The intersection of all separated subsets containing $T \subseteq \mathbb{Z}_m \times \mathbb{Z}_n$ is called the separated closure *of T and denoted by T^{sep}. Notice that the separated closure is separated.*

Example 3.12. *1. Let $f(x) = x^4$ and $g(y) = y^4 + 2y^2 + 1$. The group of permutations on pairs of roots of $f(x) - t$ and $g(y) - t$ is generated by $((0123), (0123)), ((0321), (03)(12))$ and $(id, (02))$. According to $f(x) - g(y)$ having two separated irreducible factors, $x^2 - y^2 - 1$ and $x^2 + y^2 + 1$, we find that there are two orbits, each of them forming a separated set (Figure 1).*

2. Let $f(x) - g(y) = x^6 - y^6$. Let $t^{1/6} \in \overline{\mathbb{C}(t)}$ be any 6th root of t, and let ϵ be a primitive 6th root of unity. Then the polynomials $f(x) - t$ and $g(y) - t$ have the same roots, namely:

$$\alpha_i = \beta_i = \epsilon^i t^{1/6}, \quad i \in \{0, \ldots, 5\}.$$

The Galois group of $\overline{\mathbb{C}(t)}$ permutes these elements cyclically, so the induced action on $\mathbb{Z}_6^2$ is generated by $((012345), (012345))$. Figure 2 shows the sets T for the various factors of $x^6 - y^6$. Observe that T is separated if and only if the corresponding factor is separated. Observe also that multiplying two factors corresponds to taking the union of the corresponding sets T.

Lemma 3.13. *Let $T \subseteq \mathbb{Z}_m \times \mathbb{Z}_n$ be invariant with respect to $G \subseteq \mathbf{S}_m \times \mathbf{S}_n$. Then T^{sep} is also G-invariant.*

Proof. Let $\pi = (\sigma, \tau) \in \mathbf{S}_m \times \mathbf{S}_n$, and let $S \subseteq \mathbb{Z}_m \times \mathbb{Z}_n$ be a separated set. Since $\pi(S)_{i,*} = \tau(S_{\sigma(i),*})$, we find that $\pi(S)$ is separated as well.

Assume that T^{sep} is not G-invariant, that is, there exists a $\pi \in G$ such that $\pi(T^{\text{sep}}) \neq T^{\text{sep}}$. As we have shown, $\pi(T^{\text{sep}})$ is separated, hence so is $S := T^{\text{sep}} \cap \pi(T^{\text{sep}})$. Observe that, since $\pi(T^{\text{sep}}) \neq T^{\text{sep}}$, $S \subsetneq T^{\text{sep}}$. Since T is G-invariant, $T \subseteq \pi(T^{\text{sep}})$, so $T \subseteq S$. This contradicts the minimality of T^{sep}. □

Proof of Theorem 3.5. We use Notation 3.6 with $\overline{\mathbb{K}(t)}$ being identified with a subfield of the field F of Puiseux series in t^{-1} over $\overline{\mathbb{K}}$. Let $\alpha_0, \ldots, \alpha_{m-1}$ and $\beta_0, \ldots, \beta_{n-1}$ denote the roots of $f(x) - t$ and $g(y) - t$ and $\overline{\alpha}_0, \ldots, \overline{\alpha}_{m-1}$ and $\overline{\beta}_0, \ldots, \overline{\beta}_{n-1}$ their highest degree terms. Observe that the highest degree terms are

