



UNIVERSIDAD DE GRANADA

Programa de Doctorado: Física y Matemáticas (FisyMat)

TESIS DOCTORAL

---

# **Linear Diophantine equations and applications**

---

Alfredo Sánchez-Roselly Navarro

Editorial: Universidad de Granada. Tesis Doctorales

Autor: Alfredo Sánchez Roselly Navarro

ISBN: 978-84-9125-195-8

URI: <http://hdl.handle.net/10481/40613>

El doctorando Alfredo Sánchez-Roselly Navarro y los directores de la tesis Pedro A. García Sánchez y Alberto Vigneron Tenorio. Garantizamos, al firmar esta tesis doctoral, que el trabajo ha sido realizado por el doctorando bajo la dirección de los directores de la tesis y hasta donde nuestro conocimiento alcanza, en la realización del trabajo, se han respetado los derechos de otros autores a ser citados, cuando se han utilizado sus resultados o publicaciones.

Granada, 11 de mayo de 2015

Directores de la Tesis:

Fdo: Pedro A. García Sánchez

Fdo: Alberto Vigneron Tenorio

Doctorando:

Fdo: Alfredo Sánchez-R. Navarro



Quiero expresar mi agradecimiento a Pedro A. García Sánchez y Alberto Vigneron Tenorio. Este trabajo ha sido posible gracias a su asistencia y atención, así como a su calidad y actitud docente, indispensable y motivadora.



## Abstract

The present manuscript covers the following subjects, all related to the study of non-negative integer solutions of linear systems of Diophantine equations.

- The justification and implementation of the software `DPSolve` to compute the nonnegative integer solutions of systems of linear Diophantine equations, which improves a previous procedure based on Dickson's lemma.
- The introduction and study of affine convex body semigroups, and in particular the calculation of their minimal generating sets (whenever finitely generated) and a procedure to determine when they are Buchsbaum, providing in this way plenty of examples of semigroups with this property. These methods have been implemented in Mathematica.
- The study of some factorization invariants in half-factorial monoids and the introduction of a new invariant called the homogeneous catenary degree. Both theoretical and algorithmic results are provided; implementations have been performed in GAP ([16]).
- In order to deal with the problems in the preceding paragraph we have implemented and published the `4ti2gap` package, which is a GAP wrapper for `4ti2` ([30]).

## Resumen

El presente trabajo abarca las siguientes temáticas, relacionadas con el estudio de las soluciones positivas de sistemas de ecuaciones Diofánticas lineales.

- La justificación e implementación del software `DPSolve` para el cálculo de las soluciones enteras positivas de sistemas de ecuaciones Diofánticas lineales, que mejora un algoritmo previo basado en el lema de Dickson.
- La introducción y estudio de los semigrupos afines de cuerpo convexo, y en particular el cálculo de su conjunto minimal de generadores (cuando es finitamente generado) y de un procedimiento para determinar cuando esos semigrupos son Buchsbaum, lo que permite obtener ejemplos de semigrupos con esta propiedad. Los algoritmos relacionados se han implementado en Mathematica.
- El estudio de algunos invariantes de factorización en monoides de factorización media y la introducción de un nuevo invariante llamado grado de catenaridad homogénea. Se aportan tanto resultados teóricos como algorítmicos; así como implementaciones en GAP ([16]).
- Para el tratamiento computacional de problemas relacionados con lo indicado en el párrafo anterior, se ha desarrollado y publicado el paquete `4ti2gap` para GAP, para disponer de herramientas que aporta `4ti2` mediante sus librerías.





## Contents

Introduction	1
Objectives	3
Methodology	4
Chapter 1. Solving systems of linear Diophantine equations	5
1. Notations and some fundamental concepts	5
2. Linear Diophantine equations	9
3. Computing non-negative integer solutions of linear Diophantine systems	12
Chapter 2. Affine convex body semigroups in $\mathbb{N}^2$	25
1. Preliminary concepts and results	25
2. Finding a system of generators of convex body semigroups	27
3. Affine convex body semigroups and Buchsbaum rings	43
Chapter 3. Factorizations in affine semigroups	55
1. Preliminaries	55
2. Factorizations and linear Diophantine equations	57
3. Length dependent invariants	58
4. Distance dependent invariants	59
5. Binomials, lengths and distances	65
6. Omega primality	66
7. Invariants in half-factorial affine semigroups	68
Results, conclusions and future work	75
Appendix A. CircleSG	77
1. Notes about the implementation	77
Appendix B. PSGIsBuchsbaumQ	81
1. Notes about the implementation	81
Appendix C. 4ti2gap	85
1. Introduction	85
2. Design	85
Appendix D. GAP functions	89
Bibliography	101

List of Symbols	105
Index	107

## Introduction

The resolution of systems of linear Diophantine equations is a well known complex problem with many applications. In this work we are concerned with the computation of the integer non-negative solutions of this kind of systems. Let  $A$  be a matrix with integer entries. The set of nonnegative integer solutions of  $Ax = 0$  is a submonoid,  $M$ , of  $\mathbb{N}^k$ , where  $k$  is the number of unknowns of the system. Minimal nonzero elements of  $M$  with respect to the usual partial ordering can be used to compute every other element of this set; these are usually named the generators of  $M$ . These minimal elements are a Hilbert basis of  $M$ . Computing the non-negative integer solutions of a system of linear Diophantine equations is thus equivalent to the computation of the Hilbert basis (see for instance [40]) for  $M$ .

Knowing if a system of linear Diophantine equations has or not any solution is a NP-complete problem. However a series of significant methods have progressively appeared in the literature offering responses at reasonable times, or in other words, useful when the input is not too unpleasant. In the last decade of the past century appeared the first of them, see for example in [10, 11, 40, 41]. Other more recent methods appeared in this century, such as in [5] and [29] have been used to develop software packages providing computation results at reasonable execution times (see [6] and [30] respectively). What we mean with reasonable times is that for systems of equations with  $k \leq 10$ , a personal computer can be used, by expecting a waiting time of a few minutes (as we have experienced in different examples, but not as a rule of thumb in any case). For larger systems, a supercomputer is indeed necessary to get an output in an acceptable period of time.

With all these considerations in mind, and the opportunity of the state of the art of the computing hardware and software technology available, we decided to face the problem of solving this type of equations systems developing some refinements to the algorithm by Pisón and Vigneron-Tenorio ([39]). This is the fundamental content of the first chapter of the present work, where we will present the component algorithms to be used in order to compute the solutions of a system of linear Diophantine equations using our program `DPSolve`.

One of the refinements in `DPSolve` relies in the following idea. The relations between the columns of  $A$  can be represented by considering the semigroup ideal defined as the kernel of the ring morphism that assigns to each variable in  $\mathbb{k}[x_1, \dots, x_k]$  the value  $X^c$  with  $c$  ranging in the columns of  $A$ . These relations can be obtained by Gröbner basis computations. By [32], this semigroup ideal is generated by binomials,  $\langle X^\alpha - X^\beta \mid A\alpha =$

$A\beta$ ). Besides, from [56] we know how to check for a solution of  $Ax = 0$  (even for non-homogeneous systems) by looking for the existence of certain binomial in a Gröbner basis of the semigroup ideal. We use a suited order for this Gröbner basis computation, in order to feed `DPSolve` with particular solutions. This computation is done by means of the effective software tool `4ti2` (see [30]), doing direct library calls in our code. An additional refinement is in the slicing of the values of possible solutions to check, driven by the progress of the algorithm and the solutions obtained consecutively. At the end part of this chapter, we discuss a brief comparison with programs `hilbert` (a component program included in `4ti2`) and `Normaliz` (see [6]).

The second chapter presents a generalization in two dimensions of proportionally modular numerical semigroups. Proportionally modular numerical semigroups consist in the set of numerators of rational numbers belonging to a given interval  $I = [\alpha, \beta] \subseteq \mathbb{R}_{\geq}$ , with  $\alpha < \beta$ , that is, proportionally modular numerical semigroups are monoids of the form  $\bigcup_{n \in \mathbb{N}} nI \cap \mathbb{N}$ . Equivalently, they are the set of nonnegative integer solutions of the inequality  $ax \bmod b \leq cx$ , with  $a, b, c \in \mathbb{Z}^+$  (see [49]). We introduce affine convex body semigroups defined as  $\mathcal{F} = \bigcup_{n \in \mathbb{N}} nF \cap \mathbb{N}^k$ , with  $F \subseteq \mathbb{R}_{\geq}^k$  a compact convex body. We particularize our study to  $k = 2$ . In general, convex body semigroups are not finitely generated, but under conditions related with the slopes of the extremal rays of the minimal cone containing  $\mathcal{F}$ , it is possible to compute its minimal generating set. Those convex body semigroups that are finitely generated are called affine convex body semigroups, and are characterized when  $F$  is a convex polygon or a circle. The characterization is based on the fact that the intersection of  $F$  and the rays of the pointed cone associated to  $F$  contains rational points. The non-negative integer solutions of a system of linear Diophantine equations can be used to obtain a system of generators of the pointed cone associated to a convex body semigroup (see [43]). This is the approach that we adopted in [17], whose content corresponds to the first sections of the second chapter. However here we have chosen an approach based in [51] that uses Bézout sequences (unimodular decomposition of cones in this setting) with much better results in computation time.

Most of the results in Chapter 2 are tailored for affine convex body semigroups. First we focus on procedures to compute the minimal generating set of affine convex body semigroups. For the case of the circles, the resulting method has been implemented as a Mathematica<sup>1</sup> package, called `CircleSG` (see [19]). In Appendix A we provide a block diagram describing the procedure.

The last sections of Chapter 2 show how to determine whether or not affine circles or convex polygonal semigroups are Buchsbaum. We make use of a characterization of Buchsbaum simplicial affine semigroups, based on the property of being Cohen-Macaulay ([21] and [24]). We also benefit from the fact that membership to these affine convex body

---

<sup>1</sup>Every reference to the term Mathematica in this document, is referred to the set of programs of Wolfram Research, except where it is otherwise stated. Mathematica is a registered trademark of Wolfram Research Inc.

semigroups is easy to accomplish. The test is implemented for affine polygonal convex semigroups in the Mathematica package `PolySGTools` (see [20]), which needs a more involved processing than the circle case. In Appendix B the process is illustrated also with a block diagram.

The non-negative integer solutions of a system of linear Diophantine equations appear in the context of the study of factorizations on affine semigroups: computing the set of factorizations of  $m$  in the affine semigroup  $M$  is equivalent to finding the set of nonnegative integer solutions of the system of linear Diophantine equations  $Ax = m$ , where  $A$  is a matrix whose columns are the generators of  $M$ . Under this perspective, the last chapter reviews invariants related with factorizations of elements in affine semigroups, with special focus on half-factorial monoids. Since in a half-factorial monoid all the lengths of factorizations of an element are the same, invariants such as elasticity, sets of lengths and Delta sets yield no information about how wild are the factorizations in these monoids. To this end a distance between factorizations was introduced in the literature, together with several invariants related to distances (see for example [26]). We will review these and see how they can be computed in the scope of affine semigroups. For the particular case of half-factorial affine semigroups we will show that every possible catenary degree is attained in a Betti element of the monoid (which is far from being true in general). Also we will prove that the tame degree and  $\omega$ -primality coincide for half-factorial monoids. We introduce a new invariant: the homogeneous catenary degree, which is an upper bound for the catenary degree and a lower bound for the monotone catenary degree.

From any affine semigroup  $M$  we define two new affine semigroups:  $M^{\text{eq}}$  and  $M^{\text{hom}}$ . Both monoids are half-factorial, and the catenary degree of the first coincides with the equal catenary degree of  $M$ , while that of the second with the homogeneous catenary degree of  $M$ .

In Appendix C we introduce the GAP package `4ti2gap` ([25]), which is a wrapper designed to give us an affordable way to perform affine computations using the software `4ti2` ([30]). In fact the main motivation to develop this package were the algorithms presented in Chapter 3 that rely on solving systems of linear Diophantine equations or (binomial) Gröbner basis computations. We provide an implementation in GAP of the procedures presented in Chapter 3. The corresponding functions are listed in Appendix D. Thanks to `4ti2gap` we are able to provide the versions for the affine semigroup case that now are integrated in the `numericalsgps` package (see [13]).

## Objectives

The main goals of this work are the following.

- Improve the algorithm by Pisón and Vigneron ([39]) for the computation of the set of nonnegative integer solutions of systems of linear Diophantine equations, and compare its performance with other programs.

- Develop software tools to compute the minimal generating set of affine semigroups defined by a convex body in  $\mathbb{N}^2$ . To this end some previous theoretical results are needed.
- Give procedures to determine whether or not a given affine convex semigroup is Buchsbaum; find families of semigroups with this property, which have ring theoretic interest by their own.
- Introduce a new invariant (homogeneous catenary degree) to better understand the monotone catenary degree, inspired in the projective closure of an affine variety.
- Find alternative characterizations of the equal and homogeneous catenary degree, based on the construction of new half-factorial monoids associated to a given affine semigroup.
- Study properties of the rest of well known invariants in the scope of half-factorial affine semigroups. In particular study the possible values of the catenary degree in these monoids, and the relationship between tame degree and  $\omega$ -primality.
- Improve and make widely accessible the computation of factorization invariants for affine semigroups by means of a package can make use of 4ti2 ([30]) from GAP.

### **Methodology**

This thesis was meant initially to be almost fully computational. However the search of new algorithms and procedures required the study of theoretical properties of the objects we were dealing with (mainly affine semigroups).

From the computational experiments we were able to find clues to determine new properties, and this at the same time fed the results needed to improve our algorithms.

The methodology we used is the following.

- Bound and determine the problems we wanted to study.
- Find the necessary theoretical tools to develop our algorithms.
- From the outputs of this algorithms try to find new ideas and results that eventually will improve our procedures.
- Find new places where our algorithms can be used, and related problems where these apply.
- Take advantage of computer experiments to infer new properties.
- Implement the necessary software tools, and make them publicly available. Interact and discuss with other developers.
- Contrast results and collaborate with other authors.

## CHAPTER 1

# Solving systems of linear Diophantine equations

### 1. Notations and some fundamental concepts

As highlighted in the Introduction, linear systems of Diophantine equations are fundamental in the development of this monograph. We fix in this section the basic notations and definitions used in the rest of the chapters. Also we include an algorithm based on [39].

**1.1. Monoids and semigroups.** A *monoid*  $M$  is a semigroup with identity element. Being a *semigroup* means that it is a set with an inner binary associative operation (we denote it with the sum sign  $+$ ). In this work we only consider commutative monoids and semigroups, though it will not be written explicitly.

A monoid  $M$  is *cancellative* if given any elements  $a, b, c \in M$ ,  $a + b = a + c$  implies  $b = c$ .

If there exists a finite collection of elements  $\{m_1, \dots, m_k\}$  of a monoid (or a semigroup) with which, through linear combinations using naturals, it is possible to generate every element of the monoid  $M$ , then we say that the monoid is finitely generated. We denote this by  $M = \langle m_1, \dots, m_k \rangle$ . If no proper subset of  $\{m_1, \dots, m_k\}$  generates  $M$ , then this set is called a minimal system of generators of  $M$ . Finitely generated cancellative monoids have a unique minimal generating system. We will frequently deal with finitely generated submonoids of  $\mathbb{N}^n$ , which are called *affine semigroups*.

**1.2. Lattices.** Given a set  $S \subseteq \mathbb{R}^n$ , we denote with  $\text{span}(S)$  the linear space spanned by the vectors in  $S$ , that is,  $\text{span}(S) = \{\sum_{i=0}^k \lambda_i s_i \mid \lambda_i \in \mathbb{R}, s_i \in S, k \in \mathbb{N}\}$ .

Recall that  $B \subseteq \mathbb{R}^n$  is a subgroup of  $(\mathbb{R}^n, +)$  if for all  $x, y \in B$ ,  $x - y \in B$ .

Let  $L$  be a linear subspace of  $\mathbb{R}^n$ , a subgroup  $\mathcal{L}$  is called a *lattice* of  $L$ , if  $\text{span}(\mathcal{L}) = L$ . A *basis* for a lattice in  $L$  is a set of linearly independent vectors  $a_1, \dots, a_s \in L$  such that  $\mathcal{L} = \{\mu_1 a_1 + \dots + \mu_s a_s \mid \mu_1, \dots, \mu_s \in \mathbb{Z}\}$ .

**1.3. Monomials and binomials.** Let  $\mathbb{k}$  be a field, and  $\mathbb{k}[x_1, \dots, x_k]$  be the ring of polynomials over the unknowns  $x_1, \dots, x_k$ . A *monomial* is an expression of the form  $x_1^{\alpha_1} \dots x_k^{\alpha_k}$ , where  $\alpha = (\alpha_1, \dots, \alpha_k) \in \mathbb{N}^k$ . We will write for short  $X^\alpha = x_1^{\alpha_1} \dots x_k^{\alpha_k}$ . A *binomial* is the difference of two (monic) monomials,  $X^\alpha - X^\beta$ .

**1.4. Semigroup rings and lattice ideals.** Let  $A$  be a  $n \times k$  matrix with integer entries, and let  $M \subset \mathbb{Z}^n$  be the monoid generated by the columns of  $A$ . We will assume that  $M$  is *reduced*, that is, if  $a + b = 0$  for some  $a, b \in M$ , then  $a = b = 0$ .

Let  $\chi$  be a symbol. Define  $\mathbb{k}[M] = \bigoplus_{m \in M} \mathbb{k}\chi^m$ . This set is a commutative ring with componentwise addition, and with multiplication performed following the rule  $\chi^u \chi^v = \chi^{u+v}$  (together with the distributive law). Let  $\pi : \mathbb{k}[x_1, \dots, x_k] \rightarrow \mathbb{k}[M]$  be the ring morphism determined by  $\pi(x_i) = \chi^{m_i}$ , where  $m_i = (a_{1i}, \dots, a_{ni})^T$  is the  $i$ th column of  $A$ .

The kernel of  $\pi$ ,  $\ker(\pi) = \{f \in \mathbb{k}[x_1, \dots, x_k] \mid \pi(f) = 0\}$  is usually denoted as  $l_M$ , which is an ideal of  $\mathbb{k}[x_1, \dots, x_k]$  (recall that  $I$  is an ideal of a commutative ring  $R$  if it is a subgroup of  $R$  such that  $IR \subset I$ ). It is well known (see [32]) that  $l_M$  is a binomial ideal generated by

$$\langle X^\alpha - X^\beta \mid \pi(X^\alpha) = \pi(X^\beta) \rangle = \langle X^\alpha - X^\beta \mid A\alpha = A\beta \rangle,$$

and every ideal of  $\mathbb{k}[x_1, \dots, x_n]$  is finitely generated by the Hilbert Basis Theorem (see for instance [12, Chapter 2]).

Let  $\mathcal{L}$  be a subgroup of  $\mathbb{Z}^n$ . Define  $l_{\mathcal{L}}$  to be the ideal  $\langle X^\alpha - X^\beta \mid \alpha, \beta \in \mathbb{N}^n, \alpha - \beta \in \mathcal{L} \rangle$ ; the *ideal associated* to  $\mathcal{L}$ . These ideals are known in the literature as lattice ideals. Lemma 9 in [56] states,  $l_M = l_{\ker(A)}$  (recall that  $\ker(A) = \{z \in \mathbb{Z}^n \mid Az = 0\}$ ). The morphism  $\pi$  is surjective, and thus  $\mathbb{k}[x_1, \dots, x_k]/l_M$  is isomorphic to  $\mathbb{k}[M]$ , whence  $l_M$  is a prime ideal, since  $\mathbb{k}[M]$  is a domain.

**1.5. Computing  $l_M$ .** We briefly enumerate some well known methods to compute the semigroup ideal  $l_M$  that rely on Gröbner bases computations (we will introduce this concept and monomial orders in Section 1.6).

**Elimination:** A well known method (see [11], [14]) to obtain the semigroup ideal  $l_M$  is elimination with Gröbner bases. It takes the auxiliary polynomial ring with  $n + 1$  extra coordinates,  $\mathbb{k}[y_1, \dots, y_n, t, x_1, \dots, x_k]$ , and an ideal  $l = \langle y_1 \cdots y_n \cdot t - 1, Y_j^{m_j^+} - Y_j^{m_j^-} x_j \rangle$  for  $j \in \{1, \dots, k\}$ , where we denote

$$m_j^+ = (\max\{m_{1j}, 0\}, \dots, \max\{m_{ij}, 0\}, \dots, \max\{m_{nj}, 0\})$$

and

$$m_j^- = (-\min\{m_{1j}, 0\}, \dots, -\min\{m_{ij}, 0\}, \dots, -\min\{m_{nj}, 0\}),$$

and use the convention  $Y^m = y_1^{m_1} \cdots y_n^{m_n}$  as above. Using an elimination order with  $y_j \geq t \geq x_i$  (for all  $i, j$ ) the Gröbner basis of  $l$ ,  $G$ , is calculated. The intersection  $G \cap \mathbb{k}[X]$  is a generating set  $l_M$ . The computation with this method requires to deal with Gröbner basis on a polynomial ring with  $n + k + 1$  variables. It is considered slow, because for binomial ideals the Gröbner bases computation cost grows exponentially with the number of variables ([35, Theorem 20]).

**Sturmfels:** This is performed as an iterative computation ([54, Chapter 12]). It starts from  $W$ , a lattice basis of  $\ker(A)$ , that is, any independent set of  $\mathbb{Z}$ -solutions of  $Ax = 0$ , which can be obtained in polynomial time using the Hermite normal form of  $A$ . Then the iterations begin with the assignment  $J_0 = \langle Y^{b_i^+} - Y^{b_i^-} \mid b_i \in W \rangle$ . Next for  $i \in \{1, \dots, k\}$ , a reduced Gröbner bases is calculated in order to



obtain  $J_i$  as the set of elements  $g \in \mathbb{k}[Y]$ , such that there exists  $r \in \mathbb{N}$  such that  $y_i^r g \in J_{i-1}$ . Finally, from the reduced Gröbner basis of  $J_k$  a minimal generating set is obtained.

**DiBiase-Urbanke:** Another iterative method which reduces the number of steps with respect the previous one is in [14] and [33]. It transforms some columns of the matrix  $A$  in order to have a row with all positive values, this new matrix is denoted  $A'$ . It is the number of matrix operations to find  $A'$  what sets the number of iterations (that involves Gröbner bases computations) needed to end the algorithm. Before these iterations, from  $A'$  a lattice basis is obtained, which is used as the boot up point to calculate  $\ker(A)$  by successively reversing the previous transformations.

**Hemmecke-Malkin:** It is an approach similar to that of Sturmfels. The starting point is a projection of  $\mathcal{L} = \ker(A)$ . Let  $\sigma \subseteq \{1, \dots, k\}$  and denote  $\mathcal{L}^\sigma = \rho_\sigma(\mathcal{L})$ , where  $\rho_\sigma$  is the projection operator based on the index set  $\sigma$ . The most relevant aspect that differences this method is that in each iteration the dimension of the working sets is smaller than the original dimension of the problem. For each step a partial generating set is obtained from the projected lattice as in [54], and a inverse projection is computed in order to recover the original index set. The last operation is realizable because the index set  $\sigma$  should be computed such that  $\ker(\pi_\sigma) \cap \mathcal{L} = \{0\}$ . Also when  $\sigma$  is available, a generating set of  $\mathcal{L}^\sigma$  is computed as an additional input for the so called "Project-and-Lift" algorithm. By means of a single Gröbner basis computation on the generating set obtained from the iterative steps, a minimal generating set is obtained. For the computation of the intermediate generating sets in each iteration, the authors use a completion method expressed in geometric terms, as a process that computes a connected graph. The implementation of this algorithm, among others, is present in the software package 4ti2 ([30]) and its theory is in [31].

**Hilbert Bases:** In [40] an algorithm to compute a Hilbert basis of a linear Diophantine system of homogeneous equations (actually this is one of the approaches that Normaliz offers [6]) is proposed; see the definition of Hilbert basis in Section 3. Hence we can apply it to  $(A| -A)(X|Y)^T = 0$ . Along this line, one can also use any algorithm to compute Hilbert basis of systems of linear Diophantine homogeneous equations (for instance [10]), and then duplicate the number of variables. In order to avoid this duplication of variables a different approach is given in [9], though the efficiency is not yet proved to be better than the latter approaches in all cases (see the execution time tables included in that paper).

**1.6. Gröbner bases.** In the “world” of polynomial ideals, Gröbner bases are specially useful, since they generalize the concept of division for a single variable. It is well known that  $\mathbb{k}[x]$  is an Euclidean domain, and thus membership to an ideal becomes trivial,

since every ideal  $I$  of  $\mathbb{k}[x]$  is principal. That is,  $f \in I = \langle g \rangle$  if and only if  $g$  divides  $f$ , or in other words, the remainder of the division of  $f$  by  $g$  is zero.

In order to generalize the concept of division by several polynomials, we first need to arrange the monomials in a polynomial, or equivalently, the exponents of monomials, so that the independent term is the least possible element (and thus 0 is the least possible exponent). We also need that these orderings are compatible with multiplication, or if we look at the exponents, with addition. Thus we need a total ordering compatible with addition in  $\mathbb{N}^k$ . This is known in the literature as an *admissible* ordering. Summarizing, we need an ordering  $\preceq$  on  $\mathbb{N}^k$  such that

- for every  $a, b \in \mathbb{N}^k$ , either  $a \preceq b$  or  $b \preceq a$ ,
- for all  $a \in \mathbb{N}^k$ ,  $0 \preceq a$ ,
- for every  $a, b, c \in \mathbb{N}^k$ , if  $a \preceq b$ , then  $a + c \preceq b + c$ .

These conditions, together with Dickson's Lemma, imply that  $\preceq$  is a well ordering on  $\mathbb{N}^k$ .

In this work we use different orderings (as in [12, Chapter 2]) to check when  $X^\alpha < X^\beta$ .

**Lexicographic:** the leftmost non-zero component of  $\beta - \alpha \in \mathbb{Z}^k$  is positive.

**Graded Reverse Lex:**  $\sum_{i=1}^k \alpha_i < \sum_{i=1}^k \beta_i$  or if  $\sum_{i=1}^k \alpha_i = \sum_{i=1}^k \beta_i$  the leftmost non-zero component of  $\beta - \alpha \in \mathbb{Z}^k$  is negative.

**Matrix:** the first non-zero entry of  $O(\beta - \alpha)$  is positive, where  $O \in \mathbb{Z}^{k \times k}$  is an invertible matrix with the elements in the first row zero or positive.

**Product:** this order combines various orders on disjoint sets of monomial variables. Given a sequence of monomial orders  $<_1, <_2, \dots$  then  $X^\alpha <_1 X^\beta$  or  $X^\alpha =_1 X^\beta$  and  $X^\alpha <_2 X^\beta$ , or  $X^\alpha =_{1,2} X^\beta$  and  $X^\alpha <_3 X^\beta, \dots$

The matrix order may be used to encode other orders. For instance lexicographic corresponds with  $O$  equal to the identity matrix. The graded reverse lexicographic is represented by the matrix:

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & -1 \\ 0 & 0 & 0 & \cdots & -1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & -1 & \cdots & 0 & 0 \\ 0 & -1 & 0 & \cdots & 0 & 0 \end{pmatrix},$$

and the product order:

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & 0 \\ 0 & 0 & -1 & \cdots & 0 & 0 \\ 0 & -1 & 0 & \cdots & 0 & 0 \end{pmatrix},$$

which in this case combines a lexicographic on the first variable and a graded reverse lexicographic order for the rest.

