Gröbner basis. A new algorithm for computing the Frobenius number

Marcel Morales, Dung Nguyen Thi

Gröbner basis. A new algorithm for computing the Frobenius number

Marcel Morales
Institut Fourier, Laboratoire de Mathématiques associé au CNRS, UMR 5582,
Université Joseph Fourier, B.P.74, 38402 Saint-Martin d'Hères cedex, France
and ESPE Université de Lyon, France
marcel.morales@ujf-grenoble.fr

Nguyen Thi Dung
Thai Nguyen University of Agriculture and Forestry,
Thai Nguyen, Vietnam

Abstract. [1]

Let consider n natural numbers $a_1, \ldots, a_n$. Set $A = K[t^{a_1}, \ldots, t^{a_n}] = K[x_1, \ldots, x_n]/I$. Our aim is to describe explicitly:

1. The Gröbner basis of I for the reverse lexicographic order to $x_n, \ldots, x_1$, without using Buchberger's algorithm.
2. $\text{in}(I)$ for the reverse lexicographic order to $x_n, \ldots, x_1$.
3. A as a $K[t^{a_1}]$-module.
4. The Apéry set and the Frobenius number.

The implementation of this algorithm "frobenius-number-mm" can be downloaded in https://www-fourier.ujf-grenoble.fr/ morales/frobenius-number-mm

Introduction

In the sequel we shall use the following notations. Let K be a field, $\mathcal{A}$ be a set of n natural numbers $\mathcal{A} = \{a_1, \ldots, a_n\} \subset \mathbb{N}$. S the numerical semigroup generated by $a_1, \ldots, a_n$,

[1] version of august 30 2015

that is $S = \{k_1a_1 + \dots k_na_n | k_i \in \mathbb{N}\}$. We consider the one-dimensional *toric affine ring* $A = K[t^{a_1}, \dots, t^{a_n}] \subset K[t]$, that is $A = K[t^k | k \in S] := K[S]$.
The ring $A = K[t^{a_1}, \dots, t^{a_n}] \subset K[t]$ has a presentation as a quotient of the polynomial ring $K[x_1, \dots, x_n]$, as follows:
Let $\varphi : K[x_1, \dots, x_n] \to K[t^{a_1}, \dots, t^{a_n}]$ defined by

$$\begin{array}{ccc} x_1 & \mapsto & t^{a_1} \\ & \vdots & \\ x_n & \mapsto & t^{a_n} \end{array}$$

Let $I(S)$ be the kernel of φ, that is the ideal ideal formed by all polynomials of $K[x_1, \dots, x_n]$ such that $P(t^{a_1}, \dots, t^{a_n}) = 0$.

The ideal $I(S)$ has a system of generators formed by binomials which are differences of two monomials with coefficient 1. Note that if we graded the polynomial ring $K[x_1, \dots, x_n]$ by setting $\deg(x_i) = a_i$, the morphism φ is homogeneous, and the ideal $I(S)$ is homogeneous.

The following theorem is well known, we give here a short proof for the commodity of the reader.

Theorem 0.1. *Suppose that $a_1, \dots, a_n$ are relatively prime numbers then any large integer belongs to S.*

Proof. Suppose that $n = 2$, By Bézout'theorem there exist relative integer numbers s_1, s_2 such that $s_1a_1 + s_2a_2 = 1$. We can assume that $s_1 > 0, s_2 < 0$. Let $k > 0$ big enough we can write $k = qa_2 + r$ with $0 \leq r < a_2$, which implies $k = qa_2 + r(s_1a_1 + s_2a_2) = rs_1a_1 + (q + rs_2)a_2$. Since k is large enough $(q + rs_2) > 0$, hence $k \in S$.

A similar argument works for $n > 2$. □

Definition 0.2. Suppose that $a_1, \dots, a_n$ are relatively prime numbers, the biggest integer number in $\mathbb{N} \setminus S$ is called the Frobenius number, we denote it by $g(S)$. More generally if $\gcd(a_1, \dots, a_n) = \lambda$ then the biggest integer in $\lambda\mathbb{N} \setminus S$ is called the Frobenius number, we denote it by $g(S)$.

