São Paulo Journal of Mathematical Sciences
https://doi.org/10.1007/s40863-022-00324-w

SPECIAL SECTION: IN HONOR OF RAFAEL H. VILLARREAL
ON THE OCCASION OF HIS 70TH BIRTHDAY

Restricted Gröbner fans and re-embeddings of affine algebras

Martin Kreuzer[1] · **Le Ngoc Long**[1,2] · **Lorenzo Robbiano**[3]

Accepted: 9 August 2022

Abstract
In this paper we continue the study of good re-embeddings of affine K-algebras started in Kreuzer et al. (J Algebra Appl, 2021. https://doi.org/10.1142/S0219498822501882). The idea is to use special linear projections to find isomorphisms between a given affine K-algebra $K[X]/I$, where $X = (x_1, \ldots, x_n)$, and K-algebras having fewer generators. These projections are induced by particular tuples of indeterminates Z and by term orderings σ which realize Z as leading terms of a tuple F of polynomials in I. In order to efficiently find such tuples, we provide two major new tools: an algorithm which reduces the check whether a given tuple F is Z-separating to an LP feasibility problem, and an isomorphism between the part of the Gröbner fan of I consisting of marked reduced Gröbner bases which contain a Z-separating tuple and the Gröbner fan of $I \cap K[X \setminus Z]$. We also indicate a possible generalization to tuples Z which consist of terms. All results are illustrated by explicit examples.

Keywords Affine algebra · Gröbner fan · Embedding dimension

Mathematics Subject Classification Primary 13P10 · Secondary 14Q20 · 13E15 · 14R10

Communicated by Isidoro Gitler.

✉ Lorenzo Robbiano
lorobbiano@gmail.com

Martin Kreuzer
martin.kreuzer@uni-passau.de

Le Ngoc Long
lelong@hueuni.edu.vn; ngoc-long.le@uni-passau.de

[1] Fakultät für Informatik und Mathematik, Universität Passau, 94030 Passau, Germany

[2] Department of Mathematics, University of Education – Hue University, 34 Le Loi Street, Hue City, Vietnam

[3] Dipartimento di Matematica, Università di Genova, Via Dodecaneso 35, 16146 Genoa, Italy

Published online: 03 October 2022

1 Introduction

This paper is a natural continuation of [5]. The topic treated here and there is the search for good re-embeddings of affine algebras over a field K, or equivalently, of affine schemes. What do we mean by that? It is a classical research topic in algebraic geometry to find embeddings of a given scheme into low-dimensional spaces. For affine varieties, the main result of [11] has been generalized in several directions (see for instance [10] and [9], Sect. 10.2). Here we follow a more computational approach which tries to avoid the frequently costly calculation of Gröbner bases as much as possible.

Let K be a field and I an ideal in a polynomial ring $P = K[x_1, \dots, x_n]$. We are looking for a polynomial ring $P' = K[y_1, \dots, y_m]$ and an ideal I' in P' such that $m < n$ and such that there is a K-algebra isomorphism $P/I \cong P'/I'$. In other words, we are looking for a smaller number of K-algebra generators of P/I. In general, this problem is very hard, but there are chances to get good solutions using the following type of linear projections.

Assume that $I \subseteq \langle x_1, \dots, x_n \rangle$. Let $Z = (z_1, \dots, z_s)$ be a set of distinct indeterminates in $X = (x_1, \dots, x_n)$, and suppose that there exist a term ordering σ and polynomials $f_1, \dots, f_s \in I$ with $\mathrm{LT}_\sigma(f_i) = z_i$ for $i = 1, \dots, s$ and such that this is the only appearance of z_i in a term of one of the polynomials $f_1, \dots, f_s$. Then we say that I is Z-separating and σ is a Z-separating term ordering for I. In this setting, the reduced σ-Gröbner basis of I allows us to define a K-algebra isomorphism $P/I \cong \widehat{P}/(I \cap \widehat{P})$, where $\widehat{P} = K[X \setminus Z]$, called a Z-separating re-embedding of I. Notice that the search for such $f_1, \dots, f_s \in I$ is in general non-trivial. In particular, they can be hidden and far away from a given set of generators of I (see for instance [2] and [5], Example 3.7).

