Bases of subalgebras of K[[x]] and K[x]

Abdallah Assi, Pedro A. García-Sánchez, Vincenzo Micale

BASES OF SUBALGEBRAS OF $\mathbb{K}[\![x]\!]$ AND $\mathbb{K}[x]$

A. ASSI, P. A. GARCÍA-SÁNCHEZ, AND V. MICALE

Abstract. Let $f_1, \ldots, f_s$ be formal power series (respectively polynomials) in the variable x. We study the semigroup of orders of the formal series in the algebra $K[\![f1, \ldots, f_s]\!] \subseteq K[\![x]\!]$ (respectively the semigroup of degrees of polynomials in $K[f_1, \ldots, f_s] \subseteq K[x]$). We give procedures to compute these semigroups and several applications.

1. Introduction

Let $\mathbb{K}$ be a field and let $\mathbb{K}[\![x]\!]$ (respectively $\mathbb{K}[x]$) be the ring of formal power series (respectively the ring of polynomials) over $\mathbb{K}$. Let $f_1(x), \ldots, f_s(x)$ be s elements of $\mathbb{K}[\![x]\!]$ (respectively $\mathbb{K}[x]$) and let $R = \mathbb{K}[\![f_1, \ldots, f_s]\!]$ (respectively $A = \mathbb{K}[f_1, \ldots, f_s]$) be the subalgebra of $\mathbb{K}[\![x]\!]$ (respectively $\mathbb{K}[x]$). Given $f \in R$ (respectively A), let $\mathrm{o}(f)$(respectively $\mathrm{d}(f)$) the order (respectively the degree) of f. The set $\{o(f), f \in R\}$ (respectively $\{d(f), f \in A\}$) is a submonoid $\mathrm{o}(R)$ (respectively $\mathrm{d}(A)$) of $\mathbb{N}$, and the knowledge of a system of generators of this monoid is important for the understanding of the subalgebra R (respectively A). When furthermore $\mathbb{K}[\![x]\!]$ (respectively $\mathbb{K}[x]$) is an R-module (respectively A-module) of finite length, then $\mathrm{o}(R)$ (respectively $\mathrm{d}(A)$) is a numerical semigroup.

A numerical semigroup S is a submonoid of the set of nonnegative integers under addition such that the $\mathbb{N} \setminus S$ is finite, or equivalently, $\gcd(S) = 1$ (the greatest common divisor of the elements of S), see for instance [15]. In this case, there exists a minimum $c \in S$ such that $c + \mathbb{N} \subseteq S$. We call this element the *conductor* of S, and denote it by $\mathrm{c}(S)$ (the motivation of this name and others coming from Algebraic Geometry is explained in [3, 7]).

Assume that f_i is a monomial x^{a_i} for every $i \in \{1, \ldots, s\}$. Then $\mathrm{o}(R)$ (respectively $\mathrm{d}(A)$) is generated by $a_1, \ldots, a_s$. In this case, $R \simeq \mathbb{K}[\![X_1, \ldots, X_s]\!]/T$ (respectively $A \simeq \mathbb{K}[X_1, \ldots, X_s]/T$), where T is a binomial ideal (equivalently $\mathrm{V}(T)$ is a toric variety).

Given a subalgebra $R = \mathbb{K}[[f_1, \ldots, f_s]]$ (respectively $A = \mathbb{K}[f_1, \ldots, f_s]$), the main objective of this paper is to describe an algorithm that calculates a generating system of $\mathrm{o}(R)$ (respectively $\mathrm{d}(A)$). The algorithm we present here allows us, by using the technique of homogenization, to construct a flat $\mathbb{K}[\![u]\!]$-module (respectively $\mathbb{K}[u]$-module) which is a deformation of R (respectively A) to a binomial ideal. This technique is well known when $R = \mathbb{K}[\![f_1, f_2]\!]$ and $\mathbb{K}$ is algebraically closed field of characteristic zero (see [10] and [18]). It turns out that the same holds wherever we can associate a semigroup to the local subalgebra, and also that the same technique can be adapted to the global setting. As a particular case we prove that a plane polynomial curve has a deformation into a complete intersection monomial space curve.

The paper is organized as follows. In Section 2 we focus on the local case, namely the case of a subalgebra R of $\mathbb{K}[\![x]\!]$. We introduce the notion of basis of R and we show how to construct such a basis. We also show that if $\mathrm{o}(R)$ is a numerical semigroup, then every element of a reduced basis is a polynomial. In Section 3 we show how to construct a deformation from R to a toric ideal (or a formal toric variety) by using the technique of homogenization. In Section 4 we focus on the case when $R = \mathbb{K}[[f(x), g(x)]]$ and $\mathbb{K}$ is algebraically closed field of characteristic zero. The existence in this case of the theory of Newton-Puiseux allows us to precise the results of Sections 2 and 3. The difference with the procedure presented in Section 2 is that it does not rely in the computation of successive kernels. Then in Sections 5 and 6 we adapt the local results to the case of a subalgebra A of $\mathbb{K}[x]$. When $A = \mathbb{K}[f(x), g(x)]$ and

The first author is partially supported by the project GDR CNRS 2945 and a GENIL-SSV 2014 grant.
The second author is supported by the projects MTM2010-15595, FQM-343, FQM-5849 and FEDER funds.

$\mathbb{K}$ is algebraically closed field of characteristic zero, a basis of A can be obtained by using the theory of approximate roots of the resultant of $X - f(x), Y - g(x)$, which is a polynomial with one place at infinity.

The procedures presented here have been implemented in `GAP` ([9]) and will be part of the forthcoming stable release of the package `numericalsgps` ([6]).

1.1. **Some notation.** We denote by $\langle A\rangle$ the monoid generated by A, $A \subseteq \mathbb{N}$, that is, the set $\{n_1x_1 + \cdots + n_mx_m \mid m \in \mathbb{N}, n_i \in \mathbb{N}, x_i \in A \text{ for all } i \in \{1,\dots,m\}\}$.

Associated to each numerical semigroup S we can define a natural partial ordering $\leq_S$, where for two elements s and r in S we have $s \leq_S r$ if there exists $u \in S$ such that $r = s + u$. The set g_i of minimal elements in $S \setminus \{0\}$ with this ordering is called a *minimal set of generators* for S. The set of minimal generators is finite since for any $s \in S \setminus \{0\}$, we have $x \not\equiv y \pmod{s}$ if $x \neq y$ are minimal elements with respect to $\leq_S$. The cardinality of the minimal generating system is known as the *embedding dimension* of S.

2. Semigroup of a formal space curve

Let $\mathbb{K}$ be a field. In this section we will consider rings R that are subalgebras of $\mathbb{K}[\![x]\!]$ and such that, if we denote the integral closure of R in its quotient field by $\bar{R}$, then $\bar{R} = \mathbb{K}[\![x]\!]$ and $\lambda_R(\bar{R}/R) < \infty$ where $\lambda_R(\cdot)$ is the length as R-module. Part of the results of this section are inspired in [14] and in [13]. An alternative procedure (implemented in Maple) is provided in [5]. The main different with our approach is that we do not rely on the multiplicity sequence, and thus we do not need to perform blow-ups. Also we take intrinsic advantage in our implementation of the `GAP` package `numericalsgps` ([9, 6]).

Let $f = \sum_i c_i x^i \in \bar{R}^* = \bar{R} \setminus \{0\}$. Define $\operatorname{supp}(f) = \{i, c_i \neq 0\}$. We call $\min \operatorname{supp}(f)$ the *order* of f and we denote it by $\mathrm{o}(f)$. We also set $\mathrm{M_o}(f) = c_{\mathrm{o}(f)}x^{\mathrm{o}(f)}$. If $\mathrm{M_o}(f) = x^{\mathrm{o}(f)}$, then we shall say, by abuse of notation, that f is *monic*. We set $\mathrm{o}(0) = +\infty$.

We denote by $\mathrm{o}(R)$ the set of orders of elements in $R^* = R \setminus \{0\}$, that is, $\mathrm{o}(R) = \{\mathrm{o}(f) \mid f \in R^*\}$. We finally set $\mathrm{M_o}(R) = \mathbb{K}[\mathrm{M_o}(f), f \in R^*]$.

Proposition 2.1. *Let f_1, f_2 be elements of $\bar{R}^*$ and let $a = \min\{\mathrm{o}(f_1), \mathrm{o}(f_2)\}$.*

(i) $a \leq \mathrm{o}(f_1 + f_2)$.
(ii) If $\mathrm{o}(f_1) \neq \mathrm{o}(f_2)$ *then* $a = \mathrm{o}(f_1 + f_2)$.
(iii) $\mathrm{o}(f_1f_2) = \mathrm{o}(f_1) + \mathrm{o}(f_2)$.

Proof. This follows easily from the definition of order. □

Proposition 2.2. [12, Lemma 3, p.486] *Let R_1 and R_2 be rings of our type such that $R_1 \subseteq R_2$ and $\mathrm{o}(R_1) = \mathrm{o}(R_2)$. Then $R_1 = R_2$.*

Proposition 2.3. [12, Proposition 1, p.488] *Let R be a ring of our type. Then $\lambda_R(\bar{R}/R) = |\mathbb{N} \setminus \mathrm{o}(R)|$.*

The following two results appear in [14], and since this paper is very hard to find, we include the proofs for sake of completeness.

Proposition 2.4. [14] *Let R be a ring of our type. Then $\mathrm{o}(R)$ is a numerical semigroup.*

Proof. Since R is a ring and by (iii) of Proposition 2.1, we have that $\mathrm{o}(R)$ is a subsemigroup of $\mathbb{N}$. By $\lambda_R(\bar{R}/R) < \infty$ and Proposition 2.3, we have the proof. □

Proposition 2.5. [14] *Let R be a ring of our type. Then R contains every element $f \in \mathbb{K}[\![x]\!]$ of order $\mathrm{o}(f) \geq c(\mathrm{o}(R))$.*

Proof. Use Proposition 2.2 with $R_1 = R$ and $R_2 = R + x^{\mathrm{c}(\mathrm{o}(R))}\mathbb{K}[\![x]\!]$. □

This later result allows to work with polynomials instead of series.

Let $f_1, \dots, f_s$ be in $\bar{R}^*$. Let $R = \mathbb{K}[\![f_1, \dots, f_s]\!]$ be a subalgebra of $\mathbb{K}[\![x]\!]$ as above, that is, the integral closure of R in its quotient field is $\bar{R} = \mathbb{K}[\![x]\!]$ and $\lambda_R(\bar{R}/R) < \infty$.

Under the hypotheses on R, we have that $\mathrm{o}(R)$ is a numerical semigroup (Proposition 2.4).

We say that the set $\{f_1, \dots, f_s\} \subset R^*$ is a *basis* of R if $R = \mathbb{K}[\![f_1, \dots, f_s]\!]$ and $\mathrm{o}(R) = \langle \mathrm{o}(f_1), \dots, \mathrm{o}(f_s)\rangle$. The set $\{f_1, \dots, f_s\}$ is a basis of R if and only if $\mathrm{M_o}(R) = \mathbb{K}[\mathrm{M_o}(f_1), \dots, \mathrm{M_o}(f_s)]$.

Proposition 2.6. *Let the notations be as above. Given $f(x) \in \mathbb{K}[\![x]\!]$, there exist $g(x) \in R$ and $r(x) \in \mathbb{K}[\![x]\!]$ such that the following conditions hold.*

(i) $f(x) = g(x) + r(x) = \sum_{\underline{\alpha}} c_{\underline{\alpha}} f_1^{\alpha_1} \cdots f_s^{\alpha_s} + r(x)$.
(ii) If $g(x) \neq 0$ (respectively $r(x) \neq 0$), then $\mathrm{o}(g) \geq \mathrm{o}(f)$ (respectively $\mathrm{o}(r) \geq \mathrm{o}(f)$).
(iii) Either $r(x) = 0$ or $\mathrm{supp}(r(x)) \subseteq \mathbb{N} \setminus \langle \mathrm{o}(f_1), \ldots, \mathrm{o}(f_s)\rangle$.