Suppose that $\gcd(a_1, \dots, a_n) = \lambda$, let $\widetilde{S}$ be the semigroup generated by $\frac{a_1}{\lambda}, \dots, \frac{a_n}{\lambda}$. We have that $g(S) = \lambda g(\widetilde{S})$. The problem of computing the Frobenius number is open since the end of 19th Century, for $n = 2$ there is a formula (see section 1), for $n = 3$ a formula using Euclide's algorithm for gcd was given in [8]. In 1987, in [6] the first author translate for the first time the Frobenius problem into an algebraic setting, showing that the Frobenius number is the degree of the Hilbert-Poincaré series written as a rational fraction, moreover By using [8], in the case $n = 3$ the Hilbert-Poincaré series is completely described by an algorithm using only Euclide's algorithm for gcd, that is of complexity $\ln(a)$. An

implementation in Pascal was done by the first author to compute a system of generators of the affine monomial curve $K[t^a, t^b, t^c]$ and its projective closure, which computed the Frobenius number for three natural numbers. In recent works [3] and [9], the computation of Frobenius number, is related to the computation of the Hilbert-Poincaré series. More precisely, in [9] the author deduces the Frobenius number from a Gröbner basis of the ideal $I(S)$. We recall that the computation of a Gröbner basis is double exponential complexity by using the Buchberger algorithm.

In this paper we study the Frobenius problem from algebraic point of view, this allows us to give a conceptual frame to our algorithm. Our algorithm determines completely the semigrup S and solve the membership problem, that is to decide if an integer number belong to S. We develop a stand alone algorithm which computes a Gröbner basis of the ideal $I(S)$, they are extension of the previous work and algorithm by the first author in [6], [7]. For fixed n the algorithm presented here seems to be polynomial in a, it is implemented and can be downloaded in https://www-fourier.ujf-grenoble.fr/ morales/. Note that because of the limitation of the Compiler for the moment the software works only for numbers less than 1000, but an implementation in Mathematica should allow to compute with any number of digits.

In the first section we introduce the Apéry set and we prove some known results.

In the second section we present the connection between Hilbert-Poincaré series and the Frobenius number. This connection was established by the first author for the first time in [6].

In the third section we introduce Noether normalization and we prove the connection between Apéry sets and Noether normalization.

In the last section we develop our algorithm.

In our work in preparation, we will extend the above algorithm to compute Gröbner basis of any simplicial monomial ideal.

1 Frobenius number, Apéry set

Definition 1.1. Suppose that a_1 is the smallest among $a_1, \ldots, a_n$. The Apéry set $\mathrm{Ap}(S, a_1)$ of the semigroup S with respect to a_1 is the set $\mathrm{Ap}(S, a_1) := \{s \in S | s - a_1 \notin S\}$.

Remark 1.2. The definition of Apéry set makes sense even if the numbers $a_1, \ldots, a_n$ are not relatively prime numbers. Suppose that $\gcd(a_1, \ldots, a_n) = \lambda$, let $\widetilde{S}$ be the semigroup generated by $\frac{a_1}{\lambda}, \ldots, \frac{a_n}{\lambda}$. We have that $\mathrm{Ap}(S, a_1)$ is obtained from $\mathrm{Ap}(\widetilde{S}, \frac{a_1}{\lambda})$ by multiplication by λ.

Theorem 1.3. *(Apéry [1])Suppose that $a_1, \ldots, a_n$ are natural numbers such that* $\gcd(a_1, \ldots, a_n) = \lambda$.

1. $\mathrm{Ap}(S, a_1) := \{\lambda w_0, \ldots, \lambda w_{\frac{a_1}{\lambda}-1}\}$, *where* w_i *is the smallest element is* $\widetilde{S}$ *congruent to* i *mod* $\frac{a_1}{\lambda}$.

2. $g(S) = \max\{s - a_1 | s \in \mathrm{Ap}(S, a_1)\}$.

Proof. 1. We can assume that $a_1, \ldots, a_n$ are relatively prime numbers.
First we prove that for all $i = 0, \ldots, a_1 - 1$, w_i belongs to $\mathrm{Ap}(S, a_1)$. Suppose that it is not true, that is $w_i - a_1 \in S$ for some $i = 0, \ldots, a_1 - 1$. It follows that $w_i - a_1 < w_i$ and both $w_i - a_1, w_i \in S$ are congruent to i mod a_1. This is a contradiction with the definition of w_i. As a consequence $\mathrm{Ap}(S, a_1)$ has at least a_1 elements in order to prove the claim it will be enough to show that $\mathrm{Ap}(S, a_1)$ has exactly a_1 elements. Suppose that $\mathrm{card}(\mathrm{Ap}(S, a_1)) > a_1$, then there exists two elements $s_1 < s_2$ in $\mathrm{Ap}(S, a_1)$ such that both $s_1 < s_2$ are congruent to i mod a_1 for some $i = 0, \ldots, a_1 - 1$, that is $s_2 = s_1 + ka_1$ with $k > 0$ a natural integer, hence $s_2 \notin \mathrm{Ap}(S, a_1)$, a contradiction.