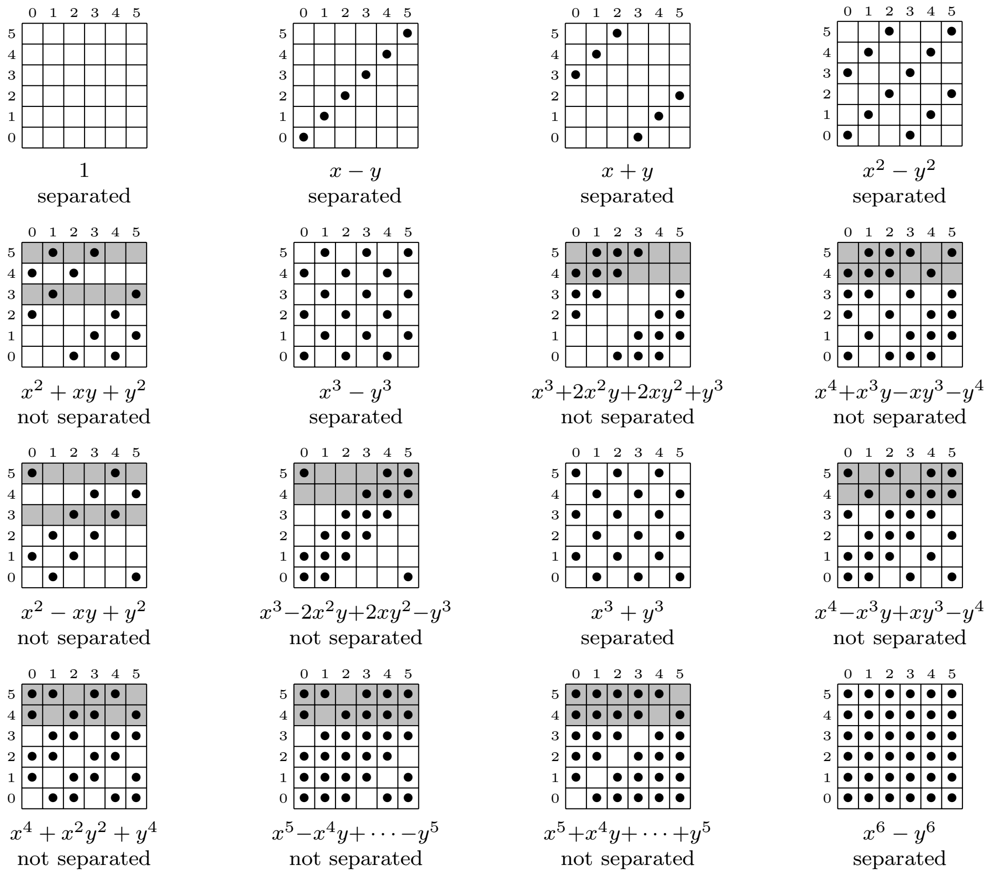


Figure 2: The factors of x^6-y^6 in $\mathbb{Q}[x,y]$ and the sets $T \subseteq \mathbb{Z}_6^2$ corresponding to them. For the unseparated cases, we highlight one choice of two incompatible rows.

proportional to $t^{1/n}$ and $t^{1/m}$, and hence they are the roots of $\mathrm{lp}_\omega(f(x))-t$ and $\mathrm{lp}_\omega(g(y))-t$, respectively. We define

$$T = \{(i,j) \in \mathbb{Z}_m \times \mathbb{Z}_n \mid p(\alpha_i, \beta_j) = 0\},$$
$$\overline{T} = \{(i,j) \in \mathbb{Z}_m \times \mathbb{Z}_n \mid \mathrm{lp}_\omega(p)(\overline{\alpha}_i, \overline{\beta}_j) = 0\}.$$

If $\mathrm{lp}_\omega(P)$ were not the minimal separated multiple of $\mathrm{lp}_\omega(p)$, by Lemma 3.10, we would have $\overline{T}^{\mathrm{sep}} \subsetneq \mathbb{Z}_m \times \mathbb{Z}_n$. Therefore, it is sufficient to show that $\overline{T}^{\mathrm{sep}} = \mathbb{Z}_m \times \mathbb{Z}_n$.

Since

$$p(\alpha_i, \beta_j) = 0 \implies \mathrm{lp}_\omega(p)(\overline{\alpha_i}, \overline{\beta_j}) = 0,$$

we have $T \subseteq \overline{T}$. By assumption, P is the minimal separated multiple of p, so, by Lemma 3.13, $T^{\mathrm{sep}} = \mathbb{Z}_m \times \mathbb{Z}_n$. Since $T^{\mathrm{sep}} \subseteq \overline{T}^{\mathrm{sep}}$, this implies that $\overline{T}^{\mathrm{sep}} = \mathbb{Z}_m \times \mathbb{Z}_n$, and finishes the proof. □

3.3 Algorithm

The algorithm for finding a generator of the algebra of separated polynomials of a principal ideal $\langle p \rangle$ is based on the results above. First, it uses Theorem 3.5 to reduce the situation to a homogeneous polynomial for a suitable grading, then, it uses Proposition 3.2 to find a degree bound for the minimal separated multiple, and finally, it uses linear algebra to determine if such a multiple exists.