Proof. The assertion is clear if $f \in \mathbb{K}$. Suppose that $f \notin \mathbb{K}$ and let $f(x) = \sum_{i \geq p} c_i x^i$ with $p = \mathrm{o}(f) \geq 0$.

(1) If $p \notin \langle \mathrm{o}(f_1), \ldots, \mathrm{o}(f_s)\rangle$, then we set $g^1 = 0, r^1 = c_p x^p$ and $f^1 = f - c_p x^p$.
(2) If $p \in \langle \mathrm{o}(f_1), \ldots, \mathrm{o}(f_s)\rangle$, then $c_p x^p = c_{\underline{\theta}} M(f_1)^{\theta_1} \cdots M(f_s)^{\theta_s}$. We set $g^1 = c_{\underline{\theta}} f_1^{\theta_1^1} \cdots f_s^{\theta_s^1}$, $r^1 = 0$ and $f^1 = f - g^1$.

In such a way that $f = f^1 + g^1 + r^1$, $g^1 \in R$, either $r^1 = 0$ or $\mathrm{supp}(r^1) \subseteq \mathbb{N} \setminus \langle \mathrm{o}(f_1), \ldots, \mathrm{o}(f_s)\rangle$, and if $f^1 \neq 0$, then $\mathrm{o}(f^1) > \mathrm{o}(f) = p$. Then we restart with f^1. We construct in this way sequences $(f^k)_{k\geq 1}, (g^k)_{k\geq 1}, (r^k)_{k\geq 1}$ such that for all $k \geq 1, f = f^k + \sum_{i=1}^k g^i + \sum_{i=1}^k r^i$, and $\mathrm{o}(f) < \mathrm{o}(f^1) < \cdots < \mathrm{o}(f^k)$, $\sum_{i=1}^k g^i \in R$, $\mathrm{supp}(\sum_{i=1}^k r^i) \in \mathbb{N}\setminus\langle \mathrm{o}(f_1), \ldots, \mathrm{o}(f_s)\rangle$ and for all $i < j \leq k$, if $g^i \neq 0 \neq g^j$ (respectively $r^i \neq 0 \neq r^j$), then $\mathrm{o}(f) \leq \mathrm{o}(g^i) < \mathrm{o}(g^j)$ (respectively $\mathrm{o}(f) \leq \mathrm{o}(r^i) < \mathrm{o}(r^j)$). Clearly $\lim_{k\longrightarrow+\infty} f^k = 0$. Hence, if $g = \lim_{k\longrightarrow+\infty} \sum_{i=1}^k g^i$ and $r = \lim_{k\longrightarrow+\infty} \sum_{i=1}^k r^i$, then $f = g + r$ and g, r satisfy the conditions above. □

We call the series $r(x)$ of the result above the *remainder* of f with respect to $\{f_1, \ldots, f_s\}$ and we denote it by $\mathrm{R_o}(f, \{f_1, \ldots, f_s\})$.

Proposition 2.7. *The set $\{f_1, \ldots, f_s\}$ is a basis of R if and only if $\mathrm{R_o}(f, \{f_1, \ldots, f_s\}) = 0$ for all $f \in R$.*

Proof. Suppose that $\{f_1, \ldots, f_s\}$ is a basis of R and let $f \in R$. Let $r(x) = \mathrm{R_o}(f, \{f_1, \ldots, f_s\})$. Then $r(x) \in R$. If $r \neq 0$, then $\mathrm{o}(r) \in \langle \mathrm{o}(f_1), \ldots, \mathrm{o}(f_s)\rangle$, which is a contradiction.

Conversely, given $0 \neq f \in R$, if $\mathrm{o}(f) \notin \langle \mathrm{o}(f_1), \ldots, \mathrm{o}(f_s)\rangle$, then $\mathrm{R_o}(f, \{f_1, \ldots, f_s\}) \neq 0$, which is a contradiction. □

Let, as above, $R = \mathbb{K}[\![f_1, \ldots, f_s]\!]$. We shall suppose that f_i is monic for all $1 \leq i \leq s$. Define

$$\phi : \mathbb{K}[X_1, \ldots, X_s] \longrightarrow \mathbb{K}[x],\ \phi(X_i) = \mathrm{M_o}(f_i) \text{ for all } i \in \{1, \ldots, s\}.$$

Let $\{F_1, \ldots, F_r\}$ be a generating system of the kernel of ϕ. Clearly for all $i \in \{1, \ldots, r\}$, F_i is a binomial. If $F_i = X_1^{\alpha_1^i} \cdots X_s^{\alpha_s^i} - X_1^{\beta_1^i} \cdots X_s^{\beta_s^i}$, we set $S_i = f_1^{\alpha_1^i} \cdots f_s^{\alpha_s^i} - f_1^{\beta_1^i} \cdots f_s^{\beta_s^i}$. Note that if $p = \sum_{k=1}^s \alpha_k^i \mathrm{o}(f_k) = \sum_{k=1}^s \beta_k^i \mathrm{o}(f_k)$, then $\mathrm{o}(S_i) > p$.

Theorem 2.8. *The system $\{f_1, \ldots, f_s\}$ is a basis of R if and only if $\mathrm{R_o}(S_i, \{f_1, \ldots, f_s\}) = 0$ for all $i \in \{1, \ldots, r\}$.*

Proof. Suppose that $\{f_1, \ldots, f_s\}$ is a basis of R. Since $S_i \in R$ for all $i \in \{1, \ldots, r\}$, then, by Proposition 2.7, $\mathrm{R_o}(S_i, \{f_1, \ldots, f_s\}) = 0$.

For the sufficiency assume to the contrary that $\{f_1, \ldots, f_s\}$ is not a basis of R. Then there exists $f \in R$ such that $\mathrm{o}(f) \notin \langle \mathrm{o}(f_1), \ldots, \mathrm{o}(f_s)\rangle$. Write

$$f = \sum_{\underline{\theta}} c_{\underline{\theta}} f_1^{\theta_1} \cdots f_s^{\theta_s}.$$

For all $\underline{\theta}$, if $c_{\underline{\theta}} \neq 0$, we set $p_{\underline{\theta}} = \sum_{i=1}^s \theta_i \mathrm{o}(f_i) = \mathrm{o}(f_1^{\theta_1} \cdots f_s^{\theta_s})$. Let $p = \min\{p_{\underline{\theta}} \mid c_{\underline{\theta}} \neq 0\}$ and let $\{\underline{\theta}^1, \ldots, \underline{\theta}^l\}$ be such that $p = \mathrm{o}(f_1^{\theta_1^i} \cdots f_s^{\theta_s^i})$ for all $i \in \{1, \ldots, l\}$ (such a set is clearly finite). Also $p \leq \mathrm{o}(f) < \infty$.

If $\sum_{i=1}^l c_{\underline{\theta}^i} \mathrm{M_o}(f_1^{\theta_1^i} \cdots f_s^{\theta_s^i}) \neq 0$, then $p = \mathrm{o}(f) \in \langle \mathrm{o}(f_1), \ldots, \mathrm{o}(f_s)\rangle$. But this is imposible. Hence, $\sum_{i=1}^l c_{\underline{\theta}^i} \mathrm{M_o}(f_1^{\theta_1^i} \cdots f_s^{\theta_s^i}) = 0$, and then $\sum_{i=1}^l c_{\underline{\theta}^i} X_1^{\theta_1^i} \cdots X_s^{\theta_s^i} \in \ker(\phi)$. Hence

$$\sum_{i=1}^l c_{\underline{\theta}^i} X_1^{\theta_1^i} \cdots X_s^{\theta_s^i} = \sum_{k=1}^r \lambda_k F_k$$

with $\lambda_k \in \mathbb{K}[X_1,\dots,X_s]$ for all $k \in \{1,\dots,r\}$ (recall that $F_1,\dots,F_r$ are binomials generating $\ker(\phi)$). This implies that

$$\sum_{i=1}^{l} c_{\underline{\theta}^i} f_1^{\theta_1^i}\cdots f_s^{\theta_s^i} = \sum_{k=1}^{r} \lambda_k(f_1,\dots,f_s)S_k.$$

From the hypothesis $\mathrm{R_o}(S_k,\{f_1,\dots,f_s\}) = 0$. Hence there is an expression of S_k of the form $S_k = \sum_{\underline{\beta}^k} c_{\underline{\beta}^k} f_1^{\beta_1^k}\cdots f_s^{\beta_s^k}$ with $\mathrm{o}(f_1^{\beta_1^k}\cdots f_s^{\beta_s^k}) \geq \mathrm{o}(S_k)$.

So by replacing $\sum_{i=1}^{l} c_{\underline{\theta}^i} f_1^{\theta_1^i}\cdots f_s^{\theta_s^i}$ with $\sum_{k=1}^{r}\lambda_k(f_1,\dots,f_s)\sum_{\underline{\beta}^k} c_{\underline{\beta}^k} f_1^{\beta_1^k}\cdots f_s^{\beta_s^k}$ in the expression of f, we can rewrite f as $f = \sum_{\underline{\theta}'} c_{\underline{\theta}'} f_1^{\theta_1'}\cdots f_s^{\theta_s'}$ with $\min\{\mathrm{o}(f_1^{\theta_1'}\cdots f_s^{\theta_s'}) \mid c_{\underline{\theta}'} \neq 0\} > p$.

Since $\mathrm{o}(f) < +\infty$, this process will stop, yielding a contradiction. □

Algorithm 2.9. Let the notations be as above.

1. If $\mathrm{R_o}(S_k,\{f_1,\dots,f_s\}) = 0$ for all $k \in \{1,\dots,r\}$, then $\{f_1,\dots,f_s\}$ is a basis of R.
2. If $r(x) = \mathrm{R_o}(S_k,\{f_1,\dots,f_s\}) \neq 0$ for some $k \in \{1,\dots,r\}$, and if $\mathrm{M_o}(r(x)) = ax^q$, then we set $f_{s+1} = \frac{1}{a}r(x)$, and we restart with $\{f_1,\dots,f_{s+1}\}$. Note that in this case,

$$\langle \mathrm{o}(f_1),\dots,\mathrm{o}(f_s)\rangle \subsetneq \langle \mathrm{o}(f_1),\dots,\mathrm{o}(f_s),\mathrm{o}(f_{s+1})\rangle \subseteq \mathrm{o}(R).$$

This process will stop, giving a basis of R, because the complement of $\mathrm{o}(R)$ in $\mathbb{N}$ is finite.

Observe that $r(x)$ is not in general a polynomial. So we must use a trick to compute it, or at least the relevant part of it. This is accomplished by using Proposition 2.5. If in the current step of the algorithm $\langle \mathrm{o}(f_1),\dots,\mathrm{o}(f_s)\rangle$ is a numerical semigroup, then we compute its conductor, say c. Then $c \geq \mathrm{c}(\mathrm{o}(R))$. To compute $\mathrm{R_o}(f,\{f_1,\dots,f_s\})$ we do the following. Let $p = \mathrm{o}(f)$.

1. If $p \geq c$, then return 0. We implicitly assume that x^a is in our generating set for $a \in c+\mathbb{N}$ (though we do not store them).
2. If $p \in \langle \mathrm{o}(f_1),\dots,\mathrm{o}(f_s)\rangle$, then $\mathrm{M_o}(f) = \sum_{\underline{\theta}} c_{\underline{\theta}} \mathrm{M_o}(f_1)^{\theta_1}\cdots \mathrm{M_o}(f_s)^{\theta_s}$. Set $f = f - \sum_{\underline{\theta}} c_{\underline{\theta}} f_1^{\theta_1}\cdots f_s^{\theta_s}$, and call recursively $\mathrm{R_o}(f,\{f_1,\dots,f_s\})$ (the process will stop because the order of the new f is larger, and eventually will become bigger than c after a finite number of steps).
3. If $p \notin \langle \mathrm{o}(f_1),\dots,\mathrm{o}(f_s)\rangle$, then return f.