2. Let $h \in \mathbb{N}$ such that $h > \max\{s - a_1 | s \in \mathrm{Ap}(S, a_1)\}$, since h is congruent to i mod a_1 for some $i = 0, \ldots, a_1 - 1$, we can write $h = w_i + \alpha a_1$, with $\alpha \in \mathbb{Z}$, hence $h = (w_i - a_1) + (\alpha + 1)a_1$, since $h > (w_i - a_1)$ we have $(\alpha + 1) > 0$, hence $\alpha \geq 0$, which implies that $h \in S$.

□

Corollary 1.4. *Let* $n = 2$ *suppose that* a_1, a_2 *are relatively prime numbers then* $g(S) = (a_1 - 1)(a_2 - 1) - 1$.

Proof. We give a combinatorial proof using Apéry sets. Since a_1, a_2 are relatively prime numbers, we have

$$\mathrm{Ap}(S, a_1) := \{0, a_2, \ldots, (a_1 - 1)a_2\},$$

hence $g(S) = (a_1 - 1)(a_2) - a_1 = (a_1 - 1)(a_2 - 1) - 1$

□

For $n = 2$, we will give an algebraic proof later.

Corollary 1.5. *For* $i = 0, \ldots, a_1 - 1$ *let* $S_i = \{s \in S | s \equiv i \bmod a_1\}$. *Then* S *is the disjoint union of* $S_0, \ldots S_{a_1 - 1}$.

2 Frobenius number and Hilbert-Poincaré series

Let $R := K[x_1, \ldots, x_n]$ be the polynomial ring graded by the weights $\deg x_1 = a_1, \ldots, \deg x_n = a_n$, and $I \subset K[x_1, \ldots, x_n]$ be a graded ideal. Let $B = R/I$, the Hilbert-function of B is defined by $H_B(l) = \dim_K B_l$, for all $l \in \mathbb{Z}$, and the Hilbert-Poincaré series of B:

$$P_B(u) = \sum_{l \in \mathbb{Z}} H_B(l) u^l.$$

We recall the following Theorem from [6]

Theorem 2.1. *Let $R := K[x_1, \ldots, x_n]$ be the polynomial ring graded by the weights $\deg x_1 = a_1, \ldots, \deg x_n = a_n$, $I \subset K[x_1, \ldots, x_n]$ be a graded ideal and $B := R/I$. Then*

1. *The Hilbert-Poincaré series of B is a rational function:*

$$P_B(u) = \frac{Q_B(u)}{(1-u^{a_1})(1-u^{a_2})\ldots(1-u^{a_n})} \quad ,$$

   where $Q_B(u)$ is a polynomial on u.

2. *There exists h polynomials with integer coefficients $\Phi_{H_B,0}(l), \ldots, \Phi_{H_B,h}(l)$ such that $H_B(lh+i) = \Phi_{H_B,i}(l)$ for $0 \leq i \leq h-1$ and l large enough. We recall that the index of regularity of the Hilbert function is the biggest integer l such that $H_B(l) \neq \Phi_{H_B,i}(l)$, for any i.*

3. *The index of regularity of the Hilbert function equals the degree of the rational fraction defining the Poincaré series.*

Corollary 2.2. *[5] Let S be the semigroup generated by $a_1, \ldots, a_n$, and $A = K[t^{a_1}, \ldots, t^{a_n}] \subset K[t]$. The Frobenius number $g(S)$ coincides with the degree of the rational fraction defining the Poincaré series $P_A(u)$ by the theorem 2.1.*

Proof. The Hilbert function of A is given by

$$H_A(l) = \begin{cases} 1 & \text{if } l \in S \\ 0 & \text{if } l \notin S. \end{cases}$$

In particular if $a_1, \ldots, a_n$ are relatively prime, $H_A(l) = 1$ for l large enough, and the Frobenius number coincides with the index of regularity of the Hilbert function $H_A(l)$, so it is the degree of the rational fraction defining the Poincaré series $P_A(u)$. □

3 Gröbner basis

Let $a_1, \ldots, a_n$ be natural numbers, $\lambda = \gcd(a_1, \ldots, a_n)$. We denote by S (resp. $\widetilde{S}$) the semigroup generated by $a_1, \ldots, a_n$ (resp. by $a_1/\lambda, \ldots, a_n/\lambda$). Note that the semigroups rings $K[S], K[\widetilde{S}]$ are isomorphic.

Let $R := K[x_1, \ldots, x_n]$ be the polynomial ring graded by the weights $\deg x_1 = a_1, \ldots, \deg x_n = a_n$. We consider $\prec_{degrevlex}$ the degree reverse lexicographical order with $x_n, \ldots, x_1$. The first statement of the following theorem is an extension to the quasi-homogeneous case of [4].