Fixed a monomial order, we can choose the largest monomial in a polynomial with respect to the fixed monomial order. This monomial is known as the *leading monomial* of the polynomial. We denote by  $\text{in}(f)$  the leading monomial of  $f$ . A finite set  $G = \{g_1, \dots, g_n\}$  is a *Gröbner basis* for  $I$  if the leading monomial set of the elements of  $G$  generates the same ideal as the leading monomials of  $I$ . As a consequence, we can divide any polynomial  $f$  by  $G$  in the following way: find the first  $i$  such that the leading monomial of  $g_i$  divides the leading monomial of  $f$  (we can assume that  $f$  is monic, and the same for all  $g_i$ 's); then replace  $f$  by  $f - (\text{in}(f)/\text{in}(g_i))g_i$ , and repeat the process until no leading monomial of  $G$  divides the leading monomial of  $f$ . This process stops after a finite number of steps, and the resulting polynomial is known as the *normal form* of  $f$  with respect to  $G$  (and the fixed monomial ordering). As a byproduct, a polynomial  $f$  is in  $I$  if and only if its normal form with respect to  $G$  is zero.

A Gröbner basis  $G$  is *reduced* if every  $g \in G_{\text{red}}$  is monic and no leading monomial in  $G \setminus \{g\}$  divides  $\text{in}(g)$ . Reduced Gröbner basis are unique (see for instance [12]).

## 2. Linear Diophantine equations

Let  $a_{ij} \in \mathbb{Z}$ ,  $i \in \{1, \dots, n\}$ ,  $j \in \{1, \dots, k\}$ , and let  $x_1, \dots, x_k$  be unknowns. A *system of linear Diophantine equations* is a system of equations of the form:

$$(1) \quad \begin{cases} a_{11}x_1 + \dots + a_{1k}x_k = 0, \\ \vdots \\ a_{n1}x_1 + \dots + a_{nk}x_k = 0. \end{cases}$$

From now on, when we use the expression *Diophantine system* we will be talking about a system like this.

The method to obtain the solutions of the system depends on the domain of the solutions. In our case, we are interested in the set of non-negative integer solutions of (1) which is a finitely generated commutative submonoid of  $\mathbb{N}^k$ . The problem of determining the generators of this monoid is a NP-complete complexity problem (see [52, Corollary 18.1a]), which depends strongly on the number of variables of the system.

Equation (1) is a homogeneous system:  $Ax = 0$ , in matrix form. We will focus on this format as the solutions of a non-homogenous system

$$(2) \quad Ax = b,$$

with  $b^T = (b_1, \dots, b_n)$  can be obtained from those of  $Cx = 0$  adding the independent term as a new column to  $A$ ,

$$C = (A | -b).$$

Bounds for the minimal solutions to the Diophantine systems can be found in [43] including systems with congruences. A method to determine if there exist a solution based on Gröbner basis computations is presented in [56], we recall it next.

**2.1. An approach with Gröbner bases to find a particular solution.** According to [56] to know if there exists a solution in  $\mathbb{N}^k$  for (1), requires searching for an special element in the ideal  $\mathfrak{l}_M$  of the monoid  $M$  generated by the columns of the coefficients  $m_j^T = (a_{1j}, \dots, a_{nj}) = (a_{ij})_{i=1, \dots, n}$ . If there is a binomial  $X^\alpha - 1$  in  $\mathfrak{l}_M$ , with  $\alpha = (\alpha_1, \dots, \alpha_k)$ , then  $\sum \alpha_i m_i = 0$  and  $(\alpha_1, \dots, \alpha_k)$  is a solution.

For the non-homogeneous system case, let  $m_{k+1}^T = b^T = (b_1, \dots, b_n)$  be the column vector of the independent terms and  $M \mid b \subset \mathbb{Z}^{k+1}$  be the monoid generated by the set  $\{m_1, m_2, \dots, m_k, m_{k+1}\}$ . So to check the existence of a  $\mathbb{N}$ -solution we search for a binomial  $x_{k+1} - X^\beta$  in  $\mathfrak{l}_{M \mid b}$ , where  $X$  does not contain the variable  $x_{k+1}$  (see [56, Proposition 16]), or fixed an order with  $x_{k+1}$  greater than the other variables, we search a binomial  $\pm(x_{k+1} - X^\beta)$  in the reduced Gröbner basis of  $\mathfrak{l}_{M \mid b}$  (in [56, Lemma 17]).

This procedure can be extrapolated to a system of equations with congruences

$$(3) \quad \begin{cases} a_{11}x_1 + \dots + a_{1k}x_k & \equiv b_1 \pmod{d_1}, \\ \vdots & \vdots \\ a_{n1}x_1 + \dots + a_{nk}x_k & \equiv b_n \pmod{d_n}, \end{cases}$$

with the following remarks ([56, Lemma 9]). Let  $s$  be the number of equations with  $d_i \neq 0$  ( $s \leq n$ ). We construct a new matrix  $A'$  to avoid the torsion terms  $d_i \in \mathbb{N}$ . Assume that the equations of (3) with  $d_i = 0$ ,  $s < i \leq n$  are those appearing at the end of (3). For  $i \in \{1, \dots, k\}$ , set  $m'_i = m_i$  with  $s$  zeros appended at the end, and for  $i \in \{k+2, \dots, k+1+s\}$ ,

$$m'_i{}^T = (0, \dots, 0, \overbrace{0, \dots, d_{i-k}, \dots}^s, 0).$$

Now by Lemma 11 in [56], after the computation of the generators of  $\ker(A')$ , by projecting onto the first  $k+1$  components of its elements we get a generating set of  $\ker(A \mid b)$ , now without congruences, and we can proceed as described above.

Next proposition summarizes how to check for a solution using Gröbner bases.

**PROPOSITION 1.1.** [56] *Let  $Ax = b \pmod{d}$  be a Diophantine system as (3).*

- *For  $b = 0$ , the following statements are equivalent:*
  - *The system  $Ax = 0 \pmod{d}$  admits solutions in  $\mathbb{N}^k$ .*
  - *For some  $\alpha \in \mathbb{N}^k$ ,  $X^\alpha - 1$  in  $\mathfrak{l}_{\ker(A)}$ .*
  - *There is a polynomial of the form  $\pm(X^\alpha - 1)$  in any binomial generating set of  $\mathfrak{l}_{\ker(A)}$ .*
- *For  $b \neq 0$ , the following statements are equivalent:*
  - *The system  $Ax = b \pmod{d}$  admits solutions in  $\mathbb{N}^k$ .*
  - *There is a binomial of the form  $x_{k+1} - X^\beta$  in  $\mathfrak{l}_{\ker(A \mid b)} \subset \mathbb{k}[x_1, \dots, x_{k+1}]$ , where  $X$  does not contain the variable  $x_{k+1}$ .*
  - *There is a binomial of the form  $\pm(x_{k+1} - X^\beta)$  in the reduced Gröbner basis of  $\mathfrak{l}_{\ker(A \mid b)}$  for any monomial order satisfying  $x_{k+1} > x_j$  for all  $j \in \{1, \dots, k\}$ .*

The case with congruences, (3), needs a preparation step, for this reason, unless necessary, it will be omitted in the next sections of this work, although applicable.

REMARK 1.2. Our implementation of Proposition 1.1 is based in the software package *4ti2* ([30]), in particular we use the results of the program *groebner*. For our purposes, this program takes only two arguments: the matrix  $A$ , and as an option, an order matrix for the computation of the binomial ideal associated to  $\ker(A)$ . Both inputs are given as text files formatted according to the manual of the program. For speed reasons we have developed a direct link with the corresponding library to avoid reading from and writing to disk.

**2.2. Optimal solution.** As we will expose in Section 3, the iterative searching process to obtain the minimal non negative solutions of a Diophantine system, needs a particular solution  $s \in \mathbb{N}^k$ , that rules, and may reduce, the number of those iterations. The values of the components of  $s$  set the range of the search. If the 1–norm of  $s$ ,  $\|s\|_1 = \sum_i |s_i|$  is a small number, it is presumable that the number of iterations will be lower than with a particular solution with a bigger 1–norm. Thus, we call *optimal solution* to any  $\mathbb{N}$ –solution with minimal 1–norm.

Gröbner bases can be used to compute an optimal solution through the use of suitable monomial orders. The next two lemmas expose the monomial orders used in this work for the homogeneous and non-homogeneous cases.

LEMMA 1.3. *Given a system  $Ax = 0$  with some nonzero  $\mathbb{N}$ –solution, there exists a monomial order such that a polynomial of the form  $X^\alpha - 1$  ( $\alpha_{k+1} = 0$ ) is in the reduced Gröbner basis of  $\mathfrak{l}_M$  with  $\alpha$  an optimal solution.*

PROOF. We only need to consider a total degree order (first compares the total degree). □

For the homogeneous setting, among all possible graded orderings, we propose the graded reverse lexicographic order due to its best computational behavior.

LEMMA 1.4.  *$Ax = b$  admits an  $\mathbb{N}$ –solution if and only if there is a binomial of the form  $x_{k+1} - X^\beta$ , with  $\beta_{k+1} = 0$ , in the reduced Gröbner basis of  $\mathfrak{l}_{\ker(A|b)}$  respect to a matrix ordering defined by a matrix of the form*

$$(4) \quad \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 1 & \cdots & 1 & 0 \\ & & & 0 & \\ & & O' & \vdots & \\ & & & 0 & \end{pmatrix} \in \mathbb{Z}^{(k+1) \times (k+1)},$$

with  $O' \in \mathbb{Z}^{(k-1) \times k}$ . Also  $\beta$  is an optimal solution.

PROOF. Fixed this monomial order, the proof is obtained from the definition of the reduced Gröbner basis and Proposition 1.1. □

For the non-homogeneous case we propose to use the matrix ordering defined by

$$(5) \quad \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 1 & 1 & \cdots & 1 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & -1 & 0 \\ 0 & 0 & 0 & \cdots & -1 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & -1 & \cdots & 0 & 0 & 0 \\ 0 & -1 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix} \in \{0, \pm 1\}^{(k+1) \times (k+1)}.$$

In Table 1 we see the behavior for this product order against the lexicographic order, which is compatible with the requirements of Proposition 1.1 for non-homogeneous systems of Diophantine equations. We omit some results where both orders end to the same particular solution. For these cases the computing times are similar and if it is not the case, the product order is fastest. When the solutions are different, the product order ends first or, as expected, it offers a solution with smaller 1–norm.

Algorithm 1.5 returns true if a solution  $s$  of a linear system of Diophantine homogeneous equations exists, and because of the orders used, it will have minimum 1–norm. Otherwise, if there is no solution it returns false. The link with *4ti2* software package is done in the line 9.

### 3. Computing non-negative integer solutions of linear Diophantine systems

Let  $R \subset \mathbb{N}^k$  be the set of  $\mathbb{N}$ –solutions of a system of linear Diophantine equations of the form (1). Then  $R$  is an affine semigroup and it is generated by its nonzero minimal elements with respect to the usual partial ordering on  $\mathbb{N}^k$ . Let us denote this set by  $H(R)$ , which is usually known as the *Hilbert basis* of  $R$ . When we deal with a non-homogeneous system,  $R$  is the set  $\bigcup_{\alpha \in H(R)} (\alpha + R')$  where  $R'$  is the semigroup of the  $\mathbb{N}$ –solutions of  $Ax = 0$ . So  $R$  is determined by its minimal elements and/or the Hilbert basis of the  $\mathbb{N}$ –solutions of its associated homogeneous system (see [38, Section 1] for details).

Denote by  $R(i, \beta) \subset \mathbb{N}^k$  the set  $\{x \in R \mid x_i = \beta\}$ . There is a one-to-one correspondence between this set and the set of  $\mathbb{N}$ –solutions of

$$(6) \quad A(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_k)^T = -\beta m_i,$$

with  $k - 1$  indeterminates. We can repeat the process for  $R(j, \alpha)$ , obtaining  $R(j, \alpha)(i, \beta) \subseteq \mathbb{N}^k$ , which is the set  $\{x \in R(j, \alpha) \mid x_i = \beta\}$  that corresponds with the set of  $\mathbb{N}$ –solutions of

$$A(x_1, \dots, x_{j-1}, 0, x_{j+1}, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_k)^T = -\alpha m_j - \beta m_i,$$

and so on.

Algorithm 1.7 states how to obtain  $H(R)$  based on the following result:

TABLE 1. Non-homogeneous Diophantine system solutions with the lexicographic and the product order.

2x7 systems					
Lexicographic order			Product order		
T(s)	1-norm	solution	T(s)	1-norm	solution
0,001	87	0 0 0 3 39 45 0	0,001	26	0 18 5 0 3 0 0
0,001	63	0 0 0 0 0 41 22	0,001	24	0 4 0 0 18 1 1
0,002	95	0 0 0 0 1 50 44	0,001	17	1 0 2 7 0 1 6
0,002	43	0 0 6 0 12 23 2	0	29	6 0 0 0 5 18 0
4x7 systems					
Lexicographic order			Product order		
T(s)	1-norm	solution	T(s)	1-norm	solution
0,002	399	0 4 59 82 101 153 0	0,001	57	19 0 3 21 3 0 11
0,003	134	0 21 18 2 39 3 51	0,002	63	15 2 9 21 1 1 14
0,001	160	0 0 7 63 50 14 26	0,001	64	0 13 0 15 5 14 17
0,001	115	0 1 11 21 8 38 36	0,001	55	22 5 1 15 2 0 10
0,002	1113	1 0 42 1 96 542 431	0	95	23 12 17 19 17 3 4
0,003	178	0 53 33 6 46 39 1	0,002	41	14 18 0 4 2 3 0
0,002	267	0 0 82 54 38 56 37	0,003	61	10 8 0 2 10 20 11
6x10 systems					
Lexicographic order			Product order		
T(s)	1-norm	solution	T(s)	1-norm	solution
0,242	389	0 10 27 8 51 118 24 90 21 40	0,048	45	12 15 16 24 10 15 22 4 15 12
0,239	150	14 23 6 8 11 13 28 4 20 23	0,062	113	15 5 3 3 15 14 17 9 11 21
0,021	299	1 1 74 3 10 52 46 24 48 40	0,052	111	21 22 20 0 6 2 18 1 9 12
0,131	126	6 19 11 10 9 15 5 18 22 11	0,067	126	6 19 11 10 9 15 5 18 22 11
0,004	6518	0 0 1120 1375 812 415 2333 75 2 386	0,099	118	22 21 16 23 7 5 5 14 0 5
0,223	144	20 7 22 24 14 15 19 14 2 7	0,218	144	23 1 21 27 7 22 15 14 5 9
0,251	146	17 18 15 16 20 0 24 3 20 13	0,157	146	17 18 15 16 20 0 24 3 20 13
0,074	118	16 21 23 1 13 3 18 21 1 1	0,012	118	16 21 23 1 13 3 18 21 1 1
0,008	992	0 102 190 1 12 158 54 205 208 62	0,04	146	18 24 10 2 16 23 10 21 19 3
0,007	501	0 0 65 97 1 48 107 30 130 23	0,071	107	0 1 9 11 3 24 23 23 13 0
0,009	586	0 75 16 100 181 48 12 134 16 4	0,023	143	21 17 15 22 4 1 22 20 10 11
0,017	127	1 9 12 22 15 7 3 23 18 17	0,017	127	1 9 12 22 15 7 3 23 18 17
0,122	118	22 7 15 17 16 12 9 10 4 6	0,02	118	22 7 15 17 16 12 9 10 4 6
0,009	367	0 74 67 49 13 37 40 49 33 5	0,015	100	15 1 11 8 4 9 20 14 3 15
0,051	209	18 51 58 3 21 3 24 2 4 25	0,016	128	22 9 22 15 3 11 16 15 10 5

LEMMA 1.6. ([39, Lemma 2.4]) Let  $s = (s_1, \dots, s_k) \in R \setminus \{0\}$  and

$$(7) \quad F = \{s\} \cup \bigcup_{i=1}^k \bigcup_{\beta=0}^{s_i-1} H(R(i, \beta)).$$

---

**Algorithm 1.5** Particular  $\mathbb{N}$ -solution of a linear Diophantine system
 

---

```

1: function SOLBYIDEAL( $A, b, s$ )
2:   if  $b \neq 0$  then
3:      $A' = A|b$  ▷  $A'$  is  $A$  with  $b$  as an additional last column
4:      $O =$  order matrix in (5)
5:   else
6:      $A' = A$ 
7:      $O =$  order matrix in (4)
8:   end if
9:   (4ti2)  $G =$  Reduced_Gröbner_basis( $A', O$ )
10:  if  $b \neq 0$  then
11:    if  $x_{k+1} - X^\beta \in G$  then
12:       $s = \beta$ 
13:      return true
14:    end if
15:  else
16:    if  $X^\alpha - 1 \in G$  then
17:       $s = \alpha$ 
18:      return true
19:    end if
20:  end if
21:  return false
22: end function

```

---

Then,  $H(R) = H(F)$  ( $\sqcup$  denotes disjoint union).

In Algorithm 1.7, every iteration controlled by the outer loop with the index  $i$  implies a reduction in one column from the original matrix  $A$ , which is translated to the independent term of the system. This reduction is a clear advantage because we use Gröbner basis to get a particular solution for each of these systems.

In order to improve it we show some interesting properties of the sets  $H(R(i, \beta))$ . But first, if  $Q$  and  $L$  are two sets of non-negative vectors, then we say that  $Q \succeq L$  if for all  $\alpha \in Q$ , there exists  $\beta \in L$  such that  $\alpha \geq \beta$ .

LEMMA 1.8. Let  $i, j \in \{1, \dots, k\}$ , with  $i \neq j$ , and  $\alpha, \beta \in \mathbb{N}$ . Then

$$H(R(j, \alpha)(i, \beta)) \succeq H(R(i, \beta)).$$

PROOF. It is trivial the inclusion  $H(R(j, \alpha)(i, \beta)) \subseteq R(i, \beta)$ , this implies that for any  $s \in H(R(j, \alpha)(i, \beta))$ , by choosing an element  $s' \in H(R(i, \beta))$  with a value in the  $j$ -th component less or equal to  $\alpha$  ensures that  $s \geq s'$ .  $\square$



**Algorithm 1.7** Computing the minimal  $\mathbb{N}$ -solutions of a Diophantine system**Input:** A system as (1).**Output:** The minimal elements of  $R$ .Take a particular  $\mathbb{N}$ -solution  $s = (s_1, \dots, s_k) \in R \setminus \{0\}$ **if**  $R$  is  $\{0\}$  or the empty set **then**

$$H(R) = R$$

**else****for**  $i = 1, \dots, k$  **do****for**  $\beta = 0, \dots, s_i - 1$  **do**Compute  $H(R(i, \beta))$  by recursively calling Algorithm 1.7 for the system

$$A(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_k)^T = -\beta m_i.$$

**end for****end for**Compute  $H(F)$  for

$$F = \{s\} \cup \bigcup_{i=1}^k \bigsqcup_{\beta=0}^{s_i-1} H(R(i, \beta)).$$

$$H(R) = H(F).$$

**end if**LEMMA 1.9. Let  $s = (s_1, \dots, s_k)$  be an  $\mathbb{N}$ -solution of the system  $Ax = 0$ , and

$$s' = (s'_1, \dots, s'_{j-1}, 0, s'_{j+1}, \dots, s'_k)$$

an  $\mathbb{N}$ -solution of the system

$$A(x_1, \dots, x_{j-1}, 0, x_{j+1}, \dots, x_k)^T = -\alpha m_j$$

with  $1 \leq j \leq k$  and  $\alpha \in \mathbb{N}$  such that  $0 \leq \alpha \leq s_j - 1$ . Then

$$(8) \quad H(R(j, \alpha)) \supseteq H \left( \{s'\} \cup \bigcup_{i=1}^{j-1} \bigsqcup_{\beta=0}^{f_i-1} H(R(i, \beta)) \cup \bigcup_{\substack{i=1 \\ i \neq j}}^k \bigsqcup_{\beta=f_i}^{s'_i-1} H(R(j, \alpha)(i, \beta)) \right),$$

where  $f = (s_1, \dots, s_{j-1}, 0, \dots, 0) \in \mathbb{N}^k$  are the first  $j-1$  components of  $s$ .

PROOF. By Lemma 1.6,

$$H(R(j, \alpha)) = H \left( \{s'\} \cup \bigcup_{\substack{i=1 \\ i \neq j}}^k \bigsqcup_{\beta=0}^{s'_i-1} H(R(j, \alpha)(i, \beta)) \right),$$

we can split the outer union as follows:

$$H(R(j, \alpha)) \supseteq H \left( \{s'\} \cup \bigcup_{i=1}^{j-1} \bigsqcup_{\beta=0}^{f_i-1} H(R(j, \alpha)(i, \beta)) \cup \bigcup_{\substack{i=1 \\ i \neq j}}^k \bigsqcup_{\beta=f_i}^{s'_i-1} H(R(j, \alpha)(i, \beta)) \right).$$

As we are looking for the minimal value solutions, the first union takes into account any solution with lower values than those of  $s$  in some or all the  $j - 1$  firsts components. Besides the second union considers the values greater than those in the first union with respect to  $s$ . Then by Lemma 1.8,

$$H(R(j, \alpha)) \supseteq H \left( \{s'\} \cup \bigcup_{i=1}^{j-1} \bigsqcup_{\beta=0}^{f_i-1} H(R(i, \beta)) \cup \bigcup_{\substack{i=1 \\ i \neq j}}^k \bigsqcup_{\beta=f_i}^{s'_i-1} H(R(j, \alpha)(i, \beta)) \right). \quad \square$$

Algorithm 1.10 is a reformulation of Algorithm 1.7 that embodies the result of Lemma 1.9. As in the first version, each variable, one by one, is explored for possible values (*test values*), leaving the rest free. Test values are upper limited by the value of the solution  $s$  as shown in Equation (7) in the upper limits of each union  $\bigsqcup$ . From the last result, another limit on the test values is established in the lower limit of  $\beta$  from the components of vector  $f$ . In order to avoid redundant computations, this vector stores for each unknown variable the respective values explored by the algorithm. In this way we are narrowing the search space.  $f$  is initialized as  $(0, \dots, 0)$  at the beginning of the process.

For each of the test values assigned to a variable, we use Algorithm 1.5 (function SOLBYIDEAL) to get a particular solution for a system of the form (6). If there is one, we proceed next by fixing each of the other variables, and we repeat the same process, now with two variables fixed to their test values.

Figure 1 shows a partial scheme of the process. For the initial system of equations, a solution is found,  $(1, 3, 1, 2, 0)$ . When this happens, a series of branches are generated, each one to test lower values than those of the given solution, for the respective variable. From the initial system, the figure shows the branch generated when the  $x_1$  variable is assigned to the first test value, in this case 0. The dotted lines show the independent terms of the systems obtained from the assignation of the corresponding test values to the fixed variable (we have omitted the left side of the equations).

Figure 2 shows the process on the subsystem generated from the initial by substitution of the variable  $x_1 = 0$ . Every subsystem showed in this figure and the previous is checked for a solution using function SOLBYIDEAL. In this figure some branches do not produce more checks for a solution, while others do not check for substitutions from previous checked variables as pointed in Lemma 1.9.

---

**Algorithm 1.10** Computing the minimal  $\mathbb{N}$ -solutions of a Diophantine system

---

**Input:** A Diophantine system as (1) and  $f$ .

**Output:** The minimal elements of  $R$ .

Take a particular  $\mathbb{N}$ -solution  $s = (s_1, \dots, s_k) \in R \setminus \{0\}$

**if**  $R$  is  $\{0\}$  or the empty set **then**

$H(R) = R$

**else**

**for**  $i = 1, \dots, k$  **do**

**for**  $\beta = f_i, \dots, s_i - 1$  **do**

Compute  $H(R(i, \beta))$  by recursively calling Algorithm 1.10 for the system

$$A(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_k)^T = -\beta m_i \text{ and } f$$

**end for**

$f_i = s_i$

**end for**

Compute  $H(F)$  for

$$F = \{s\} \cup \bigcup_{i=1}^k \bigcap_{\beta=0}^{s_i-1} H(R(i, \beta))$$

$H(R) = H(F)$

**end if**

---

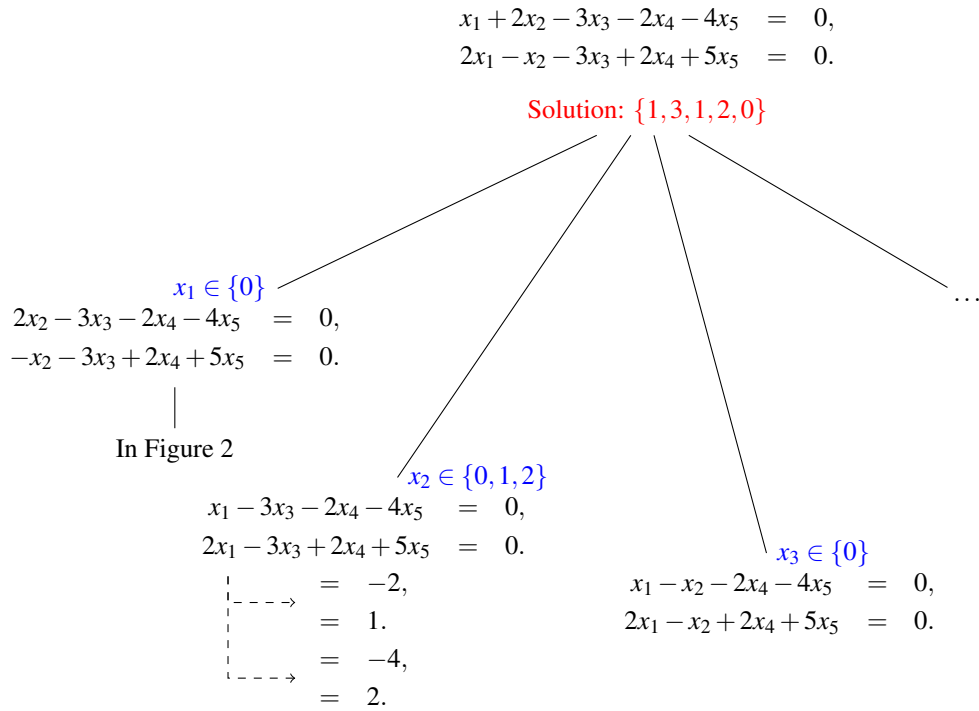


FIGURE 1. The initial explorations of the recursive process to find the minimal solutions of a linear Diophantine system of equations.