Algorithm 3.14. *Input:* $p \in \mathbb{K}[x,y] \setminus (\mathbb{K}[x] \cup \mathbb{K}[y])$.
Output: $a \in \mathbb{K}[x] \times \mathbb{K}[y]$ *such that* $\mathbb{K}[a] = A(\langle p \rangle)$. *The algorithm returns* $a = (1,1)$ *iff* $A(\langle p \rangle) \cong \mathbb{K}$.

1 *let* $\omega_x, \omega_y \in \mathbb{N}$ *be maximal such that* p *contains monomials* $x^{\omega_y}y^0$ *and* $x^0y^{\omega_x}$. *Such parameters exist because* p *is not univariate.*

2 *set* $h = \mathrm{lp}_\omega(p)$ *with* $\omega(x^iy^j) := \omega_x i + \omega_y j$.

3 *if h does not contain x^{ω_y}, return* $(1,1)$.

4 *let $\{\zeta_1,\dots,\zeta_m\} \subseteq \overline{\mathbb{K}}$ be the roots of $h(x,1) \in \mathbb{K}[x]$. If any of them is not a simple root, return* $(1,1)$.

5 *let $N \in \mathbb{N}$ be minimal such that $(\zeta_i/\zeta_j)^N = 1$ for all i,j. If no such N exists, return* $(1,1)$.

6 *make an ansatz*

$$f = \sum_{i=0}^{N} a_i x^i, \quad g = \sum_{j=0}^{N\omega_x/\omega_y} b_j y^j,$$

compute $\operatorname{rem}_x(f-g,p)$ *in* $\mathbb{K}(a_0,\dots,a_N,b_0,\dots,b_{N\omega_x/\omega_y},y)[x]$. *The result of the reduction belongs to* $\mathbb{K}[a_0,\dots,a_N,b_0,\dots,b_{N\omega_x/\omega_y},y,x]$ *because the leading coefficient of p is in* $\mathbb{K}$.

7 *equate the coefficients of* $\operatorname{rem}_x(f-g,p)$ *with respect to x,y to zero and solve the resulting linear system for the unknowns* a_i, b_j.

8 *if there is a nonzero solution, return the corresponding pair (f,g), otherwise return* $(1,1)$.

When $\mathbb{K}$ is a number field, Step 5 can be carried out as follows: for each ratio ζ_i/ζ_j, one should check whether the minimal polynomial of this ratio over $\mathbb{Q}$ is a cyclotomic polynomial Φ_n and, if yes, return such n. This check can be performed using a bound from [18, Theorem 15] that yields the upper bound on n based on the degree of the polynomial.

Proposition 3.15. *Algorithm 3.14 is correct.*

Proof. The algorithm consists of an application of the results of the previous section and a handling of degenerate cases not covered by these results. In Steps 3–5, it is correct to return $(1,1)$ in the indicated situations because Proposition 3.2 implies that h is not separable in these cases, which in combination with Lemma 3.3 implies that p is not separable either.

By Proposition 3.2, when h has a separated multiple at all, it has one of weight $N\omega_x$, and by Theorem 3.5, when p has a separated multiple at all, it also has one of weight $N\omega_x$. Therefore, if p has a separated multiple, it will have one of the shape set up Step 6. For $f-g$ to be a separated multiple of p is equivalent to $\operatorname{rem}_x(f-g,p)=0$, which we can safely view as univariate division with respect to the variable x because the leading coefficient of p with respect to x does not contain y (nor any of the undetermined coefficients). It is checked in Step 7 whether there is a way to instantiate the undetermined coefficients in such a way that this remainder becomes zero. If so, any such way translates into a separated multiple, and by [15, Theorem 2.3], it is a generator of $A(I)$. If there is no non-zero solution, it is correct to return $(1,1)$. □

4 Arbitrary bivariate Ideals

The case of an arbitrary ideal $I \subseteq \mathbb{K}[x,y]$ is reduced to the two cases discussed in Sections 2 and 3. Every ideal $I \subseteq \mathbb{K}[x,y]$ can be written as $I = \bigcap_{i=1}^k P_i$, where the P_i's are primary ideals. Unless $I = \{0\}$ or $I = \langle 1\rangle$, these primary ideals have dimensions zero or one. Primary ideals in $\mathbb{K}[x,y]$ of dimension 1 must be principal ideals, because $\dim(P_i)=1$ together with Bezout's theorem implies that P_i cannot contain any elements p,q with $\gcd(p,q)=1$, and then P_i being primary implies that P_i is generated by some power of an irreducible polynomial.