Theorem 3.1. *Let $A := K[t^{a_1}, \ldots, t^{a_n}] \simeq R/I(S)$.*

1. *The polynomial ring $K[x_1] \subset A$ is a Noether normalization. Moreover let $G(S)$ be a Gröbner basis for $\prec_{revlex}$ and $in(I(S))$ be the initial ideal then*

$$A \simeq \oplus_{x_2^{k_2}\ldots x_n^{k_n} \notin in(I(S))} K[t^{a_1}][t^{k_2a_2+\ldots+k_na_n}].$$

2. *The Hilbert-Poincaré series is given by:*

$$P_A(t) = \frac{\sum_{x_2^{k_2}\ldots x_n^{k_n} \notin in(I(S))} t^{k_2a_2+\ldots+k_na_n}}{1-t^{a_1}}$$

3. *The Frobenius number $g(\widetilde{S}) = \frac{\max\{k_2a_2+\ldots+k_na_n | x_2^{k_2}\ldots x_n^{k_n} \notin in(I(S))\}-a_1}{\lambda}$.*

Proof. 1. We have that for any $i = 2, \ldots, n$, $(t^{a_i})^{a_1} - (t^{a_1})^{a_i} = 0$, so $K[t^{a_1}, \ldots, t^{a_n}]$ is integral over $K[t^{a_1}]$, both rings have dimension one so $K[t^{a_1}] \subset K[t^{a_1}, \ldots, t^{a_n}]$ is a Noether normalization, also both rings are Cohen-Macaulay. By the Auslander-Buschsbaum formula we get that $K[t^{a_1}, \ldots, t^{a_n}]$ is a free $K[t^{a_1}]$-module. This is the same to say that $R/I(S)$ is a free $K[x_1]$-module. Since $R/I(S)$ is a graded $K[x_1]$-module, we can use Nakayama's lemma, hence any $K-$basis of $R/(I(S), x_1)$ gives us a basis of $R/I(S)$ as a free $K[x_1]$-module. Let $G(S)$ be a Gröbner basis for $\prec_{revlex}$ and $in(I(S))$ be the initial ideal, by definition of $\prec_{degrevlex}$, x_1 does not divides any of the elements in $in(I(S))$. On the other hand Macaulay's theorem [2][Theorem 15.3]says us that the set of monomials not in $in(I(S))$ is a basis of $R/I(S)$ as a free $K[x_1]$-module.

2. It is clear that the Hilbert-Poincaré series of $K[t^{a_1}]$ is $\frac{1}{1-t^{a_1}}$, the Hilbert-Poincaré series is an additive function, hence we have the formula for the Hilbert-Poincaré series of A.

3. By 2.1 The Frobenius number of S is the degree of the Hilbert-Poincaré series of A. □

We have the following consequence which will be important for our algorithm:

Corollary 3.2. *We have that*

1. $\mathrm{Ap}(S, a_1) = \{k_2a_2 + \ldots + k_na_n | x_2^{k_2} \ldots x_n^{k_n} \notin in(I(S))\}$. *In particular*

$$\mathrm{card}\{x_2^{k_2} \ldots x_n^{k_n} \notin in(I(S))\} = \frac{a_1}{\gcd(a_1, \ldots, a_n)}.$$

2. *Let $s \in \mathrm{Ap}(S, a_1)$, such that $s = k_2a_2 + \ldots + k_na_n$ and $x_2^{k_2} \ldots x_n^{k_n} \notin in(I(S))$. Suppose that $s = l_2a_2 + \ldots + l_na_n$ for some natural numbers $l_2, \ldots, l_n$, then $x_2^{k_2} \ldots x_n^{k_n} \prec_{revlex} x_2^{l_2} \ldots x_n^{l_n}$.*

Proof. We can assume that $\gcd(a_1, \ldots, a_n) = 1$.

1. By the above theorem $K[t^{a_1}, \ldots, t^{a_n}] \simeq \oplus_{s_i \in H} K[t^{a_1}][t^{s_i}]$ where $H = \{k_2a_2 + \ldots + k_na_n | x_2^{k_2} \ldots x_n^{k_n} \notin in(I(S))\}$, now we prove that $H = \mathrm{Ap}(S, a_1)$. Let $s \in H$ suppose that $s \notin \mathrm{Ap}(S, a_1)$, hence $s - a_1 \in S$, by the above decomposition there exists unique $s_i \in H, l \in \mathbb{N}$ such that $s - a_1 = s_i + la_1$ that is $s = s_i + (l+1)a_1$ a contradiction to the direct sum decomposition. Reciprocally, let $s \in \mathrm{Ap}(S, a_1)$, then there exists unique $s_i \in H, l \in \mathbb{N}$ such that $s = s_i + la_1$, if $l > 0$ then $s - a_1 \in S$ a contradiction , hence $s = s_i \in H$.