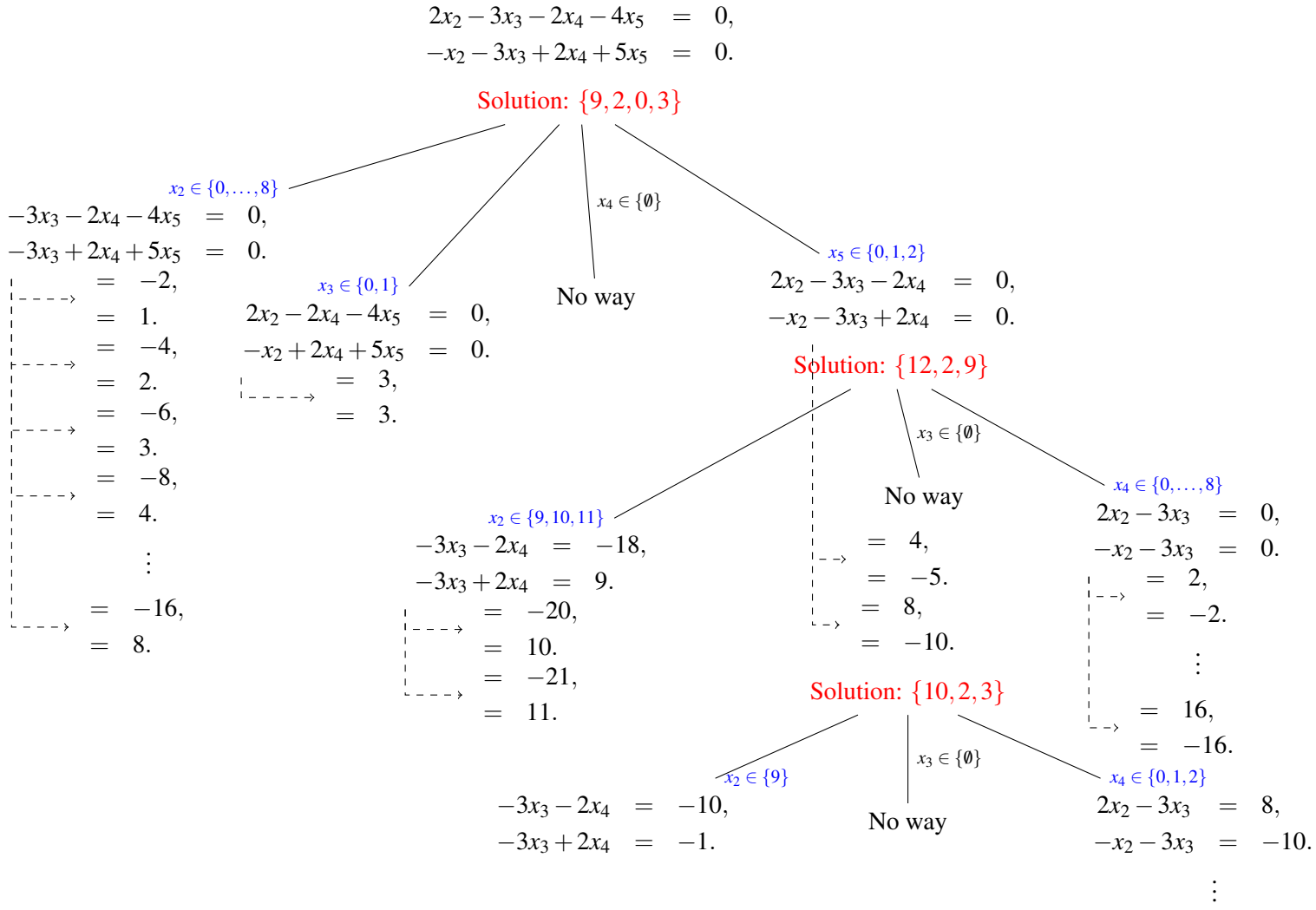


FIGURE 2. Recursive process to find the minimal solutions of a linear Diophantine system of equations.

**COROLLARY 1.11.** *Let  $t \in \mathbb{N}$ ,  $Ax = tb$  admits an  $\mathbb{N}$ -solution and  $Ax = jb$  does not admit  $\mathbb{N}$ -solution for  $j \in \{1, \dots, t-1\}$  if and only if there is a binomial  $x_{k+1}^t - X^\beta$  in the reduced Gröbner basis of  $\mathfrak{l}_{\ker(A|b)}$  respect to a matrix ordering defined by*

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 1 & \cdots & 1 & 0 \\ \vdots & & \ddots & & \vdots \\ \vdots & & \cdots & & 0 \end{pmatrix} \in \mathbb{Z}^{(k+1) \times (k+1)}.$$

*So  $\beta$  is an optimal solution of  $Ax = tb$ .*

*Moreover, for  $j > t$ ,  $Ax = jb$  admits an  $\mathbb{N}$ -solution if and only if the normal form of the monomial  $x_{k+1}^j$  modulo the ideal  $\mathfrak{l}_{\ker(A|b)}$  is a monomial  $X^{\beta'} \in \mathbb{k}[x_1, \dots, x_k]$ . The exponent  $\beta'$  is an optimal solution of  $Ax = jb$ .*

This result reduces the number of iterations in Algorithm 1.10 for some subsystems obtained from homogeneous systems. In these cases, we only need to compute an optimal solution of the system  $A(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_k)^T = -\alpha m_i$  for  $\alpha = 1, \dots, s_i - 1$ , and these optimal solutions can be obtained by using the normal form.

**3.1. Improvement for the homogeneous case.** Algorithm 1.12 shows the procedure DPSOLVE as a more detailed version of Algorithm 1.10. We are going to discuss a little improvement based on the steps of this procedure.

Observe that inside the scope of the loop from lines 12 to 18 (Algorithm 1.12), a series of linear Diophantine equations systems are constructed. From one of the columns of  $A$ , a new independent term  $b'$  is computed for every value of  $\alpha$ . Besides, in line 14, a Gröbner basis is computed for each one. When  $b' = 0$ , it is possible to process this new system without computing a Gröbner basis for every value of  $\alpha$ .

From a matrix  $A = (m_1|m_2|\dots|m_k) \in \mathbb{Z}^{n \times k}$ , being  $m_j$  its columns, consider a submatrix  $A' = (m_{j_1}|m_{j_2}|\dots|m_{j_{k-1}})$  of  $A$  obtained as in Algorithm 1.12, line 8, and  $b' = 0$  computed in line 13. Let  $s'$  be a particular solution for this homogeneous system of Diophantine equations  $A'x' = 0$  (recall that  $s'$  comes from a binomial in  $\mathfrak{l}_{M'}$ ). We use the letter  $j$  to identify the index of the columns of the matrix  $A'$ , which are processed for the possible values of  $\alpha = \{0, \dots, s'_j - 1\}$ . For these values we have the following cases.

- When  $\alpha = 0$ , then we have a new system of linear Diophantine equations:  $A'x' = 0$ , which produces a new recursive call on procedure DPSOLVE.
- If  $\alpha = 1$ , let  $\mathfrak{l}_{M'_j}$  denote the ideal of the monoid  $M'_j$  generated by the columns of  $A'$  with the sign of column  $m_j$  reversed. The computation of  $\mathfrak{l}_{M'_j}$  Gröbner basis is done using  $\mathfrak{l}_{M'}$ : from [54, Proposition 12.5], we calculate a generating set of  $\mathfrak{l}_{M'_j}$  by flipping the variable  $x_j$  in the binomials of a Gröbner basis of  $\mathfrak{l}_{M'}$  using an elimination order on  $x_j$ . In this situation, we apply Corollary 1.11 to solve the problem.

**Algorithm 1.12** Non-negative integer solutions of linear Diophantine systems

---

```

1: procedure DPSOLVE( $A, b, f, s, S$ )
2:    $k \leftarrow$  number of columns of  $A$ 
3:   if  $k = 1$  and  $(\nexists s \in \mathbb{N}^k, s' \neq 0, \text{ where } As' = b)$  then
4:     return  $H\{s, s'\}$ 
5:   end if
6:    $Q := \{s\}$ 
7:   for  $j \leftarrow 1, \dots, k$  do
8:      $A' \leftarrow A \setminus (m_j)$   $\triangleright$  delete the  $j$ -column of  $A$ 
9:      $f' \leftarrow f \setminus (f_j)$   $\triangleright$  delete the  $j$ -coordinate of  $f$ 
10:     $x' \leftarrow x \setminus (x_j)$   $\triangleright$  delete the  $j$ -coordinate of  $x$ 
11:     $\alpha \leftarrow f_j$ 
12:    while  $f_j \leq \alpha \leq s_j - 1$  do
13:       $b' \leftarrow b - \alpha m_j$ 
14:      if SOLBYIDEAL( $A', b', s'$ ) then
15:        DPSOLVE( $A', b', f', s', T$ )
16:         $T \leftarrow \{(\beta_1, \dots, \beta_{j-1}, \alpha, \beta_{j+1}, \dots, \beta_k) \mid \beta \in T\}$ 
17:         $Q \leftarrow H(Q \cup T)$ 
18:      end if
19:       $\alpha \leftarrow \alpha + 1$ 
20:    end while
21:     $f_j \leftarrow s_j$ 
22:  end for
23:   $S \leftarrow H(Q)$ 
24: end procedure

```

---

With this exposed treatment, given a particular solution with high values for the variables of the system, we can suppress the computation of an important number of Gröbner basis. Unfortunately, it is very unlikely to get to homogeneous systems during the algorithm computation. For this reason, and after different essays, we discarded this modification of the algorithm.

**3.2. Performance of DPSolve compared to other related software.** When we finished the first implementation of DPSolve, we had the intention of characterizing suitable systems that would, in a reasonable amount of time, work well with this algorithm. We began with exploratory comparisons with an efficient implementation called `systema`<sup>1</sup> of the procedure proposed by Contejean and Devie in [10]. Also, we used `hilbert` from the software package `4ti2` (see [30]) and the program `normaliz` (see [6]). The election of these tools was driven mainly by the easy or public access to them.

<sup>1</sup>by Pablo Rodriguez Archilla for the Dept. of Algebra, Univ. of Granada.

Each of these tools needs one file with the system of equations expressed with its own format. The name of this file is one of the arguments to specify in a command-line (these tools do not have a graphical interface, except `Normaliz` which has both types of interfaces). For `sistema` and `DPSolve` it is a text file with a series of lines, corresponding with an equation, separated by commas, with the last one ending with a point. `sistema` can take also another file to specify the torsion terms. An example of an input to `sistema` or `DPSolve` could be the next:

```
2 5 -3 7 11 15 -4 = 12,
7 9 2 -22 1 17 5 = 9,
5 -1 9 33 -4 15 -23 = 35.
```

The result of the computations is showed to the standard output, then it can be redirected to a file. The default mode of computation of this programs uses 64 bits arithmetic.

The name of the input file for `hilbert` must end with the letters `.mat`. It should contain the matrix size, in the first line, and each of its rows in the next rows. The input equivalent to the previous programs could be:

```
3 8
2 5 -3 7 11 15 -4 -12
7 9 2 -22 1 17 5 -9
5 -1 9 33 -4 15 -23 -35
```

Note that it is necessary to homogenize the equations. The output of `hilbert` is a file named as the input file, but with the letters `.mat` changed to `.hil`. With the parameter `-p=32` and `-p=64` it is possible to choose between 32 or 64 bits arithmetic mode. The default mode is 32 bits.

The expected name for the input file to `Normaliz` ends with the sequence of letters `.in`. Its format is similar to this previous, but in this case, we can specify that the system is inhomogeneous:

```
3 8
2 5 -3 7 11 15 -4 -12
7 9 2 -22 1 17 5 -9
5 -1 9 33 -4 15 -23 -35
inhom_equations
```

By changing `inhom_equations` to `equations`, the input rows are treated as homogeneous equations. The output file name changes the `.in` ending part of original input name to `.out`. For our purposes, the parameters necessary to execute `Normaliz` are `-N` or `-d`, and `-x=1` to force just one thread of execution for comparison with the other programs. By default, it uses as many as the operating system allows. The parameters `-N` and `-d` enable to choose between two methods to get the Hilbert basis of the monoid generated by the column vectors, that is, the minimal solutions we are interested in. The authors of `Normaliz` recommend the use of the `-d` option for computations like the ones we are



dealing with. Indeed, from the computation experiments accomplished, we detected that some inputs generated errors due to overflows. In this cases, the parameter `-d` avoids this problem, being more convenient than trying the computation with multiple precision based on the GnuMP library ([42]). In general, we have avoided the use of this option with `hilbert` and `Normaliz` since it slows down seriously the process. The default mode of computation of `Normaliz` uses 64 bits arithmetic.

From the initial tests for debugging and comparison we found examples where `DPSolve` performance was worst than the others, and in other cases, the others where slower to end. As we have noted, the problem we are facing is complex enough to expect this kind of results. Even, for some particular examples, `hilbert` program and `Normaliz` often ended with an error, or aborted its execution unexpectedly. But in recent versions of this programs they have corrected these problems, and improved the running times. As we have observed in several examples, there is a big difference with `DPSolve` and `sisyema`. Usually, for the problem we are interested in, `Normaliz` achieves the quickest outputs.

We present an anecdotic example, for which `DPSolve` is the only that has ended in a reasonable amount of time, while the other programs did not.

EXAMPLE 1.13. The input file is an inhomogeneous Diophantine system with 6 equation and 12 variables:

$$\begin{array}{r}
 2 \ -7 \ -3 \ -1 \ -2 \ -4 \ -7 \ -1 \ 3 \ -7 \ 5 \ 3 \ = \ -222, \\
 1 \ -3 \ 1 \ -5 \ 1 \ 0 \ -3 \ 0 \ 0 \ 7 \ -2 \ -7 \ = \ -331, \\
 6 \ -3 \ -5 \ 6 \ 1 \ 4 \ 1 \ -2 \ 0 \ -4 \ -6 \ 6 \ = \ 267, \\
 1 \ 5 \ 4 \ 5 \ -7 \ -6 \ -3 \ 7 \ -5 \ 7 \ 7 \ 4 \ = \ 139, \\
 6 \ -5 \ -1 \ 2 \ 3 \ 5 \ 1 \ 0 \ 6 \ 0 \ 5 \ 2 \ = \ 170, \\
 2 \ 1 \ -1 \ -6 \ -2 \ 0 \ 5 \ 6 \ -5 \ 2 \ 2 \ 2 \ = \ -8.
 \end{array}$$

With 18 solutions:

$$\begin{array}{r}
 2 \ 12 \ 8 \ 20 \ 11 \ 9 \ 16 \ 2 \ 6 \ 4 \ 0 \ 28 \\
 0 \ 21 \ 3 \ 14 \ 24 \ 11 \ 5 \ 4 \ 7 \ 8 \ 0 \ 38 \\
 0 \ 15 \ 1 \ 23 \ 35 \ 2 \ 10 \ 13 \ 2 \ 4 \ 1 \ 29 \\
 1 \ 16 \ 0 \ 22 \ 14 \ 10 \ 13 \ 8 \ 7 \ 3 \ 1 \ 24 \\
 1 \ 11 \ 9 \ 21 \ 32 \ 1 \ 13 \ 7 \ 1 \ 5 \ 0 \ 33 \\
 1 \ 20 \ 5 \ 16 \ 11 \ 21 \ 5 \ 3 \ 4 \ 3 \ 2 \ 30 \\
 2 \ 6 \ 6 \ 29 \ 22 \ 0 \ 21 \ 11 \ 1 \ 0 \ 1 \ 19 \\
 10 \ 27 \ 2 \ 15 \ 26 \ 3 \ 8 \ 4 \ 9 \ 4 \ 0 \ 31 \\
 6 \ 24 \ 3 \ 15 \ 8 \ 16 \ 8 \ 1 \ 9 \ 3 \ 1 \ 28 \\
 15 \ 29 \ 3 \ 17 \ 31 \ 0 \ 8 \ 6 \ 6 \ 0 \ 1 \ 26 \\
 5 \ 23 \ 4 \ 16 \ 29 \ 8 \ 5 \ 6 \ 4 \ 4 \ 1 \ 33 \\
 10 \ 25 \ 5 \ 18 \ 34 \ 5 \ 5 \ 8 \ 1 \ 0 \ 2 \ 28 \\
 14 \ 34 \ 6 \ 9 \ 41 \ 1 \ 0 \ 2 \ 6 \ 5 \ 0 \ 40 \\
 12 \ 18 \ 7 \ 21 \ 13 \ 1 \ 19 \ 2 \ 8 \ 0 \ 0 \ 21
 \end{array}$$

```
15 33 8 11 28 11 0 1 3 0 2 32
6 19 12 14 26 7 8 0 3 5 0 37
11 21 13 16 31 4 8 2 0 1 1 32
7 14 9 22 16 6 16 4 3 0 1 23
```

For this example, testing `hilbert` program we observe that after several hours, it began to consume all the available memory, and we killed the process. `Normaliz` aborted the computation almost immediately. And we killed `systema` after several hours of computation. `DPSolve` ended in 331.937 seconds.

## CHAPTER 2

### Affine convex body semigroups in $\mathbb{N}^2$

A *convex body* of  $\mathbb{R}^k$  is a compact (closed and bounded) convex subset with non-empty interior. Associated to a convex body  $F \subseteq \mathbb{R}_{\geq}^k$  we can define the following *cone*

$$\mathbf{L}_{\mathbb{Q}_{\geq}}(F) = \left\{ \sum_{i=1}^p q_i f_i \mid p \in \mathbb{N}, q_i \in \mathbb{Q}_{\geq}, f_i \in F \right\}.$$

From  $F$  also we are going to define the set  $\mathbf{F}$  that we will call a convex body monoid (see Proposition 2.1), contained in  $\mathbf{L}_{\mathbb{Q}_{\geq}}(F)$ . Membership to this kind of monoids is easy to test.

In some cases the generating system of  $\mathbf{F} \cap \mathbb{N}^k$  is finite. We characterize conditions for those cases in  $\mathbb{N}^2$ , and if so, we present procedures to compute its minimal generating set. In particular, we study the cases when  $F$  is a circle or a polygon. Finally, we give a way to check if these affine convex body semigroups are Buchsbaum.

#### 1. Preliminary concepts and results

Let  $F$  be a convex body of  $\mathbb{R}_{\geq}^2$ . A ray  $\tau$  of  $\mathbf{L}_{\mathbb{Q}_{\geq}}(F)$  is a halfline such that  $0 \in \tau \subseteq \mathbf{L}_{\mathbb{Q}_{\geq}}(F)$ , and thus it is determined by any of its nonzero elements.

For  $k = 2$ , denote by  $\{\tau_1, \tau_2\}$  a set of *extremal rays* of  $\mathbf{L}_{\mathbb{Q}_{\geq}}(F)$ , that is,  $\mathbf{L}_{\mathbb{Q}_{\geq}}(\{\tau_1, \tau_2\}) = \mathbf{L}_{\mathbb{Q}_{\geq}}(F)$ . We will assume without loss of generality that the slope of  $\tau_1$  is greater than the slope of  $\tau_2$ .

Define

$$\mathbf{F} = \left\{ X \in \mathbb{R}_{\geq}^2 \mid \text{there exists } i \in \mathbb{N} \text{ such that } \frac{X}{i} \in F \right\} \cup \{0\} = \bigcup_{i=0}^{\infty} iF \subseteq \mathbf{L}_{\mathbb{Q}_{\geq}}(F),$$

where  $iF = \{iX \mid X \in F\}$  with  $i \in \mathbb{N}$ . Define  $\mathcal{F} = \bigcup_{i=0}^{\infty} iF \cap \mathbb{N}^2$ . The next result shows that being  $F$  a convex body, the set  $\mathbf{F}$  is a monoid and  $\mathcal{F}$  is a semigroup.

**PROPOSITION 2.1.** *Under the standing hypothesis,  $\mathbf{F}$  is a submonoid of  $\mathbb{R}^2$ .*

**PROOF.** Let  $P, Q \in \mathbf{F}$ . There exist  $i, j \in \mathbb{N}$  and  $P', Q' \in F$  such that  $P = iP'$  and  $Q = jQ'$ . Then

$$P + Q = iP' + jQ' = (i + j) \left( \frac{i}{i + j} P' + \left(1 - \frac{i}{i + j}\right) Q' \right).$$

Using the convexity of  $F$  we obtain  $\frac{i}{i + j} P' + \left(1 - \frac{i}{i + j}\right) Q' \in F$  and so  $P + Q \in \mathbf{F}$ . □

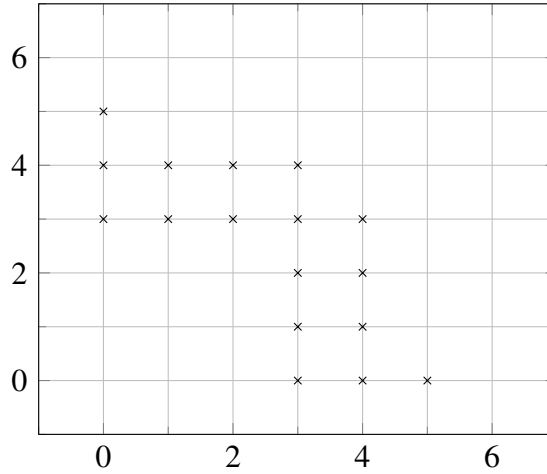


FIGURE 1.  $\{X \in \mathbb{R}_{\geq}^2 \mid 3 \leq d(X) \leq 5\}$ .

Denote by  $d(P, Q)$  the Euclidean distance between two elements  $P, Q \in \mathbb{R}^2$  and by  $d(P)$  the distance  $d(P, 0)$ . We see the convexity property is necessary to  $\mathbf{F}$  be a monoid. If  $F$  is the compact and not convex set

$$\{X \in \mathbb{R}_{\geq}^2 \mid 3 \leq d(X) \leq 5\},$$

the elements  $(4, 0), (0, 4)$  are in  $\mathbf{F}$  but  $(4, 0) + (0, 4)$  is not in  $\mathbf{F}$  (see Figure 1).

Given a convex body  $F$ , we say that  $\mathbf{F}$  is the *convex body monoid* generated by  $F$ . Respectively,  $\mathcal{F}$  is the *convex body semigroup* generated by  $F$ , or in other words, it is the intersection of the convex body monoid  $\mathbf{F}$  with  $\mathbb{N}^2$ . In general, these semigroups are not full affine semigroups. An affine semigroup  $S \subseteq \mathbb{N}^k$  is *full* if  $G(S) \cap \mathbb{N}^k = S$  (see [45, Chapter 7];  $G(S)$  stands for the group generated by  $S$ , that is, linear combinations of elements from  $S$  with integer coefficients). To see this, take  $F$  to be the convex hull of  $\{(0, 0), (2, 1), (1, 2)\}$ . As  $(1, 1) \in F \cap \mathbb{N}^2 \subseteq \mathcal{F}$ , we deduce that  $(1, 0) = (2, 1) - (1, 1) \in G(\mathcal{F})$  and analogously,  $(0, 1) = (1, 2) - (1, 1) \in G(\mathcal{F})$ . Hence  $G(\mathcal{F}) = \mathbb{Z}^2$ , which yields  $G(\mathcal{F}) \cap \mathbb{N}^2 = \mathbb{N}^2 \neq \mathcal{F}$ , because for instance  $(1, 0) \in \mathbb{N}^2 \setminus \mathcal{F}$ .

Let  $T$  be a submonoid of  $\mathbb{R}_0^+$  generated by the interval  $[\alpha, \beta] = \{x \in \mathbb{R} \mid \alpha \leq x \leq \beta\}$  with  $\alpha, \beta \in \mathbb{R}^+$  and  $\alpha < \beta$ . A *proportionally modular Diophantine inequality* is an expression of the form:  $ax \bmod b \leq cx$ , with  $a, b$  and  $c$  positive integers (this equation has the same nonnegative integer solutions as  $\frac{a}{c} \bmod \frac{b}{c} \leq x$ , and so we could have defined a proportionally modular Diophantine inequality as an expression of the form  $ax \bmod b \leq x$  with  $a, b \in \mathbb{R}^+$ ). In [49] this expression is used to characterize submonoids of  $\mathbb{R}_0^+$  generated by intervals, where it is shown that every submonoid of this form is the set of nonnegative integer solutions of a proportionally modular Diophantine inequality. The integers  $a, b$  and  $c$  are called the factor, modulus and proportionality, respectively. The following result is a generalization in  $\mathbb{R}^2$  of [49, Theorem 8] for convex body monoids

and semigroups and it provides an inequality which characterizes the elements of a convex body monoid of  $\mathbb{R}^2$  (the same works in higher dimensions).

Observe that if a ray intersects with  $F$  in only a point (respectively a segment), then the intersection of the ray with any other  $iF$  with  $i > 1$  is also a point (respectively a segment). We denote by  $\overline{PQ}$  the segment joining  $P$  and  $Q$ .

**PROPOSITION 2.2.** *Let  $\tau$  be a ray of  $L_{\mathbb{Q}_{\geq}}(F)$ . Then, for all  $X \in \mathbf{F} \cap \tau$  there exist  $a, b \in \mathbb{R}_{\geq}$  with  $1 < a < b$ , such that*

$$(9) \quad a \cdot d(X) \bmod b \leq d(X).$$

**PROOF.** If  $X \in \mathbf{F} \cap \tau$ , then there exists  $i \in \mathbb{N}$  such that  $X \in iF$ . If  $i = 0$ , then  $X = 0$  and there exist  $a, b \in \mathbb{R}_{\geq}$  such that the inequality is clearly satisfied.

Assume that  $X \in iF$ , with  $i > 0$ . We have two cases:

- If  $\tau \cap iF = \{X\}$ , then there exists  $P \in F$  such that  $X = iP$  and  $d(X) = id(P)$ . Taking now a number  $a \in (1, \infty)$  we obtain  $a < ai$  and  $ad(X) \bmod aid(P) = 0 \leq d(X)$ .
- If  $\tau \cap iF = \overline{PQ}$  (assume  $d(P) < d(Q)$ ), then  $X \in i\overline{PQ}$  and  $d(X)$  belongs to a submonoid of  $\mathbb{R}_{\geq}$  generated by  $[d(P), d(Q)]$ . By Theorem 8 of [49] we conclude there exist  $a, b \in (1, \infty)$  with  $a < b$  such that  $ad(X) \bmod b \leq d(X)$ .

□

From the above proposition it can be deduced that  $a$  and  $b$  depend only of the vector  $\overrightarrow{OX}$ . This fact allows us to characterize the elements of a convex body semigroup from an inequality. Denote by  $\tau$  the ray containing the point  $X$ .

In the following, when we talk about interior of  $\mathbf{F}$ , denoted by  $\text{int}(\mathbf{F})$ , we mean the set of elements in  $\mathbf{F}$  that are not in  $\tau_1 \cup \tau_2$  (the extremal rays of the cone spanned by  $\mathbf{F}$ ).

**COROLLARY 2.3.** *Let  $X \in \mathbb{N}^k$  and  $\tau$  be the ray (half-line) determined by  $X$ . Then  $X$  belongs to  $\text{int}(\mathbf{F})$  if and only if the following conditions are fulfilled:*

- (1)  $\tau \cap F$  is a segment  $\overline{PQ}$  with  $P, Q \in \text{int}(\mathbf{F})$ ,
- (2)  $\frac{d(Q)}{d(Q) - d(P)} d(X) \bmod \frac{d(P)d(Q)}{d(Q) - d(P)} \leq d(X)$ .

**PROOF.** It is straightforward from Proposition 2.2 and the proof of Theorem 8 in [49]. □

Let  $F$  be a convex body of  $\mathbb{R}_{\geq}^2$  with non-empty (topological) interior, and  $\tau_1, \tau_2$  be the extremal rays of  $L_{\mathbb{Q}_{\geq}}(F)$  (assume that the slope of  $\tau_1$  is greater than the slope of  $\tau_2$ ). Observe that  $\mathbf{F}$  is contained in the cone  $L_{\mathbb{Q}_{\geq}}(F)$ . We denote by  $\mathcal{C}$  the monoid  $L_{\mathbb{Q}_{\geq}}(F) \cap \mathbb{N}^2$ .

## 2. Finding a system of generators of convex body semigroups

The present section shows instrumental results that we will use to compute the minimal generating set for a convex body semigroup  $\mathcal{F}$  from the cone associated  $L_{\mathbb{Q}_{\geq}}(F) \cap \mathbb{N}^2$ .

Some of them are very specific and with strong hypothesis, but the reader must keep in mind that they are specifically made for dealing with convex body semigroups.

We start by showing how to compute the minimal generators of “linear slices” of  $\mathcal{F}$ .

LEMMA 2.4. *Let  $\tau$  be a ray and let  $P, Q \in \tau$  (assume  $d(P) < d(Q)$ ). Then the semigroup  $\mathcal{S} = (\bigcup_{i \in \mathbb{N}} i\overline{PQ}) \cap \mathbb{N}^2$  is finitely generated and there exists an algorithm for computing its minimal system of generators.*

PROOF. If  $\tau$  is the  $y$ -axis, then the set of  $y$ -coordinates of  $\mathcal{S}$  is a proportionally modular numerical semigroup. Hence we can use [49] to find the minimal generating system of  $\mathcal{S}$ . So we may assume that the first coordinate of  $P$  (and thus  $Q$ ) is nonzero. If  $\tau$  does not intersect  $\mathbb{N}^2 \setminus \{0\}$ , then  $\mathcal{S} = \{0\}$ , and trivially is finitely generated (this may happen if the slope of  $\tau$  is irrational or if  $\tau$  is not in the positive orthant of  $\mathbb{N}^2$ ). Thus, we assume that  $\tau$  is included in the positive orthant and that its slope is rational, say  $a/b$  with  $a, b$  positive coprime integers. This means that the elements in  $\mathcal{S}$  are of the form  $(x, ax/b)$ , with  $x \in \mathbb{N}$ , and consequently  $b \mid x$  (or in other words  $x \in b\mathbb{N}$ ).