The intersection of zero-dimensional ideals is zero-dimensional and the intersection of principal ideals is principal, so there exists a zero-dimensional ideal I_0 and a principal ideal I_1 such that $I = I_0 \cap I_1$. These ideals are obtained as the intersections of the respective primary components of I. When $I_0 = \langle 1\rangle$ or $I_1 = \langle 1\rangle$, we have $I = I_1$ or $I = I_0$, respectively, and are in one of the cases already considered. Assume now that I_1, I_0 are both different from $\langle 1\rangle$.

In order to use the results of Section 3, we have to make sure that the generator of I_1 contains both variables. If this is not the case, say if $I_1 = \langle h\rangle$ for some $h \in \mathbb{K}[x]\setminus\mathbb{K}$, then the separated polynomials in I are precisely the elements of $I \cap \mathbb{K}[x]$. If p is such that $\langle p\rangle = I \cap \mathbb{K}[x]$, then the pairs $(x^i p, 0)$ for $i = 0,\dots,\deg_x p - 1$ are generators of $A(I)$ (see the proof of Proposition 2.2), so this case is settled. Therefore, from now on we assume that the generator of I_1 contains both the variables.

We can compute generators of the algebra $A(I_0) \subseteq \mathbb{K}[x]\times\mathbb{K}[y]$ of separated polynomials in I_0 as described in Section 2 and a generator of the algebra $A(I_1) \subseteq \mathbb{K}[x]\times\mathbb{K}[y]$ of separated polynomials in I_1 as described in Section 3. Clearly, the algebra $A(I) \subseteq \mathbb{K}[x]\times\mathbb{K}[y]$ of separated polynomials in I is $A(I) = A(I_0)\cap A(I_1)$. It thus remains to compute generators for this intersection. In order to do so, we will exploit that the codimension of $A(I_0)$ as $\mathbb{K}$-subspace of $\mathbb{K}[x]\times\mathbb{K}[y]$ is finite (Lemma 2.4), and that $A(I_1) = \mathbb{K}[a]$ for some $a \in \mathbb{K}[x]\times\mathbb{K}[y]$. We have to find all polynomials p such that $p(a) \in A(I_0)$.

Polynomials p with a prescribed finite set of monomials can be found with the help of Lemma 2.4 as follows.

Algorithm 4.1. *Input: $a \in \mathbb{K}[x]\times\mathbb{K}[y]$, $A(I_0)$ and V as in Lemma 2.4, and a finite set $S = \{s_1, \dots, s_m\} \subseteq \mathbb{N}$.*
Output: a $\mathbb{K}$-vector space basis of the space of all polynomials p with $p(a) \in A(I_0)$ such that p involves only monomials with exponents in S.

1 *for $i = 1, \dots, m$, compute $r_i \in V$ such that $a^{s_i} - r_i \in A(I_0)$*
2 *compute a basis B of the space of all $(c_1, \dots, c_m) \in \mathbb{K}^m$ with $c_1 r_1 + \dots + c_m r_m = 0$*
3 *for every element $(c_1, \dots, c_m) \in B$, return $c_1 t^{s_1} + \dots + c_m t^{s_m}$.*

Proposition 4.2. *Algorithm 4.1 is correct.*

Proof. If $(c_1, \dots, c_m) \in \mathbb{K}^m$ is such that $\sum_{i=1}^m c_i a^{s_i} \in A(I_0)$, then $\sum_{i=1}^m c_i r_i \in A(I_0)$, and since $r_i \in V$ for all i and $A(I_0) \cap V = \{0\}$, we have $\sum_{i=1}^m c_i r_i = 0$. Therefore $(c_1, \dots, c_m)$ is among the vectors computed in step 2, so the algorithm does not miss any solutions. Conversely, if $(c_1, \dots, c_m) \in \mathbb{K}^m$ is such that $\sum_{i=1}^m c_i r_i = 0$, then $\sum_{i=0}^m c_i a^{s_i} = \sum_{i=0}^m c_i(a^{s_i} - r_i) \in A(I_0)$, so the algorithm does not return any wrong solutions. □