If $\langle \mathrm{o}(f_1),\dots,\mathrm{o}(f_s)\rangle$ is not a numerical semigroup, let d be its greatest common divisor. Set $c = d\mathrm{c}(\langle \mathrm{o}(f_1),\dots,\mathrm{o}(f_s)\rangle/d)$. In this case we proceed as follows.

1. If $p \geq c$, then return f. We cannot ensure here that f will be reduced to zero, so we add it just in case.
2. If $p \in \langle \mathrm{o}(f_1),\dots,\mathrm{o}(f_s)\rangle$, then $\mathrm{M_o}(f) = \sum_{\underline{\theta}} c_{\underline{\theta}} \mathrm{M_o}(f_1)^{\theta_1}\cdots \mathrm{M_o}(f_s)^{\theta_s}$. Set $f = f - \sum_{\underline{\theta}} c_{\underline{\theta}} f_1^{\theta_1}\cdots f_s^{\theta_s}$, and call recursively $\mathrm{R_o}(f,\{f_1,\dots,f_s\})$.
3. If $p \notin \langle \mathrm{o}(f_1),\dots,\mathrm{o}(f_s)\rangle$, then return f. One might check first if d does not divide p, because in this case for sure $p \notin \langle \mathrm{o}(f_1),\dots,\mathrm{o}(f_s)\rangle$.

Observe that by adding the conditions $p \geq c$, we are avoiding entering in an eventual infinite loop.

Suppose that $\{f_1,\dots,f_s\}$ is a basis of R. Also suppose that for all $i \in \{1,\dots,s\}$, f_i is monic. We say that $\{f_1,\dots,f_s\}$ is a *minimal basis* of R if $\mathrm{o}(f_1),\dots,\mathrm{o}(f_s)$ generate minimally the semigroup $\mathrm{o}(R)$. We say that $\{f_1,\dots,f_s\}$ is a *reduced basis* of R if $\mathrm{supp}(f_i(x) - \mathrm{M_0}(f_i)) \subseteq \mathbb{N}\setminus \mathrm{o}(R)$. Let $i \in \{1,\dots,s\}$. If $\mathrm{o}(f_i) \in \langle \mathrm{o}(f_1),\dots,\mathrm{o}(f_{i-1}),\mathrm{o}(f_{i+1}),\dots,\mathrm{o}(f_s)\rangle$, then $\{f_1,\dots,f_{i-1},f_{i+1},\dots,f_s\}$ is also a basis of R. Furthermore, by applying the division process of Proposition 2.6 to $f_i - \mathrm{M_o}(f_i)$, we can always construct a reduced basis of R.

Corollary 2.10. *The algebra R has a unique minimal reduced basis.*

Proof. Let $\{f_1,\dots,f_s\}$ and $\{g_1,\dots,g_{s'}\}$ be two minimal reduced bases of R. Hence s is the embedding dimension of $\mathrm{o}(R)$, and the same holds for s'; whence they are equal. Let $i = 1$. There exists j_1 such that $\mathrm{o}(f_1) = \mathrm{o}(g_{j_1})$, because minimal generating systems of numerical semigroups are unique. If $f_1 - g_{j_1} \neq 0$, then $\mathrm{o}(f_1 - g_{j_1}) \notin \mathrm{o}(R)$ (the basis is reduced), which is a contradiction because $f_1 - g_{j_1} \in R$. The same argument shows that $\{f_1,\dots,f_s\} = \{g_1,\dots,g_s\}$ □

Remark 2.11. Let $R = \mathbb{K}[\![f_1, \ldots, f_s]\!]$ and assume that f_i is monic for all $1 \leq i \leq s$. Also assume that $\mathrm{o}(f_1) \leq \mathrm{o}(f_2) \leq \ldots \leq \mathrm{o}(f_s)$. Set $n = \mathrm{o}(f_1)$ and let $f_1 = x^n + \sum_{i>n} c_i^1 x^i$. By an analytic change of variables, we may assume that $f_1 = x^n$, hence, up to an analytic isomorphism, we may assume that $R = \mathbb{K}[\![x^n, f_2, \ldots, f_s]\!]$. In particular, we may assume that R has a minimal reduced basis of the form $x^n, g_2(x), \ldots, g_{s'}(x)$.

Example 2.12. Let $R = \mathbb{K}[\![x^4 + x^5, x^6, x^{15} + x^{16}]\!]$, with $\mathbb{K}$ a field of characteristic zero. Then R is a one-dimensional ring and we will show that $\lambda_R(\mathbb{K}[\![X]\!]/R) < \infty$. Let us denote $x^4 + x^5$ by f_1, x^6 by f_2 and $x^{15} + x^{16}$ by f_3. After computing the kernel of $\phi : \mathbb{K}[X_1, X_2, X_3] \longrightarrow \mathbb{K}[x]$, $\phi(X_1) = x^4$, $\phi(X_2) = x^6$ and $\phi(X_3) = x^{15}$, we get $S_1 = \frac{1}{3}x^{15} + x^{14} + x^{13}$ and $S_2 = \frac{1}{2}x^{32} + x^{31}$. As $13 \notin \langle 4, 6, 15\rangle$, we add it as $f_4 = S_1$. We do not care about S_2, because the conductor of $\langle 4, 6, 15\rangle$ is 18.

Now, the conductor of $\langle 4, 6, 13, 15\rangle$ is 12. If we compute the kernel of $\varphi : \mathbb{K}[X_1, X_2, X_3, X_4] \longrightarrow \mathbb{K}[x]$, $\phi(X_1) = x^4$, $\phi(X_2) = x^6$, $\phi(X_3) = x^{15}$ and $\phi(X_4) = x^{13}$, then all the elements S_i have orders greater than 12, and so the algorithm ends. We conclude that $\mathrm{o}(R) = \langle 4, 6, 13, 15\rangle$.

We have implemented this algorithm in the `numericalsgps` ([6]) `GAP` ([9]) package. Next we illustrate how to compute this semigroup with the functions we have implemented (that will be available in the next release of the package).

```
gap> x:=X(Rationals,"x");;
gap> l:=[x^4+x^5,x^6,x^15+x^16];;
gap> s:=SemigroupOfValuesOfCurve_Local(l);;
gap> MinimalGeneratingSystem(s);
[ 4, 6, 13, 15 ]
gap> SemigroupOfValuesOfCurve_Local(l,13);
x^13
```

Remark 2.13. It is known (cf. [3, Section II.1]) that there exist relations between algebraic characters and invariants of the semigroup $\mathrm{o}(R)$ and the ring R. Hence, in the Example 2.12, from $\mathrm{o}(R) = \langle 4, 6, 13, 15\rangle = \{0, 4, 6, 8, 10, 12, \longrightarrow\}$, we have that $\lambda_R(\bar{R}/R) = |[0, \mathrm{c}(\mathrm{o}(R)) - 1] \cap (\mathbb{N} \setminus \mathrm{o}(R))| = 7$, $\lambda_R(R/(R : \bar{R})) = |[0, \mathrm{c}(\mathrm{o}(R)) - 1] \cap \mathrm{o}(R)| = 5$, $\mathrm{t}(R) \leq \mathrm{t}(\mathrm{o}(R)) = 3$, where $\mathrm{t}(R)$ is the type of the ring R.

Example 2.14. Let $R = \mathbb{K}[\![x^4, x^6 + x^7, x^{13} + a_{14}x^{14} + a_{15}x^{15} + \ldots]\!]$ with $\mathbb{K}$ a field. Using the same argument as in the Example 2.12, we find that if char $\mathbb{K} \neq 2$, we have that if $a_{15} - a_{14} + 1/2 = 0$, then $\{x^4, x^6 + x^7, x^{13}\}$ is the reduced basis of R. Furthermore, since $\langle 4, 6, 13\rangle$ is a symmetric numerical semigroup (the number of nonnegative integers not in the semigroup equals the conductor divided by two), then, by [11], R is Gorenstein. Finally $\lambda_R(\bar{R}/R) = 8$. Otherwise if $a_{15} - a_{14} + 1/2 \neq 0$, then $\{x^4, x^6 + x^7, x^{13}, x^{15}\}$ is the reduced basis of R with R a non Gorenstein ring. Furthermore $\lambda_R(\bar{R}/R) = 7$.

Otherwise, if char $\mathbb{K} = 2$, then the reduced basis of R is $\{x^4, x^6 + x^7, x^{13}, x^{15}\}$ and R is not a Gorenstein ring. Here, $\lambda_R(\bar{R}/R) = 7$.

Example 2.15. Let $R = \mathbb{K}[\![x^8, x^{12} + x^{14} + x^{15}]\!]$, with $\mathbb{K}$ a field of characteristic zero. Using the same argument as in the Example 2.12, we have that

$$\{x^8, x^{12} + x^{14} + x^{15}, x^{26} + x^{27} + x^{29} - \frac{1}{2}x^{31}, \\ x^{53} + \frac{1}{2}x^{55} - \frac{1}{2}x^{57} - \frac{1}{8}x^{63} + \frac{25}{8}x^{67} - \frac{95}{32}x^{71} - \frac{15}{16}x^{75} - \frac{135}{32}x^{83}\}$$

is the reduced basis of the Gorenstein ring R. Furthermore, we have $\lambda_R(\bar{R}/R) = 42$.

```
gap> l:=[x^8,x^12+x^14+x^15];;
gap> SemigroupOfValuesOfCurve_Local(l,"basis");
[ x^8, x^15+x^14+x^12, -1/2*x^31+x^29+x^27+x^26,
-135/32*x^83-15/16*x^75-95/32*x^71+25/8*x^67-1/8*x^63-1/2*x^57+1/2*x^55+x^53 ]
```

Example 2.16. The following battery of examples was provided by Lance Bryant as a test for our algorithm.

```
gap> l:=[ [ x^6,x^8+x^9,x^19], [x^7,x^9+x^10,x^19,x^31], [x^7,x^21+x^28+x^33],
[x^4,x^6+x^7,x^13], [x^6,x^8+x^11,x^10+2*x^13,x^21], [x^5,-x^18-x^21,-x^23,-x^26],
[x^5,-x^18-x^21,-x^26], [x^5,-x^18-x^21,x^23-x^26], [x^6,x^9+x^10,x^19],
[x^7,x^9+x^10,x^19], [x^8,x^9+x^10,x^19], [x^7,x^9+x^10,x^17,x^19] ] ;;
gap> List(l, i->MinimalGeneratingSystem(SemigroupOfValuesOfCurve_Local(i)));
[ [ 6, 8, 19, 29 ], [ 7, 9, 19, 29, 31 ], [ 7, 33 ], [ 4, 6, 13, 15 ],
  [ 6, 8, 10, 21, 23, 25 ], [ 5, 18, 26, 39, 47 ], [ 5, 18, 26, 39, 47 ],
  [ 5, 18, 26, 39, 47 ], [ 6, 9, 19, 20 ], [ 7, 9, 19, 29 ], [ 8, 9, 19, 30 ],
  [ 7, 9, 17, 19, 29 ] ]
```

3. Deformation to a toric ideal

Let the notations be as in Section 2. Given $f(x)=\sum_{i\geq p}c_ix^i\in\mathbb{K}[\![x]\!]$, we set $H_f(u,x)=\sum_{i\geq p}c_iu^{i-p}x^i$. In particular, if we consider the linear form $L:\mathbb{N}^2\longrightarrow\mathbb{N}, L(a,b)=b-a$, then H_f is L-homogeneous of degree p, that is, $L(i-p,i)=p$ for all $i\in\operatorname{supp}(f)$. We set $H_R=\mathbb{K}[\![H_f, f\in R]\!]$. With these notations we have the following.