2. If $s = l_2a_2 + \ldots + l_na_n$ with $(k_1, \ldots, k_n) \neq (l_1, \ldots, l_n)$ and $x_2^{l_2} \ldots x_n^{l_n} \prec_{revlex} x_2^{k_2} \ldots x_n^{k_n}$ then $x_2^{k_2} \ldots x_n^{k_n} \in in(I(S))$, a contradiction.

□

Example 3.3. Let $n = 2$, and a_1, a_2 be natural numbers, $\lambda = gcd(a_1, a_2)$, we have that $K[t^{a_1}, t^{a_2}] \simeq K[x_1, x_2]/(x_2^{a_1/\lambda} - x_1^{a_2/\lambda})$ it is clear that that $x_2^{a_1/\lambda} - x_1^{a_2/\lambda}$ is a Gröbner basis of the ideal $(x_2^{a_1/\lambda} - x_1^{a_2/\lambda})$ for $\prec_{revlex}$. We have $in(x_2^{a_1/\lambda} - x_1^{a_2/\lambda}) = (x_2^{a_1/\lambda})$, hence $K[t^{a_1}, t^{a_2}] =\simeq \oplus_{k=0}^{a_1/\lambda - 1} K[t^{a_1}][t^{ka_2}]$, the Poincaré series is given by: $P_A(t) = \dfrac{\sum_{k=0}^{a_1/\lambda - 1} t^{ka_2}}{1 - t^{a_1}}$. if a_1, a_2 are coprime then the Frobenius number is $(a_1 - 1)a_2 - a_1 = (a_1 - 1)(a_2 - 1) - 1$.

4 Frobenius number, Hilbert-Poincaré series, the case $n = 3$

This section is a short version of [6] and [7].

Let consider three natural numbers a, b, c and S be the semigroup generated by a, b, c. First, remark that any solution $\alpha := (u, v, w)$ of the Diophantine equation $ua + vb + wc = 0$ gives rise to a binomial in the ideal $I(S)$ in the following way:
we write the vector $\alpha = \alpha_+ - \alpha_-$, where the components of both α_+, α_- are nonnegative then $\underline{\mathbf{x}}^{\alpha_+} - \underline{\mathbf{x}}^{\alpha_-} \in I(S)$, where $\underline{\mathbf{x}}^{\alpha_+} = x_1^{\alpha_{+1}} x_2^{\alpha_{+2}} x_3^{\alpha_{+3}}$. Reciprocally if $\underline{\mathbf{x}}^{\alpha} - \underline{\mathbf{x}}^{\beta} \in I(S)$ and $\underline{\mathbf{x}}^{\alpha}, \underline{\mathbf{x}}^{\beta}$ have not common factors then $(u, v, w) := \alpha - \beta$ is a solution of the equation $ua + vb + wc = 0$.
Second, it is clear that find solutions (u, v, w) of the Diophantine equation $ua + vb + wc = 0$ is equivalent to find solutions (s, p, r) of the Diophantine equation $sb - pc = ra$.
Let s_0 be the smallest natural number such that $(s_0, 0, r_0)$ is solution of the equation $sb - pc = ra$. We set $p_0 = 0$.
Let p_1 be the smallest natural number such that (s_1, p_1, r_1) is solution of the equation $sb - pc = ra$, with $0 \leq s_1 < s_0$. Note that $s_0 = \frac{a}{\gcd(a,b)}$ and $p_1 = \frac{\gcd(a,b)}{\gcd(a,b,c)}$. The numbers s_1 can be got from the extended Euclide's algorithm for the computation of the greatest common divisor of a, b.

Let consider the Euclides' algorithm with negative rest:

$$\begin{cases} s_0 &= q_2 s_1 - s_2 \\ s_1 &= q_3 s_2 - s_3 \\ \dots &= \dots \\ s_{m-1} &= q_{m+1} s_m \\ s_{m+1} &= 0 \end{cases}$$

$q_i \geq 2$, $s_i \geq 0 \ \ \forall i$.

Let define the sequences: p_i, r_i $(0 \leq i \leq m+1)$, by:

$$p_{i+1} = p_i q_{i+1} - p_{i-1} \ , r_{i+1} = r_i q_{i+1} - r_{i-1} \ , (1 \leq i \leq m).$$

Note that from [7] we have for $i = 0, \dots, m$ that $s_i p_{i+1} - s_{i+1} p_i = s_0 p_1 = \frac{a}{\gcd(a,b,c)}$. Let μ the unique integer such that $r_\mu > 0 \geq r_{\mu+1}$.