To find a set of generators of $A(I_0) \cap A(I_1)$, we apply Algorithm 4.1 repeatedly. First call it with $S = \{1, \dots, \dim V + 1\}$. Since $|S| > \dim V$, the output must contain at least one nonzero polynomial p_1. If d_1 is its degree, we can restrict the search for further generators to subsets S of $\mathbb{N} \setminus d_1\mathbb{N}$, because when q is such that $q(a) \in A(I_0)$, then we can subtract a suitable linear combination of powers of p_1 to remove from q all monomials whose exponents are multiples of d_1. When $d_1 = 1$, we have $A(I_0) \cap A(I_1) = \mathbb{K}[a]$ and are done. Otherwise, $\mathbb{N} \setminus d_1\mathbb{N}$ is still an infinite set, so we can choose $S \subseteq \mathbb{N} \setminus d_1\mathbb{N}$ with $|S| > \dim V$ and call Algorithm 4.1 to find another nonzero polynomial p_2, say of degree d_2. The search for further generators can be restricted to polynomials consisting of monomials whose exponents belong to $\mathbb{N} \setminus (d_1\mathbb{N} + d_2\mathbb{N})$. We can continue to find further generators of degrees $d_3, d_4, \dots$ with $d_i \in \mathbb{N} \setminus (d_1\mathbb{N} + \dots + d_{i-1}\mathbb{N})$ for all i. Since the monoid $(\mathbb{N}, +)$ has the ascending chain condition, this process must come to an end.

The end is clearly not reached as long as $g := \gcd(d_1, \dots, d_m) \neq 1$, because then $\mathbb{N} \setminus g\mathbb{N}$ is an infinite subset of $\mathbb{N} \setminus (d_1\mathbb{N} + \dots + d_m\mathbb{N})$. Once we have reached $g = 1$, it is well known [2, 17] that $\mathbb{N} \setminus (d_1\mathbb{N} + \dots + d_m\mathbb{N})$ is a finite set, and there are algorithms [5] for computing its largest element (known as the Frobenius number of $d_1, \dots, d_m$). We can therefore constructively decide when all generators have been found.

Putting all steps together, our algorithm for computing the separated polynomials in an arbitrary ideal of $\mathbb{K}[x, y]$ works as follows. We use the notation $\langle d_1, \dots, d_m\rangle$ for the submonoid $d_1\mathbb{N} + \dots + d_m\mathbb{N}$ generated by $d_1, \dots, d_m$ in $\mathbb{N}$.

Algorithm 4.3. *Input: an ideal $I \subseteq \mathbb{K}[x, y]$, given as a finite set of ideal generators*
Output: a finite set of generators for the algebra $A(I)$ of separated polynomials of I

1 *if $\dim I = 0$, call Algorithm 2.1, return the result.*
2 *compute a zero-dimensional ideal I_0 and a principal ideal $I_1 = \langle h\rangle$ with $I = I_0 \cap I_1$ (for example, using Gröbner bases [4] and the remarks at the beginning of this section).*
3 *if $h \in \mathbb{K}[x]$, compute p such that $\langle p\rangle = I \cap \mathbb{K}[x]$, return the pairs $(x^i p, 0)$ for $i = 0, \dots, \deg_x p - 1$. Likewise if $h \in \mathbb{K}[y]$.*
4 *call Algorithm 2.1 to get generators of $A(I_0)$, and let V be as in Lemma 2.4.*
5 *call Algorithm 3.14 to get an $a \in \mathbb{K}[x] \times \mathbb{K}[y]$ with $A(I_1) = \mathbb{K}[a]$. If $A(I_1) \cong \mathbb{K}$, return $(1, 1)$.*
6 *$G = \emptyset$, $\Delta = \emptyset$.*
7 *while $\gcd(\Delta) \neq 1$, do:*
8 *select a set $S \subseteq \mathbb{N} \setminus \langle\Delta\rangle$ with $|S| > \dim V$ and call Algorithm 4.1 to find a nonzero polynomial p with $p(a) \in A(I_0)$ consisting only of monomials with exponents in S.*
9 *$G = G \cup \{p\}$, $\Delta = \Delta \cup \{\deg_x p\}$*
10 *call Algorithm 4.1 with $S = \mathbb{N} \setminus \langle\Delta\rangle$ (which is now a computable finite set) and add the resulting polynomials to G.*
11 *return G*

An implementation of the algorithm in Mathematica can be found on the website of the second author. Incidentally, the algorithm also shows that $A(I)$ is always a finitely generated $\mathbb{K}$-algebra.