As explained in [5], the discovery of Z-separating re-embeddings for non-trivial ideals I relies on the study of the Gröbner fan $\mathrm{GFan}(I)$ which was introduced first in [8]. As mentioned above, it may not be possible to use a Z-separating re-embedding to get an optimal re-embedding $P/I \cong P'/I'$ in the sense that $\dim(P')$ is the embedding dimension of P/I, i.e., the smallest possible number. Moreover, the usage of Gröbner fans has the added disadvantage that their computation is prohibitively expensive in all but the smallest examples.

This brings us to the main topic of this paper, namely the task to improve the search for Z-separating re-embeddings and to use a smaller portion of the Gröbner fan which is easier to compute. To achieve this goal, we take a markedly different point of view than in [5]. Here we concentrate not on specific Z-separating tuples, but on finding suitable tuples Z and the corresponding Z-separating tuples for a given ideal I. As a consequence, we have to study the intimate relationships between the given ideal I, possible tuples Z, and possible Z-separating tuples of polynomials $F = (f_1, \dots, f_s)$ with $f_i \in I$ very carefully, and in fact the entire Sect. 2 is devoted to this clarification task. In particular, Proposition 2.2 explains the relationship between Z-separating tuples and elimination orderings for Z.

Another novelty relates to the search for suitable Z-separating tuples. Suppose we have a reasonable candidate for $Z = (z_1, \dots, z_s)$ and for a Z-separating tuple

$F = (f_1, \dots, f_s)$ of polynomials in I. How can we check if F is indeed a Z-separating tuple for I? Recall that this means that we need to find a term ordering σ such that $\mathrm{LT}_\sigma(f_i) = z_i$ for $i = 1, \dots, s$. In Sect. 3 we show how to convert this problem to a Linear Programming (LP) feasibility problem (see Proposition 3.3). The usage of LP solvers for this task is explained in detail in Corollary 3.5. Several examples illustrate the efficiency and power of this approach.

In Sect. 4, we characterize Z-separating term orderings for I by the shape of their reduced Gröbner basis (see Proposition 4.2). This Gröbner basis allows us then to construct the desired re-embeddings of I which we called Z-separating re-embeddings in [5]. Altogether, we arrive at an efficient strategy for finding good re-embeddings of I which does not require the (possibly expensive) pre-calculation of a reduced Gröbner basis of I:

(1) Find a (large) tuple of indeterminates $Z = (z_1, \dots, z_s)$ and a tuple of polynomials $F = (f_1, \dots, f_s)$ such that f_i is z_i-separating for $i = 1, \dots, s$.
(2) Using an LP solver, verify that F is Z-separating and obtain a Z-separating term ordering for I.
(3) With the help of some inexpensive interreduction steps, create polynomials $z_1 - h_1, \dots, z_s - h_s$ in I with $h_i \in \widehat{P} = K[X \setminus Z]$.
(4) Using the polynomials $h_1, \dots, h_s$, define the Z-separating re-embedding $\Phi_Z : P/I \longrightarrow \widehat{P}/(I \cap \widehat{P})$ of I.

The viability and efficiency of this strategy is then demonstrated using some concrete examples.

The theoretical main result of this paper is contained in Sect. 5. Recall that the Gröbner fan $\mathrm{GFan}(I)$ of I consists of all marked reduced Gröbner bases of I. In non-trivial cases, it tends to be huge and very demanding to compute. In Definition 5.1 we introduce the notion of the Z-restricted Gröbner fan of I, denoted by $\mathrm{GFan}_Z(I)$, which is the set of all marked reduced Gröbner bases containing a Z-separating tuple of polynomials. Then, in Theorem 5.5, we prove that there is a bijective map $\Gamma_Z : \mathrm{GFan}_Z(I) \longrightarrow \mathrm{GFan}(I \cap \widehat{P})$. Since $\widehat{P} = K[X \setminus Z]$ may have considerably fewer indeterminates than P, this turns out to be a nice tool which can simplify the search for a good, and possibly optimal, re-embedding of I. Some examples illustrate this phenomenon.