Now let us consider  $\pi$  to be the projection on the  $x$ -coordinate. Then  $\pi(\mathcal{S})$  is a submonoid of  $\mathbb{N}$  (in fact of  $b\mathbb{N}$ ). Let us determine this monoid. Set  $I$  to be the interval  $[\pi(P), \pi(Q)]$ , and  $S$  be the proportionally modular numerical semigroup  $S = \bigcup_{i \in \mathbb{N}} iI$  ([49]). We prove that  $\pi(\mathcal{S}) = S \cap b\mathbb{N}$ .

Take  $x \in \pi(\mathcal{S})$ . Then as we have seen above,  $x \in b\mathbb{N}$ . Also there exists  $y, i \in \mathbb{N}$  such that  $(x, y) \in i\overline{PQ} \cap \mathbb{N}^2$ . Hence  $x \in i[\pi(P), \pi(Q)] \cap \mathbb{N} = iI \cap \mathbb{N} \subseteq S$ .

Now let  $x \in S \cap b\mathbb{N}$ . Take  $y = ax/b$ , which is in  $\mathbb{N}$ . Since  $x \in S$ , there exists  $i \in \mathbb{N}$  such that  $x \in iI \cap \mathbb{N} = i[\pi(P), \pi(Q)] \cap \mathbb{N}$ . It follows that  $(x, y) \in i\overline{PQ} \cap \mathbb{N}^2 \subseteq \mathcal{S}$ , and consequently  $x \in \pi(\mathcal{S})$ .

The fact that  $\mathcal{S}$  is finitely generated follows from the fact that  $\mathcal{S}$  is isomorphic to the its projection on the  $x$ -coordinate, which is a submonoid of  $\mathbb{N}$ . Let us see how to compute its minimal system of generators.

Consider  $S/b = \{x \in \mathbb{N} \mid bx \in S\}$ . This is again a numerical semigroup which can be calculated with [49, Lemma 18]. Observe that  $S \cap b\mathbb{N} = b(S/b)$ . Thus once we have a minimal generating system for  $S/b$ , we multiply its elements by  $b$  and we obtain a minimal generating system for  $S \cap b\mathbb{N}$ .  $\square$

Next result will help us to add the generators in the extremal rays of affine convex semigroups, once we have computed the generators in the interior. Though the hypothesis might seem extremely specific, this is actually the situation we will afford later.

LEMMA 2.5. *Let  $\{g_1, \dots, g_p\} \subset \mathbb{N}^2$  be the minimal system of generators of an affine semigroup  $M$ . Assume that  $\tau = g_1\mathbb{Q}_{\geq}$  is an extremal ray of  $L_{\mathbb{Q}_{\geq}}(M)$  and that  $g_1$  generates  $\mathbb{N}^2 \cap \tau$ . Let  $\{s_1, \dots, s_t\}$  be the minimal system of generators of a subsemigroup of  $\mathbb{N}^2 \cap \tau$ .*

Let  $M'$  be the semigroup generated by  $B = B_1 \cup B_2$  with

$$B_1 = \{s_1, \dots, s_t, g_2, \dots, g_p\},$$

$$B_2 = \bigcup_{i=2}^p \{g_i + g_1, g_i + 2g_1, \dots, g_i + (\lambda_t - 2)g_1, g_i + (\lambda_t - 1)g_1\},$$

where  $0 < \lambda_1 < \dots < \lambda_t$  are the integers such that  $s_i = \lambda_i g_1$ . Then the semigroup  $M'$  verifies:

- $M' \cap \tau = \langle s_1, \dots, s_t \rangle$ ,
- $M' \setminus \tau = M \setminus \tau$ .

PROOF. Clearly  $M' \cap \tau = \langle s_1, \dots, s_t \rangle$ .

Let  $g \in M' \setminus \tau$ . There exist  $\mu_1, \dots, \mu_p \in \mathbb{N}$  with  $\sum_{i=2}^p \mu_i \neq 0$ , such that  $g = \sum_{i=1}^p \mu_i g_i$ . Without loss of generality we can assume that  $\mu_2 \geq 1$ . There are three possibilities.

- If  $\mu_1 = 0$ , then it is trivial that  $g \in M' \setminus \tau$ .
- If  $\lambda_t > \mu_1 > 0$ , then  $g = \underbrace{g_2 + \mu_1 g_1}_{\in B_2} + (\mu_2 - 1) \underbrace{g_2}_{\in B_1} + \sum_{i=3}^p \mu_i \underbrace{g_i}_{\in B_1}$ .
- If  $\mu_1 \geq \lambda_t > 0$ , then there exist  $u, v \in \mathbb{N}$  such that  $\mu_1 = u\lambda_t + v$ , with  $\lambda_t > v$ . Thus,  $g = u \underbrace{(\lambda_t g_1)}_{\in B_1} + \underbrace{g_2 + v g_1}_{\in B_2} + (\mu_2 - 1) \underbrace{g_2}_{\in B_1} + \sum_{i=3}^p \mu_i \underbrace{g_i}_{\in B_1}$ .

In any of the above cases we obtain that  $g \in M' \setminus \tau$  and we can conclude that  $M' \setminus \tau = M \setminus \tau$  (trivially  $M' \setminus \tau \subset M \setminus \tau$ ).  $\square$

The first part of following lemma is a well known result particularized to affine semi-groups of  $\mathbb{N}^2$  (see [46, Lemma 1.3]).

LEMMA 2.6. *Let  $M \subset \mathbb{N}^2$  be an affine semigroup and  $a \in M \setminus \{0\}$ . The set  $M \setminus \{a\}$  is a semigroup if and only if  $a$  is a minimal generator of  $M$ . Moreover, if  $B = \{a, f_2, \dots, f_t\}$  is the minimal system of generators of  $M$ , then the semigroup  $M \setminus \{a\}$  is generated by*

$$\{f_2, \dots, f_t, f_2 + a, \dots, f_t + a, 2a, 3a\}.$$

PROOF. Assume that  $M \setminus \{a\}$  is a semigroup and that  $a$  is not a minimal generator of  $M$ . Then there exist  $a_1, a_2 \in M \setminus \{a\}$  such that  $a = a_1 + a_2$ , which contradicts the fact that  $M \setminus \{a\}$  is a semigroup.

Conversely, assume that  $a$  is a minimal generator of  $M$  (remind the semigroup  $M$  has a unique minimal system of generators). To prove that  $M \setminus \{a\}$  is a semigroup it is only necessary to show that the addition is an operation on this set. Let  $x, y \in M \setminus \{a\}$ , then  $x + y \in M \setminus \{a\}$  (if not we have that  $x + y = a$ , which is impossible because  $a$  is a minimal generator of  $M$ ).

Let  $B = \{a, f_2, \dots, f_t\}$  be the minimal set of generators of  $M$  (without loss of generality we assume that  $a$  is the first element of  $B$ ). Trivially,  $\{f_2, \dots, f_t, f_2 + a, \dots, f_t + a, 2a, 3a\} \subset M \setminus \{a\}$ . Let  $f \in M \setminus \{a\} \subset M$ , therefore there exists  $\lambda, \lambda_2, \dots, \lambda_t \in \mathbb{N}$  such

that  $f = \lambda a + \sum_{i=2}^t \lambda_i f_i$ . If  $\lambda \neq 1$ , there exist  $\alpha, \beta \in \mathbb{N}$  verifying that  $\lambda = 2\alpha + 3\beta$ , thus

$$f = \lambda a + \sum_{i=2}^t \lambda_i f_i = \alpha(2a) + \beta(3a) + \sum_{i=2}^t \lambda_i f_i.$$

If  $\lambda = 1$ , since  $a \notin M \setminus \{a\}$ , there exists  $\lambda_{i_0} \geq 1$ , such that

$$f = a + \sum_{i=2}^t \lambda_i f_i = (f_{i_0} + a) + (\lambda_{i_0} - 1)f_{i_0} + \sum_{i=2, i \neq i_0}^t \lambda_i f_i.$$

In any case,  $\{f_2, \dots, f_t, f_2 + a, \dots, f_t + a, 2a, 3a\}$  is a system of generators of  $M \setminus \{a\}$ .  $\square$

**COROLLARY 2.7.** *Let  $M$  be a finitely generated semigroup and  $A \subset M$  be a finite subset. If  $M \setminus A$  is a semigroup, then  $M \setminus A$  is a finitely generated semigroup. Furthermore, there exists an algorithm to compute a system of generators of  $M \setminus A$ .*

**PROOF.** Assume that  $A = \{a_1, \dots, a_n\} \subset M$  and assume that  $B$  is the minimal system of generators of  $M$ . Using the proof of Lemma 2.6, at least an element of  $A$  has to be an element of  $B$ . Take  $a_1 \in B$ , then we obtain that  $M_1 = M \setminus \{a_1\}$  is a subsemigroup of  $\mathbb{N}^2$ . Denote by  $B_1$  to the minimal system of generators of the semigroup  $M_1$  which is obtained from the system of generators of  $M_1$  constructed as in Lemma 2.6. Using again the above reasoning with the sets  $A_1 = A \setminus \{a_1\}$ ,  $M_1$  and  $B_1$ , we obtain a new semigroup  $M_2 = M_1 \setminus \{a_i\}$ , where  $a_i \in A_1 \cap B_1$  with  $i \in \{2, \dots, n\}$ . Since  $A$  is finite, this method stops after a finite number of steps and we obtain a finite system of generators  $B_n$  of the semigroup  $M_n = M \setminus A$ .  $\square$

To end this section we recall how to compute a minimal generating system (a Hilbert basis) of a cone in the positive orthant of  $\mathbb{N}^2$  with rational extremal rays. We follow [22], though there are other approaches using continued fractions (see for instance [36, Section 1.6]).

**LEMMA 2.8.** *Let  $a, b \in \mathbb{N}^2$  with  $\det(a, b) = 1$ . Then  $L_{\mathbb{Q}_{\geq}}(a, b) \cap \mathbb{N}^2 = \langle a, b \rangle$ .*

**PROOF.** Let  $x \in L_{\mathbb{Q}_{\geq}}(a, b) \cap \mathbb{N}^2$ . Then there exists  $\lambda, \mu \in \mathbb{Q}_{\geq}$  such that  $x = \lambda a + \mu b$ . The fact  $\det(a, b) = 1$  implies that  $\mathbb{Z}^2$  is generated as a group by  $\{a, b\}$ . Whence there exists  $\alpha, \beta \in \mathbb{Z}$  such that  $x = \alpha a + \beta b$ . Since  $\{a, b\}$  is also a basis of  $\mathbb{R}^2$  and coordinates with respect to a basis are unique, we obtain  $\lambda = \alpha$  and  $\mu = \beta$ . This yields  $\lambda, \mu \in \mathbb{N}$ , and consequently  $x \in \langle a, b \rangle$ . This proves  $L_{\mathbb{Q}_{\geq}}(a, b) \cap \mathbb{N}^2 \subseteq \langle a, b \rangle$ . The other inclusion is trivial.  $\square$

Observe that if  $a, b \in \mathbb{Q}^2$ , then  $L_{\mathbb{Q}_{\geq}}(a, b) = L_{\mathbb{Q}_{\geq}}(\lambda a, \lambda b)$  for every positive rational number  $\lambda$ . This in particular implies that whenever the extremal rays are rational, we can replace them with vectors with integer coordinates.

**LEMMA 2.9.** *Let  $a, b \in \mathbb{N}^2 \setminus \{0\}$ . Assume that there exists  $a = a_1, \dots, a_n = b \in \mathbb{N}^2$  such that for all  $i \in \{1, \dots, n-1\}$ ,  $\det(a_i, a_{i+1}) = 1$ . Then  $L_{\mathbb{Q}_{\geq}}(a, b) = L_{\mathbb{Q}_{\geq}}(a_1, a_2) \cup \dots \cup L_{\mathbb{Q}_{\geq}}(a_{n-1}, a_n)$ . In particular,  $L_{\mathbb{Q}_{\geq}}(a, b) \cap \mathbb{N}^2 = \langle a_1, \dots, a_n \rangle$ .*



PROOF. Write  $a_i = (a_{i1}, a_{i2})$ . The condition  $\det(a_i, a_{i+1}) = 1$  implies that the slope of the ray  $\mathbb{Q}_{\geq} a_i$  is greater than that of  $\mathbb{Q}_{\geq} a_{i+1}$ . Hence every element in  $L_{\mathbb{Q}_{\geq}}(a, b)$  must be in one of the cones  $L_{\mathbb{Q}_{\geq}}(a_i, a_{i+1})$  for some  $i$ . The second assertion now follows from Lemma 2.8.  $\square$

We say that a sequence of fractions  $\frac{a_{11}}{a_{12}} < \dots < \frac{a_{n1}}{a_{n2}}$  is a *Bézout sequence* if for every  $i \in \{1, \dots, n-1\}$ ,  $a_{i1}a_{(i+1)2} - a_{i2}a_{(i+1)1} = 1$ . We allow the fraction  $\frac{1}{0}$  to occur in the sequence. We say that the sequence is *proper* if it cannot be refined to another Bézout sequence, that is, one cannot find  $i < j$  with  $j \neq i+1$  such that  $\frac{a_{i1}}{a_{i2}} < \frac{a_{j1}}{a_{j2}}$  is a Bézout sequence. In [51, Theorem 7] there is a procedure to compute a proper Bézout sequence joining two fractions  $\frac{a_1}{a_2} < \frac{b_1}{b_2}$ .

Observe that for  $a = (a_1, a_2)$  and  $b = (b_1, b_2)$ ,  $\det(a, b) = 1$  if and only if  $a_1b_2 - a_2b_1 = 1$ . As in the proof of the Lemma 2.8, this in particular implies that  $\gcd(a_1, a_2) = \gcd(b_1, b_2) = 1$ . Also, the sequence of fractions  $\frac{b_1}{b_2} < \frac{a_1}{a_2}$  is a Bézout sequence.

PROPOSITION 2.10. *Let  $a, b \in \mathbb{Q}^2$ . Then there is a procedure to compute a minimal generating system of  $L_{\mathbb{Q}_{\geq}}(a, b) \cap \mathbb{N}^2$ .*

PROOF. As we have pointed out already, we can assume that  $a, b \in \mathbb{N}^2$ . Also we can take them so that their coordinates are coprime (just dividing by their greatest common divisor). Assume that  $a = (a_1, a_2)$  and that  $b = (b_1, b_2)$ . Without loss of generality we can also assume that  $\frac{a_1}{a_2} < \frac{b_1}{b_2}$ . Construct as explained in [51] a proper Bézout sequence joining  $\frac{a_1}{a_2}$  and  $\frac{b_1}{b_2}$ . Assume that this sequence is  $\frac{a_1}{a_2} = \frac{p_{11}}{p_{12}} < \dots < \frac{p_{n1}}{p_{n2}} = \frac{b_1}{b_2}$ . Set  $\alpha_i = (p_{i1}, p_{i2})$  for  $i \in \{1, \dots, n\}$ . As a consequence of Lemma 2.9,  $L_{\mathbb{Q}_{\geq}}(a, b) \cap \mathbb{N}^2 = \langle \alpha_1, \dots, \alpha_n \rangle$ .

In order to prove that  $\{\alpha_1, \dots, \alpha_n\}$  is a minimal generating system, we use that the Bézout sequence we used to define it is proper and that in this setting there exists  $h \in \{1, \dots, n\}$  such that

$$p_{11} \geq p_{21} \geq \dots \geq p_{h1} \leq p_{(h+1)1} \leq \dots \leq p_{n1}$$

(this is a direct consequence of [51, Corollary 18]).  $\square$

As a direct consequence of the proof of this last result, the minimal generators of  $L_{\mathbb{Q}_{\geq}}(a, b) \cap \mathbb{N}^2$  can be arranged so that their slopes are in a (strictly) decreasing sequence. Hence we obtain the following corollary.

COROLLARY 2.11. *Let  $a, b \in \mathbb{Q}^2$  and let  $\{m_1, \dots, m_k\}$  be a minimal generating system of  $L_{\mathbb{Q}_{\geq}}(a, b) \cap \mathbb{N}^2$ . For every  $i \neq j$ ,  $m_i \notin L_{\mathbb{Q}_{\geq}}(m_j)$ . In particular, for  $i \in \{1, 2\}$ ,  $(L_{\mathbb{Q}_{\geq}}(a, b) \cap \mathbb{N}^2) \cap \tau_i = \langle m_{j_i} \rangle$  for some  $j_i \in \{1, \dots, k\}$ .*

**2.1. Circle semigroups.** Let  $C$  be the circle with center  $(a, b)$  and positive radius  $r$ , which is a particular case of convex body. Denote by  $C_i$  the circle with center  $(ia, ib)$  and radius  $ir$ , that is,  $C_i = iC$ . Let  $\mathcal{S} = \bigcup_{i=0}^{\infty} C_i \cap \mathbb{N}^2$  be the semigroup of the non-negative points inside  $C$  and its multiples  $C_i$ . Again, denote by  $\tau_1$  and  $\tau_2$  the extremal rays of

$L_{\mathbb{Q}_{\geq}}(C \cap \mathbb{R}_{\geq}^2) = \{\sum_{i=1}^p q_i a_i \mid p \in \mathbb{N}, q_i \in \mathbb{Q}_{\geq}, a_i \in C \cap \mathbb{R}_{\geq}^2\}$ , choosing the ray with greatest slope<sup>1</sup> as  $\tau_1$ . Let  $\mathcal{C}$  denote the positive integer cone  $L_{\mathbb{Q}_{\geq}}(C \cap \mathbb{R}_{\geq}^2) \cap \mathbb{N}^2$ . In this setting,  $\text{int}(\mathcal{C}) = \mathcal{C} \setminus \{\tau_1, \tau_2\}$ .

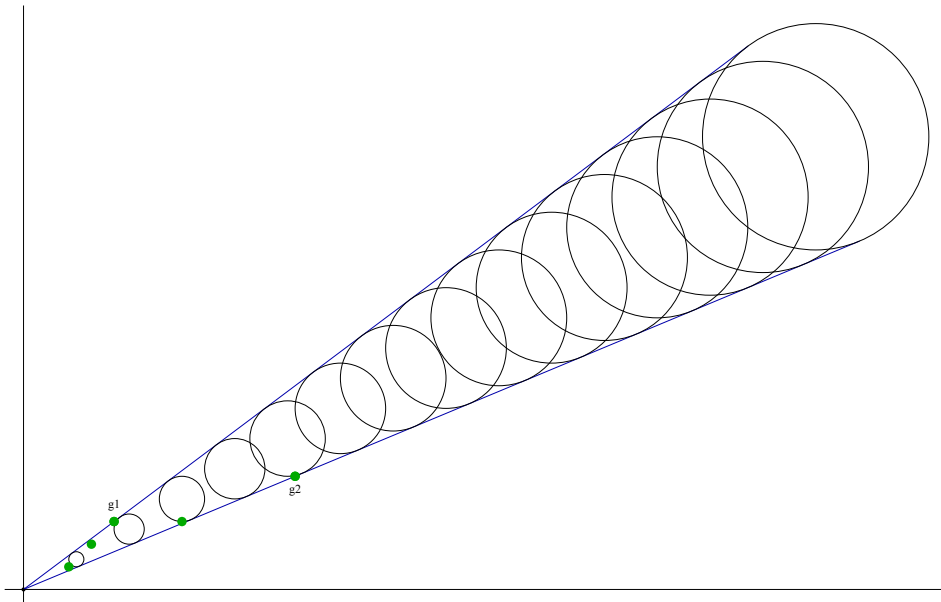


FIGURE 2. The minimal generator set of the semigroup of the cone generated by the circle with center  $(7/3, 4/3)$  and radius  $1/3$ . The integer vectors  $g_1$  and  $g_2$  are the generators of the rays.

Consider the circle  $C$  centered in  $(7/3, 4/3)$  with radius  $1/3$  and the sequence of circles  $C_i$ . The integer cone  $\mathcal{C}$  has minimal generating set  $\{(4, 3), (12, 5), (2, 1), (3, 2), (7, 3)\}$  (the green points in Figure 2). In the next sections we will show how to obtain  $\mathcal{S}$  from this set.

2.1.1. *Computing the minimal generators of the rays.* In order to find the minimal generators of  $\mathcal{C} = L_{\mathbb{Q}_{\geq}}(C \cap \mathbb{R}_{\geq}^2) \cap \mathbb{N}^2$  we first find the pair of tangent lines to the circle that passes through  $(0, 0)$ , and intersects in one point to the circle, to get the cone extremal rays. We take into account the case when the circle cuts  $x$ -axis or  $y$ -axis, in which case the intersection will be a segment. It will be shown (Theorem 2.16) that the intersection of rays and  $C$  must have rational points in order to  $\mathcal{S}$  be finitely generated. Hence we assume that the extremal rays are generated by a rational point. We can now use Proposition 2.10 to compute a minimal generating system of  $\mathcal{C}$ .

If an extremal ray  $\tau$  is tangent to the circle  $C$ , then the semigroup of elements in  $\mathcal{S}$  that are in this ray is generated by multiples of the tangent point. Let  $P = (a/b, c/d)$  be the tangent point (the irrational setting is not finitely generated as mentioned above, so we focus in the rational case). Assume that  $\gcd(a, b) = \gcd(c, d) = 1$ . Then  $\text{lcm}(b, d)P$  generates  $\tau \cap \mathcal{S}$ .

<sup>1</sup>We will use the name of the rays  $\tau_1$  and  $\tau_2$  to reference its slopes, where necessary.

If we are not in the case described in the preceding paragraph, then  $C$  cuts one of the axis (or both) in a segment. Thus this axis becomes an extremal ray of  $\mathcal{C}$ , and the set of elements in  $\mathcal{S}$  and in this extremal ray are a proportionally modular numerical semigroup. Consequently we can compute its minimal generators by using either [49] or [51].

2.1.2. *Affine convex body semigroup generators.* At this point, from the previous section, we have a set of minimal generators of the cone  $\mathcal{C}$ , say  $\{g_1, \dots, g_n\}$ . Using this set as the input data, we want to find the corresponding set of minimal generators of the circle convex body semigroup.

Assume without loss of generality that  $g_1 \in \tau_1$  and  $g_2 \in \tau_2$ . From the way the minimal generating set of  $\mathcal{C}$  is constructed, it follows that no other minimal generators will be in the extremal rays of  $\mathcal{C}$ . Therefore  $\langle g_i \rangle = \tau_i \cap \mathcal{C}$ , for  $i \in \{1, 2\}$ . Hence we can use Lemma 2.5 to replace  $g_1$  and  $g_2$  in  $\mathcal{C}$  with the generators of  $\mathcal{S}$  that are in the extremal rays.

So for now, we focus on the interior points of the cone. The next results are needed to prove that  $\text{int}(\mathcal{C}) \setminus \text{int}(\mathcal{S})$  has a finite number of points if  $C \subset \mathbb{R}_{\geq}^2$  (Lemma 2.15).

LEMMA 2.12. *Let  $\tau$  be a ray with a rational point. Let  $g \in \tau \cap \mathbb{Q}_{\geq}^2$ ,  $s \in \tau \cap \mathbb{N}^2$  and  $\vec{u} \in \mathbb{R}^2$ . Define  $R_i$  to be the parallelogram determined by the elements  $g + (i-1)s$ ,  $g + is$  and  $g + (i-1)s + \vec{u}$  with  $i \in \mathbb{N}$ . If  $R_1 \subset \mathbb{R}_{\geq}^2$ , then  $R_i \cap \mathbb{N}^2 = (R_1 \cap \mathbb{N}^2) + (i-1)s$ .*

PROOF. By construction  $R_i = R_1 + (i-1)s$  for every  $i \in \mathbb{N}$ . Since  $s \in \mathbb{N}^2$ , then  $R_i \cap \mathbb{Z}^2 = (R_1 \cap \mathbb{Z}^2) + (i-1)s$ . In the case  $R_1 \subset \mathbb{R}_{\geq}^2$ , we obtain  $R_i \cap \mathbb{N}^2 = (R_1 \cap \mathbb{N}^2) + (i-1)s$ .  $\square$

LEMMA 2.13. *Suppose that  $C \cap \tau_2$  is a point ( $\tau_2$  is tangent to  $C$ ). If  $P_i$  is the closest point to  $\tau_2$  belonging to  $C_i \cap C_{i+1}$ <sup>2</sup>, then  $\lim_{i \rightarrow \infty} d(P_i, \tau_2) = 0$ .*

PROOF. Observe that whenever  $C_i$  intersects  $C_{i+1}$ , the set  $C_i \cap C_{i+1}$  is a compact, and thus  $P_i$  exists. Denote by  $h_i$  the distance  $d(P_i, \tau_2)$ . Without loss of generality, assume that  $\tau_2$  is the line  $\{y = 0\}$ . This is possible since the distances between the points of our construction are invariant under rotation. Graphically the situation is as shown in Figure 3.

Since the slope of  $\tau_2$  is zero, the circles have radius  $bi$  and therefore  $h_i = d(P_i, \tau_2)$  is equal to the second coordinate of  $P_i$ .

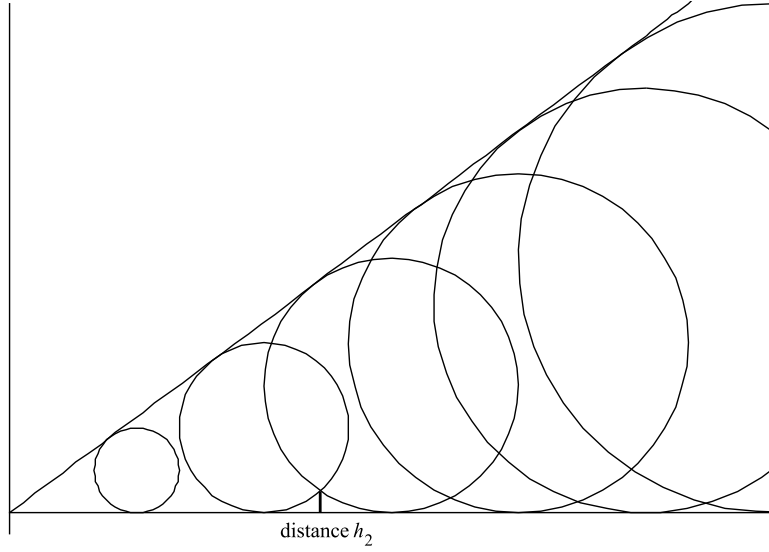
With these hypothesis, the point  $P_i$  is the solution of the following system of equations closest to the axis  $OX$ :

$$\begin{cases} C_i & \equiv & (x - ai)^2 + (y - bi)^2 & = & (bi)^2 \\ C_{i+1} & \equiv & (x - a(i+1))^2 + (y - b(i+1))^2 & = & b^2(i+1)^2. \end{cases}$$

That is,

$$x = \frac{a^3 + 2a^3i + \sqrt{-a^4b^2 + 4a^2b^4i + 4a^2b^4i^2}}{2(a^2 + b^2)},$$

<sup>2</sup>For the initial values of  $i$  it is possible to obtain that  $C_i \cap C_{i+1} = \emptyset$ , see Figure 3.

FIGURE 3. Distance  $h_2$ .

$$y = \frac{a^2 b^2 (1 + 2i) - a \sqrt{-a^2 b^2 (a^2 - 4b^2 i - 4b^2 i^2)}}{2b(a^2 + b^2)}.$$

Then the distance is

$$(10) \quad h_i = d(P_i, \tau_2) = \frac{a^2 b^2 (1 + 2i) - a \sqrt{-a^2 b^2 (a^2 - 4b^2 i - 4b^2 i^2)}}{2b(a^2 + b^2)}.$$

It is easy to prove that  $\lim_{i \rightarrow \infty} h_i = 0$ . □

REMARK 2.14. Assume that  $C \cap \tau_1$  has only a point ( $\tau_1$  is tangent to  $C$ ). Denote by  $P'_i$  the point of  $C_i \cap C_{i+1}$  closest to  $\tau_1$  (whenever this intersection is not empty). Using the symmetry of  $\bigcup_{i=0}^{\infty} C_i$  with respect to the line joining the centers of the circles, we obtain that  $d(P'_i, \tau_1) = d(P_i, \tau_2)$ .