Proposition 3.1. *The set $\{f_1,\dots,f_s\}$ is a basis of R if and only if $H_R=\mathbb{K}[\![H_{f_1},\dots,H_{f_s}]\!]$.*

Proof. Suppose that $\{f_1,\dots,f_s\}$ is a basis of R and let $f(x)\in R$. Write $H_f(u,x)=\sum_{i\geq p}c_iu^{i-p}x^i$. We have $\mathrm{M_o}(f)=c_px^p=c_p\prod_{i=1}^s M_{\mathrm{o}}(f_i)^{p_i^k}$, hence

$$H_f-c_p\prod_{i=1}^s H_{f_i}^{p_i^k}=u^qH_{f^1}$$

with $f^1\in R$ and either $f^1=0$, or $\mathrm{o}(f^1)>p$. In the second case we restart with f^1. A similar argument as in Proposition 2.6. proves our assertion.
Conversely, suppose that $H_R=\mathbb{K}[\![H_{f_1},\dots,H_{f_s}]\!]$ and let $f\in R$. Let $P(X_1,\dots,X_s)\in\mathbb{K}[\![X_1,\dots,X_s]\!]$ such that $H_f=P(H_{f_1},\dots,H_{f_s})$. If $u=0$, then $M_{\mathrm{o}}(f)=P(M_{\mathrm{o}}(f_1),\dots,M_{\mathrm{o}}(f_s))\in\mathbb{K}[\![M_{\mathrm{o}}(f_1),\dots,M_{\mathrm{o}}(f_s)]\!]$, hence $M_{\mathrm{o}}(f)\in\mathbb{K}[M_{\mathrm{o}}(f_1),\dots,M_{\mathrm{o}}(f_s)]$. □

Remark 3.2. Suppose that $\{f_1,\dots,f_r\}$ is a basis of R. Then $T=\mathbb{K}[\![u]\!][\![H_{f_1},\dots,H_{f_s}]\!]$ is a $\mathbb{K}[\![u]\!]$-module. When $u=1$ (respectively $u=0$), we get $T\mid_{u=1}=R$ (respectively $T\mid_{u=0}=\mathbb{K}[\![M(f_1),\dots,M(f_s)]\!]$). Hence we get a deformation from R to $\mathbb{K}[\![M_{\mathrm{o}}(f_1),\dots,M_{\mathrm{o}}(f_s)]\!]$. More precisely let

$$\psi:\mathbb{K}[\![X_1,\dots,X_s]\!]\longrightarrow R=\mathbb{K}[\![f_1,\dots,f_s]\!]$$

and

$$H_\psi:\mathbb{K}[\![u]\!][\![X_1,\dots,X_s]\!]\longrightarrow T=\mathbb{K}[\![u]\!][\![H_{f_1},\dots,H_{f_s}]\!]$$

be the morphisms of rings such that $H_\psi(u)=u$, $\psi(X_i)=f_i$ and $H_\psi(X_i)=H_{f_i}$ for all $i\in\{1,\dots,s\}$. For all $i\in\{1,\dots,r\}$, let

$$S_i=f_1^{\alpha_1^i}\cdots f_s^{\alpha_s^i}-f_1^{\beta_1^i}\cdots f_s^{\beta_s^i}=\sum_{\underline{\theta}^i}c^i_{\underline{\theta}^i}f_1^{\theta_1^i}\cdots f_s^{\theta_s^i}$$

with $\mathrm{o}(f_1^{\theta_1^i}\cdots f_s^{\theta_s^i})=D^i_{\underline{\theta}^i}>\sum_{k=1}^s\alpha_k^i\mathrm{o}(f_k)=\sum_{k=1}^s\beta_k^i\mathrm{o}(f_k)=p_i$. Let I (respectively J) be the ideal generated by $(X_1^{\alpha_1^i}\cdots X_s^{\alpha_s^i}-X_1^{\beta_1^i}\cdots X_s^{\beta_s^i}-\sum_{\underline{\theta}^i}c^i_{\underline{\theta}^i}X_1^{\theta_1^i}\cdots X_s^{\theta_s^i})_{1\leq i\leq r}$ (respectively $(X_1^{\alpha_1^i}\cdots X_s^{\alpha_s^i}-X_1^{\beta_1^i}\cdots X_s^{\beta_s^i}-\sum_{\underline{\theta}^i}u^{D^i_{\underline{\theta}^i}-p_i}c^i_{\underline{\theta}^i}X_1^{\theta_1^i}\cdots X_s^{\theta_s^i})_{1\leq i\leq r}$) in $\mathbb{K}[\![X_1,\dots,X_s]\!]$ (respectively $\mathbb{K}[\![u]\!][\![X_1,\dots,X_s]\!]$).

Since $\{f_1,\dots,f_s\}$ is a basis of R, the kernel of ψ (respectively $H(\psi)$) is generated by I (respectively J). Now the morphism

$$\mathbb{K}[\![u]\!]\longrightarrow\mathbb{K}[\![u]\!][\![X_1,\dots,X_s]\!]/J$$

is flat because u is not a zero divisor. Hence we get a family of formal space curves parametrized by u which gives us a deformation from $\mathbb{K}[\![X_1,\dots,X_r]\!]/I$ to $\mathbb{K}[\![X_1,\dots,X_r]\!]/(F_1,\dots,F_r)$.

In particular we get the following.

Theorem 3.3. *Every formal space curve of $\mathbb{K}^l$, parametrized by $Y_1 = g_1(x), \ldots, Y_l = g_l(x)$ has a deformation into a formal monomial curve of $\mathbb{K}^r$ for some positive integer r.*

4. Basis of $\mathbb{K}[\![f(x), g(x)]\!]$

In [19] the case of finding an algebra basis for $\mathbb{K}[f(x), g(x)]$ with f and g polynomials is treated. Here we will do the analogue for $\mathbb{K}[[f(x), g(x)]]$.

Let $f(x) = \sum_{i\geq n} a_i x^i$ and $g(x) = \sum_{j\geq m} b_j x^j$ be two elements of $\mathbb{K}[\![x]\!]$ and suppose, without loss of generality, that the following conditions hold:

(1) $a_n = b_m = 1$.
(2) $n \leq m$.
(3) For all $d > 1$, $f(x), g(x) \notin \mathbb{K}[\![x^d]\!]$ (i.e. the gcd of $\mathrm{supp}(f(x)) \cup \mathrm{supp}(g(x)) = 1$).

Let the notations be as in Section 2, in particular $R = \mathbb{K}[\![f, g]\!]$. By the analytic change of variables $f(x) = \tilde{x}^n$, we may assume that $R = \mathbb{K}[\![x^n, g(x)]\!]$. Let $F(X, Y)$ be the x-resultant of $X - x^n, Y - g(x)$, that is, $F(X, Y)$ is the generator of the kernel of the map $\rho : \mathbb{K}[\![X, Y]\!] \longrightarrow \mathbb{K}[\![x]\!]$, $\rho(X) = x^n$ and $\rho(Y) = g(x)$. Since $\mathbb{K}[\![f, g]\!] = \mathbb{K}[\![f, g - f^k]\!]$ for all $k \geq 1$, then we shall assume that $n < m$ and also that n does not divide m. Given a nonzero element $G(X, Y) \notin (F(X, Y))\mathbb{K}[\![X, Y]\!]$, we set $\mathrm{int}(F, G) = \mathrm{o}(G(f(x), g(x)))$. The set of $\mathrm{int}(F, G), G(X, Y) \notin (F(X, Y))\mathbb{K}[\![X, Y]\!]$, is a numerical semigroup. We denote it by $\Gamma(F)$. We have the following.

Proposition 4.1. $\mathrm{o}(R) = \Gamma(F)$.

Proof. We have $a \in \Gamma(F)$ if and only if $a = \mathrm{o}(G(f(x), g(x)))$ for some $G(X, Y) \in \mathbb{K}[\![X, Y]\!]$ if and only if $a \in \mathrm{o}(R)$. □

Suppose that $\mathbb{K}$ is algebraically closed with characteristic zero, and let $d_1 = n$, $m_1 = \inf\{i \in \mathrm{supp}(g) \mid d_1 \nmid i\}$, that is, $m_1 = m$, and $d_2 = \gcd(n, m_1)$. For all $k \geq 2$ we set $m_k = \inf\{i \in \mathrm{supp}(g) \mid d_k \nmid i\}$ and $d_{k+1} = \gcd(d_k, m_k)$. It follows that there exists $h \geq 1$ such that $d_{h+1} = 1$. The set $\{m_1, \ldots, m_h\}$ is called the *set of Newton-Puiseux exponents* of $F(X, Y)$. Let $e_k = \frac{d_k}{d_{k+1}}$ for all $1 \leq k \leq h$ and define the sequence $(r_k)_{0\leq k\leq h}$ as follows: $r_0 = n, r_1 = m$, and for all $2 \leq k \leq h, r_k = r_{k-1}e_{k-1} + m_k - m_{k-1}$. With these notations we have the following:

(1) $\Gamma(F) = \mathrm{o}(R)$ is generated by $\{r_0, r_1, \ldots, r_h\}$.
(2) $r_k d_k < r_{k+1} d_{k+1}$ for all $k \in \{1, \ldots, h-1\}$.
(3) $\Gamma(F) = \mathrm{o}(R)$ is free with respect to the arrangement $(r_0, \ldots, r_h)$. More precisely, let $e_k = \frac{d_k}{d_{k+1}}$ for all $k \in \{1, \ldots, h\}$. Then $e_k r_k \in \langle r_0, \ldots, r_{k-1}\rangle$.
(4) $C = \sum_{k=1}^{h}(e_k - 1)r_k - n + 1$ is the conductor of $\Gamma(F) = \mathrm{o}(R)$.

Example 4.2. Let $f = x^7$ and $g = x^4 + x^2$. The above resultant is then $F = y^7 - 7x^2y^3 - x^4 - 14x^2y^2 - 7x^2y - x^2$. Then $\Gamma(F) = \mathrm{o}(R) = \langle 2, 7\rangle$.

```
gap> Resultant(x-t^7, y-t^4-t^2,t);
y^7-7*x^2*y^3-x^4-14*x^2*y^2-7*x^2*y-x^2
gap> s:=SemigroupOfValuesOfCurve_Local([t^7,t^4+t^2]);
<Modular numerical semigroup satisfying 7x mod 14 <= x >
gap> MinimalGeneratingSystem(last);
[ 2, 7 ]
gap> IsFreeNumericalSemigroup(s);
true
```

Let the notations be as above. For all $k \geq 2$, let $G_k(X, Y) \in \mathbb{K}[\![X, Y]\!]$ such that $\mathrm{o}(G_k(x^n, g(x))) = r_k$. It follows from [1] that $\deg_Y G_k = \frac{n}{d_k}$. If $g_k(x) = G_k(x^n, g(x))$, then we have the following.