Section 6 provides several heuristics and approaches for actually finding good re-embeddings of I, and it explains how to overcome some difficulties that may arise. In particular, Example 6.5 deals with the problem that the hypothesis $I \subseteq \langle x_1, \dots, x_n \rangle$, which we were using throughout the paper, may not be satisfied. Therefore we may need to perform a linear change of coordinates such that the origin is contained in $\mathcal{Z}(I)$. Which point should we move to the origin? By [5], Theorem 4.1, the dimension of the cotangent space at the origin is a lower bound for the embedding dimension of P/I. Therefore we should move the *worst* singularity of P/I to the origin. Since there is a unique K-rational singular point in this example, we know what we have to do, but the general situation may be more challenging. On the positive side, at the end of this section we also provide

a criterion which allows us to show that some re-embeddings are actually isomorphisms between the given scheme and an affine space (see Proposition 6.7).

Finally, in Sect. 7 we generalize the approach from using Z-separating tuples of polynomials to T-separating tuples, where $T = (t_1, \dots, t_s)$ denotes a tuple of terms that we try to realize as leading terms of polynomials in I. To adapt the definitions to this more general setting, we let Z be the tuple of indeterminates dividing one of the terms in T and $Y = X \setminus Z$. Using a suitable definition of a T-separating Gröbner fan $\mathrm{GFan}_T(I)$, we show that there is a free module M over $K[Y]$ such that the elements of $\mathrm{GFan}_T(I)$ are related to $K[Y]$-module Gröbner bases of $I \cap M$ and such that a T-separating module re-embedding $P/I \cong M/(I \cap M)$ of I results. However, we were not able to find an analogue of Theorem 5.5 in this setting and leave this task for future research.

True to our preferred style, we have sprinkled this paper generously with many illustrative examples. The calculations underlying these examples were performed using the computer algebra system CoCoA (see [1]) and with the help of the several CoCoA-packages written by the second and third authors. For the notation and definitions used throughout the paper, we follow [6] and [7].

2 Z-Separating polynomials, tuples, and ideals

In this section we use the notation introduced in [5] with some appropriate changes and extensions. Specifically, we let K be a field, let $P = K[x_1, \dots, x_n]$, and let $\mathfrak{M} = \langle x_1, \dots, x_n \rangle$. The tuple formed by the indeterminates of P is denoted by $X = (x_1, \dots, x_n)$. Furthermore, we let $1 \leq s \leq n$, let $z_1, \dots, z_s$ be pairwise distinct indeterminates in X, and let $Z = (z_1, \dots, z_s)$. The remaining indeterminates are denoted by $\{y_1, \dots, y_{n-s}\} = \{x_1, \dots, x_n\} \setminus \{z_1, \dots, z_s\}$, and we let $Y = (y_1, \dots, y_{n-s})$. Finally, given a term ordering σ on P, its restriction to $K[Y] = K[y_1, \dots, y_{n-s}]$ is denoted by σ_Y.

The following definition extends [5], Definitions 2.1 and 2.5.

Definition 2.1 In the above setting, let $f_1, \dots, f_s \in \mathfrak{M} \setminus \{0\}$, let $F = (f_1, \dots, f_s)$, and let $I_F = \langle f_1, \dots, f_s \rangle$ be the ideal generated by $\{f_1, \dots, f_s\}$.

(a) Given $i \in \{1, \dots, s\}$, we say that the polynomial f_i is *z_i-separating* if $z_i \in \mathrm{Supp}(f_i)$ and z_i does not divide any other term in $\mathrm{Supp}(f_i)$.
(b) The tuple F is called *Z-separating* if there exists a term ordering σ such that $\mathrm{LT}_\sigma(f_i) = z_i$ for $i = 1, \dots, s$. In this case σ is called a *Z-separating term ordering* for F.
(c) The tuple F is called *coherently Z-separating* if it is Z-separating, i.e., there exists a term ordering σ such that $\mathrm{LT}_\sigma(f_i) = z_i$ for $i = 1, \dots, s$, and if, additionally, the reduced σ-Gröbner basis of I_F is $\{\frac{1}{c_1} f_1, \dots, \frac{1}{c_s} f_s\}$, where $c_i = \mathrm{LC}_\sigma(f_i)$ for $i = 1, \dots, s$.