Example 4.4. *For the ideal*

$$I = \langle (x^2 - xy + y^2)(x^3 - 2xy^2 - 1), (x^2 - xy + y^2)(y^3 - 2x^2y - 1) \rangle$$

we have $I_0 = \langle x^3 - 2xy^2 - 1, y^3 - 2x^2y - 1 \rangle$ *and* $I_1 = \langle x^2 - xy + y^2 \rangle$. *Algorithm 2.1 yields a somewhat lengthy list of generators for* $A(I_0)$ *from which it can be read off that a suitable choice for* V *is the* $\mathbb{K}$*-vector space generated by* $(0, y^i)$ *for* $i = 0, \ldots, 8$. *In particular,* $\dim V = 9$. *Algorithm 3.14 yields* $A(I_1) = \mathbb{K}[(x^3, -y^3)]$.

Making an ansatz for a polynomial p *of degree at most* 10 *such that* $p(a) \in A(I_0)$, *we find a solution space of dimension 7. Its lowest degree element is* $t^4 - 2t^2$, *giving rise to the element* $(x^{12} - 2x^6, y^{12} - 2y^6)$ *of* $A(I_0) \cap A(I_1)$. *If we discard the other solutions and continue with the next iteration, we search for polynomials* p *whose support is contained* $\{x^s : s \in S\}$ *for* $S = \{1, 2, 3, 5, 6, 7, 9, 10, 11, 13\}$. *Again, the solution space turns out to have dimension 7. The lowest degree element is now* $9t^5 - 26t^3 + 17$. *Since* $\gcd(4, 5) = 1$, *we can exit the while loop. In step 10 of the algorithm, we get* $S = \{1, 2, 3, 6, 7, 11\}$, *and this exponent set leads to a solution space of dimension three, generated by the polynomials* $81t^6 - 323t^3$, $81t^7 - 539t^3 + 458$, *and* $6561t^{11} - 191125t^3 + 184564$. *The resulting generators of* $A(I) = A(I_0) \cap A(I_1)$ *are therefore the pairs* $p((x^3, -y^3))$ *where* p *runs through the five polynomials found by the algorithm.*

5 More than two variables

It is a natural question whether anything more can be said about the case of several variables. Incidentally, a multivariate version would be needed in order to solve the combinatorial problem that motivated this research in the first place.

Algorithm 2.1 for bivariate zero-dimensional ideals works in the same way for zero-dimensional ideals of $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ for arbitrary n, m. Also Lemma 2.4 generalizes without problems. We believe that with some further work, our results for principal ideals can also be generalized to the case of several variables. However, in general, not every polynomial ideal with more than two variables is the intersection of a principal ideal and a zero-dimensional ideal, so the route taken in Section 4 is blocked. Also, as the next example shows we cannot expect an algorithm that finds the algebra of separated polynomials for an arbitrary ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$, since it does not need to be finitely generated.

Example 5.1 ($A(I)$ is not necessarily finitely generated)**.** *It is shown in [16, Example 1.3] that the algebra*

$$R := \mathbb{C}[t_1^2, t_1^3, t_2] \cap \mathbb{C}[t_1^2, t_2 - t_1] \subset \mathbb{C}[t_1, t_2]$$

is not finitely generated. Consider the ideal

$$\begin{aligned} I &= \langle x_1 - t_1^2, x_2 - t_1^3, x_3 - t_2, \\ &\qquad y_1 - t_1^2, y_2 - (t_2 - t_1) \rangle \cap \mathbb{C}[x_1, x_2, x_3, y_1, y_2] \\ &= \langle x_1 - y_1, -x_2 + x_3y_1 - y_1y_2, x_3^2 - y_1 - 2x_3y_2 + y_2^2 \rangle. \end{aligned}$$

We claim that $A(I) \cong R$ *as* $\mathbb{C}$*-algebras, implying that* $A(I)$ *is not finitely generated. We show that* $\phi\colon A(I) \to R$ *defined by* $\phi(f, g) = f(t_1^2, t_1^3, t_2)$ *is an isomorphism:*

- ϕ *is well-defined (the image is contained in* $R \subseteq \mathbb{C}[t_1^2, t_1^3, t_2]$*). To see this, note that,* $(f, g) \in A(I)$ *means* $f - g \in I$, *which by definition of* I *means* $f(t_1^2, t_1^3, t_2) = g(t_1^2, t_2 - t_1)$. *Therefore,* $f(t_1^2, t_1^3, t_2) \in \mathbb{C}[t_1^2, t_2^3, t_2] \cap \mathbb{C}[t_1^2, t_2 - t_1] = R$.