Proposition 4.3. *The set $\{x^n, g, g_2, \ldots, g_h\}$ is a basis of R, that is, $R = \mathbb{K}[\![x^n, g, g_2, \ldots, g_h]\!]$ and $\mathrm{M_o}(R) = \mathbb{K}[\![x^n, x^m, x^{r_2}, \ldots, x^{r_h}]\!]$.*

Note that, by a similar argument as in Section 2, we may assume that $f = x^n, g = x^m + \sum_{i\in \mathrm{G}(\Gamma(F))} c_i^1 x^i$, and for all $k \geq 2, g_k = x^{r_k} + \sum_{i\in \mathrm{G}(\Gamma(F))} c_i^k x^i$, where $\mathrm{G}(\Gamma(F)) = \{j \in \mathbb{N} \mid j \notin \Gamma(F)\}$ is the set of gaps of $\Gamma(F)$.
Let the notations be as in Section 3. The morphism

$$D : \mathbb{K}[\![u]\!] \longrightarrow T = \mathbb{K}[\![u]\!][\![H_f, H_g, H_{g_2}, \ldots, H_{g_h}]\!]$$

gives us a deformation of $T\mid_{u=1} = R = \mathbb{K}[\![f(x), g(x), g_2(x), \ldots, g_h(x)]\!]$ to $T\mid_{u=0} = \mathbb{K}[\![x^n, x^m, x^{r_2}, \ldots, x^{r_h}]\!]$. Note that, since $\langle n, m, r_2, \ldots, r_h\rangle$ is free with respect to the given arrangement, then it is a complete intersection (see for instance [15]). For all $k \in \{1, \ldots, h\}$, write $e_k r_k = \sum_{i=0}^{k-1} \theta_i^k r_i$ with $0 \leq \theta_i^k < e_i$ for all $i \in \{1, \ldots, k-1\}$. If B is the ideal of $\mathbb{K}[X_0, X_1, \ldots, X_h]$ generated by

$$\{X_1^{e_2} - X_0^{\frac{m}{d_2}}, X_2^{e_2} - X_0^{\theta_0^2} X_1^{\theta_1^2}, \ldots, X_h^{e_h} - X_0^{\theta_0^h} X_1^{\theta_1^h} \ldots X_{h-1}^{\theta_{h-1}^h}\}$$

then

$$\mathbb{K}[\![x^n, x^m, x^{r_2}, \ldots, x^{r_h}]\!] \simeq \mathbb{K}[\![X_0, X_1, \ldots, X_h]\!]/B.$$

Let $\bar{F}(X, Y)$ be the x-resultant of $X - x^n, y - g(x)$. By hypothesis, $\bar{F}(X, Y)$ is a polynomial. Furthermore, $\bar{F}(X, Y) = Y^n + a_1(X)Y^{n-1} + \ldots + a_n(X)$ with $\mathrm{o}(a_i(X)) > i$ for all $2 \leq i \leq n$. Set $G_{h+1} = \bar{F}$ and for all $k \geq 1$, let

$$G_{k+1} = G_k^{e_k} - X^{\theta_0^k} \prod_{i=1}^{k-1} G_i^{\theta_i^k} + \sum_{\underline{\alpha}^k} c_{\underline{\alpha}^k}^k X^{\alpha_0^k} G_1^{\alpha_1^k} \cdots G_k^{\alpha_k^k},$$

where the following conditions hold:

(1) for all $i \in \{0, \ldots, k-1\}$, $0 \leq \theta_i^k < e_i$;
(2) for all $\underline{\alpha}^k$, if $c_{\underline{\alpha}^k}^k \neq 0$, then for all $i \in \{1, \ldots, k\}$, $0 \leq \alpha_i^k < e_i$;
(3) for all $\underline{\alpha}^k$, if $c_{\underline{\alpha}^k}^k \neq 0$, then $\alpha_0^k n + \sum_{i=1}^k \alpha_i^k r_i = D_i^k > e_k r_k = \theta_0^k r_0 + \sum_{i=1}^{k-1} \theta_i^k r_i$.

It follows from Section 3. that if I (respectively J) is the ideal generated by

$$(X_k^{e_k} - X_0^{\theta_0^k} \prod_{i=1}^{k-1} X_i^{\theta_i^k} + \sum_{\underline{\alpha}^k} c_{\underline{\alpha}^k}^k X_0^{\alpha_0^k} X_1^{\alpha_1^k} \cdots X_k^{\alpha_k^k})_{1\leq k\leq h}$$

(respectively $(X_k^{e_k} - X_0^{\theta_0^k} \prod_{i=1}^{k-1} X_i^{\theta_i^k} + \sum_{\underline{\alpha}^k} c_{\underline{\alpha}^k}^k u^{D_i^k - e_k r_k} X_0^{\alpha_0^k} X_1^{\alpha_1^k} \cdots X_k^{\alpha_k^k})_{1\leq k\leq h}$) in $\mathbb{K}[\![X_0, \ldots, X_h]\!]$ (respectively $\mathbb{K}[\![u]\!][\![X_0, \ldots, X_h]\!]$), then

$$R = \mathbb{K}[\![x^n, g(x), g_2(x), \ldots, g_h(x)]\!] \simeq \mathbb{K}[\![X_0, X_1, \ldots, X_h]\!]/I$$

and

$$\mathbb{K}[\![u]\!][\![x^n, H_g, H_{g_2}, \ldots, H_{g_h}]\!] \simeq \mathbb{K}[\![u]\!][\![X_0, X_1, \ldots, X_h]\!]/J.$$

Furthermore, $\mathbb{K}[\![u]\!][\![X_0, X_1, \ldots, X_h]\!]/J$ is a flat $\mathbb{K}[\![u]\!]$-module. This gives us a family of formal space curves parametrized by u which is a deformation from $\mathbb{K}[\![X_0, X_1, \ldots, X_h]\!]/I$ to the formal toric variety $\mathbb{K}[\![X_0, X_1, \ldots, X_h]\!]/B$. The later being a complete intersection, we get the following.

Theorem 4.4. *Every irreducible singularity of a plane curve $X = f(x), Y = g(x)$ of $\mathbb{K}^2$ has a deformation into a formal monomial complete intersection curve of $\mathbb{K}^{h+1}$ for some $h \geq 1$.*

Example 4.5. Let $f(x) = x^4, g(x) = x^6 + x^7$. The minimal polynomial of $(f(x), g(x))$ is given by:

$$F(X, Y) = Y^4 - 2X^3Y^2 + X^6 - 4X^5Y - X^7 = (Y^2 - X^3)^2 - 4X^5Y - X^7$$

Let $r_0 = 4 = d_1, r_1 = 6 = m_1$ and $G_1 = Y$. We have $d_2 = \gcd(6, 4) = 2$, hence $m_2 = 7$. It follows that $r_2 = 13$. Note that if $G_2 = Y^2 - X^3$, then $g_2(x) = G_2(f(x), g(x)) = 2x^{13} + x^{14}$. Hence $\Gamma(F) = \mathrm{o}(R) = \langle 4, 6, 13\rangle$ and $\{f(x), g(x), g_2(x)\}$ is a basis of R. Let us double check it.

```
gap> SemigroupOfValuesOfCurve_Local([x^4,x^6+x^7],"basis");
[ x^4, x^7+x^6, -1/2*x^15+x^13 ]
```

(Observe that the output is different, since this is a reduced basis: we change $2x^{13}+x^4$ with $x^{13}+\frac{1}{2}x^{14}$, and then using that $14=2\times 4+6$, we replace this last polynomial with $x^{13}-\frac{1}{2}x^{15}$.)

Consequently, $H_R=\mathbb{K}[\![x^4,x^6+ux^7,2x^{13}+ux^{14},u^4,u^6,u^{13}]\!]$. With the notations above, $e_1=3,e_2=2$, hence $\mathbb{K}[\![x^4,x^6,x^{13}]\!]\simeq T=\mathbb{K}[\![X_0,X_1,X_2]\!]/(X_1^2-X_0^3,X_2^2-X_0^5X_1)$, and

$$\mathbb{K}[\![u]\!]\longrightarrow \mathbb{K}[\![u]\!][\![X_0,X_1,X_2]\!]/(X_1^2-X_0^3,X_2^2-4X_0^5X_1-u^2X_0^7)$$

gives us a deformation from R to T (we can also change X_2 with $\frac{1}{2}X_2$, and then $B=(X_1^2-X_0^3,X_2^2-4X_0^4X_1)$).

5. Semigroup of a polynomial curve

Let $\mathbb{K}$ be a field and let $f_1(x),\dots,f_s(x)$ be s polynomials of $\mathbb{K}[x]$. Let $A=\mathbb{K}[f_1,\dots,f_s]$ be a subalgebra of $\mathbb{K}[x]$, and assume, without loss of generality, that f_i is monic for all $i\in\{1,\dots,s\}$. Given $f(x)=\sum_{i=0}^p c_ix^i\in A$, with $c_p\neq 0$, we set $\mathrm{d}(f)=p$ and $\mathrm{M}(f)=c_px^p$, the *degree* and *leading monomial*, respectively. We also define $\mathrm{supp}(f)=\{i\mid c_i\neq 0\}$. The set $\mathrm{d}(A)=\{\mathrm{d}(f)\mid f\in A\}$ is a submonoid of $\mathbb{N}$. We shall assume that $\lambda_A(\mathbb{K}[x]/A)<\infty$. In particular $\mathrm{d}(A)$ is a numerical semigroup. We say that $\{f_1,\dots,f_s\}$ is a *basis* of A if $\{\mathrm{d}(f_1),\dots,\mathrm{d}(f_s)\}$ generates $\mathrm{d}(A)$. Clearly, $\{f_1,\dots,f_s\}$ is a basis of A if and only if $\mathbb{K}[M(f),f\in A]=\mathbb{K}[M(f_1),\dots,M(f_s)]$. For several variables, these basis are known in the literature as SAGBI basis ([16, 4]).

The following result is the analogue to Proposition 2.6. Actually, in this section we follow a similar argument to the one used in Section 2, with the advantage that sequences of degrees decrease, and thus the finiteness conditions are easier to deduce.

Proposition 5.1. *Given $f(x)\in\mathbb{K}[x]$, there exist $g(x)\in A$ and $r(x)\in\mathbb{K}[x]$ such that the following conditions hold:*

(1) $f(x)=g(x)+r(x)=\sum_{\underline{\alpha}}c_{\underline{\alpha}}f_1^{\alpha_1}\cdots f_s^{\alpha_s}+r(x)$,
(2) if $g(x)\neq 0$ (respectively $r(x)\neq 0$), then $\mathrm{d}(g)\leq\mathrm{d}(f)$ (respectively $\mathrm{d}(r)\leq\mathrm{d}(f)$),
(3) $\mathrm{supp}(r(x))\subseteq\mathbb{N}\setminus\langle\mathrm{d}(f_1),\dots,\mathrm{d}(f_s)\rangle$.

Proof. The assertion is clear if $f\in\mathbb{K}$. Suppose that $f\notin\mathbb{K}$ and let $f(x)=\sum_{i=0}^p c_ix^i$ with $p=\mathrm{d}(f)>0$.

(1) If $p\notin\langle\mathrm{d}(f_1),\dots,\mathrm{d}(f_s)\rangle$, then we set $g^1=0,r^1=c_px^p$ and $f^1=f-c_px^p$.
(2) If $p\in\langle\mathrm{d}(f_1),\dots,\mathrm{d}(f_s)\rangle$, then $c_px^p=c_{\underline{\theta}}M(f_1)^{\theta_1}\cdots M(f_s)^{\theta_s}$. We set $g^1=c_{\underline{\theta}}f_1^{\theta_1}\cdots f_s^{\theta_s}$, $r^1=0$ and $f^1=f-g^1$.

In this way, $f=f^1+g^1+r^1$, $g^1\in\mathbf{A}$, $\mathrm{supp}(r^1)\subseteq\mathbb{N}\setminus\langle\mathrm{d}(f_1),\dots,\mathrm{d}(f_s)\rangle$, and if $f^1\notin\mathbb{K}$, then $\mathrm{d}(f^1)<\mathrm{d}(f)=p$. Then we restart with f^1. Clearly there is $k\geq 1$ such that $f^k\in\mathbb{K}$. We set $g=g^1+\cdots+g^k+f^k$ and $r=r^1+\cdots+r^k$. □

We call the polynomial $r(x)$ of the theorem above the *remainder* of f with respect to $\{f_1,\dots,f_s\}$ and we denote it by $\mathrm{R}(f,\{f_1,\dots,f_s\})$. This is an adaptation of the procedure called subduction in [16], with the difference that we are adding f^k to g, and thus whenever the subduction process produces a constant, the remainder is zero.