Theorem 4.1. *([5], [6] and [7]) The set*

$$x_2^{s_\mu} - x_1^{r_\mu} x_3^{p_\mu}, x_3^{p_{\mu+1}} - x_1^{-r_{\mu+1}} x_2^{s_{\mu+1}}, x_2^{s_\mu - s_{\mu+1}} x_3^{p_{\mu+1} - p_\mu} - x_1^{r_\mu - r_{\mu+1}}$$

is a Gröbner basis of $I(S)$ for $\prec_{revlex}$ with x_3, x_2, x_1. In particular $in(I(S) = (x_2^{s_\mu}, x_3^{p_{\mu+1}}, x_2^{s_\mu - s_{\mu+1}} x_3^{p_{\mu+1}})$, and

$$\mathbb{N}^2 \setminus exp(in(I(S)) = \{(k,l) \in \mathbb{N}^2 | 0 \leq k < s_\mu - s_{\mu+1}, 0 \leq l < p_{\mu+1}\} \cup$$
$$\{(k,l) \in \mathbb{N}^2 | s_\mu - s_{\mu+1} \leq k < s_\mu, 0 \leq l < p_{\mu+1} - p_\mu\}.$$

$$K[t^a, t^b, t^c] \simeq \oplus_{(k,l) \in \mathbb{N}^2 \setminus exp(in(I(S))} K[t^a][t^{kb+lc}].$$

In particular the Poincaré series is given by:

$$P_A(t) = \frac{\sum_{(k,l) \in \mathbb{N}^2 \setminus exp(in(I(S))} t^{kb+lc}}{1 - t^a}$$

and if the numbers a, b, c are relatively prime the Frobenius number is

$$g(S) = \max \{kb + lc | (k,l) \in \mathbb{N}^2 \setminus exp(in(I(S))\} - a_1.$$

Proof. we can give a new and shorter proof than the one given in the general case in [7]. We can assume that the numbers a, b, c are relatively prime. Let consider the three elements of $I(S)$: $x_2^{s_\mu} - x_1^{r_\mu} x_3^{p_\mu}, x_3^{p_{\mu+1}} - x_1^{-r_{\mu+1}} x_2^{s_{\mu+1}}, x_2^{s_\mu - s_{\mu+1}} x_3^{p_{\mu+1} - p_\mu} - x_1^{r_\mu - r_{\mu+1}}$. It then follows that $J := (x_2^{s_\mu}, x_3^{p_{\mu+1}}, x_2^{s_\mu - s_{\mu+1}} x_3^{p_{\mu+1}}) \subset in(I(S)$. Now we count the numbers of monomial not in J,

$$\text{card}(\mathbb{N}^2 \setminus exp(J)) = (s_\mu - s_{\mu+1}) p_{\mu+1} + s_{\mu+1}(p_{\mu+1} - p_\mu) = s_\mu p_{\mu+1} - s_{\mu+1} p_\mu = a.$$

On the other hand by Corollary 3.2, $\text{card}(\mathbb{N}^2 \setminus exp(in(I(S))) = a$ this implies $in(I(S) = J$, hence the set $x_2^{s_\mu} - x_1^{r_\mu} x_3^{p_\mu}, x_3^{p_{\mu+1}} - x_1^{-r_{\mu+1}} x_2^{s_{\mu+1}}, x_2^{s_\mu - s_{\mu+1}} x_3^{p_{\mu+1} - p_\mu} - x_1^{r_\mu - r_{\mu+1}}$ is a Gröbner basis of $I(S)$ for $\prec_{revlex}$ with x_3, x_2, x_1. The other claims follows from the Theorem 3.1 □

5 Algorithm for the case $n \geq 4$

For $n = 3$, we have seen that the algorithm use only Euclide's algorithm. Let $n \geq 4$. Let $a_1, \ldots, a_n$ be relatively prime natural numbers, S the semigroup generated by $a_1, \ldots, a_n$. Let $R := K[x_1, \ldots, x_n]$ be the polynomial ring graded by the weights $\deg x_1 = a_1, \ldots, \deg x_n = a_n$. We consider $\prec_{degrevlex}$ the degree reverse lexicographical order with $x_n, \ldots, x_1$, $A = K[t^{a_1}, \ldots, t^{a_n}] \simeq R/I(S)$.

The algorithm is inductive on n.

Algorithm 5.1. Frobenius MM-DD:

Input: $a_1, \ldots, a_n$

Ouput: The Grobner basis of $I(S)$, the Noether decomposition, the Apéry set of S with respect to a_1. The Frobenius number of S.