- ϕ *is surjective. For every* $p \in R$ *there exist polynomials* f, g *with* $p = f(t_1^2, t_1^3, t_2) = g(t_1^2, t_2 - t_1)$. *By definition of* I *we have* $f(x_1, x_2, x_3) - g(y_1, y_2) \in I$, *hence* $(f, g) \in A(I)$. *Now* $\phi(f) = p$, *so* p *is in the image of* ϕ.

- ϕ *is injective. This follows from* $I \cap \mathbb{C}[y_1, y_2] = \{0\}$. □

It would still make sense to ask for an algorithm that decides whether $A(I)$ is nontrivial. We do not have such an algorithm, but being able to solve the problem in the bivariate case gives rise to a necessary condition.

Proposition 5.2. *Let*

$$\xi\colon \mathbb{K}[x_1,\dots,x_n] \to \mathbb{K}[x] \quad \text{and} \quad \eta\colon \mathbb{K}[y_1,\dots,y_m] \to \mathbb{K}[y]$$

be two homomorphisms, and let $I \subseteq \mathbb{K}[x_1,\dots,x_n,y_1,\dots,y_m]$ *be an ideal such that*

$$I \cap \mathbb{K}[y_1,\dots,y_m] = \{0\} \quad \text{and} \quad (\mathrm{id}\otimes\eta)(I) \cap \mathbb{K}[x_1,\dots,x_n] = \{0\}.$$

If the algebra of separated polynomials of I *is non-trivial, then so is the algebra of separated polynomials of* $J := (\xi\otimes\eta)(I) \subseteq \mathbb{K}[x,y]$.

Proof. Let (f,g) be an arbitrary, non-constant element of $A(I)$. If $(\xi(f),\eta(g)) \in A(J)$ were a $\mathbb{K}$-multiple of $(1,1)$, we would find that $f-\eta(g)$ were an element of $(\mathrm{id}\otimes\eta)(I)\cap\mathbb{K}[x_1,\dots,x_n]$, and hence, by our assumption, that f itself were a constant. So $f-g \in I\cap\mathbb{K}[y_1,\dots,y_m]$, and hence, by assumption, $g=f$ is a constant as well, contradicting that (f,g) is not a constant. □

The examples below show different reasonable choices for homomorphisms ξ and η.

Example 5.3. *Consider the polynomial* $p = x^2 + xy_1y_2 + y_1^2 + y_2^2$. *Let* $\xi = \mathrm{id}$ *and let* η *be defined by* $\eta(y_1) = y$, $\eta(y_2) = 2$. *Notice that* η *is just the evaluation of* y_2 *at* 2. *Then* $(\xi\otimes\eta)(p) = x^2 + 2xy_1 + y_1^2 + 4$, *a polynomial that is not separable. Hence* p *is not separable.*

Example 5.4. *Consider the polynomial* $p = x^2 + xy_1 + y_1^2 + y_2^4$. *We cannot use the same strategy as in the previous example because any evaluation of* y_1 *or* y_2 *results in a separable polynomial. Nevertheless, the homomorphism defined by* $\xi(x) = x$, $\eta(y_1) = y^2$, *and* $\eta(y_2) = y$ *maps* p *to* $(\xi\otimes\eta)(p) = x^2 + xy^2 + 2y^4$, *a polynomial which is not separable. So* p *is not separable either.*

Acknowledgements. We thank Erhard Aichinger and Josef Schicho for sharing their thoughts on the topic and for providing pointers to the literature. We also thank the referees for their careful reading and their valuable suggestions. MB was supported by the Austrian FWF grant F5004. Part of this work was done during the visit of MB to HSE University. MB would like to thank the Faculty of Computer Science of HSE for its hospitality. MK was supported by the Austrian FWF grants F5004 and P31571-N32. GP was supported by NSF grants CCF-1564132, CCF-1563942, DMS-1853482, DMS-1853650, and DMS-1760448, by PSC-CUNY grants #69827-0047 and #60098-0048.