LEMMA 2.15. *Let  $C \subset \mathbb{R}_{\geq}^2$  be a circle. There exists  $d \in \mathbb{R}_{\geq}$  such that*

$$\{P \in \text{int}(\mathcal{C}) \mid d(P) > d\} \subset \mathcal{S}.$$

*Furthermore,  $d$  can be computed algorithmically.*

PROOF. Consider two rectangles in  $\mathcal{C}$  whose bases are segments determined by the first two consecutive points of the semigroup in  $\tau_1$  for the first rectangle and in  $\tau_2$  for the second, and with height (the same for both) a value small enough to obtain no points of  $\mathbb{N}^2$  in them (except in their bases). Denote by  $d'$  this height. For  $\tau_2 = \{y = 0\}$ , these rectangles are as in Figure 4.

Denote by  $T_1, T_2 \in \mathcal{S}$  the vertices of the base of the rectangle over the line  $\tau_2$ .

Consider now the region of the cone obtained applying to the above rectangle all the translations defined by the vector  $\overrightarrow{OT_1}$  and all its positive multiples. This construction is

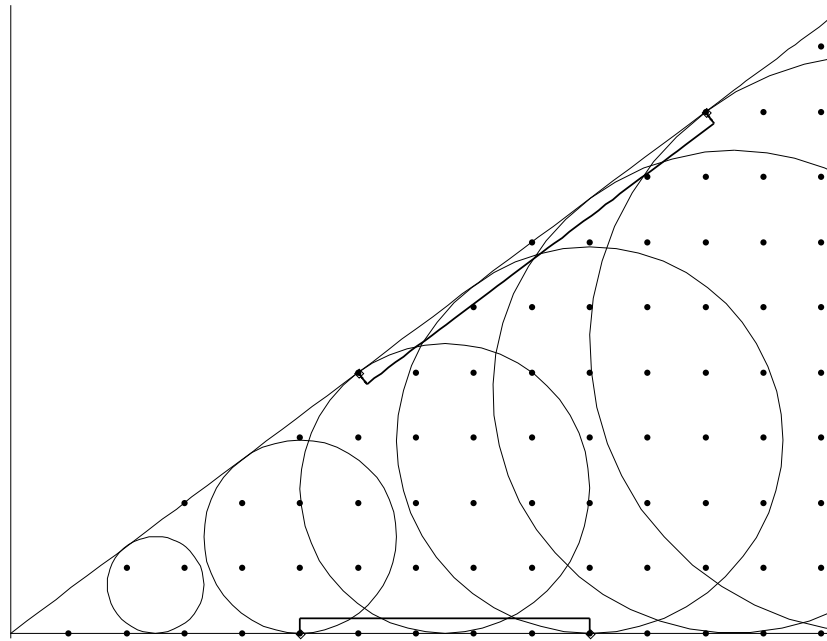


FIGURE 4. Construction 1.

done over  $\tau_1$  and over  $\tau_2$  (see Figure 5). In this region there are no integer points (Lemma 2.12).

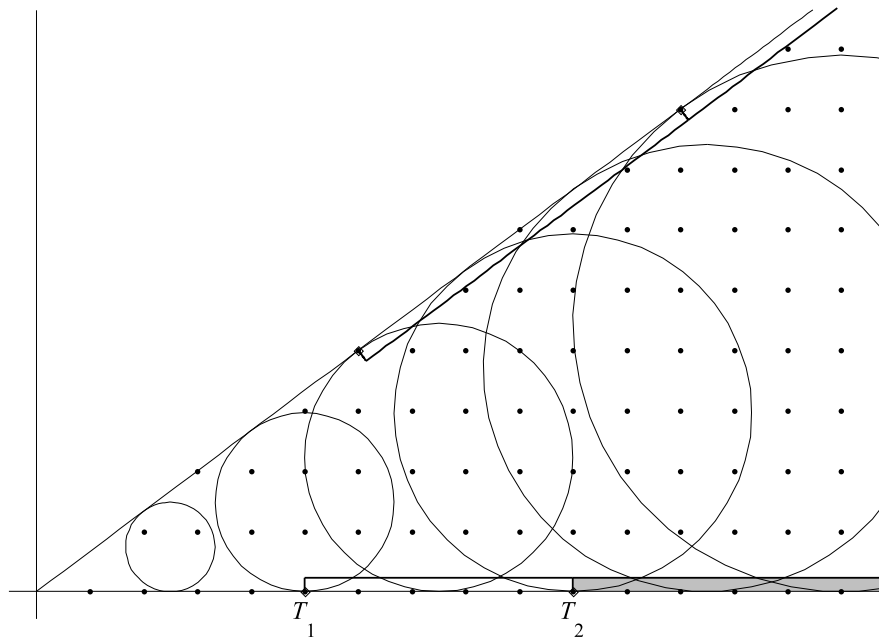


FIGURE 5. Construction 2.

Let  $i_0 \in \mathbb{N}$  be the first term of the sequence of heights  $\{h_i\}_i$  (defined in (10)) such that  $h_{i_0} < d'$ . Lemma 2.13 asserts the existence of  $i_0$ .

Then there exists  $d \in \mathbb{R}_{\geq}$  determined by the circle  $C_{i_0}$  such that  $\{P \in \text{int}(\mathcal{C}) \mid d(P) > d\} \subset \bigcup_{i \geq i_0} C_i \cap \mathbb{N}^2 \subset \mathcal{S}$ .  $\square$

In Figure 6, observe that  $i_0$  from the above prove equals 6.

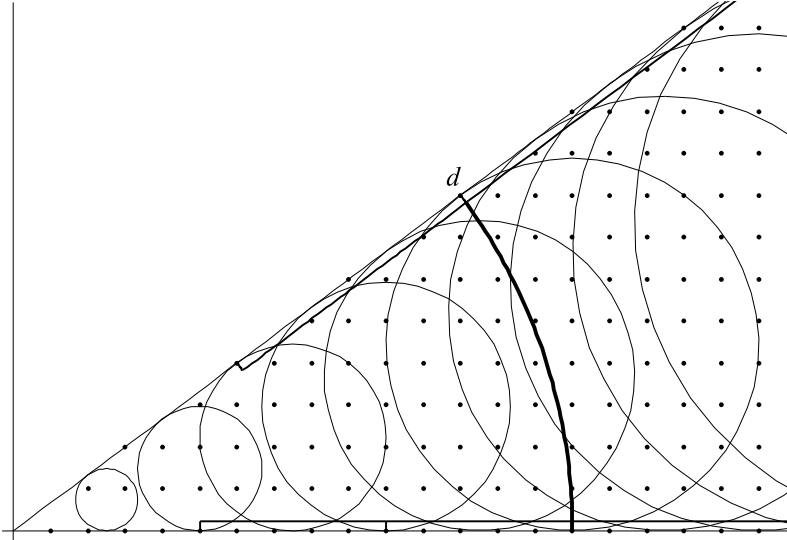


FIGURE 6. Construction 3.

From the generating set of  $\mathcal{C}$ , and the generators of  $\mathcal{S} \cap \tau_1$  and  $\mathcal{S} \cap \tau_2$ , using now Lemma 2.5 we can construct  $\mathcal{S}'$  such that  $\mathcal{S}' \setminus \tau_1 \cup \tau_2 = \mathcal{S} \setminus \tau_1 \cup \tau_2$  and  $\mathcal{S}' \cap \tau_i = \mathcal{S} \cap \tau_i$  for  $i \in \{1, 2\}$ . It follows from Lemma 2.15 that  $\mathcal{S}' \setminus \mathcal{S}$  has finitely many elements and consequently we can now use Corollary 2.7 to compute a minimal generating system of  $\mathcal{S}$ . This proves one of the directions of the following theorem. Recall that membership to  $\mathcal{S}$  is computationally easy to check.

**THEOREM 2.16.** *The semigroup  $\mathcal{S}$  is finitely generated if and only if  $C \cap \tau_1$  and  $C \cap \tau_2$  have rational points. Furthermore, in such case the minimal system of generators of  $\mathcal{S}$  can be computed algorithmically.*

**PROOF.** The sufficiency is already proven. For the necessity assume that  $\mathcal{S}$  is finitely generated and that  $C \cap \tau_1 \subseteq \mathbb{R}_{\geq}^2 \setminus \mathbb{Q}^2$ . Let  $G = \{s_1, s_2, \dots, s_r\}$  be a system of generators of  $\mathcal{S}$ . This implies that  $\mathcal{S} \cap \tau_1 = \emptyset$ . Consider  $s_k \in G$  such that the vector  $\overrightarrow{Os_k}$  has maximum slope respect to the points of  $G$ . There exists at least an element  $Q \in \mathbb{Q}^2$  in the interior of the cone delimited by  $\tau_1$  and the ray defined by  $s_k$ . There exists  $u \in \mathbb{N}$  such that  $uQ$  belongs to a circle  $C_{i_0} \cap \mathbb{N}^2 \subseteq \mathcal{S}$ . However  $uQ$  is not in  $\langle G \rangle$ , which is a contradiction. If  $C \cap \tau_2$  has not rational points, the proof follows analogously.  $\square$

EXAMPLE 2.17. We complete now the example of the circle  $C$  centered in  $(7/3, 4/3)$  with radius  $1/3$ . By using the procedure proposed in Proposition 2.10, we have for the integer cone  $\mathcal{C}$  the generators

$$\{(4, 3), (12, 5), (2, 1), (3, 2), (7, 3)\}$$

(see Figure 2 on page 32).

Now using Lemma 2.5, the semigroup  $\mathcal{S}'$  is minimally generated by

$$\left\{ (2, 1), (3, 2), (7, 3), (7, 5), (11, 8), (15, 11), (19, 14), (23, 17), (27, 20), (31, 23), \right. \\ \left. (32, 24), (96, 40), (19, 8), (31, 13), (43, 18), (55, 23), (67, 28), (79, 33), (91, 38) \right\}.$$

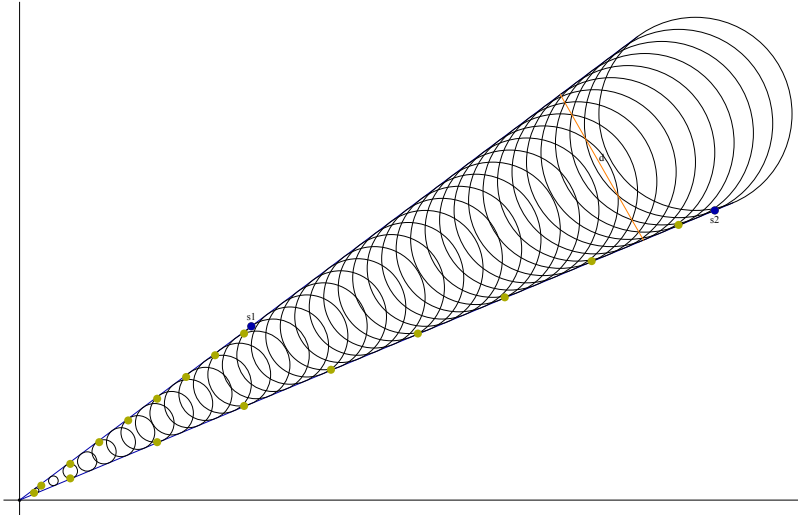
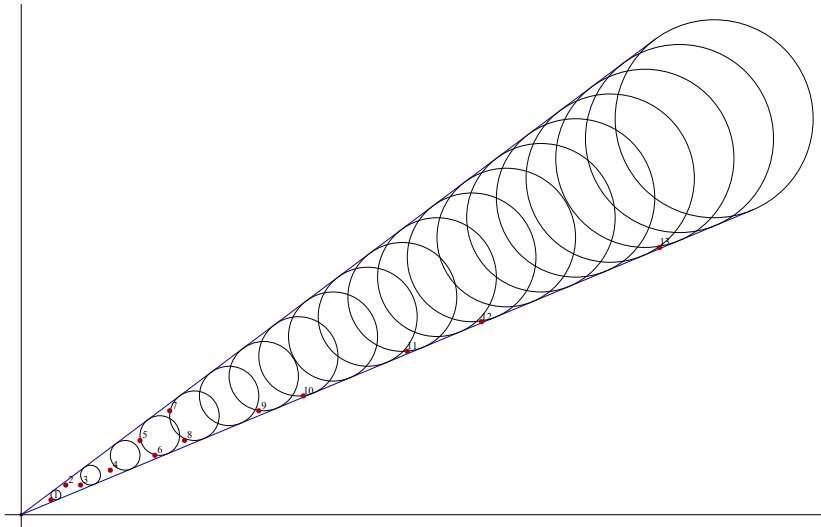
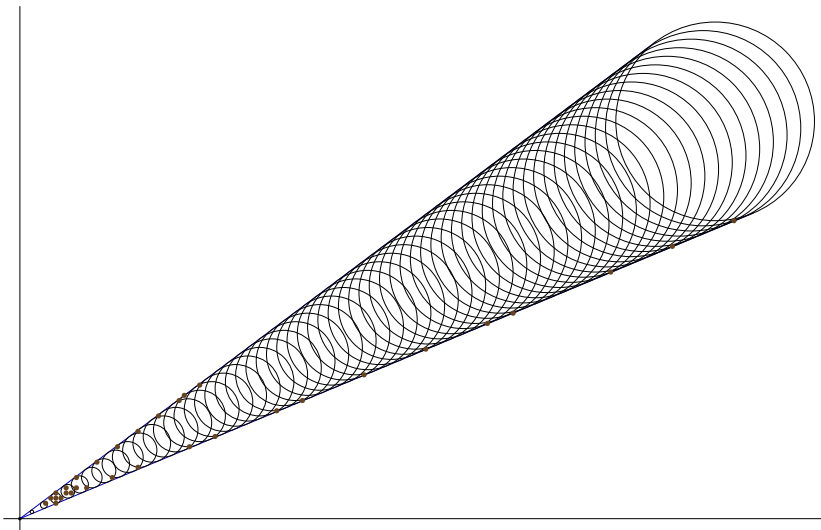


FIGURE 7. Generators of the semigroup  $\{\mathcal{S}' \cap \tau_1\} \cup \{\mathcal{S}' \cap \tau_2\} \cup \text{int}(\mathcal{C})$ .

This semigroup is equal to  $\mathcal{S}$  in their extreme rays and equal to  $\mathcal{C}$  in its interior (see Figure 7).

The finite set  $\mathcal{S}' \setminus \mathcal{S}$  has 13 points (see Figure 8). By using Corollary 2.7, we eliminate every point of  $\mathcal{S}' \setminus \mathcal{S}$  from  $\mathcal{S}'$  obtaining the minimal system of generators of  $\mathcal{S}$  (see Figure 9):

$$\left\{ (5, 3), (6, 4), (7, 3), (7, 4), (7, 5), (8, 4), (9, 5), (9, 6), (10, 5), (11, 6), (11, 8), \right. \\ (13, 6), (15, 11), (18, 8), (19, 14), (23, 10), (23, 17), (27, 20), (31, 23), (32, 24), \\ (33, 14), (35, 26), (38, 16), (50, 21), (55, 23), (67, 28), (79, 33), (91, 38), (96, 40), \\ \left. (115, 48), (127, 53), (139, 58) \right\}.$$

FIGURE 8.  $\mathcal{S}' \setminus \mathcal{S}$ .FIGURE 9.  $\mathcal{S}$  minimal generating set.

The results of this section are used in the developed `CircleSG` Mathematica<sup>3</sup> package, which is described in Appendix A. The implementation presented in our work [17] is slightly different to that given in [19], mainly due to the fact that we are using [22], which simplifies the explanation of the algorithm for the step where it computes the minimal generating set of the cone associated. Fortunately, we do not only obtain a simplification of the theory, but also a faster procedure to make this initial computation.

<sup>3</sup>Every reference to the term Mathematica in this document, is referred to the set of programs of Wolfram Research, except where it is otherwise stated. Mathematica is a registered trademark of Wolfram Research Inc.



**2.2. Convex polygonal semigroups.** In this section some results on semigroups generated by convex polygons are presented and the affine convex polygonal semigroups are characterized.

Denote by  $P_i = (p_{i1}, p_{i2})$  with  $i \in \{1, \dots, n\}$  the vertices of a compact convex polygon  $F \subset \mathbb{R}_{\geq}^2$  ordered in the clockwise direction. We set  $\mathbf{P} = \{P_1, \dots, P_n\}$  and denote by  $\mathcal{P}$  the associated semigroup,  $\mathcal{P} = \bigcup_{i \in \mathbb{N}} iF \cap \mathbb{N}^2$ . As in the preceding section, we denote by  $\mathcal{C} = \mathbf{L}_{\mathbb{Q}_{\geq}}(F) \cap \mathbb{N}^2$ .

**PROPOSITION 2.18.** *If  $\mathbf{P} \subset \mathbb{Q}_{\geq}^2$ , then  $\mathcal{P}$  is finitely generated. Furthermore, there exists an algorithm which determines its minimal system of generators.*

**PROOF.** Let  $\mathbf{P} = \{P_1, \dots, P_n\}$  the set of vertices of  $F$  and consider the set of points  $\mathbf{P}' = \{(P_1, 1), \dots, (P_n, 1)\} \subset \mathbb{Q}_{\geq}^3$ . Take now the cone  $\overline{\mathcal{C}} = \mathbf{L}_{\mathbb{Q}_{\geq}}(\mathbf{P}') \cap \mathbb{N}^3$ . Since this cone is defined by rational inequalities, it is finitely generated.

Let  $(x, y, z) \in \overline{\mathcal{C}}$ . Then there exists  $\lambda_1, \dots, \lambda_n \in \mathbb{Q}_{\geq}$  such that  $(x, y, z) = \sum_{i=1}^n \lambda_i P'_i$ . Thus  $(x, y) = \sum_{i=1}^n \lambda_i P_i$  and  $z = \sum_{i=1}^n \lambda_i \in \mathbb{N}$ . Hence  $(x, y) = \sum_{i=1}^n \frac{\lambda_i}{z} z P_i$ , with  $\sum_{i=1}^n \frac{\lambda_i}{z} = 1$ . This implies that  $(x, y) \in zF$ , and consequently  $(x, y) \in \mathcal{P}$ .

Now take  $(x, y) \in \mathcal{P}$ . Then there exists  $z \in \mathbb{N}$  such that  $(x, y) \in zF$ . Hence  $(x, y) = \sum_{i=1}^n \lambda_i z P_i$  with  $\lambda_1, \dots, \lambda_n \in \mathbb{Q}_{\geq}$  and  $\sum_{i=1}^n \lambda_i = 1$ . This implies that  $(x, y, z) = \sum_{i=1}^n (z \lambda_i) P'_i$ , and clearly  $z \lambda_1, \dots, z \lambda_n \in \mathbb{Q}_{\geq}$ , which means that  $(x, y, z) \in \overline{\mathcal{C}}$ .

Therefore, a system of generators of  $\mathcal{P}$  is the set formed by the projection onto the first two coordinates of a system of generators of  $\overline{\mathcal{C}}$ . From this set of generators of  $\mathcal{P}$  one can compute its minimal system of generators.  $\square$

We will show that even if some of the vertices have not rational coordinates, the finitely generated condition can prevail. Actually the condition is that in the intersection of  $F$  with extremal rays there are points with rational coordinates. The idea is that we can perturbate slightly the vertices in the interior of  $\mathcal{C}$  so that we can choose them to be rational and  $\mathcal{P}$  remains the same, as occurs with the intervals defining proportionally modular numerical semigroups (see [49]). In order to prove this fact, we will slice  $F$  in at most three pieces. Two triangles if the intersection of  $F$  with the rays are single vertices, and a central polygon (see Figure 13), for which the complement in the corresponding cone will be finite.

Suppose now that  $\tau_1 \cap F = \{P_1\}$ . Denote by  $V_i$  the intersection of the lines passing through  $iP_1$  and  $iP_2$ , and  $(i+1)P_n$  and  $(i+1)P_1$  for every  $i \in \mathbb{N}$ . Note that for the initial values of  $i$  it is possible that these points are out  $\mathcal{C}$  (see Figure 10).

**LEMMA 2.19.** *Every point  $V_i$  belongs to a parallel line to  $\tau_1$ .*

**PROOF.** Clearly  $\overline{(iP_1)(iP_2)}$  and  $\overline{((i+1)P_n)((i+1)P_1)}$  are not parallel, their lengths increase with no limit and keep one of their vertices in the ray  $\tau_1$ . The lines passing through these segments intersect in only one point  $V_i$  for any  $i \geq 0$ .

After some basic computations the reader can check that the distance between  $V_i$  and  $\tau_1$  is constant and equal to

$$\left| \frac{p_{12}^2 p_{21} p_{n1} - p_{12} p_{21} p_{11} p_{n2} + a_1^2 p_{n2} p_{22} - p_{11} p_{22} p_{12} p_{n1}}{(-p_{22} p_{n1} + p_{11} p_{22} + p_{12} p_{n1} + p_{n2} p_{21} - p_{n2} p_{11} - b_1 p_{21}) \sqrt{p_{12}^2 + p_{11}^2}} \right|.$$

Thus, the points  $V_i$  are in a line parallel to  $\tau_1$ .  $\square$

Thus, in this case there exists  $i_0$  such that  $V_i \in L_{\mathbb{Q}_{\geq}}(F)$  for all  $i \geq i_0$ . It follows that

$$\mathcal{P} \setminus (\tau_1 \cup \tau_2) \subset \text{int}(\mathcal{C}) \setminus \bigcup_{i \geq i_0} \text{triangle}(\{iP_1, (i+1)P_1, V_i\}).$$

For instance, in Figure 10  $i_0 = 5$ .

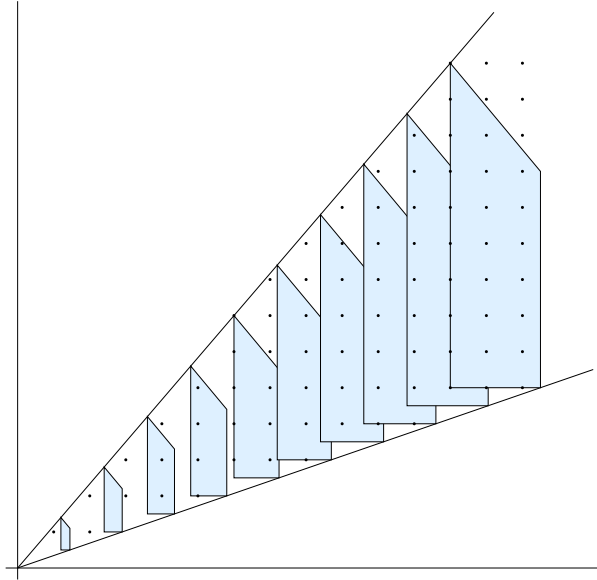


FIGURE 10. Image of a convex polygonal semigroup.

For the sake of simplicity we have used the points  $P_1, P_2$  and  $P_n$  in the above results, but the result can be extended to the intersection of  $F$  and an extremal ray when this intersection is only a point.

We focus now our attention when  $F$  is a particular triangle.

**PROPOSITION 2.20.** *Let  $F$  be a triangle delimited by  $\{P_1, P_2, P_3\}$  with  $P_1 \in \mathbb{Q}_{\geq}^2$  and  $P_2, P_3 \in \mathbb{R}_{\geq}^2 \setminus \mathbb{Q}^2$ , such that  $P_1 \in \tau_1$  and  $\overline{P_2 P_3} \subset \tau_2$ , where  $\tau_1$  and  $\tau_2$  are the extremal rays of  $L_{\mathbb{Q}_{\geq}}(F)$  and the slope of  $\tau_2$  is rational. Then  $\mathcal{P}$  is finitely generated and there exists an algorithm to compute its minimal system of generators.*

**PROOF.** As in the case of circles, the semigroup  $\tau_1 \cap \mathcal{P}$  is generated by a multiple of  $P_1$ , say  $s_1$ .

In light of Lemma 2.19 the elements  $V_i$  are all in the same line. Let  $j_0$  be the least positive integer such that  $V_{j_0} \in L_{\mathbb{Q}_{\geq}}(F)$ . Then  $j_0 P_1 + s_1$  is a multiple of  $P_1$ , since  $s_1$  is a multiple of  $P_1$ . Hence there exists a positive integer  $j_1$  such that  $j_1 P_1 = j_0 P_1 + s_1$ .

Let  $T_1$  the set of integer points in the triangle with vertices  $O$ ,  $j_0P_1$  and  $j_0P_2$ . Let  $T_2$  be the parallelogram determined by  $j_0P_1$ ,  $j_1P_1$  and  $V_{j_0}$ . Define  $T = T_1 \cup T_2$  (see Figure 11).

From the construction of  $T_2$ , Lemma 2.19, and Lemma 2.12, we know that the elements of  $\mathcal{P}$  that are not in  $\mathcal{P} \cup T_1$  are in a translation of  $T_2$ . Hence the distance from the elements with integer coordinates that are in  $L_{\mathbb{Q}_{\geq}}(F) \setminus \mathcal{P}$  to those in  $\mathcal{P}$  is reached in the region  $T_1 \cup T_2$ , and thus is a positive amount. We can move in  $\tau_2$  the vertices  $P_2$  and  $P_3$

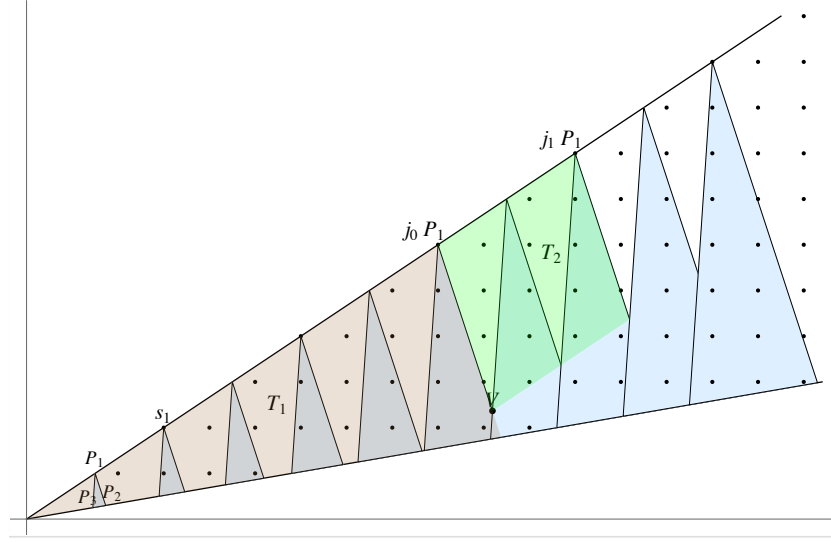


FIGURE 11. Set  $T = T_1 \cup T_2$ .

until we reach two rational points  $P'_2$  and  $P'_3$  (since the slope of  $\tau_2$  is rational, there are an infinite number of possibilities to take these points into segments including  $\overline{P_2P_3}$ ) to form a new triangle  $F'$  with rational vertices  $\{P_1, P'_2, P'_3\}$  such that  $F \subseteq F'$  and  $iF'$  does not contain any point with integer coordinates that is not in  $\mathcal{P}$ . It follows that

$$\mathcal{P} = \left( \bigcup_{i \in \mathbb{N}} iF' \right) \cap \mathbb{N}^2,$$

as shown in Figure 12, where dotted lines correspond to the new rational triangle with rational vertices. As the vertices of  $F'$  are rational, the semigroup  $\mathcal{P}$  is finitely generated and its minimal system of generators can be computed as explained in Proposition 2.18.  $\square$

The following result considers convex polygons with two sides as segments over the rays of the cone. These will play the role of the central slice in the general case.