Begin

1. For any subset $T \subset \{x_1, \ldots, x_n\}$ such that $x_1 \in T$ and $3 \leq \text{card}(T) \leq n-1$ compute the Noether decomposition as in the Theorem 3.1, where we assume that the ring $K[T]$ is provided with the induced order of $\prec_{revlex}$.

2. For $i = 2, \ldots, n$ let S_i the semigroup generated by $\mathcal{A} \setminus \{a_i\}$. Let G_i be a Gröbner basis for the semigroup ring $K[S_i]$ as a quotient of $K[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$. For any two distinct integers $i, k \in \{2, \ldots, n\}$, let $g_{k,i}$ be the small integer such that $x_k^{g_{k,i}} \in in(G_i)$. Let $g_k = \min\{g_{k,i} | i = 2, \ldots, n, i \neq k\}$. In order to look for monomials not in $in(I(S)$ we need only to check for monomials $x_2^{k_2} \ldots x_n^{k_n}$ with $k_i < g_i$. Moreover by 3.2 we have $\text{card}\{x_2^{k_2} \ldots x_n^{k_n} \notin in(I(S))\} = a_1$.

3. For $i = 2, \ldots, n$ let S_i the semigroup generated by $\mathcal{A} \setminus \{a_i\}$. Let G_i be a Gröbner basis for the semigroup ring $K[S_i]$ as a quotient of $K[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$ for the induced order of $\prec_{revlex}$. For any two distinct integers $i, k \in \{2, \ldots, n\}$, let $g_{k,i}$ be the small integer such that $x_k^{g_{k,i}} \in in(G_i)$, and $g_k = \max\{g_{k,i} | i \neq k\}$

4. For $i = 2$ to $i = n$, and for $s = 1$ to $s = g_i$ check if the monomial $x_i^s \in in(I(S)$. Let $\overline{g}_i$ the small integer s such that $x_i^s \in in(I(S)$.

5. For $s = 0$ to $s = \overline{g}_2 + \ldots + \overline{g}_n - (n-1)$ and any monomial $M := x_2^{k_2} \ldots x_n^{k_n}$, such that $k_i < \overline{g}_i$ for all $i = 2, \ldots, n$, check if the monomial $M \in in(I(S)$.

6. In both cases, by a simple test we can assume that there is not a proper monomial $M' \in in(I(S)$ dividing M.

7. The algorithm has a second stop since the number of monomials not in $in(I(S)$ is exactly a_1.

End (of the algorithm).

Let precise the consistence of the steps 4 and 5, since they are similar we only prove the step 5:

Let $supp(M)$ be the set of integers i such that x_i divides M, and $\overline{supp(M)} := \{1, \ldots, n\} \setminus supp(M)$. Let $S_{\overline{supp(M)}}$ be the semigroup generated by all the numbers a_i such that $a_i \in \overline{supp(M)}$. $M \in in(I(S)$ if and only if there is a binomial $x_2^{k_2} \ldots x_n^{k_n} - \Pi_{i \in \overline{supp(M)}} x_i^{l_i} \in I(S)$ such that $\Pi_{i \in \overline{supp(M)}} x_i^{l_i} \prec_{revlex} x_2^{k_2} \ldots x_n^{k_n}$. This is equivalent to show that there exists $\sum_{i \in \overline{supp(M)}} l_i a_i \in S_{\overline{supp(M)}}$ such that $k_2 a_2 + \ldots + k_n a_n = \sum_{i \in \overline{supp(M)}} l_i a_i$ and $\Pi_{i \in \overline{supp(M)}} x_i^{l_i} \prec_{revlex} x_2^{k_2} \ldots x_n^{k_n}$.

Let $\lambda_M = \gcd\{a_i | i \in \overline{supp(M)}$, and $\overline{a}_1 = \frac{a_1}{\lambda_M}$. By the theorem 3.1 and its corollary 3.2 we have $K[S_{\overline{supp(M)}}] \simeq \oplus_{i=0}^{\overline{a}_1 - 1} K[t^{a_1}][t^{w_i}]$, where $w_i \in \mathrm{Ap}(\mathrm{S}_{\overline{\mathrm{supp(M)}}}, \mathrm{a}_1), w_i \equiv \lambda_M i \bmod a_1$.