Proof To prove (a), it suffices to note that the complement of the monoideal generates by $\{t_1, \dots, t_s\}$ in $\mathbb{T}(Z)$ is an order ideal, i.e., for $u \in \mathcal{O}_T$ and $v \in \mathbb{T}(Z)$ such that $v \mid u$ we have $v \notin \langle t_1, \dots, t_s \rangle$ and hence $v \in \mathcal{O}_T$.

To show (b), we first note that σ_M is clearly a $K[Y]$-module term ordering on M. Since the polynomials $g_{s+1}, \dots, g_r$ are fully reduced against the polynomials $t_1 - h_1, \dots, t_s - h_s$, no term in their supports is divisible by a term in T. Hence they are contained in $I \cap M$. It remains to show that their leading terms generate the leading term module of $I \cap M$. For $f \in I \cap M$, we have $\mathrm{NF}_G(f) = 0$. However, since the support of f is contained in M, only $g_{s+1}, \dots, g_r$ can be involved in the reduction steps $f \xrightarrow{G} 0$. We may assume that in each reduction step a polynomial of the form $ug_i \in M$ with $u \in \mathbb{T}^n$ and $i \in \{s+1, \dots, r\}$ is subtracted. We write $u = u'\,u''$ with $u' \in \mathbb{T}(Z)$ and $u'' \in \mathbb{T}(Y)$. Then the reduction step subtracts a $K[Y]$-multiple of $u'g_i \in M$. Hence f can be reduced to zero in the $K[Y]$-module $I \cap M$ via the elements of H, and the claim is proved.

Finally, we note that the map NF_F in part (c) is well-defined, because $\mathcal{O}_T \cdot \mathbb{T}(Y)$ are the terms in the complement of the monoideal generated by $t_1, \dots, t_s$. The map NF_F is $K[Y]$-linear, as the indeterminates in Y do not divide any term in T. Letting $\epsilon : M \longrightarrow M/(I \cap M)$ be the canonical surjection, it is clear that the composed map $\epsilon \circ \mathrm{NF}_F : P \longrightarrow M \longrightarrow M/(I \cap M)$ is surjective. Hence it suffices to show that the kernel of $\epsilon \circ \mathrm{NF}_F$ is I. This follows from the fact that a polynomial $f \in P$ satisfies $\mathrm{NF}_F(f) \in I$ if and only if f reduces to zero via $g_{s+1}, \dots, g_r$, and this is equivalent to $f \in I \cap M$. □

Notice that the $K[Y]$-module M is not necessarily finitely generated. To get a full analogue to Theorem 5.5 in the T-separating case, one would have to develop a theory of Gröbner fans for modules and then examine which Gröbner bases of $I \cap M$ result from the restriction given in part (b) of the proposition. We leave this task to the interested readers and end this paper by applying the proposition to an easy example and to the setting of Example 7.3b.

Example 7.5 Let $P = \mathbb{Q}[x, y]$, let $T = (x^3)$, and let $G = \{g_1, g_2\}$, where $g_1 = x^3 - x$ and $g_2 = xy$. Let us look at the various statements of the proposition.

(a) We have $X = (x, y)$ and $Z = (x)$ and $Y = (y)$. The order ideal $\mathcal{O}_T \subseteq \mathbb{T}(Z)$ is given by $\mathcal{O}_T = \{1, x, x^2\}$.
(b) The module M is the free $\mathbb{Q}[y]$-module $M = \mathbb{Q}[y] \oplus x\,\mathbb{Q}[y] \oplus x^2\,\mathbb{Q}[y]$. The set $H = \{g_2, xg_2\} = \{xy, x^2y\}$ is a σ_M-Gröbner basis of the $\mathbb{Q}[y]$-module $I \cap M$, and hence $I \cap M = \mathbb{Q}[y] \cdot xy \oplus \mathbb{Q}[y] \cdot x^2y$.
(c) The T-separating module re-embedding of I is given by the $\mathbb{Q}[y]$-isomorphism $P/I \cong (\mathbb{Q}[y] \oplus x\,\mathbb{Q}[y] \oplus x^2\,\mathbb{Q}[y])/(\mathbb{Q}[y] \cdot xy \oplus \mathbb{Q}[y] \cdot x^2y)$.