The following characterization of basis is analogous to that given in Proposition 2.7 for formal space curves; we omit the proof since it is roughly the same.

Proposition 5.2. *The set $\{f_1,\dots,f_s\}$ is a basis of A if and only if $\mathrm{R}(f,\{f_1,\dots,f_s\})=0$ for all $f\in A$.*

Let the notations be as above and let

$$\phi:\mathbb{K}[X_1,\dots,X_s]\longrightarrow\mathbb{K}[x],\ \phi(X_i)=\mathrm{M}(f_i),\ \text{for all } i\in\{1,\dots,s\}.$$

Let $\{F_1,\dots,F_r\}$ be a generating system of the kernel of ϕ. Clearly for all $i=1,\dots,r$, F_i is a binomial. If $F_i=X_1^{\alpha_1^i}\cdots X_s^{\alpha_s^i}-X_1^{\beta_1^i}\cdots X_s^{\beta_s^i}$, we set $S_i=f_1^{\alpha_1^i}\cdots f_s^{\alpha_s^i}-f_1^{\beta_1^i}\cdots f_s^{\beta_s^i}$. Observe that if $d=\sum_{k=1}^s\alpha_k^i\mathrm{d}(f_k)=\sum_{k=1}^s\beta_k^i\mathrm{d}(f_k)$, then $\mathrm{d}(S_i)<d$. With this we obtain the following particular case of [17, Corollary 11.5] (taking into account that the subduction process is not exactly our remainder).

Theorem 5.3. *The set $\{f_1,\dots,f_s\}$ is a basis of A if and only if $\mathrm{R}(S_i,\{f_1,\dots,f_s\})=0$ for all $i\in\{1,\dots,r\}$.*

Proof. The proof goes as in Theorem 2.8, but now the inequalities are reversed and p is defined as a maximum instead of a minimum. □

Algorithm 5.4. Let the notations be as above.

(1) If $\mathrm{R}(S_k(f_1,\dots,f_s),\{f_1,\dots,f_s\})=0$ for all $k=1,\dots,r$, then $\{f_1,\dots,f_s\}$ is a basis of A.
(2) If $r(x)=\mathrm{R}(S_k(f_1,\dots,f_s),\{f_1,\dots,f_s\})\neq 0$ for some $1\leq k\leq r$, and if $\mathrm{M}(r)=ax^q$, then we set $f_{s+1}=\frac{1}{a}r(x)$, and we restart with $\{f_1,\dots,f_{s+1}\}$. Note that in this case, $\langle \mathrm{d}(f_1),\dots,\mathrm{d}(f_s)\rangle \subsetneq \langle \mathrm{d}(f_1),\dots,\mathrm{d}(f_s),\mathrm{d}(f_{s+1})\rangle$.

This process will stop, giving a basis of A.

Suppose that $\{f_1,\dots,f_s\}$ is a basis of A. Also suppose that f_i is monic for all $i\in\{1,\dots,s\}$. We say that $\{f_1,\dots,f_r\}$ is a *minimal basis* of A if $\{\mathrm{d}(f_1),\dots,\mathrm{d}(f_s)\}$ minimally generates the semigroup $\mathrm{d}(A)$. We say that $\{f_1,\dots,f_r\}$ is a *reduced basis* of A if $\mathrm{supp}(f_i(x)-\mathrm{M}(f_i))\in\mathbb{N}\setminus \mathrm{d}(A)$.

Let $i\in\{1,\dots,s\}$. If $\mathrm{d}(f_i)\in\langle \mathrm{d}(f_1),\dots,\mathrm{d}(f_{i-1}),\mathrm{d}(f_{i+1}),\dots,\mathrm{d}(f_s)\rangle$, then $\{f_1,\dots,f_{i-1},f_{i+1},\dots,f_s\}$ is also a basis of A. Furthermore, by applying the division process of Proposition 5.1 to $f_i-\mathrm{M}(f_i)$, we can always construct a reduced basis of A. Minimal reduced basis are not unique as in the formal space curve case, but "almost" unique.

Corollary 5.5. *Up to constants, the algebra A has a unique minimal reduced basis.*

Proof. Let $\{f_1,\dots,f_s\}$ and $\{g_1,\dots,g_{s'}\}$ be two minimal reduced bases of A. Clearly $s=s'$. Let $i=1$. There exists j_1 such that $\mathrm{d}(f_1)=\mathrm{d}(g_{j_1})$. If $f_1-g_{j_1}\notin\mathbb{K}$, then $\mathrm{d}(f_1-g_{j_1})\notin\Gamma(\mathbf{A})$, which is a contradiction because $f_1-g_{j_1}\in A$. The same agrument shows that for all $i\geq 2$, there exists j_i such that $f_i-g_{j_i}\in\mathbb{K}$. □

Corollary 5.6. *Let $\{f_1,\dots,f_s\}$ be a reduced basis of A. For all $i\in\{1,\dots,s\}$, $\mathrm{supp}(f_i-\mathrm{M}(f_i))\subseteq \mathrm{G}(\Gamma A)$.*

Example 5.7. We compute $\mathrm{d}(R)$ for $R=\mathbb{K}[x^6+x^3,x^4+x^2]$; $f_1=x^6+x^3$ and $f_2=x^4+x^2$. We start by computing the kernel of $\phi:\mathbb{K}[X_1,X_2]\to\mathbb{K}[x]$, with $\phi(X_1)=x^6$ and $\phi(X_2)=x^4$. This kernel is generated by $F_1=X_1^2-X_2^3$. Hence $S_1=-3x^{10}+2x^9-3x^8$. Since $10\in\langle 4,6\rangle$, $\mathrm{R}(S_1,\{f_1,f_2\})=\frac{-2}{3}x^9-x^7-x^5$. We add $f_3=x^9+\frac{3}{2}x^7+\frac{3}{2}x^5$ to our generating set.

In the next step $\phi:\mathbb{K}[X_1,X_2,X_3]\to\mathbb{K}[x]$, with $\phi(X_1)=x^6$, $\phi(X_2)=x^4$ and $\phi(X_3)=x^9$; $\ker\phi=(X_1^2-X_2^3,X_1^3-X_3^2)$, whence $S_1=x^{16}-x^{15}+\frac{7}{4}x^{14}+\frac{1}{2}x^{12}+\frac{3}{4}x^{10}-\frac{1}{3}x^9$ and $S_2=x^{10}-\frac{2}{3}x^9+x^8$. It turns out that $\mathrm{R}(S_1,\{f_1,f_2,f_3\})=0=\mathrm{R}(S_2,\{f_1,f_2,f_3\})$, and consequently $\{f_1,f_2,f_3\}$ is a (reduced minimal) basis of R. Also $\mathrm{d}(R)=\langle 4,6,9\rangle$.

Example 5.8. Let us compute $K[x^7,x^9+x^{10},x^{17},x^{19}]$ with our implementation.

```
gap> MinimalGeneratingSystem(SemigroupOfValuesOfCurve_Global(
[x^7,x^9+x^10,x^17,x^19]);
[ 7, 10, 16, 19, 25 ]
```

6. Deformation to a toric ideal

Let the notations be as in Section 5. Given $f(x)=\sum_{i=0}^p c_i x^i\in\mathbb{K}[x]$, we set $h_f(u,x)=\sum_{i=0}^p c_i u^{p-i}x^i$. We set $h_A=\mathbb{K}[h_f\mid f\in A]$. With these notations we have the following result, and its proof is similar to that of Proposition 3.1.

Proposition 6.1. *The set $\{f_1,\dots,f_r\}$ is a basis of A if and only if $h_A=\mathbb{K}[h_{f_1},\dots,h_{f_s},u^{\mathrm{d}(f_1)},\dots,x^{\mathrm{d}(f_s)}]$.*

Remark 6.2. Suppose that $\{f_1,\dots,f_s\}$ is a basis of A. By the inclusion morphism of rings $D:\mathbb{K}[u]\longrightarrow B=\mathbb{K}[u,h_{f_1},\dots,h_{f_s}]$, B is a $\mathbb{K}[u]$-module. When $u=1$ (respectively $u=0$), we get $B\mid_{u=1}=A$ (respectively $B\mid_{u=0}=\mathbb{K}[\mathrm{M}(f_1),\dots,\mathrm{M}(f_s)]$). Hence we get a deformation from A to $\mathbb{K}[\mathrm{M}(f_1),\dots,\mathrm{M}(f_s)]$. More precisely let

$$\psi:\mathbb{K}[X_1,\dots,X_s]\longrightarrow\mathbb{K}[f_1,\dots,f_s]$$

and

$$h_\psi:\mathbb{K}[u][X_1,\dots,X_s]\longrightarrow\mathbb{K}[u][h_{f_1},\dots,h_{f_s}]$$

be the morphisms of rings such that $h_\psi(u) = u$, $\psi(X_i) = f_i$ and $h_\psi(X_i) = h_{f_i}$ for all $i = 1, \dots, s$. For all $i = 1, \dots, r$, let

$$S_i = f_1^{\alpha_1^i} \cdots f_s^{\alpha_s^i} - f_1^{\beta_1^i} \cdots f_s^{\beta_s^i} = \sum_{\underline{\theta}^i} c^i_{\underline{\theta}^i} f_1^{\theta_1^i} \cdots f_s^{\theta_s^i}$$

with $\mathrm{d}(f_1^{\theta_1^i} \cdots f_s^{\theta_s^i}) = D^i_{\underline{\theta}^i} < \sum_{k=1}^s \alpha_k^i \mathrm{d}(f_k) = \sum_{k=1}^s \beta_k^i \mathrm{d}(f_k) = p_i$. Let I (respectively J) be the ideal generated by $(X_1^{\alpha_1^i} \cdots X_s^{\alpha_s^i} - X_1^{\beta_1^i} \cdots X_s^{\beta_s^i} - \sum_{\underline{\theta}^i} c^i_{\underline{\theta}^i} X_1^{\theta_1^i} \cdots X_s^{\theta_s^i})_{1 \le i \le r}$ (respectively $(X_1^{\alpha_1^i} \cdots X_s^{\alpha_s^i} - X_1^{\beta_1^i} \cdots X_s^{\beta_s^i} - \sum_{\underline{\theta}^i} u^{p_i - D^i_{\underline{\theta}^i}} c^i_{\underline{\theta}^i} X_1^{\theta_1^i} \cdots X_s^{\theta_s^i})_{1 \le i \le r}$) in $\mathbb{K}[X_1, \dots, X_s]$ (respectively $\mathbb{K}[u][X_1, \dots, X_s]$).

Since $\{f_1, \dots, f_s\}$ is a basis of A, then the kernel of ψ (respectively h_ψ) is generated by I (respectively J). Now the morphism

$$\mathbb{K}[u] \longrightarrow \mathbb{K}[u][X_1, \dots, X_r]/J$$

is flat (because $p(u)$ is not a zero divisor for all $p(u) \in \mathbb{K}[u]$. Hence we get a family of polynomial space curves parametrized by u which gives us a deformation from $\mathbb{K}[X_1, \dots, X_r]/I$ to $\mathbb{K}[X_1, \dots, X_r]/(F_1, \dots, F_r)$.

In particular we get the following analogue to Theorem 3.3.