**PROPOSITION 2.21.** *Let  $F \subset \mathbb{R}_{\geq}^2$  be a convex polygon fulfilling that  $\tau_1$  and  $\tau_2$  have rational points and  $\tau_1 \cap F$  and  $\tau_2 \cap F$  are segments. Then  $\mathcal{P}$  is finitely generated and there exists an algorithm which determines its minimal system of generators.*

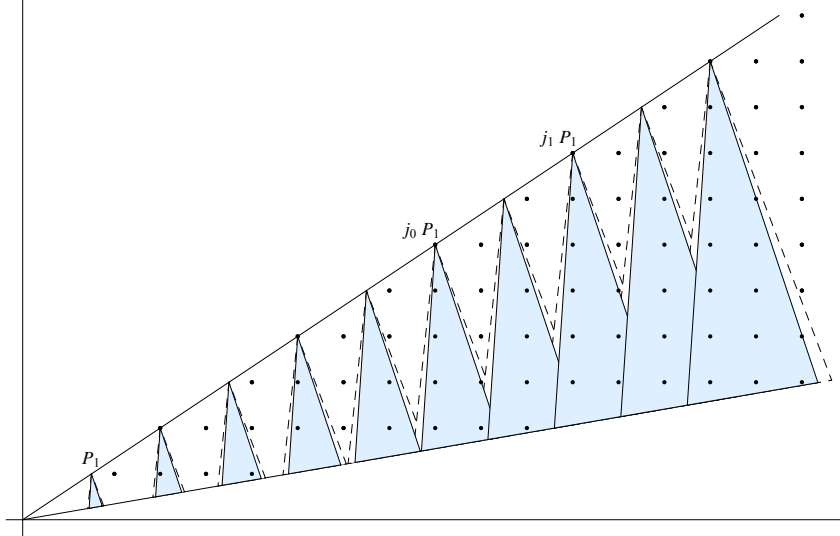


FIGURE 12. Construction of a triangle with rational vertices.

PROOF. Let  $\tau_1 \cap F = S_1 = \overline{P_1 P_2}$  and  $\tau_2 \cap F = S_2 = \overline{P_{l+1} P_l}$ . By construction there exists a least integer  $j$ , such that the segments  $jS_1$  and  $(j+1)S_1$  overlap, and the same for  $S_2$ . Let  $T$  be the triangle with vertices  $O$ ,  $jP_1$  and  $jP_{l+1}$ . Every element in  $\mathcal{C}$  that is not in  $T$  belongs to  $\mathcal{P}$ , which in particular means that there are only finitely many elements in  $\mathcal{C} \setminus (\tau_1 \cup \tau_2)$  that are not in  $\mathcal{P}$ . We can proceed now as with circle convex body affine semigroups.

By using Lemma 2.4 we compute generators for  $\mathcal{P} \cap \tau_1$  and  $\mathcal{P} \cap \tau_2$ . Next we construct a semigroup  $\mathcal{P}'$  verifying  $\mathcal{C}' \cap \tau_1 = \mathcal{P} \cap \tau_1$ ,  $\mathcal{C}' \cap \tau_2 = \mathcal{P} \cap \tau_2$  and  $\mathcal{C}' \setminus (\tau_1 \cup \tau_2) = \mathcal{C} \setminus (\tau_1 \cup \tau_2)$  (use Lemma 2.5). It follows that  $\mathcal{C}' \setminus \mathcal{P}$  has finitely many elements. Thus by using Lemma 2.6 we find a minimal generating system of  $\mathcal{P}$ .  $\square$

**THEOREM 2.22.** *The semigroup  $\mathcal{P}$  is finitely generated if and only if  $F \cap \tau_1$  and  $F \cap \tau_2$  contain rational points. Furthermore, in such case there exists an algorithm to compute the minimal system of generators of  $\mathcal{P}$ .*

PROOF. The necessity goes as in the proof of Theorem 2.16.

For the sufficiency, assume the intersections of  $F$  with  $\tau_1$  and  $\tau_2$  contain rational points. We will slice our polygon so that the pieces fit in one of the above propositions.

- (1) If  $\tau_1 \cap F$  and  $\tau_2 \cap F$  are segments, the result is just Proposition 2.21.
- (2) If  $\tau_1 \cap F$  has only a point and  $\tau_2 \cap F$  is a segment, then take  $\tau'_1$  a ray with rational point such that the intersection of the polygon  $F$  with the region delimited by  $\tau_1$  and  $\tau'_1$  is a triangle  $F'_1$ . The set  $F'_2 = F \setminus F'_1$  verifies the conditions of Proposition 2.21.

The minimal system of generators of the semigroup generated by  $F'_1$  can be computed in light of Proposition 2.20.

Analogously, the minimal system of generators of the semigroup generated by  $F'_2$  can be computed with Proposition 2.21. Since  $\mathcal{P}$  is the union of the semigroups generated by  $F'_1$  and  $F'_2$ , the semigroup  $\mathcal{P}$  is finitely generated by the union of the above systems of generators.

- (3) If  $\tau_1 \cap F$  and  $\tau_2 \cap F$  are two points, we proceed as follows. Take  $\tau'_1$  and  $\tau'_2$  two rays with rational points such that the polygons obtained from the intersection of  $F$  and the region delimited by  $\tau_1$  and  $\tau'_1$ , and by  $\tau_2$  and  $\tau'_2$ , are two triangles. The intersection of the polygon  $F$  and the region delimited by  $\tau'_1$  and  $\tau'_2$  verifies the condition of Proposition 2.21 (see Figure 13).

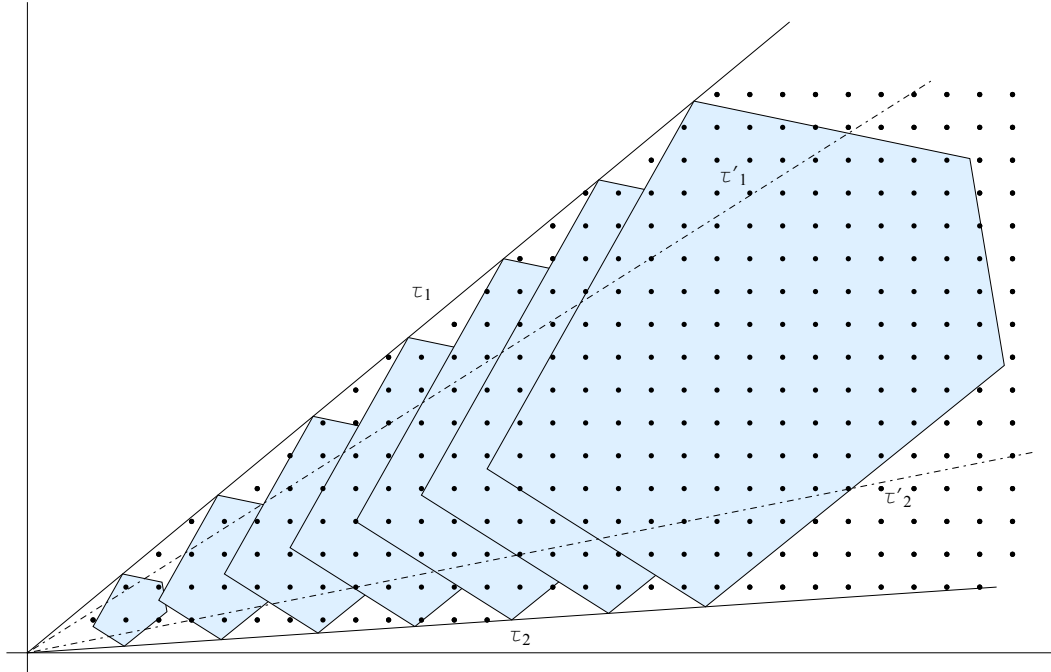


FIGURE 13. Polygon with only a vertex in each extremal rays.

Once again, a system of generators of  $\mathcal{P}$  can be obtained by applying Proposition 2.20 and Proposition 2.21 to the above regions.

In any case the semigroup  $\mathcal{P}$  is finitely generated and its minimal system of generated can be computed algorithmically.  $\square$

### 3. Affine convex body semigroups and Buchsbaum rings

Recall that a *numerical semigroup* is a submonoid of  $\mathbb{N}$  with finite complement in  $\mathbb{N}$  and from [46, Proposition 1.2] every affine semigroup in  $\mathbb{N}$  is isomorphic to a numerical semigroup (just dividing the affine semigroup by its greatest common divisor). Let  $S$  be a numerical semigroup. Fix  $m \in S \setminus \{0\}$  and let  $s \in S$ . Then ([46, Lemma 1.6]) there exists unique  $k, w \in \mathbb{N}$  such that

- $s = km + w$ ,

- $w \in S$  and  $w - m \notin S$ .

Actually there are exactly  $m$  elements  $w$  in  $S$  such that  $w - m \notin S$  (this is known as the Apéry set of  $m$  in  $S$ , we will come back to this concept later).

We can think of a direct generalization to this fact for two dimensions. Let  $M$  be an affine semigroup with  $M \subseteq \mathbb{N}^2$ . If we fix  $m \in M \setminus \{0\}$ , the set of elements  $w \in M$  such that  $w - m \notin M$  has infinite cardinality. So we do not recover a result as nice as for the numerical case.

Assume that  $\{m_1, \dots, m_e\}$  is the minimal generating system of  $M$ . Also suppose without loss of generality that  $m_1$  and  $m_2$  generate the extremal rays of  $L_{\mathbb{Q}_{\geq}}(M)$  (in this way  $M$  is not isomorphic to a numerical semigroup and  $L_{\mathbb{Q}_{\geq}}(M) = L_{\mathbb{Q}_{\geq}}(m_1, m_2)$ ). The set of elements  $w \in M$  such that  $w - m_1 \notin M$  and  $w - m_2 \notin M$  has finitely many elements (see for instance [44]). So we can think about writing any  $s \in M$  as  $s = k_1 m_1 + k_2 m_2 + w$  with  $(k_1, k_2) \in \mathbb{N}^2$  and  $w \in M$  such that  $w - m_1, w - m_2 \notin M$ . We say that  $M$  is *Cohen-Macaulay* if  $(k_1, k_2)$  and  $w$  are unique (these monoids are named in this way because it is known that  $M$  is Cohen-Macaulay if and only the semigroup ring  $\mathbb{k}[M]$  is Cohen-Macaulay in the classical Commutative Algebra sense; see [44], though we will not deal with the Commutative Algebra definition). Notice that for the numerical semigroup case, every  $m \in S \setminus \{0\}$  becomes a generator of the unique extremal ray of  $\mathbb{Q}_{\geq} (= L_{\mathbb{Q}_{\geq}}(m) = L_{\mathbb{Q}_{\geq}}(S))$ , and so this concept generalizes the idea of numerical semigroup in two dimensions.

Let  $M$  be as above, we define the *closure* of  $M$  as  $\bar{M} = \{a \in \mathbb{N}^2 \mid a + M \subseteq M\}$ . We say that  $M$  is *Buchsbaum* if and only if  $\bar{M}$  is Cohen-Macaulay (again this name is inherited from the Buchsbaum property of the semigroup ring  $\mathbb{k}[M]$ , see [24]).

The above idea can be generalized to any simplicial affine semigroup of  $\mathbb{N}^r$  for any positive integer  $r$ . By *simplicial* we mean that the cone spanned by the monoid is the same as the cone spanned by  $r$  of its minimal generators (these do not be to be unique). Notice that any affine semigroup in  $\mathbb{N}^2$  is simplicial. Since we are working in dimension two, we will omit this adjective.

Convex affine semigroups that are Cohen-Macaulay are characterized in [21]. In this section we are interested in determining whether or not a given affine convex body semigroup is Buchsbaum. Some examples of papers devoted to the study of Buchsbaum affine semigroup rings are [3, 4, 24, 34, 53, 55] and the references therein. Our aim is to find easy examples of Buchsbaum semigroup rings.

Notice that if  $a \in \bar{M}$ , then in particular  $a + m_1, a + m_2 \in M \subseteq \mathcal{C} = L_{\mathbb{Q}_{\geq}}(M) \cap \mathbb{N}^2$ . It follows that  $a \in \mathcal{C}$ . Hence  $M \subseteq \bar{M} \subseteq \mathcal{C}$ .

We are going to use the following two results from [21]. For  $M \subseteq \mathbb{N}^2$  an affine semigroup, let  $m_1 \in \tau_1$  be the element of  $M \cap \tau_1$  with less module. Define  $m_2 \in \tau_2$  analogously.

**COROLLARY 2.23.** [21, Corollary 2] *Let  $M \subseteq \mathbb{N}^2$ , the following conditions are equivalent:*

- (1)  $M$  is Cohen-Macaulay.

(2) For all  $a \in \mathcal{C} \setminus M$ ,  $a + m_1$  or  $a + m_2$  does not belong to  $M$ .

LEMMA 2.24. [21, Lemma 3] *Let  $M \subseteq \mathbb{N}^2$  be an affine semigroup such that  $\text{int}(\mathcal{C}) \setminus \text{int}(M)$  is a non-empty finite set. Then  $M$  is not Cohen-Macaulay.*

**3.1. Buchsbaum affine circle semigroups.** Let  $C \subseteq \mathbb{R}^2$  be a circle. Recall that  $\mathcal{S} = \bigcup_{i=0}^{\infty} C_i \cap \mathbb{N}^2$  is the circle semigroup associated to  $C$ , and that Theorem 2.16 characterizes these circle semigroups that are affine (finitely generated). In this section, we consider that  $\mathcal{S}$  is always a simplicial affine circle semigroup. Let  $\overline{\mathcal{S}}$  be the closure of  $\mathcal{S}$ , and let  $\{m_1, m_2, \dots, m_k\}$  be the minimal system of generators of  $\mathcal{S}$ .

PROPOSITION 2.25. *Let  $\mathcal{S} \subset \mathbb{N}^2$  be an affine circle semigroup. The semigroup  $\mathcal{S}$  is Buchsbaum if and only if  $\text{int}(\mathcal{C}) = \text{int}(\overline{\mathcal{S}})$  and  $\overline{\mathcal{S}} \cap \tau_j$  is generated only by one element for  $j \in \{1, 2\}$ .*

PROOF. Since  $\mathcal{S}$  is Buchsbaum if and only if  $\overline{\mathcal{S}}$  is Cohen-Macaulay, we prove that  $\overline{\mathcal{S}}$  is Cohen-Macaulay if and only if  $\text{int}(\mathcal{C}) = \text{int}(\overline{\mathcal{S}})$  and  $\overline{\mathcal{S}} \cap \tau_j$  is generated by only one element for  $j \in \{1, 2\}$ .

Assume that  $\overline{\mathcal{S}}$  is Cohen-Macaulay and suppose that  $\text{int}(\mathcal{C}) \setminus \text{int}(\overline{\mathcal{S}}) \neq \emptyset$ . Let  $m'_j$  be an element in the minimal system of generators of  $\overline{\mathcal{S}} \cap \tau_j$  with  $j \in \{1, 2\}$ . Since there exists a real number  $d > 0$  such that  $\{a \in \text{int}(\mathcal{C}) \mid d(a) > d\} \subset \mathcal{S}$  (see Lemma 2.15), the set  $\text{int}(\mathcal{C}) \setminus \text{int}(\mathcal{S})$  is finite, and thus  $\text{int}(\mathcal{C}) \setminus \text{int}(\overline{\mathcal{S}})$  is finite too. Take  $a \in \text{int}(\mathcal{C}) \setminus \text{int}(\overline{\mathcal{S}})$  verifying that  $d(a) = \max\{d(a') \mid a' \in \text{int}(\mathcal{C}) \setminus \text{int}(\overline{\mathcal{S}})\}$ . The elements  $a + m'_1$  and  $a + m'_2$  are in  $\overline{\mathcal{S}}$  and by Corollary 2.23 the semigroup  $\overline{\mathcal{S}}$  is not Cohen-Macaulay which is a contradiction.

Let us prove now that  $\overline{\mathcal{S}} \cap \tau_j$  is generated by only one element for  $j \in \{1, 2\}$ . We consider two different cases depending on if  $\mathcal{S} \cap \tau_j$  is generated only by one element or not.

- If there exist  $m_j \in \mathbb{N}^2$  such that  $\mathcal{S} \cap \tau_j = \langle m_j \rangle$  for some  $j \in \{1, 2\}$ , then for every  $a \in (\tau_j \setminus \mathcal{S}) \cap \mathbb{N}^2$  we have that  $a + m_j \in \tau_j \setminus \mathcal{S}$  and hence we have that  $a \notin \overline{\mathcal{S}}$ . Then  $\overline{\mathcal{S}} \cap \tau_j = \mathcal{S} \cap \tau_j = \langle m_j \rangle$ .
- We consider now the case that  $\mathcal{S} \cap \tau_j$  is minimally generated by two or more elements with  $j \in \{1, 2\}$ . We have that  $C \cap \tau_j$  is a segment and that  $(\mathcal{C} \setminus \mathcal{S}) \cap \tau_j$  is a finite non-empty set. This implies that  $(\mathcal{C} \setminus \overline{\mathcal{S}}) \cap \tau_j$  is finite. If it is a non-empty set, take the element  $a \in (\mathcal{C} \setminus \overline{\mathcal{S}}) \cap \tau_j$  such that  $d(a) = \max\{d(a') \mid a' \in (\mathcal{C} \setminus \overline{\mathcal{S}}) \cap \tau_j\}$ . It verifies that  $a + m'_1$  and  $a + m'_2$  belong to  $\overline{\mathcal{S}}$  and therefore  $\overline{\mathcal{S}}$  is not Cohen-Macaulay (Corollary 2.23). Hence  $\mathcal{C} \cap \tau_j = \overline{\mathcal{S}} \cap \tau_j$ . By Corollary 2.11,  $\mathcal{C} \cap \tau_j = \langle m \rangle$  for some  $m \in \mathbb{N}^2$ , and consequently  $\overline{\mathcal{S}} \cap \tau_j = \langle m \rangle$ .

Assume now that  $\text{int}(\mathcal{C}) = \text{int}(\overline{\mathcal{S}})$  and that  $\overline{\mathcal{S}} \cap \tau_j$  is generated by only one element for  $j \in \{1, 2\}$ . Let  $m'_j \in \mathbb{N}^2$  such that  $\overline{\mathcal{S}} \cap \tau_j = \langle m'_j \rangle$  for  $j \in \{1, 2\}$ . From the first assumption, any  $a \in \mathcal{C} \setminus \overline{\mathcal{S}}$  has to be on the rays of  $\mathcal{C}$ , either  $\tau_1$  or  $\tau_2$ . If we suppose that  $a + m'_1 \in \overline{\mathcal{S}}$  and  $a + m'_2 \in \overline{\mathcal{S}}$ , then for  $a \in \tau_1$ , saying  $a + m'_1 \in \overline{\mathcal{S}}$  is equivalent to say that  $a + m'_1 = tm'_1$  for

some  $t \in \mathbb{N}$ , then  $a = (t-1)m'_1 \in \overline{\mathcal{F}}$ . This contradicts that  $a \in \mathcal{C} \setminus \overline{\mathcal{F}}$ . The same argument can be repeated for  $a \in \tau_2$ . Finally, by Corollary 2.23,  $\overline{\mathcal{F}}$  is Cohen-Macaulay.  $\square$

By using the above proof, the conditions of Proposition 2.25 can be determined from the initial circle. To check whether  $\text{int}(\mathcal{C}) = \text{int}(\overline{\mathcal{F}})$ , we only have to compute the finite set  $\text{int}(\mathcal{C}) \setminus \text{int}(\overline{\mathcal{F}})$  by using the bound provided by Lemma 2.15. The second condition is satisfied whether  $C \cap \tau_j$  is a point or, in case  $C \cap \tau_j$  is a segment, if the generator of  $\mathcal{C} \cap \tau_j$  belongs to  $\overline{\mathcal{F}}$ . Both conditions can be checked algorithmically.

EXAMPLE 2.26. Let  $C$  be the circle with center  $(7/5, 4/5)$  and radius  $1/5$ . Computing with the program `CircleSG` (see [19]), we obtain that the affine circle semigroup<sup>4</sup>  $\mathcal{S}$  associated to  $C$  is minimally generated by the set

$$\begin{aligned} & \left\{ (4,2), (5,3), (6,3), (6,4), (7,3), (7,4), (7,5), (8,5), (9,4), (9,6), (10,7), \right. \\ & (11,8), (15,11), (19,8), (19,14), (23,17), (27,20), (31,13), (31,23), (32,24), \\ & \left. (35,26), (43,18), (55,23), (67,28), (79,33), (91,38), (96,40) \right\} \end{aligned}$$

and  $\text{int}(\mathcal{C}) \setminus \text{int}(\mathcal{S})$  is  $\{(2,1), (3,2)\}$  (see Figure 14). It is easy to check that the points

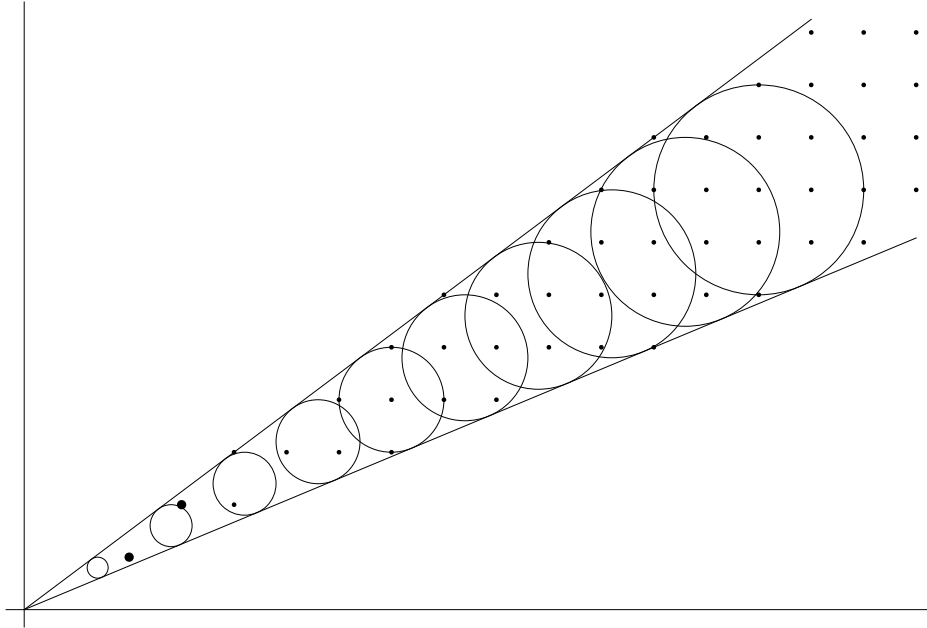


FIGURE 14. Affine circle semigroup associated to the circle with center  $(7/5, 4/5)$  and radius  $1/5$ .

$(2,1)$  and  $(3,2)$  belong to  $\overline{\mathcal{F}}$ . Thus, we obtain  $\text{int}(\mathcal{C}) = \text{int}(\overline{\mathcal{F}})$ . Besides,  $\overline{\mathcal{F}} \cap \tau_1 = \langle (32,24) \rangle$  and  $\overline{\mathcal{F}} \cap \tau_2 = \langle (96,40) \rangle$ . By Proposition 2.25, the affine circle semigroup  $\mathcal{S}$  is Buchsbaum.

<sup>4</sup>Note that  $C \cap \tau_1 = (32/25, 24/25)$  and  $C \cap \tau_2 = (96/65, 8/13)$ .



**3.2. Buschsbaum affine convex polygonal semigroups.** We assume that  $\mathcal{P}$  is a simplicial affine convex polygonal semigroup. Denote  $\overline{\mathcal{P}}$  be the closure of  $\mathcal{P}$ . As in Section 2.2, we assume that  $\mathbf{P} = \{P_1, \dots, P_n\}$ .

In this section, we consider different subsets of the cone  $\mathcal{C}$  and some points and lines in  $L_{\mathbb{Q}_{\geq}}(F \cap \mathbb{R}_{\geq}^2)$ . We distinguish two cases,  $F \cap \tau_i$  is a point or it is formed by more than one point.

Assume  $F \cap \tau_1 = \{P_1\} \subset \mathbf{P}$ . Recall that  $\mathcal{P} \cap \tau_1$  is generated by a multiple of  $P_1$ , say  $m_1$ . Also, in this setting, there exists a least positive integer  $j$  such that  $j\overline{P_1P_2} \cap (j+1)\overline{P_1P_n}$  is not empty. Let  $\{V_1\} = j\overline{P_1P_2} \cap (j+1)\overline{P_1P_n}$ . Recall that Lemma 2.19 ensures that the intersections of  $i\overline{P_1P_2} \cap (i+1)\overline{P_1P_n}$ ,  $i \in \mathbb{N} \setminus \{0\}$ , are all in a line parallel to  $\tau_1$ . Denote this line by  $v_1$ .

Denote by  $T_1$  the triangle with vertex set  $\{O, P_1, V_1 - jP_1\}$ , and by  $\mathring{T}_1$  its topological interior. Note that  $\mathring{T}_1 \cap \mathcal{P} = \emptyset$  and also that  $(\mu P_1 + (\mathring{T}_1 \cup (\overline{OP_1} \setminus \{O, P_1\}))) \cap \mathcal{P} = \emptyset$  for all  $\mu \in \mathbb{Z}_{\geq}$ . This construction allows us to define the set

$$L_1 = \{D + \lambda m_1 \mid D \in \overline{(jP_1)V_1} \text{ and } \lambda \in \mathbb{Q}_{\geq}\} \cap \mathcal{C}$$

whose elements are in  $\mathcal{P}$  or they are in  $\bigcup_{\mu \in \mathbb{N}, \mu \geq j} (\mu P_1 + (\mathring{T}_1 \cup (\overline{OP_1} \setminus \{O, P_1\})))$  (see

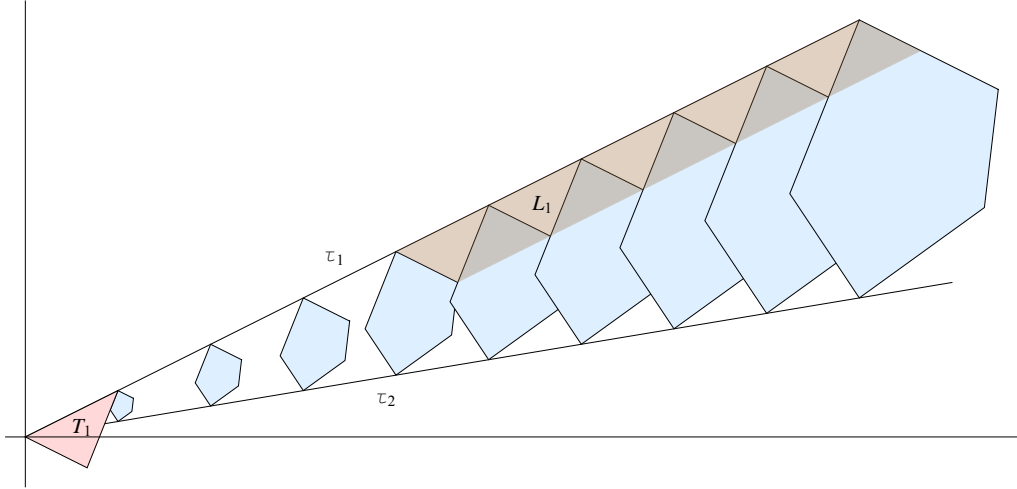
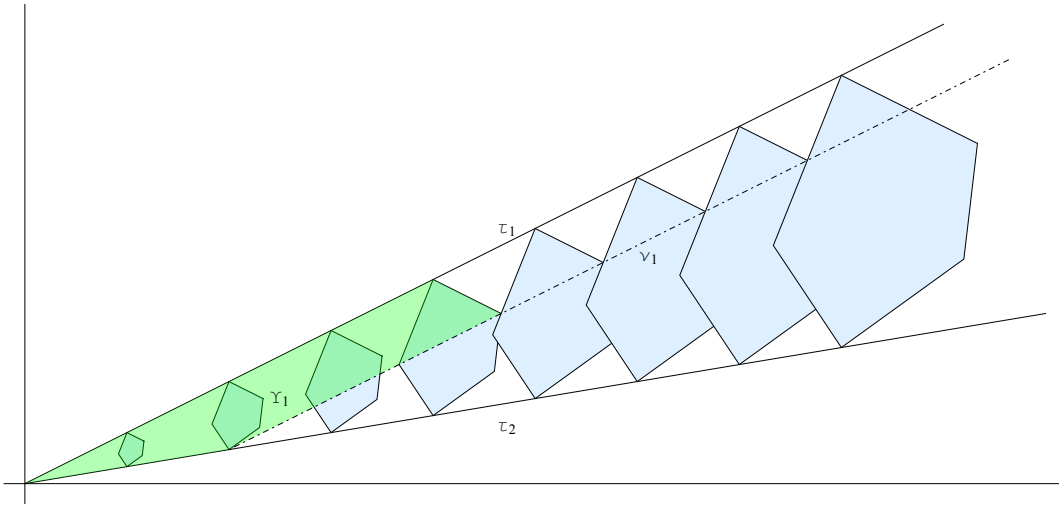


FIGURE 15. Regions  $T_1$  and  $L_1$ .