Example 7.6 Let $P = \mathbb{Q}[x, y, z, w]$, let $T = (x, yz)$, and let $G = \{g_1, g_2, g_3\}$, where $g_1 = x - y^2 - w + y$, $g_2 = w^2 + w - y$, and $g_3 = yz + y^4 + 3y^2w - 2y^3 - 3yw + y^2 - 2w + 2y$. Here the term ordering σ

satisfies $\mathrm{LT}_\sigma(g_1) = x$, $\mathrm{LT}_\sigma(g_2) = w^2$, and $\mathrm{LT}_\sigma(g_3) = yz$. Thus we have $Z = (x, y, z)$ and $Y = (w)$. Let us look at the various statements of the proposition.

(a) The order ideal $\mathcal{O}_T$ is given by $\mathcal{O}_T = \{1, y, z, y^2, z^2, \dots\}$.
(b) The module M is the free $\mathbb{Q}[w]$-module

$$M = \mathbb{Q}[w] \oplus y\,\mathbb{Q}[w] \oplus z\,\mathbb{Q}[w] \oplus y^2\,\mathbb{Q}[w] \oplus z^2\,\mathbb{Q}[w] \oplus \cdots$$

The set $H = \{g_2, yg_2, y^2g_2, \dots\}$ is a σ_M-Gröbner basis of the $\mathbb{Q}[w]$-module $I \cap M$, and hence $I \cap M = \mathbb{Q}[y, w] \cdot g_2$.
(c) The T-separating module re-embedding of I is given by the $\mathbb{Q}[w]$-isomorphism $P/I \cong M/\mathbb{Q}[y, w] \cdot g_2 \cong \mathbb{Q}[y, w]/\langle g_2 \rangle \oplus \bigoplus_{i \geq 1} \mathbb{Q}[w]\, z^i$.

Acknowledgement The second author is partially supported by the Hue University under grant number DHH2021-03-159.

References

1. Abbott, J., Bigatti, A.M., Robbiano, L.: CoCoA: a system for doing computations in commutative algebra, available at http://cocoa.dima.unige.it
2. Crachiola, A.J.: The hypersurface $x + x^2y + z^2 + t^3$ over a field of arbitrary characteristic. Proc. Am. Math. Soc. **134**, 1289–1298 (2005)
3. Karmarkar, N.: A new polynomial-time algorithm for linear programming. Combinatorica **4**, 373–396 (1984)
4. Khachiyan, L.G.: A polynomial algorithm in linear programming. Dokl. Acad. Nauk. **244**, 1093–1096 (1979)
5. Kreuzer, M., Long, L.N., Robbiano, L.: Cotangent spaces and separating re-embeddings. J. Algebra Appl. (2021). https://doi.org/10.1142/S0219498822501882
6. Kreuzer, M., Robbiano, L.: Computational Commutative Algebra 1. Springer-Verlag, Berlin Heidelberg (2000)
7. Kreuzer, M., Robbiano, L.: Computational Commutative Algebra 2. Springer-Verlag, Berlin Heidelberg (2005)
8. Mora, T., Robbiano, L.: The Gröbner fan of an ideal. J. Symb. Comput. **6**, 183–208 (1988)
9. Ramos, Z., Simis, A.: Graded Algebras in Algebraic Geometry. de Gruyter, Berlin (2022)
10. Shpilrain, V., Yu, J.T.: Embedding of hypersurfaces in affine spaces. J. Algebra **239**, 161–173 (2001)
11. Srinivasan, V.: On the embedding dimension of an affine variety. Math. Ann. **289**, 125–132 (1991)