Let $\rho = k_2 a_2 + \ldots + k_n a_n \bmod a_1$. If $\rho \notin \lambda_M \mathbb{N}$ then $x_2^{k_2} \ldots x_n^{k_n} \notin in(I(S))$. Otherwise $k_2 a_2 + \ldots + k_n a_n = w_{\frac{\rho}{\lambda_M}} + \alpha a_1$, with $\alpha \in \mathbb{Z}$. Let $w_{\frac{\rho}{\lambda_M}} = \sum_{i \in \overline{supp(M)}} l_i a_i$ such that $\Pi_{i \in \overline{supp(M)}} x_i^{l_i} \notin in(I(S_{\overline{supp(M)}}))$. We have three cases:

1. If $\alpha < 0$ then $x_2^{k_2} \ldots x_n^{k_n} \notin in(I(S))$.
2. If $\alpha > 0$ then the binomial $x_2^{k_2} \ldots x_n^{k_n} - x_1^{\alpha} \Pi_{i \in \overline{supp(M)}} x_i^{l_i} \in I(S)$ and $\Pi_{i \in \overline{supp(M)}} x_i^{l_i} \prec_{revlex} x_2^{k_2} \ldots x_n^{k_n}$, so $x_2^{k_2} \ldots x_n^{k_n} \in in(I(S)$.
3. If $\alpha = 0$, let j the smallest number such that $l_j > 0$,
   (a) if $j < i$ for any $i \in supp(M)$ then as above $x_2^{k_2} \ldots x_n^{k_n} - \Pi_{i \in \overline{supp(M)}} x_i^{l_i} \in I(S)$ and $\Pi_{i \in \overline{supp(M)}} x_i^{l_i} \prec_{revlex} x_2^{k_2} \ldots x_n^{k_n}$, so $x_2^{k_2} \ldots x_n^{k_n} \in in(I(S)$.
   (b) If $j > i$ for some $i \in supp(M)$, then we have $x_2^{k_2} \ldots x_n^{k_n} \prec_{revlex} \Pi_{i \in \overline{supp(M)}} x_i^{l_i}$. On the other hand if $\sum_{i \in \overline{supp(M)}} l_i a_i = \sum_{i \in \overline{supp(M)}} l'_i a_i$ for some other numbers l'_i we have $\Pi_{i \in \overline{supp(M)}} x_i^{l_i} \prec_{revlex} \Pi_{i \in \overline{supp(M)}} x_i^{l'_i}$ because $\Pi_{i \in \overline{supp(M)}} x_i^{l_i} \notin in(I(S_{\overline{supp(M)}}))$. Hence $x_2^{k_2} \ldots x_n^{k_n} \prec_{revlex} \Pi_{i \in \overline{supp(M)}} x_i^{l'_i}$ for any natural integers $l'_i, i \in \overline{supp(M)}$, such that $k_2 a_2 + \ldots + k_n a_n = \sum_{i \in \overline{supp(M)}} l'_i a_i$, which implies that $x_2^{k_2} \ldots x_n^{k_n} \notin in(I(S)$.

Our algorithm is complete.

Remark 5.2. Since the number of monomials not in $in(I(S)$ is exactly a_1, we will have that $g_{k,i}, g_i, \overline{g}_i$ are strictly bounded above by a_1. Moreover by the same reason $\overline{g}_2 + \ldots + \overline{g}_n - (n-1)$ is strictly bounded above by a_1, hence the number of tests in the step 4 of the algorithm is at most a_1^2 and the number of tests in the step 5 of the algorithm is at most $a_1 \binom{a_1+n-2}{n-1}$.

References

[1] R. Apéry, Sur les branches superlinéaires des courbes algébriques, C.R. Acad. Sci. Paris 222 (1946), 1198-1200.

[2] D. Eisenbud, Commutative algebra with a view toward algebraic geometry. Graduate Texts in Math., vol. 150 (1995), Springer-Verlag, Berlin and New York.

[3] Einstein, David, et al. "Frobenius numbers by lattice point enumeration.." Integers 7.1 (2007)

[4] Monique Lejeune-Jalabert, Effectivité des calculs polynomiaux, Courd de DEA 1984-1985, Institut Fourier, Université de Grenoble I.

[5] Morales Marcel, *Fonctions de Hilbert, genre géométrique d'une singularité quasi-homogène Cohen-Macaulay*. CRAS Paris, t.301, série A n^o 14 **(1985)**.

[6] Morales M.- Syzygies of monomial curves and a linear diophantine problem of Frobenius, Preprint Max Planck Institut für Mathematik (Bonn-RFA) (1987

[7] M. Morales, Équations des variétés monomiales en codimension deux, J. Algebra **175** (1995) 1082-1095.

[8] J. Rodseth, On a linear Diophantine problem of Frobenius, J. reine angew. Math., 301(1978) 171-178

[9] B.H. Roune, Solving Thousand Digit Frobenius Problems Using Grobner Bases, Journal of Symbolic Computation volume 43(1) 2008,1-7.