Figure 15). The elements of  $L_1$  verify that if  $P \in L_1 \setminus \mathcal{P}$ , then  $P + m_1 \notin \mathcal{P}$ , and thus  $P \notin \overline{\mathcal{P}}$ . This implies that  $\mathcal{P} \cap L_1 = \overline{\mathcal{P}} \cap L_1$ . Denote by  $Y_1$  the finite set  $\text{ConvexHull}(\{O, jP_1, V_1, v_1 \cap \tau_2\}) \cap \mathbb{N}^2$  (see Figure 16).

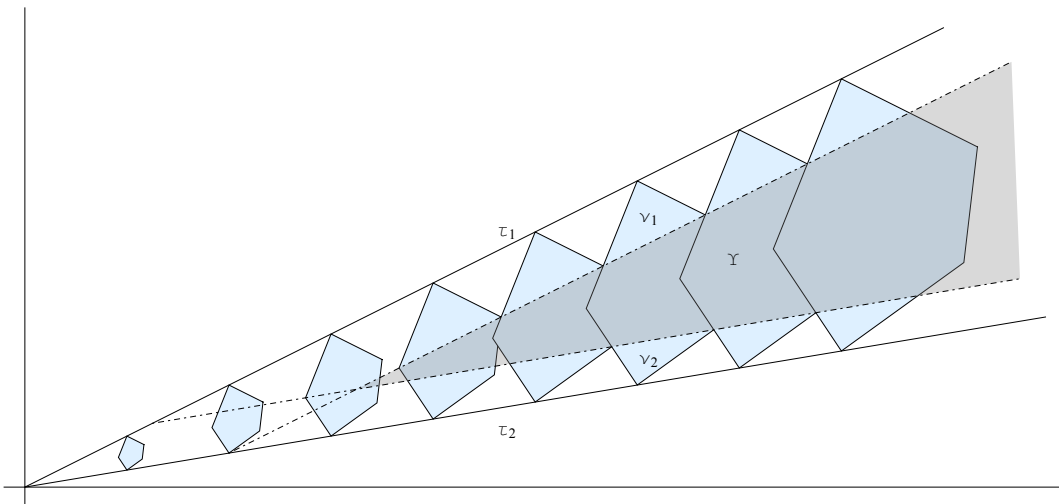
Analogously, if the set  $F \cap \tau_2 = \{P_1\} \subset \mathbf{P}$ , we call it again  $P_1$  for sake of simplicity, there exists the least integer  $j$  such that  $j\overline{P_1P_2} \cap (j+1)\overline{P_1P_n}$  is equal to  $\{V_2\}$ . Let  $T_2$  be the triangle with vertex set  $\{O, P_1, V_2 - jP_1\}$ , and denote by  $v_2$  the line containing the points  $\{h\overline{P_1P_2} \cap (h+1)\overline{P_1P_n} \mid h \geq j, h \in \mathbb{N}\}$  and by  $L_2$  the set  $\{D + \lambda m_2 \mid D \in \overline{(jP_1)V_2} \text{ and } \lambda \in \mathbb{Q}_{\geq}\} \cap \mathcal{C}$ . All of the properties of these sets are analogous to the properties of the sets

FIGURE 16. Region  $\Upsilon_1$ .

defined previously for  $\tau_1$ . Denote by  $\Upsilon_2$  the finite set  $\text{ConvexHull}(\{O, jP_2, V_2, v_2 \cap \tau_1\}) \cap \mathbb{N}^2$ .

In case  $F \cap \tau_i$  is a segment for some  $i \in \{1, 2\}$ , we take  $v_i = \tau_i$  and  $\Upsilon_i = \{O\}$ .

We define the set  $\Upsilon = (Q + L_{\mathbb{Q}_{\geq}}(F)) \cap \mathbb{N}^2 \subset \mathcal{C}$  with  $\{Q\} = v_1 \cap v_2 \subset L_{\mathbb{Q}_{\geq}}(F)$  (see Figure 17). Note that the boundary lines of the set  $\Upsilon$  intersect with two different sides of

FIGURE 17. Region  $\Upsilon$ .

the polygon  $i_0F$  when  $i_0 \gg 0$  and therefore the sets  $\Upsilon \setminus \mathcal{P}$  and  $\Upsilon \setminus \overline{\mathcal{P}}$  are finite. The last set we define is the finite set  $\Upsilon' = \{a \in (\Upsilon_1 \cup \Upsilon_2) \setminus \overline{\mathcal{P}} \mid a + m'_1, a + m'_2 \in \overline{\mathcal{P}}\}$ , where  $m'_i$  is a minimal generator of  $\overline{\mathcal{P}}$  in  $\tau_i$ ,  $i \in \{1, 2\}$ . It is straightforward to prove that the cone  $\mathcal{C}$  is the union of  $L_1, L_2, \Upsilon_1, \Upsilon_2$  and  $\Upsilon$ .

**THEOREM 2.27.** *Let  $\mathcal{P}$  be a simplicial affine convex polygonal semigroup. Then*

- (1) if  $\text{int}(\mathcal{C}) = \text{int}(\overline{\mathcal{P}})$ , the semigroup  $\mathcal{P}$  is Buchsbaum if and only if for  $j = \{1, 2\}$ ,  $\overline{\mathcal{P}} \cap \tau_j$  is generated by only one element,
- (2) if  $\text{int}(\mathcal{C}) \neq \text{int}(\overline{\mathcal{P}})$ , the semigroup  $\mathcal{P}$  is Buchsbaum if and only if  $\Upsilon' = \emptyset$  and  $\Upsilon \subset \overline{\mathcal{P}}$ .

PROOF. We prove that  $\overline{\mathcal{P}}$  is Cohen-Macaulay if and only if the conditions of the theorem are fulfilled.

Case (1) is similar to the Proposition 2.25. We begin assuming that  $\overline{\mathcal{P}}$  is Cohen-Macaulay. Again we have to check two different possibilities:  $\mathcal{P} \cap \tau_j$  is generated only by one element or not.

- If there exists  $m_j \in \mathbb{N}^2$  such that  $\mathcal{P} \cap \tau_j = \langle m_j \rangle$  for some  $j \in \{1, 2\}$ , then for every  $a \in (\tau_j \setminus \mathcal{P}) \cap \mathbb{N}^2$  we have that  $a + m_j \in \tau_j \setminus \mathcal{P}$ , whence we have that  $a \notin \overline{\mathcal{P}}$ . Then  $\overline{\mathcal{P}} \cap \tau_j = \mathcal{P} \cap \tau_j$ .
- The other possibility is  $\mathcal{P} \cap \tau_j$  is minimally generated by two or more elements for some  $j \in \{1, 2\}$ , that is  $F \cap \tau_j$  is a segment and so  $(\mathcal{C} \setminus \mathcal{P}) \cap \tau_j$  is a finite non-empty set. This implies that  $(\mathcal{C} \setminus \overline{\mathcal{P}}) \cap \tau_j$  is a finite set. The argument follows as in Proposition 2.25.

The converse of Case (1) is analogous to the converse of Propositions 2.25.

To prove Case (2), assume that  $\text{int}(\mathcal{C}) \neq \text{int}(\overline{\mathcal{P}})$  and that  $\overline{\mathcal{P}}$  is Cohen-Macaulay. By Corollary 2.23, the set  $\Upsilon'$  has to be empty. If  $\Upsilon \not\subset \overline{\mathcal{P}}$ , choose  $a \in \Upsilon \setminus \overline{\mathcal{P}}$  such that  $d(a) = \max\{d(a') \mid a' \in \Upsilon \setminus \overline{\mathcal{P}}\}$ . Then  $a + m'_1$  and  $a + m'_2$  belong to  $\overline{\mathcal{P}}$ , which implies that  $\overline{\mathcal{P}}$  is not Cohen-Macaulay (again by Corollary 2.23). Thus  $\Upsilon \subset \overline{\mathcal{P}}$ .

Conversely, assume that  $\Upsilon' = \emptyset$  and  $\Upsilon \subset \overline{\mathcal{P}}$  and let us prove that  $\overline{\mathcal{P}}$  is Cohen-Macaulay. We use Corollary 2.23. Let  $a$  be an element of  $\mathcal{C} \setminus \overline{\mathcal{P}}$ . We have to prove that either  $a + m'_1$  or  $a + m'_2$  is not in  $\overline{\mathcal{P}}$ . Note that if  $F \cap \tau_1$  and  $F \cap \tau_2$  are both segments, by construction,  $\mathcal{C} = \Upsilon$  and consequently  $\mathcal{C} = \overline{\mathcal{P}}$ , and thus there is no  $a$  to consider. So we may assume that either  $F \cap \tau_1$  or  $F \cap \tau_2$  is a single point.

As  $\Upsilon \subset \overline{\mathcal{P}}$ , we have that  $a \notin \Upsilon \subset \overline{\mathcal{P}}$ . Hence either  $a$  belongs to the strip bounded by  $\tau_1$  and  $\nu_1$  or in the strip determined by  $\nu_2$  and  $\tau_2$ . We distinguish these two cases.

- Assume that  $a$  belongs to the strip bounded by the parallel lines  $\tau_1$  and  $\nu_1$ .
  - If  $F \cap \tau_1 = \{P_1\}$ , then we know that  $\mathcal{P} \cap \tau_1 = \langle m_1 \rangle$ . By using the argument in Case (1), we deduce that  $\mathcal{P} \cap \tau_1 = \overline{\mathcal{P}} \cap \tau_1$  and  $m_1 = m'_1$ . By construction of  $L_1$  and  $\Upsilon_1$ , the element  $a$  belongs to  $\Upsilon_1 \setminus \overline{\mathcal{P}}$  or it belongs to  $L_1 \setminus \overline{\mathcal{P}}$ . Since  $\Upsilon' = \emptyset$ , if  $a \in \Upsilon_1 \setminus \overline{\mathcal{P}}$ , the element  $a + m'_1$  or  $a + m'_2$  does not belong to  $\overline{\mathcal{P}}$ . If  $a \in L_1 \setminus \overline{\mathcal{P}}$ , then  $a + m_1 = a + m'_1 \notin \overline{\mathcal{P}}$ .
  - If  $F \cap \tau_1$  is a segment, by construction  $a \in \tau_1 = \nu_1$ . Also  $a$  would be in the strip bounded by  $\nu_2$  and  $\tau_2$ . We are assuming that  $F \cap \tau_2$  is not a segment ( $F \cap \tau_1$  is already a segment), and so it is a point and we can apply the argument of the preceding paragraph.
- The case  $a$  is in the strip bounded by  $\nu_2$  and  $\tau_2$  follows by symmetry. □

**3.3. Effective test for the Buchsbaum property in affine convex polygonal semigroups.** According to Theorem 2.27, in order to determine whether or not  $\mathcal{P}$  is Buchsbaum, we need to check if  $\text{int}(\mathcal{C}) = \text{int}(\overline{\mathcal{P}})$ . The different situations are the following.

- (1) If  $F \cap \tau_1$  and  $F \cap \tau_2$  are segments, say  $\overline{P_1 P_t}$  and  $\overline{P_{d-1} P_d}$ , the set  $Y$  is equal to the positive integer cone  $\mathcal{C}$  and the sets  $\mathcal{C} \setminus \mathcal{P}$  and  $\mathcal{C} \setminus \overline{\mathcal{P}}$  are finite. Let  $j \in \mathbb{N}$  be the least integer such that  $j\overline{P_1 P_t} \cap (j+1)\overline{P_1 P_t} \neq \emptyset$  and  $j\overline{P_{d-1} P_d} \cap (j+1)\overline{P_{d-1} P_d} \neq \emptyset$ , and let  $T$  be the triangle with vertex set  $\{O, jP_1, jP_d\}$ . Clearly,  $T \cap \mathbb{N}^2$  is finite and  $\text{int}(\mathcal{C}) \setminus \text{int}(\overline{\mathcal{P}}) \subseteq T \cap \mathbb{N}^2$ . This is illustrated in Figure 18. In this particular example,  $\mathcal{P} \cap \tau_1 = \langle m_1 = (52, 25) \rangle$ , and  $\mathcal{P} \cap \tau_2 = \langle m_2 = (8, 1) \rangle$ . As shown in the proof of Theorem 2.27, this forces  $\overline{\mathcal{P}} \cap \tau_j$  to be generated by a single element for  $j \in \{1, 2\}$ . The points  $(4, 1)$  and  $(7, 3)$  are in  $\overline{\mathcal{P}}$  (in color red in the Figure 18). Therefore  $\mathcal{P}$  in this example is Buchsbaum.

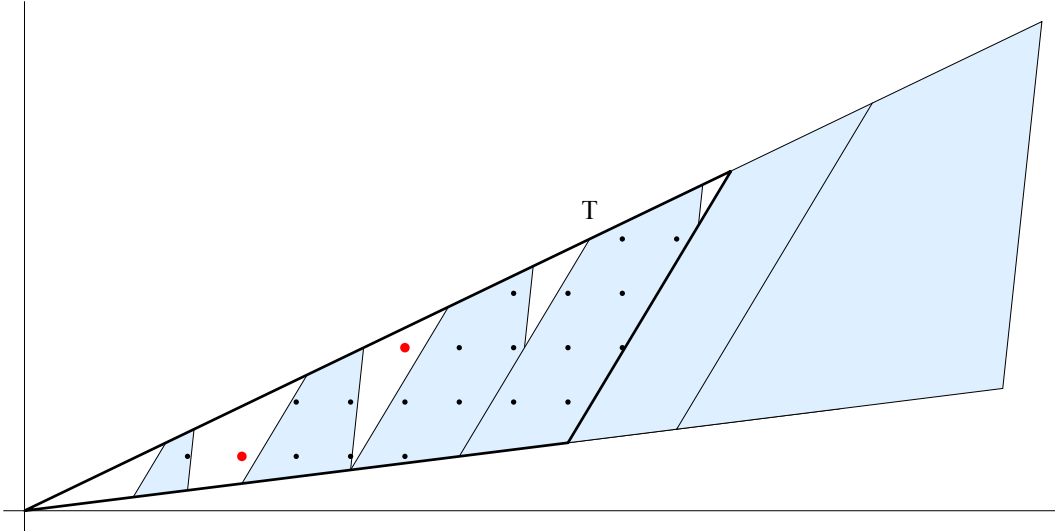


FIGURE 18. Affine polygonal semigroup  $\mathcal{P}$  associated to the polygon  $\{(2, 0.25), (3, 0.375), (2.6, 1.25), (3.12, 1.5)\}$ .

- (2) If  $F \cap \tau_1$  and  $F \cap \tau_2$  are points, say  $P_1$  and  $P_d$ , we need to consider the following different areas inside the cone.
- For  $P \in (\text{int}(\mathcal{C}) \cap (L_1 \cup L_2)) \setminus \text{int}(\mathcal{P})$ , the elements  $P + m_1$  and  $P + m_2$  do not belong to  $\mathcal{P}$  and thus  $P \notin \overline{\mathcal{P}}$  (Corollary 2.23). This implies that  $\mathcal{P} \cap (L_1 \cup L_2) = \overline{\mathcal{P}} \cap (L_1 \cup L_2)$ . Let  $j \in \mathbb{N}$  such that  $j\overline{P_1 P_2} \cap (j+1)\overline{P_1 P_n} = \{V_1\}$  and let  $t \in \mathbb{N}$  satisfying  $tP_1 = m_1$ . For every  $r, k \in \mathbb{Z}_{\geq}$  there exists  $h \in \{0, \dots, t-1\}$  such that  $(\mathring{T}_1 + (r+j)P_1) \cap \mathbb{N}^2 = (\mathring{T}_1 + (h+j)P_1) \cap \mathbb{N}^2 + km_1$ . Note that this construction is for  $L_1$  and that for  $L_2$  we must proceed similarly with the triangle  $T_2$ . So to compare  $\text{int}(\mathcal{C}) \cap (L_1 \cup L_2)$  with  $\text{int}(\overline{\mathcal{P}}) \cap (L_1 \cup L_2)$  it is only necessary to check if there are nonnegative integer points in the sets  $\mathring{T}_1 + (h+j)P_1$  (with  $h \in \{0, \dots, t-1\}$ ). If there exists such points, then  $\text{int}(\mathcal{C}) \neq \text{int}(\overline{\mathcal{P}})$ . This process has to be done,

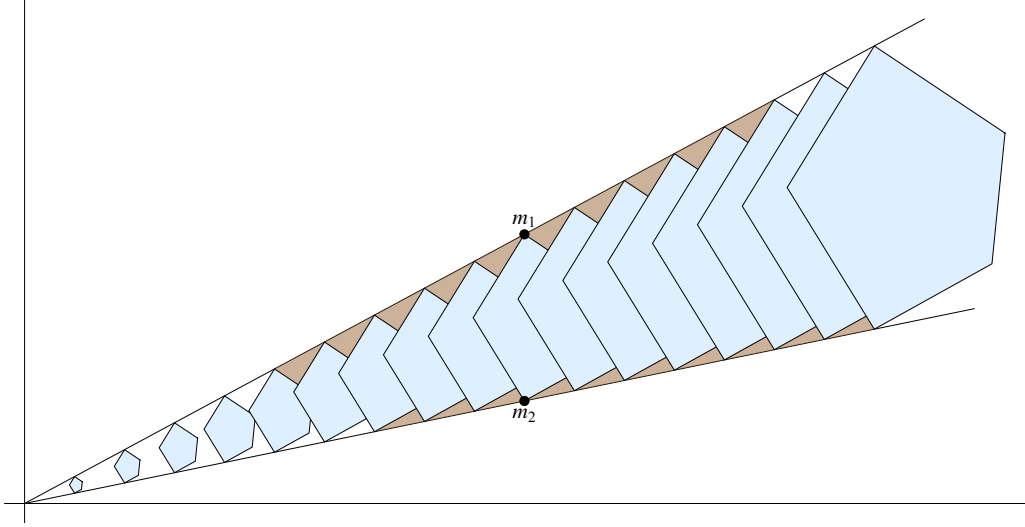


FIGURE 19. Affine polygonal semigroup  $\mathcal{P}$  associated to the polygon  $\{(3.9, 2.1), (3.9, 0.8), (3.5, 1.45), (4.5, 1.7), (4.44, 1.1)\}$ .

analogously, in corresponding translations of  $\mathring{T}_2$  in the direction of  $P_d$ . In Figure 19, the shaded areas between the rays and the affine polygonal semigroup are the sets  $\{\mathring{T}_1 + (h+5)(39/10, 21/10) \mid h \in \{0, 9\}\}$  and  $\{\mathring{T}_2 + (h+7)(39/10, 4/5) \mid h \in \{0, 9\}\}$ , respectively.

- Besides, since  $\Upsilon_1$  and  $\Upsilon_2$  are parallelograms (see for instance Figure 16 to get an idea on how these sets look like),  $(\Upsilon_1 \cup \Upsilon_2) \cap \mathbb{N}^2$  is a finite set and therefore  $(\text{int}(\mathcal{C}) \cap (\Upsilon_1 \cup \Upsilon_2)) \setminus \text{int}(\overline{\mathcal{P}})$  can be computed.
  - Finally, in order to compute  $(\text{int}(\mathcal{C}) \cap \Upsilon) \setminus \text{int}(\overline{\mathcal{P}})$ , just take  $j \in \mathbb{N}$  to be the least integer such that both sets  $j\overline{P_1 P_t} \cap (j+1)\overline{P_1 P_2}$  and  $j\overline{P_d P_{d+1}} \cap (j+1)\overline{P_d P_{d-1}}$  are singletons. Assume that  $j\overline{P_1 P_t} \cap (j+1)\overline{P_1 P_2} = \{V\}$  and  $j\overline{P_d P_{d+1}} \cap (j+1)\overline{P_d P_{d-1}} = \{V'\}$ , and let  $T$  be the triangle with vertex set  $\{Q, V, V'\}$ . By construction, the sets  $(\text{int}(\mathcal{C}) \cap \Upsilon) \setminus T$  and  $(\text{int}(\mathcal{P}) \cap \Upsilon) \setminus T$  are equal. Therefore  $\text{int}(\mathcal{C}) \cap \Upsilon = \text{int}(\overline{\mathcal{P}}) \cap \Upsilon$  if and only if the finite sets  $\text{int}(\mathcal{C}) \cap T$  and  $\{a \in \text{int}(\mathcal{P}) \cap T \mid a + \mathcal{P} \in \mathcal{P}\}$  are equal (in order to check that  $a + \mathcal{P} \subseteq \mathcal{P}$ , we only have to see if  $a + m \in \mathcal{P}$  for every minimal generator  $m$  of  $\mathcal{P}$ ). This case is illustrated in Example 2.28 (see Figure 20).
- (3) If  $F \cap \tau_1 = \{P_1\}$  and  $F \cap \tau_2$  is a segment  $\overline{P_{d-1} P_d}$ , for comparing the sets  $\text{int}(\mathcal{C}) \setminus \Upsilon$  and  $\text{int}(\overline{\mathcal{P}}) \setminus \Upsilon$ , we proceed as in the second case with the sets  $L_1$  and  $\Upsilon_1$ . Let now  $j \in \mathbb{N}$  be the least integer such that  $j\overline{P_1 P_t} \cap (j+1)\overline{P_1 P_2}$  is a point  $V$  and  $j\overline{P_{d-1} P_d} \cap (j+1)\overline{P_{d-1} P_d} \neq \emptyset$ , and let  $T$  be the triangle with vertex set  $\{Q, V, jP_d\}$  (in this case  $Q \in \tau_2$ ). Then  $\text{int}(\mathcal{C}) \cap \Upsilon = \text{int}(\overline{\mathcal{P}}) \cap \Upsilon$  if and only if the finite sets  $\text{int}(\mathcal{C}) \cap T$  and  $\text{int}(\overline{\mathcal{P}}) \cap T$  are equal.
- (4) Finally, the case  $F \cap \tau_2$  is a point and  $F \cap \tau_1$  is a segment is analogous to the above case.

In any case, all the necessary sets required to compare  $\text{int}(\mathcal{C})$  and  $\text{int}(\overline{\mathcal{P}})$  are finite and can be obtained algorithmically. Besides, the conditions  $Y' = \emptyset$  and  $Y \subset \overline{\mathcal{P}}$  can be checked algorithmically and “ $\overline{\mathcal{P}} \cap \tau_j$  is generated by only one element” can be tested in a similar way to the case of circle semigroups.

EXAMPLE 2.28. Let  $F$  be the polygon determined by the rational points

$$\{(3.6, 1.8), (3.6, 0.6), (3.3, 1.05), (4.2, 1.5), (4.14, 0.99)\}$$

and  $\mathcal{P}$  its associated affine convex polygonal semigroup (the region confined inside the polygons series in Figure 20). The minimal system of generators of  $\mathcal{P}$  can be computed with the program `PolygonalSG` of the `PolySGTools` package (see [20]),

```
In[1] := PolygonalSG[{{3.6, 1.8}, {3.6, 0.6}, {3.3, 1.05},
                    {4.2, 1.5}, {4.14, 0.99}}]
Out[1] = {{4, 1}, {7, 2}, {7, 3}, {8, 3}, {10, 3}, {11, 2}, {11, 5}, {14, 3},
          {18, 3}, {18, 9}, {20, 8}, {23, 10}}
```

We obtain that  $\mathcal{P}$  is minimally generated by

$$G = \{(18, 9), (18, 3), (4, 1), (20, 8), (23, 10), (8, 3), \\ (11, 5), (11, 2), (10, 3), (14, 3), (7, 2), (7, 3)\}.$$

Using basic tools of Linear Algebra we compute the sets  $Y_1$ ,  $Y_2$ , the triangle  $T$  and the necessary translations of  $T_1$  and  $T_2$  (the above sets are needed to check the conditions of Theorem 2.27). Those translations are the brown triangles in Figure 20,  $(Y_1 \cup Y_2) \setminus \mathcal{P}$  is the region in green. The dashed edges region encloses  $(\text{int}(\mathcal{C}) \setminus \text{int}(\mathcal{P})) \cap Y = (T \cap \mathbb{N}^2) \setminus \mathcal{P} = \{(13, 4)\}$ . Since  $(13, 4)$  does not belong to  $\mathcal{P}$ , by Corollary 2.23, the semigroup  $\mathcal{P}$  is not Cohen-Macaulay. We also have  $(13, 4) + m \in \mathcal{P}$  for all  $m \in G$ . Thus  $(13, 4) \in \overline{\mathcal{P}}$  and therefore  $Y \subset \overline{\mathcal{P}}$ . This can be checked with the function `BelongToSG` also in the `PolySGTools` package ([20]). For example,

```
In[2] := BelongToSG[{13, 4} + {18, 9}, {{3.6, 1.8}, {3.6, 0.6},
                    {3.3, 1.05}, {4.2, 1.5}, {4.14, 0.99}}]
Out[2] = True
```

The set  $(\text{int}(\mathcal{C}) \setminus \text{int}(\mathcal{P})) \cap (Y_1 \cup Y_2)$  is equal to

$$D = \{(3, 1), (5, 1), (5, 2), (6, 2), (9, 2), (10, 2), (9, 3), (13, 3), \\ (16, 3), (17, 3), (9, 4), (10, 4), (17, 4), (12, 5), (13, 5), (13, 6)\},$$

but none of these points are in  $\overline{\mathcal{P}}$ . Besides, for all  $a \in D$ ,  $a + m'_1$  or  $a + m'_2$  does not belong to  $\overline{\mathcal{P}}$ . Therefore  $Y'$  is the empty set. By Theorem 2.27, we conclude that  $\mathcal{P}$  is a non-Cohen-Macaulay Buchsbaum affine semigroup.

If we use the method of Theorem 9 in [24], it is necessary to compute the intersection of the Apéry set of  $m_1$  and the Apéry set of  $m_2$  by checking if  $2 \times 7771556800000$  elements belong to  $\mathcal{P}$ ; clearly, for this class of semigroups, the cost of the computation described in the present section is more affordable.