References

[1] E. Aichinger and S. Steinerberger. A proof of a theorem by Fried and MacRae and applications to the composition of polynomial functions. *Archiv der Mathematik*, 97:115–124, 2011. URL `https://doi.org/10.1007/s00013-011-0280-z`.

[2] J. L. R. Alfonsín. *The Diophantine Frobenius Problem.* Oxford University Press, 2006.

[3] R. M. Beals, J. L. Wetherell, and M. E. Zieve. Polynomials with a common composite. *Israel Journal of Mathematics*, 174(1):93–117, 2009. URL `https://doi.org/10.1007/s11856-009-0105-y`.

[4] T. Becker, V. Weispfenning, and H. Kredel. *Gröbner Bases.* Springer, 1993.

[5] D. Beihoffer, J. Hendry, A. Nijenhuis, and S. Wagon. Faster algorithms for Frobenius numbers. *Electronic Journal of Combinatorics*, 12:R27, 2005. URL `https://www.combinatorics.org/ojs/index.php/eljc/article/view/v12i1r27`.

[6] Y. Bilu and R. Tichy. The diophantine equation $f(x) = g(y)$. *Acta Arithmetica*, 95(3):261–288, 2000. URL `http://eudml.org/doc/207451`.

[7] Y. F. Bilu. Quadratic factors of $f(x) - g(y)$. *Acta Arithmetica*, 90(4):341–355, 1999. URL `http://eudml.org/doc/207332`.

[8] F. Binder. Fast computations in the lattice of polynomial rational function fields. In *Proceedings of ISSAC'96*, pages 43–48, 1996. URL `https://doi.org/10.1145/236869.236895`.

[9] M. Bousquet-Mélou. An elementary solution of Gessel's walks in the quadrant. *Advances in Mathematics*, 303:1171–1189, 2016. URL `https://doi.org/10.1016/j.aim.2016.08.038`.

[10] J. W. S. Cassels. Factorization of polynomials in several variables. In K. E. Aubert and W. Ljunggren, editors, *Proceedings of the 15th Scandinavian Congress Oslo 1968*, pages 1–17. Springer Berlin Heidelberg, 1969. ISBN 978-3-540-36246-3. URL https://doi.org/10.1007/BFb0060248.

[11] P. Cassou-Noguès and J.-M. Couveignes. Factorisations explicites de $g(y) - h(z)$. *Acta Arithmetica*, 87(4):291–317, 1999. URL https://doi.org/10.4064/aa-87-4-291-317.

[12] H. Davenport, D. J. Lewis, and A. Schinzel. Equations of the form $f(x) = g(y)$. *The Quarterly Journal of Mathematics*, 12(1):304–312, 1961. URL https://doi.org/10.1093/qmath/12.1.304.

[13] H. T. Engstrom. Polynomial substitutions. *American Journal of Mathematics*, 63(2):249–255, 1941. URL https://jstor.org/stable/2371520.

[14] M. D. Fried. The field of definition of function fields and a problem in the reducibility of polynomials in two variables. *Illinois Journal of Mathematics*, pages 128–146, 1973. URL https://projecteuclid.org/download/pdf_1/euclid.ijm/1256052044.

[15] M. D. Fried and R. E. MacRae. On curves with separated variables. *Mathematische Annalen*, 180: 220–226, 1969. URL https://doi.org/10.1007/BF01350739.

[16] P. Mondal. When is the intersection of two finitely generated subalgebras of a polynomial ring also finitely generated? *Arnold Mathematical Journal*, 3(3):333–350, 2017. URL https://doi.org/10.1007/s40598-017-0068-8.

[17] R. W. Owens. An algorithm to solve the Frobenius problem. *Mathematics Magazine*, 76(4):264–275, 2003. URL https://doi.org/10.2307/3219081.

[18] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois Journal of Mathematics*, 6(1):64–94, 1962. URL https://doi.org/10.1215/ijm/1255631807.

[19] J. Schicho. A note on a theorem of Fried and MacRae. *Archiv der Mathematik*, 65:239–243, 1995. URL https://doi.org/10.1007/BF01195093.