Theorem 6.3. *Every polynomial space curve of $\mathbb{K}^l$, parametrized by $Y_1 = g_1(x), \dots, Y_l = g_l(x)$ has a deformation into a monomial curve of $\mathbb{K}^r$ for some positive integer r.*

7. Basis of $K[f(x), g(x)]$

Let $f(x) = \sum_{i=1}^n a_i x^i$ and $g(x) = \sum_{j=1}^m b_j x^j$ be two polynomials of $\mathbb{K}[x]$ and suppose, without loss of generality, that the following conditions hold:

(1) $a_n = b_m = 1$.
(2) $n \ge m$,
(3) for all $d > 1$, $f(x), g(x) \notin \mathbb{K}[x^d]$ (that is, the gcd of $\mathrm{supp}(f(x)) \cup \mathrm{supp}(g(x)) = 1$).

Let the notations be as in Section 5, in particular $A = \mathbb{K}[f, g]$. Let also $F(X, Y)$ be the x-resultant of $X - f(x), Y - g(x)$, that is, $F(X, Y)$ is the generator of the kernel of the map $\psi : \mathbb{K}[X, Y] \longrightarrow \mathbb{K}[x], \psi(X) = f(x)$ and $\psi(Y) = g(x)$. Since $\mathbb{K}[f, g] = \mathbb{K}[f, g - f]$, then we shall assume that $n > m$. Write $F(X, Y) = Y^n + c_1(X)Y^{n-1} + \cdots + c_n(X)$. Given a polynomial $G(X, Y) \notin (F(X, Y))\mathbb{K}[X, Y]$, we set $\mathrm{int}(F, G) = \deg_x G(f(x), g(x))$. Assume that $\mathbb{K}$ is algebraically closed with characteristic zero. Let d be a divisor of n, and let G be a monic polynomial in $\mathbb{K}[X][Y]$ of degree $\frac{n}{d}$ in Y. Write $F = G^d + \alpha_1(X, Y)G^{d-1} + \cdots + \alpha_d(X, Y)$ where for all $k \in \{1, \dots, d\}$, if $\alpha_k \ne 0$, then $\deg_Y \alpha_k < \frac{n}{d}$. We say that G is a dth *approximate root* of F if $\alpha_1 = 0$. There is a unique dth approximate root of F. We denote it by $\mathrm{App}(F, d)$. The following results can be found in [1].

Theorem 7.1. *Under the standing hypothesis.*

(1) $F(X, Y)$ has one place at infinity, that is, for all $k \in \{1, \dots, n\}$, if $c_k(X) \ne 0$, then $\deg_X c_k(X) < k$.
(2) $\{\mathrm{int}(F, G) \mid G \in \mathbb{K}[X, Y] \setminus (F)\}$ is a numerical semigroup.
(3) Let $D(n)$ be the set of divisors of n. The set $\{\mathrm{int}(F, \mathrm{App}(F, d)) \mid d \in D(n)\}$ generates $\Gamma(F)$.

We call $\{\mathrm{int}(F, G) \mid G \in \mathbb{K}[X, Y] \setminus (F)\}$ the semigroup of F, and we denote it by $\Gamma(F)$.

Corollary 7.2. *Let the notations be as above. We have $\mathrm{d}(A) = \Gamma(F)$.*

Proof. In fact, $h(x) \in A$ if and only if $h(x) = P(f(x), g(x))$ for some $P(X, Y) \in \mathbb{K}[X, Y]$. Hence $a \in \mathrm{d}(A)$ if and only if $a = \mathrm{int}(F, P), P \in \mathbb{K}[X, Y]$ which means that $a \in \Gamma(F)$. □

Let $F(X, Y) = Y^n + c_1(X)Y^{n-1} + \cdots + c_n(X)$ be as above, and assume, after a possible change of variables $X' = X, Y' = Y + \frac{c_1}{n}$, that $c_1(X, Y) = 0$ (note that this does not change A). In particular $\mathrm{App}(F, n) = Y$. A system of generators of $\Gamma(F)$ can be found algorithmically in the following way.

Let $r_0 = d_1 = n = \mathrm{int}(F, X), r_1 = \deg_X a_n(X) = \mathrm{int}(F, \mathrm{App}(F, n))$, and $d_2 = \gcd(r_0, r_1)$. We set $G_2 = \mathrm{App}(F, d_2), r_2 = \mathrm{int}(F, G_2) = \deg_x G_2(f(x), g(x))$, and $d_3 = \gcd(r_3, d_2)$, and so on... With these notations we have the following:

(1) $d_1 > d_2 > \ldots$ and there exists $h \geq 1$ such that $d_{h+1} = 1$;
(2) $\Gamma(F) = \mathrm{d}(A)$ is generated by $\{r_0, r_1, \ldots, r_h\}$;
(3) $r_k d_k > r_{k-1} d_{k-1}$ for all $k \in \{1, \ldots, h\}$;
(4) $\Gamma(F) = \mathrm{d}(A)$ is free with respect to the arrangement $(r_0, \ldots, r_h)$. More precisely, let $e_k = \frac{d_k}{d_{k+1}}$ for all $k \in \{1, \ldots, h\}$. Then $e_k r_k \in \langle r_0, \ldots, r_{k-1} \rangle$;
(5) $C = \sum_{k=1}^{h} (e_k - 1) r_k - n + 1$ is the conductor of $\Gamma(F) = \mathrm{d}(A)$.

Lemma 7.3. *If $A = \mathbb{K}[x]$, then $r_k = d_{k+1}$ for all $k = 1, \ldots, h$. In particular $\deg_x G_h(f(x), g(x)) = 1$ and m divides n.*

Proof. If $A = \mathbb{K}[x]$ then $C = 0$, hence $\sum_{k=1}^{h} (e_k - 1) r_k = n - 1$. Since $r_k \geq d_{k+1}$, then $\sum_{k=1}^{h} (e_k - 1) r_k \geq n - 1$ with equality if and only if $r_k = d_{k+1}$ for all $k = 1, \ldots, h$. Since $m = r_1 = d_2 = \gcd(n, m)$, then m divides n. □

Lemma 7.4. [19, Theorem 2] *If $\gcd(n, m) = 1$, then $\{f(x), g(x)\}$ is a basis of A.*

Proof. If $\gcd(n, m) = 1$, then $\Gamma(F) = \mathrm{d}(A) = \langle n, m \rangle$. Hence $\{f(x), g(x)\}$ is a basis of A. □

Lemma 7.5. *Suppose that $\gcd(n, m) = p_1 \cdots p_l$ where p_i is a positive prime number for all $i \in \{1, \ldots, l\}$ (and the p_i's are not necessarily distinct). The set $\{f(x), g(x)\}$ is not a basis of A. Furthermore, if c is the cardinality of a basis of A, then $2 \leq c \leq l + 2$. In particular, if $\gcd(n, m)$ is a prime number $p > 1$, then a basis of A has either two or three elements.*

Proof. Since $\gcd(n, m) > 1$, then the first assertion is clear. On the other hand, since $d_2 = \gcd(n, m) = p_1 \cdots p_r$, we have $A \neq \mathbb{K}[x]$, and $h \leq l + 1$. Hence $\Gamma(F) = \mathrm{d}(A)$ has at most $l + 2$ generators. The result now follows. □

Remark 7.6. Let $\underline{r} = (r_0 = n, r_1 = m, r_2, \ldots, r_h)$ be a sequence of integers and for all $k \geq 1$, let $d_k = \gcd(r_0, \cdots, r_{k-1})$ and $e_k = \frac{d_k}{d_{k+1}}$. Assume that the following conditions hold:

(1) $d_1 > d_2 > \ldots > d_{h+1} = 1$;
(2) $r_k d_k > r_{k-1} d_{k-1}$ for all $k \in \{1, \ldots, h\}$;
(3) $e_k r_k \in < r_0, \ldots, r_{k-1} >$ for all $k = 1, \ldots, h$.

Such a sequence is called a *δ-sequence* and it is well known (see [1]) that there exists a polynomial $\tilde{F}(X, Y)$ with one place at infinity such that the semigroup $\{\mathrm{rank}_{\mathbb{K}} \mathbb{K}[X, Y]/(\tilde{F}, G), G \notin (F)\}$ is generated by $\underline{r}$.

Abhyankar asked whether every semigroup generated by a δ-sequence is the semigroup of a polynomial curve (for example, the δ-sequence $(10, 4, 5)$ generates the semigroup $\langle 4, 5 \rangle$ which is the semigroup of the polynomial curve $A = \mathbb{K}[x^4, x^5]$). It has been proved recently that the answer is no ([8]). It would be nice to see which supplementary conditions a δ-sequence should satisfy in order to generate the semigroup of a polynomial curve.

Remark 7.7. Let $f(x)$ and $g(x)$ be as above, and let $A = \mathbb{K}[f(x), g(x)]$. Let also $F(X, Y)$ be the x-resultant of $X - f(x)$ and $Y - g(x)$. Let $r_0 = n, r_1 = m, r_2, \ldots, r_h$ be the generators of $\Gamma(F)$ calculated as above. Let $1 \leq k \leq h$ and let $G_k(X, Y) = \mathrm{App}(F, d_k)$. We have $\mathrm{d}(G_k(f(x), g(x)) = r_k$, but G_k is not the unique polynomial with this condition (for example, $\mathrm{d}((G_k + \lambda)(f(x), g(x))) = r_k$ for all $\lambda \neq 0$). Hence it is natural to ask the following: is there a polynomial $G(X, Y)$ (of degree $< n$ in Y) such that G is parametrized by polynomials in x? Such a polynomial, if it exists, should be of degree $\frac{n}{d_k}$ and should have the contact with F at a characteristic exponent of F (see [1] for the definition of the characteristic exponents of a curve with one place at infinity). Hence the existence of such a polynomial implies that a polynomial curve can be approximated by polynomial curves.

Let the notations be as above, in particular $F(X, Y) = Y^n + c_1(X) Y^{n-1} + \cdots + c_n(X)$ is the x-resultant of $(X - f(x), Y - g(x))$. Let $G_1 = Y, G_2, \ldots, G_h$ be the set of approximate roots of $F(X, Y)$ constructed algorithmically as above. In particular $r_0 = n, r_1 = m, r_2 = \mathrm{int}(F, G_2), \ldots, r_h = \mathrm{int}(F, G_h)$ generate $\mathrm{d}(A)$. For all $k = 2, \ldots, h$, let $g_k(x) = G_k(f(x), g(x))$ and let $\mathrm{M}(g_k) = b_{r_k} x^{r_k}$. We have $A = \mathbb{K}[f(x), g(x), g_2(x), \ldots, g_h(x)]$. Furthermore, the map

$$D : \mathbb{K}[u] \longrightarrow B = \mathbb{K}[u][h_f, h_g, h_{g_2}, \ldots, h_{g_h}]$$

introduced in Remark 6.2 gives us a deformation of the polynomial curve $B\ |_{u=1}= A$ into $B\ |_{u=0}= \mathbb{K}[t^n, t^m, t^{r_2}, \ldots, t^{r_h}]$. Note that, since $\langle n, m, r_2, \ldots, r_h\rangle$ is free with respect to the given arragement, then it is a complete intersection. For all $k \in \{1, \ldots, h\}$, write $e_k r_k = \sum_{i=0}^{k-1} \theta_i^k r_i$ with $0 \leq \theta_i^k < e_i$ for every $i \in \{1, \ldots, k-1\}$. With the notations above, if T is the ideal of $\mathbb{K}[X_0, X_1, \ldots, X_h]$ generated by

$$\{X_1^{e_2} - X_0^{\frac{m}{d_2}}, X_2^{e_2} - X_0^{\theta_0^2} X_1^{\theta_1^2}, \ldots, X_h^{e_h} - X_0^{\theta_0^h} X_1^{\theta_1^h} \ldots X_{h-1}^{\theta_{h-1}^h}\},$$

then

$$\mathbb{K}[x^n, x^m, x^{r_2}, \ldots, x^{r_h}] \simeq \mathbb{K}[X_0, X_1, \ldots, X_h]/T.$$

Set $G_{h+1} = F$ and for all $k \geq 1$, let

$$G_{k+1} = G_k^{e_k} - X^{\theta_0^k} \prod_{i=1}^{k-1} G_i^{\theta_i^k} + \sum_{\underline{\alpha}^k} c_{\underline{\alpha}^k}^k X^{\alpha_0^k}.G_1^{\alpha_1^k} \cdots G_k^{\alpha_k^k},$$

where the following conditions hold:

(1) for all $i \in \{0, \ldots, k-1\}$, $0 \leq \theta_i^k < e_i$;
(2) for all $\underline{\alpha}^k$, if $c_{\underline{\alpha}^k}^k \neq 0$, then for all $i \in \{1, \ldots, k\}$, $0 \leq \alpha_i^k < e_i$,
(3) for all $\underline{\alpha}^k$, if $c_{\underline{\alpha}^k}^k \neq 0$, then $\alpha_0^k n + \sum_{i=1}^k \alpha_i^k r_i = D_i^k < e_k r_k = \theta_0^k r_0 + \sum_{i=1}^k \theta_i^k r_i$.

It follows from Section 6 that if I (respectively J) is the ideal generated by $(X_k^{e_k} - X_0^{\theta_0^k} \prod_{i=1}^{k-1} X_i^{\theta_i^k} + \sum_{\underline{\alpha}^k} c_{\underline{\alpha}^k}^k X_0^{\alpha_0^k}.X_1^{\alpha_1^k} \cdots X_k^{\alpha_k^k})_{1\leq k\leq h}$ (respectively $(X_k^{e_k} - X_0^{\theta_0^k} \prod_{i=1}^{k-1} X_i^{\theta_i^k} + \sum_{\underline{\alpha}^k} c_{\underline{\alpha}^k}^k u^{e_k r_k - D_i^k} X_0^{\alpha_0^k}.X_1^{\alpha_1^k} \cdots X_k^{\alpha_k^k})_{1\leq k\leq h}$) in $\mathbb{K}[X_0, \ldots, X_h]$ (respectively $\mathbb{K}[u][X_0, \ldots, X_h]$), then

$$A = \mathbb{K}[x^n, g(x), g_2(x), \ldots, g_h(x)] \simeq \mathbb{K}[X_0, X_1, \ldots, X_h]/I$$

and

$$\mathbb{K}[u][x^n, h_{g(x)}, h_{g_2(x)}, \ldots, h_{g_h(x)}] \simeq \mathbb{K}[u][X_0, X_1, \ldots, X_h]/J.$$

Furthermore, $\mathbb{K}[u][X_0, X_1, \ldots, X_h]/J$ is a flat $\mathbb{K}[u]$-module. This gives us a family of space curve parametrized by u which is a deformation from $\mathbb{K}[X_0, X_1, \ldots, X_h]/I$ to the toric variety $\mathbb{K}[X_0, X_1, \ldots, X_h]/T$. The later being a complete intersection, we get the following result.

Theorem 7.8. *Every polynomial curve $X = f(x), Y = g(x)$ of $\mathbb{K}^2$ has a deformation into a monomial complete intersection curve of $\mathbb{K}^{h+1}$ for some positive integer h.*

Example 7.9. Let $f(x) = x^6 + x^3, g(X) = x^4$. The minimal polynomial of $(f(x), g(x))$ is given by:

$$F(X, Y) = Y^6 - 2X^2Y^3 - 4XY^3 - Y^3 + X^4.$$

Let $r_0 = 6 = d_1, r_1 = 4$ and $G_1 = Y$. We have $d_2 = \gcd(6, 4) = 2$, and $G_2 = \mathrm{App}(F, 2) = Y^3 - X^2 - 2X - \frac{1}{2}$. Since $g_2(x) = G_2(f(x), g(x)) = -2x^9 - 3x^6 - 2x^3 - \frac{1}{2}$, then $r_2 = 9$ and $d_3 = 1$, hence $\Gamma(F) = \mathrm{d}(A) = \langle 6, 4, 9\rangle$ and $\{f(x), g(x), g_2(x)\}$ is a basis of A. Consequently, $h_A = \mathbb{K}[x^6 + u^3x^3, x^4, 2x^9 + 3u^3x^6 + 2u^6x^3 + \frac{1}{2}u^9, u^6, u^4, u^9]$. Note that, with the notations above, $e_1 = 3, e_2 = 2$, hence $\mathbb{K}[x^6, x^4, 2x^9] \simeq \mathbb{K}[X_0, X_1, X_2]/(X_1^3 - X_0^2, X_2^2 - 4X_0^3) = \mathbb{K}[X_0, X_1, X_2]/T$, $\mathbb{K}[x^6 + x^3, x^4, 2x^9 - 3x^6 - 2x^3 - \frac{1}{2}] \simeq \mathbb{K}[X_0, X_1, X_2]/(X_1^3 - X_0^2 - 2X_0 - \frac{1}{2}, X_2^2 - 4X_0^3 - 5X_0^2 - 2X_0 - \frac{1}{4})$, and

$$\mathbb{K}[u] \longrightarrow \mathbb{K}[u][X_0, X_1, X_2]/(X_1^3 - X_0^2 - 2u^6X_0 - \frac{1}{2}u^9, X_2^2 - 4X_0^3 - 5u^6X_0^2 - 2u^{12}X_0 - \frac{1}{4}u^{18})$$

gives us a deformation from A to $\mathbb{K}[X_0, X_1, X_2]/T$.

The computation of the approximate roots and of $\Gamma(F)$ can be performed with the algorithm presented in [2].

```
gap> f:=y^6-2*x^2*y^3-4*x*y^3-y^3+x^4;;
gap> SemigroupOfValuesOfPlaneCurveWithSinglePlaceAtInfinity(f);
<Numerical semigroup with 3 generators>
gap> MinimalGeneratingSystem(last);
[ 4, 6, 9 ]
gap>SemigroupOfValuesOfPlaneCurveWithSinglePlaceAtInfinity(f);
```

```
[ [ 6, 4, 9 ], [ y, y^3-x^2-2*x-1/2 ] ]
```

Example 7.10. Let $f(x) = x^6 + x, g(x) = x^4$. The minimal polynomial of $(f(x), g(x))$ is given by:

$$F(X,Y) = Y^6 - 2X^2Y^3 - 4XY^2 - Y + X^4.$$

Let $r_0 = 6 = d_1, r_1 = 4$ and $G_1 = Y$. We have $d_2 = \gcd(6,4) = 2$, and $G_2 = \mathrm{App}(F,2) = Y^3 - X^2$. Since $g_2(x) = G_2(f(x), g(x)) = -2x^7 - x^2$, then $r_2 = 7$ and $d_3 = 1$, hence $\Gamma(F) = \mathrm{d}(A) = \langle 6,4,7\rangle$ and $\{f(x), g(x), g_2(x)\}$ is a basis of A. Consequently, $h_A = \mathbb{K}[x^6 + u^5x, x^4, 2x^7 + u^5x^2, u^6, u^4, u^7]$. Note that, with the notations above, $e_1 = 3, e_2 = 2$, hence $\mathbb{K}[x^6, x^4, x^7] \simeq \mathbb{K}[X_0, X_1, X_2]/(X_1^3 - X_0^2, X_2^2 - X_0X_1^2) = \mathbb{K}[X_0, X_1, X_2]/T$, and

$$\mathbb{K}[u] \longrightarrow \mathbb{K}[u][X_0, X_1, X_2]/(X_1^3 - X_0^2, X_2^2 - 4X_0X_1^2 - u^{10}X_1)$$

gives us a deformation from A to $\mathbb{K}[X_0, X_1, X_2]/T$ (we can also change X_2 with $\frac{1}{2}X_2$, and then $T = (X_1^3 - X_0^2, X_2^2 - 4X_0X_1^2)$).

Acknowledgements

The authors would also like to thank Lance Bryant for providing plenty of examples for testing our algorithms, as well as suggesting us to implement new functionalities, that are now given as an extra argument of the function `SemigroupOfValuesOfCurve_Local`.

References

[1] S.S. Abhyankar, On the semigroup of a meromorphic plane curve, Part I, in Proceedings of International Symposium on Algebraic Geometry (1977), 240–414.
[2] A. Assi, P. A. García-Sánchez, On curves with one place at infinity, arXiv:1407.0490.
[3] V. Barucci, D. E. Dobbs, M. Fontana, Properties in numerical semigroups and applications to one-dimensional analytically irreducible local domains, Mem. Amer. Math. Soc. vol 125, **598** (1997).
[4] A. Bravo, Some facts about canonical subalgebra bases, Trends in Commutative Algebra, **51**, (2004), 247–254.
[5] A. Castellanos, J. Castellanos, Algorithm for the Semigroup of a Space Curve Singularity, Semigroup Forum **70** (2005) 44–60.
[6] M. Delgado, P. A. García-Sánchez, J. Morais, "NumericalSgps", A GAP package for numerical semigroups. Available via `http://www.gap-system.org`.
[7] R. Fröberg-C. Gottlieb-R. Häggkvist, On numerical semigroups, Semigroup forum **35** (1987), 63–83.
[8] M. Fujimoto, M. Suzuki, K. Yokoyama, On polynomial curves in the affine plane. Osaka J. Math. **43** (2006), no. 3, 597–608.
[9] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.7.5; 2014, `http://www.gap-system.org`.
[10] R. Goldin, B. Teissier, Resolving singularities of plane analytic branches with one toric morphism. Resolution of singularities (Obergurgl, 1997), Progr. Math., **181**, Birkhauser, Basel, 2000, 315–340.
[11] E. Kunz, The value-semigroup of a one-dimensional Gorenstein ring, Proc. Amer. Math. Soc. **25** (1970), 748–751.
[12] T. Matsuoka, On the degree of singularity of one-dimensional analytically irreducible noetherian local rings, J. Math. Kyoto Univ., **11-3** (1971), 485–494.
[13] V. Micale, Order bases of subalgebras of power series rings, Comm. Algebra **31** (2003), no. 3, 1359–1375.
[14] V. Micale, G. Molica, B. Torrisi, Order bases of subalgebras of $k[\![X]\!]$, Commutative rings, 193–199, Nova Sci. Publ., Hauppauge, NY, 2002.
[15] J. C. Rosales, P. A. García-Sánchez, Numerical semigroups, Developments in Mathematics, 20. Springer, New York, 2009.
[16] L. Robbiano and M. Sweedler, Subalgebra bases, pp. 61–87 in Commutative Algebra (Salvador, 1988), edited by W. Bruns and A. Simis, Lecture Notes in Math. **1430**, Springer, Berlin, 1990.
[17] B. Sturmfels, Gröbner bases and convex polytopes, University Lecture Series **8**, Amer. Math. Soc., Providence, 1996.
[18] B. Teissier, Appendice, pp. 145–199 in Le problème des pour les branches planes, by O. Zariski, Centre de Mathématiques de l'Ecole Polytechnique, Paris, 1975. Second edition, Hermann, 1986.
[19] A. Torstensson, Canonical bases for subalgebras on two generators in the univariate polynomial ring. Beiträge Algebra Geom. **43** (2002), 565–577.

Université d'Angers, Mathématiques, 49045 Angers ceded 01, France
E-mail address: assi@univ-angers.fr

Departamento de Álgebra and CITIC-UGR, Universidad de Granada, E-18071 Granada, España
E-mail address: pedro@ugr.es

Dipartimento di Matematica e Informatica, Viale A. Doria, 6 - I 95125 Catania, Italia
E-mail address: vmicale@dmi.unict.it