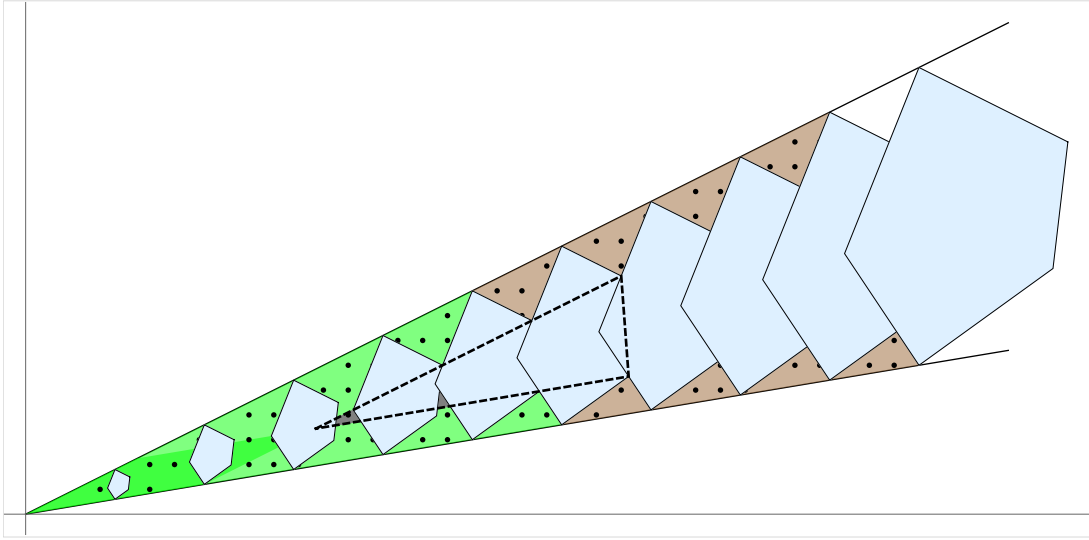


FIGURE 20. Affine polygonal semigroup  $\mathcal{P}$  associated to the polygon  $\{(3.6, 1.8), (3.6, 0.6), (3.3, 1.05), (4.2, 1.5), (4.14, 0.99)\}$ .

The description made in the previously to check if a affine convex polygonal semigroup is Buchsbaum, and either the more detailed before in this actual Section, is implemented as part of the cited package `PolySGTools`. It includes a function called `PSGIs-BuchsbaumQ` to answer `True` or `False`, given an polygon as the input parameter. See Appendix B for further description.

**3.4. Buchsbaum rings examples.** In Example 2.28, it is used only Elementary Algebra, but Buchsbaum semigroups can be generated using an even simpler approach. The following results provide two user-friendly properties which allow us to obtain easily Buchsbaum rings.

**COROLLARY 2.29.** *Every affine convex polygonal semigroup associated to a triangle with rational vertices is Buchsbaum.*

**PROOF.** Let  $T_2$  be the triangle defined as in Proposition 2.20, and let  $m_1$  be the generator of  $\mathcal{P} \cap \tau_1$ . Then every element in the cone that is not in  $\mathcal{P}$  is a translation of an element in  $T_2$  by a multiple of  $m_1$ . In particular this implies that  $\mathcal{P}$  and  $\overline{\mathcal{P}}$  are equal. Corollary 12 in [21] proves that every affine convex polygonal semigroup associated to a triangle with rational vertices is Cohen-Macaulay. Thus,  $\overline{\mathcal{P}}$  is Cohen-Macaulay and therefore  $\mathcal{P}$  is Buchsbaum.  $\square$

**COROLLARY 2.30.** *Let  $F$  be a convex polygon with vertices  $P_1, \dots, P_4 \in \mathbb{Q}_{\geq}^2$  and let  $\mathcal{P}$  be its associated affine convex polygonal semigroup. If  $P_1 \in \mathcal{P} \cap \tau_1$ ,  $P_3 \in \mathcal{P} \cap \tau_2$  and the points  $O, P_2$  and  $P_4$  are aligned,  $\mathcal{P}$  is Buchsbaum.*

**PROOF.** Let  $\mathcal{C}_1$  be the positive integer cone delimited by the ray  $\tau_1$  and the line  $OP_2$ , and let  $\mathcal{C}_2$  be the cone delimited by the ray  $\tau_2$  and the line  $OP_2$ . Trivially  $\mathcal{C} = L_{\mathbb{Q}_{\geq}}(F) \cap$

$\mathbb{N}^2$  is the union of  $\mathcal{C}_1$  and  $\mathcal{C}_2$ , and the semigroup  $\mathcal{P}$  is the union of the affine convex polygonal semigroups,  $\mathcal{P}_1$  and  $\mathcal{P}_2$ , associated to the triangles with vertex sets  $\{P_1, P_2, P_4\}$  and  $\{P_2, P_3, P_4\}$ , respectively. With that decomposition of the affine convex polygonal semigroup  $\mathcal{P}$  and from the hypothesis, we can assert  $\mathcal{P}$  is equal to  $\overline{\mathcal{P}}$ ,  $\Upsilon \subset \mathcal{P}$  and  $\mathcal{P} \cap \tau_1$  and  $\mathcal{P} \cap \tau_2$  are generated by only one element each (Figure 21 illustrates this situation). Under such conditions, let  $a$  be an element belonging to  $\mathcal{C} \setminus \mathcal{P}$ . Note that if  $a \in \mathcal{C}_1 \setminus \mathcal{P}_1$

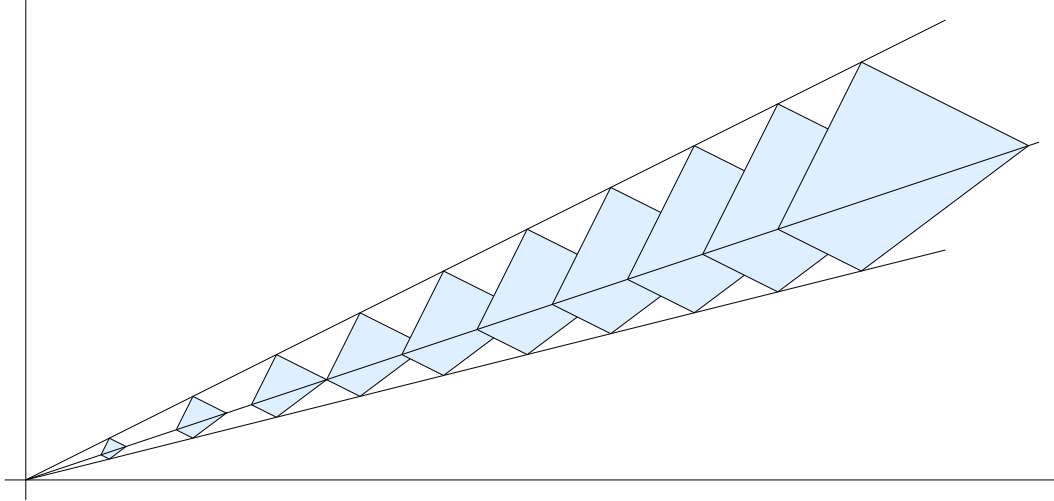


FIGURE 21. Affine polygonal semigroup  $\mathcal{P}$  associated to the polygon  $\{(3.6, 1.2), (4.8, 1.6), (4, 2), (4, 1)\}$ .

then  $a + m_1 \notin \mathcal{P}$ , otherwise, if  $a \in \mathcal{C}_2 \setminus \mathcal{P}_2$  then  $a + m_2 \notin \mathcal{P}$ . In any case,  $a + m_1$  or  $a + m_2$  does not belong to  $\mathcal{P}$ . Thus  $\overline{\mathcal{P}} (= \mathcal{P})$  is Cohen-Macaulay (Corollary 2.23) and then  $\mathcal{P}$  is Buchsbaum.  $\square$



## CHAPTER 3

### Factorizations in affine semigroups

#### 1. Preliminaries

Let  $M$  be a monoid, an element  $m \in M$  is a *unit* if there exists  $m' \in M$  such that  $m + m' = 0$ . Recall that a monoid is called *reduced* when its only unit is the 0 element. The monoid  $M$  is *torsion free* if for every  $m, m' \in M$  and  $c \in \mathbb{N} \setminus \{0\}$ , the equality  $cm = cm'$  implies  $m = m'$ .

Recall that an affine semigroup is finitely generated, cancellative, torsion free and reduced monoid whose elements are in  $\mathbb{N}^k$ . An affine semigroup  $M$  admits a unique minimal system of generators, that is, the elements in  $M$  that cannot be expressed as a sum of two nonzero elements. These elements are known in the literature as *atoms* or *irreducibles*.

Let  $M = \langle m_1, \dots, m_k \rangle \subseteq \mathbb{Z}^n$  be an affine semigroup. The morphism

$$\begin{aligned} \phi : \mathbb{N}^k &\longrightarrow M, \\ \phi(a_1, \dots, a_k) &= \sum_{i=1}^k a_i m_i, \end{aligned}$$

is an epimorphism (known as the factorization homomorphism of  $M$ ). Thus  $M$  is isomorphic to  $\mathbb{N}^k / \ker(\phi)$  (see for instance [45, Theorem 1.2]), where

$$\ker(\phi) = \{(a, b) \in \mathbb{N}^k \times \mathbb{N}^k \mid \phi(a) = \phi(b)\}$$

is the *kernel congruence* of  $\phi$ .

A *presentation* of  $M$  is a generating system of  $\ker(\phi)$  as a congruence. By Redei's theorem,  $M$  is finitely presented, that is, it admits a finite presentation. If  $\{m_1, \dots, m_k\}$  is the minimal generating system of  $M$ , a *minimal presentation* is a minimal generating system of  $\ker(\phi)$  with respect to cardinality and set inclusion (see [45]).

Let  $m \in M$ . The set  $\phi^{-1}(m)$  corresponds with all the possible expressions of  $m$  in terms of the generators of  $M$ . We denote this set by  $Z(m)$ , and we call it *the set of factorizations of  $m$  in  $M$* .

The *associated graph to an element  $m \in M$*  is  $G_m = (V_m, E_m)$ , with  $V_m = \{m_i \mid m - m_i \in M\}$  and  $E_m = \{m_i m_j \mid i \neq j, m - (m_i + m_j) \in M\}$ . In this graph the vertices are the generators that occur in a factorization of  $m$ . When there is no edge between two vertices, then these two generators can not appear in the same expression of  $m$ . An element  $m \in M$  is a *Betti element* of  $M$  if  $G_m$  is not connected. We denote by  $\text{Betti}(M)$  the set of Betti elements of  $M$ .

Following [50] (or [45, Chapter 9]), for every  $m \in M$  we define on  $Z(m)$  the relation: given  $a, b \in Z(m)$ ,  $a \mathcal{R} b$  if there exists  $z_1, \dots, z_t \subset Z(m)$  such that  $z_1 = a$ ,  $z_t = b$  and  $z_i \cdot$

$z_{i+1} \neq 0$  for  $i \in \{1, \dots, t-1\}$ . It can be shown that the number of connected components of  $G_m$  coincides with the number of  $\mathcal{R}$ -classes of  $Z(m)$  (see for instance [45, Proposition 9.7]). Thus an element  $m$  is a Betti element of  $M$  if  $Z(m)$  has more than one  $\mathcal{R}$ -class.

Observe that the  $\mathcal{R}$ -classes of  $Z(m)$  correspond with the connected components of the graph  $\nabla(m)$  with vertices  $Z(m)$  and edges  $ab$  such that  $a \cdot b \neq 0$ .

For every  $m \in M$ , set  $\rho_m = \emptyset$  when  $G_m$  is connected, otherwise if  $G_m$  is not connected and  $\mathcal{R}_1, \dots, \mathcal{R}_q$  are the different  $\mathcal{R}$ -classes of  $Z(m)$ , then choose  $z_i \in \mathcal{R}_i$  for all  $i \in \{1, \dots, q\}$  and set  $\rho_m = \{(z_1, z_2), \dots, (z_1, z_q)\}$ . Then  $\rho = \bigcup_{m \in M} \rho_m$  is a minimal presentation of  $M$ . Indeed, any minimal presentation can be constructed in this way: the only pairs we need are those that “connect” all possible  $\mathcal{R}$ -classes ([45, Proposition 9.2]).

EXAMPLE 3.1. Let  $M = \langle 10, 11, 23, 35 \rangle \subset \mathbb{N}$ . Let us compute its Betti elements, and from its factorizations a minimal presentation for  $M$ .

```
gap> s:=NumericalSemigroup(10,11,23,35);
<Numerical semigroup with 4 generators>
gap> BettiElementsOfNumericalSemigroup(s);
[ 33, 45, 46, 70 ]
gap> List(last,x->FactorizationsElementWRTNumericalSemigroup(x,s));
[ [ [ 0, 3, 0, 0 ], [ 1, 0, 1, 0 ] ],
  [ [ 0, 2, 1, 0 ], [ 1, 0, 0, 1 ] ],
  [ [ 0, 0, 2, 0 ], [ 0, 1, 0, 1 ] ],
  [ [ 7, 0, 0, 0 ], [ 0, 0, 0, 2 ] ] ]
```

Note that in this example every Betti element has exactly two  $\mathcal{R}$ -classes, and each  $\mathcal{R}$ -class is a singleton. So to compute a minimal presentation it suffices to take pairs formed by factorizations in each of these  $\mathcal{R}$ -classes.

```
gap> MinimalPresentationOfNumericalSemigroup(s);
[ [ [ 0, 0, 2, 0 ], [ 0, 1, 0, 1 ] ],
  [ [ 0, 2, 1, 0 ], [ 1, 0, 0, 1 ] ],
  [ [ 0, 3, 0, 0 ], [ 1, 0, 1, 0 ] ],
  [ [ 7, 0, 0, 0 ], [ 0, 0, 0, 2 ] ] ]
```

Let us compute now the set of factorizations of 77 and its  $\mathcal{R}$ -classes.

```
gap> FactorizationsElementWRTNumericalSemigroup(77,s);
[ [ 0, 7, 0, 0 ], [ 1, 4, 1, 0 ], [ 2, 1, 2, 0 ], [ 2, 2, 0, 1 ] ]
gap> RClassesOfSetOfFactorizations(last);
[ [ [ 0, 7, 0, 0 ], [ 1, 4, 1, 0 ], [ 2, 1, 2, 0 ],
  [ 2, 2, 0, 1 ] ] ]
```

Finally, let us draw a couple of graphs associated to elements in  $M$ .

```
gap> GraphAssociatedToElementInNumericalSemigroup(46,s);
[ [ 11, 23, 35 ], [ [ 11, 35 ] ] ]
gap> GraphAssociatedToElementInNumericalSemigroup(77,s);
```

[ [ 10, 11, 23, 35 ],  
 [ [ 10, 11 ], [ 10, 23 ], [ 10, 35 ], [ 11, 23 ], [ 11, 35 ] ] ]



To end with this preliminaries review, recall that a *numerical monoid* is a submonoid of  $\mathbb{N}$  with finite complement in  $\mathbb{N}$ . Let  $M = \langle m_1, \dots, m_k \rangle$  be a numerical monoid, we define the *Apéry set* of  $m$  in  $M$ , as

$$\text{Ap}(M, m) = \{n \in M \mid n - m \notin M\},$$

which has exactly  $m$  elements, one in each congruence class modulo  $m$ . Thus this set can be written as  $\text{Ap}(M, m) = \{0 = w_0, w_1, \dots, w_{m-1}\}$ , with  $w_i$  the least element in  $M$  congruent with  $i$  modulo  $m$ . Membership problem to  $M$  is trivial once we know  $\text{Ap}(M, m)$  for some nonzero integer  $m \in M$ . This is due to the following property: for  $n \in \mathbb{Z}$ ,  $n \in M$  if and only if  $w_{n \bmod m} \leq n$  (see for instance [46, Chapter 1]). In particular, the computation of  $G_n$  becomes trivial once one of the Apéry sets is known; if  $G_n$  is not connected, then  $n = \omega + m_j$  for some  $\omega \in \text{Ap}(M, m_1) \setminus \{0\}$  and  $j \in \{2, \dots, k\}$  ([46, Proposition 8.19]).

EXAMPLE 3.2. We continue with  $M = \langle 10, 11, 23, 35 \rangle$ .

```
gap> AperyListOfNumericalSemigroup(s);
[ 0, 11, 22, 23, 34, 35, 46, 57, 58, 69 ]
```

We already know that 33 is a Betti element of  $M$ , and  $33 = 22 + 11$ , with  $22 \in \text{Ap}(M, 10)$  and  $j = 2$  in this setting.

## 2. Factorizations and linear Diophantine equations

Recall that we use  $Z(m)$  to denote the set of factorizations of an element  $m \in M$ . Taking  $A$  as the matrix whose columns are  $m_1, \dots, m_k$ ,  $Z(m)$  is the set of nonnegative integer solutions of the system of linear Diophantine equations,  $Ax = m$ .

The set  $Z(m)$  has finitely many elements. We can see this by considering  $x, x' \in \mathbb{N}^k$  such that  $Ax = m$  and  $Ax' = m$ . If  $x \leq x'$ , with the usual product order, then  $x' = x + y$ , with  $y \in \mathbb{N}^k$ , and  $Ax = m = Ax' = Ax + Ay$ . In consequence  $Ay = 0$ . If  $y = e_i$ , then  $m_i = 0$ , this a contradiction. And if  $y = y_1 + y_2$ , with  $y_1 \neq 0 \neq y_2$ ,  $Ay_1 = s_1$  and  $Ay_2 = s_2$ , then  $s_1 + s_2 = 0$ . If  $s_1 = 0$ , then we replace  $y$  by  $s_1$  and argue in the same way. Since  $y_1 < y$ , this process stops after a finite number of steps, arriving either to  $y_1 = e_i$  (which we know it is impossible) or to  $s_1 + s_2 = 0$  with  $s_1 \neq 0 \neq s_2$ . But this implies that  $M$  has units, another contradiction. We have shown that the elements of  $Z(m)$  are not comparable. Then by Dickson's Lemma, this implies that  $Z(m)$  is finite.

The elements of  $\ker(\phi)$  are couples of factorizations of elements of  $M$ . The congruence  $\ker(\phi)$  is also a cancellative monoid and it is generated by its irreducible elements.

To see which are these irreducibles we follow [45]. Let  $H$  be the subgroup of  $\mathbb{Z}^k$  defined by the  $n$  equations  $Ax = 0$ . Since  $M$  is cancellative, from [45, Proposition 1.4]), it follows that  $\ker(\phi) = \sim_M$ , where

$$(11) \quad \sim_M = \{(a, b) \in \mathbb{N}^k \times \mathbb{N}^k \mid a - b \in H\}.$$

Hence  $(x, y) \in \ker(\phi)$  if and only if

$$(12) \quad (A \mid -A) \begin{pmatrix} x \\ y \end{pmatrix} = 0,$$

which is a system of linear Diophantine equations with  $n$  equations and  $2k$  unknowns. The set of atoms (or irreducibles) of  $\ker(\phi)$ , denoted by  $\mathcal{F}(\sim_M)$  coincides with the set  $\text{Minimals}_{\leq}(\ker(\phi) \setminus \{(0, 0)\})$ , where  $\leq$  is the usual partial ordering.  $\mathcal{F}(\sim_M)$  is itself a “redundant” presentation of  $M$ . Redundant because every time  $(a, b) \in \ker(\phi)$ ,  $(b, a) \in \ker(\phi)$ , and we can remove one of them in a presentation. Also  $(e_i, e_i) \in \mathcal{F}(\sim_M)$ , for  $i \in \{1, \dots, k\}$ , which are not needed in a presentation. The set  $\mathcal{F}(\sim_M) \setminus \{(e_i, e_i) \mid i \in \{1, \dots, k\}\}$  are known as *primitive* elements of  $\sim_M$ . For  $(a, b)$  primitive, by abusing of notation, we say that  $\phi(a)$  ( $= \phi(b)$ ) is a *primitive element* of  $M$ .

EXAMPLE 3.3. Let  $M$  be as in Example 3.1. Recall that a minimal presentation for  $M$  is

$$\{((0, 0, 2, 0), (0, 1, 0, 1)), ((0, 2, 1, 0), (1, 0, 0, 1)), ((0, 3, 0, 0), (1, 0, 1, 0)), \\ ((7, 0, 0, 0), (0, 0, 0, 2))\}.$$

However  $\mathcal{F}(\sim_M)$  has 256 elements. Even dividing by two and removing the elements  $(e_i, e_i)$  we still have 124.

### 3. Length dependent invariants

In this section we recall some factorization invariants related with the concept of the length of a factorization (see [7] and [48]).

The *length of a factorization* is the number of atoms appearing in it. If  $m \in M$  with  $m = \sum_{i=1}^k a_i m_i$ , we have  $a = (a_1, \dots, a_k) \in Z(m)$ , and its length is  $|a| = \sum_{i=1}^k a_i$ .

The set of lengths of  $m \in M$  is

$$L(m) = \{|a| \mid a \in Z(m)\}.$$

For  $M$ , the *set of lengths* of factorizations is  $L(M) = \bigcup_{m \in M} L(m)$ .

The set  $L(m)$  is bounded since  $\sharp Z(m) < \infty$ . Hence  $L(m)$  is of the form  $\{l_1, \dots, l_p\}$  with  $l_1 < \dots < l_p$ . The *Delta set* of  $m \in M$  is  $\Delta(m) = \{l_i - l_{i-1} \mid 2 \leq i \leq p\}$  (if  $p = 1$ ,

$\Delta(m) = \emptyset$ ). And for the entire monoid

$$\Delta(M) = \bigcup_{m \in M} \Delta(m).$$

In [7, Theorem 2.5] it is shown that the maximum of  $\Delta(M)$  is reached on the maximum of the set

$$\bigcup_{m \in \text{Betti}(M)} \Delta(m).$$

A monoid is *half-factorial* when its elements have all its factorizations with the same length. Note that if  $M$  is half-factorial, then  $\sharp L(m) = 1$  for all  $m \in M$  and  $\Delta(M) = \emptyset$ . The elasticity was introduced to measure how far a monoid is from being half-factorial. The *elasticity*  $e(m)$  is

$$e(m) = \frac{\max L(m)}{\min L(m)}.$$

For the monoid  $M$  the elasticity is defined by  $e(M) = \sup_{m \in M} e(m)$ .

In [48, Corollary 20] it is shown that for affine semigroups this supremum is a maximum, i.e. there is  $m \in M$  with  $e(m) = e(M)$ . The elasticity can be computed from  $\mathcal{J}(\sim_M)$  (see [48, Theorem 15]). Philipp proved in [37, Lemma 2.3.5]) that we do not need all the elements in this set. Indeed he showed that  $e(M) = \max\{|a|/|b| \mid (a, b) \text{ a circuit of } \sim_M\}$ , where a *circuit* is an element of minimal support in  $\sim_M$  (the *support* of  $a \in \mathbb{N}^k$  is  $\text{supp}(a) = \{i \in \{1, \dots, k\} \mid a_i \neq 0\}$ ). Circuits can be easily computed by using determinants, [15, Lemma 8.8].

EXAMPLE 3.4. In Example 3.1 we saw the set of factorizations of 77 were

$$\{(0, 7, 0, 0), (1, 4, 1, 0), (2, 1, 2, 0), (2, 2, 0, 1)\}.$$

Hence  $L(77) = \{5, 6, 7\}$ ,  $\Delta(77) = \{1\}$ , and  $e(77) = 7/5$ .

#### 4. Distance dependent invariants

For half-factorial monoids, the invariants presented in the preceding section give no relevant information. So we need new invariants, and these are based on the concept of distance between factorizations. We first define this measure as in [26] but with additive notation.

For the elements of  $\mathbb{N}^k$ ,  $a = (a_1, \dots, a_k)$  and  $b = (b_1, \dots, b_k)$  we write

$$a \wedge b = (\min\{a_1, b_1\}, \dots, \min\{a_k, b_k\}),$$

which is the analog to greatest common divisor. Now the *distance between the factorizations*  $a$  and  $b$  is

$$d(a, b) = \max\{|a - a \wedge b|, |b - a \wedge b|\}$$

**4.1. Catenary degree.** Given  $m \in M$ , an  $N$ -chain of factorizations from  $a, b \in Z(m)$  is a sequence  $z_0, \dots, z_t \in Z(m)$  such that  $z_0 = a$  and  $z_t = b$  and  $d(z_i, z_{i+1}) \leq N$ , for all  $i \in \{0, \dots, t-1\}$ .

The *catenary degree* of  $m$ ,  $c(m)$  is the minimum  $N \in \mathbb{N}_0 \cup \{\infty\}$  such that for any two factorizations  $a, b \in Z(m)$  there is an  $N$ -chain from  $a$  to  $b$ . The catenary degree for  $M$ ,  $c(M)$ , is defined by

$$c(M) = \sup\{c(m) \mid m \in M\}.$$

An algorithm to compute  $c(m)$  first computes  $Z(m)$  and next the complete graph with vertices  $Z(m)$ , and edges labelled with the distances between the ends. Then it proceeds by eliminating first the edges with greater weight. The algorithm stops when a new deletion of the candidate edge produces a non connected graph. The weight of this candidate edge is the catenary degree of the element. Listing D.2 reproduces the code in GAP ([16]) to compute the catenary degree of a set of factorizations.

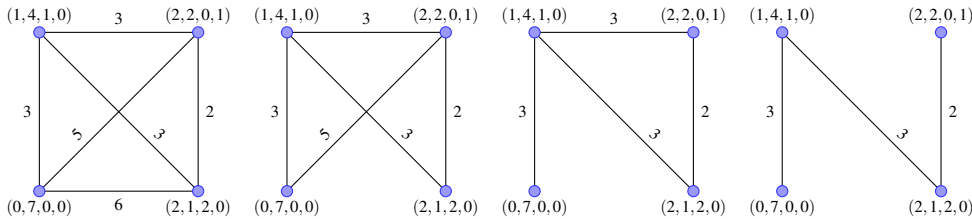
From the proof of [8, Theorem 3.1] it follows that the catenary degree of  $M$  is reached in one of its Betti elements and thus the above supremum is a maximum:

$$c(M) = \max\{c(m) \mid m \in \text{Betti}(M)\}.$$

This theorem also gives a procedure to compute  $c(M)$ : first we obtain the  $\mathcal{R}$ -classes of the Betti elements, and then we find the minimum length of the factorizations in each  $\mathcal{R}$ -class; finally we take the maximum of these lengths as  $c(M)$ . Basically, it computes the maximum of  $c(m)$ , with  $m$  ranging in the Betti elements of  $M$ . For numerical semigroups, recall that the Betti elements can be described with the Apéry set of one of the minimal generators (see Section 1).

For the affine case see Listing D.5, where we take the maximum catenary of the Betti elements.

**EXAMPLE 3.5.** We now compute the catenary degree of  $77 \in M = \langle 10, 11, 23, 35 \rangle$  (Example 3.1). The set  $Z(77) = \{(0, 7, 0, 0), (1, 4, 1, 0), (2, 1, 2, 0), (2, 2, 0, 1)\}$ . We start by drawing a complete graph with vertices the factorizations of 77 and edges labelled with the distances between them. Then we remove the edge with maximum distance, and we repeat the process until we find a bridge.



The catenary degree of  $M$  is 7, which is the catenary degree of the Betti element 70:  $Z(70) = \{(7, 0, 0, 0), (0, 0, 0, 2)\}$ .

4.1.1. *Monotone catenary degree.* An  $N$ -chain is called *monotone* if  $|z_0| \leq \dots \leq |z_t|$  or  $|z_0| \geq \dots \geq |z_t|$ . With this condition the definition of the *monotone catenary degree* of  $m$ ,  $c_{\text{mon}}(m)$ , is similar to the catenary degree considering a monotone  $N$ -chain. For  $M$ ,  $c_{\text{mon}}(M) = \sup\{c_{\text{mon}}(m) \mid m \in M\}$ .

The computation of the monotone catenary degree for a set of factorizations is in Listing D.6. It proceeds computing two adjacency matrices. One of them represents a directed graph of factorizations, with edges sourcing from factorizations with smaller length to longer length factorizations. The second matrix represents a graph with its edges weighted with the corresponding distance between the factorizations vertices. As for the catenary degree computation, in every step an edge with the greater weight is eliminated. The second matrix tells the number of paths with length  $n$  for every pair of vertices, we can check the connectivity using the graph of factorizations after every edge elimination.

An alternative way to compute the monotone catenary degree makes use of the next two invariants, being the monotone catenary degree the supremum of them (see Lemma 3.6 below). This is a more convenient method to use when the number of factorizations is high.

4.1.2. *Equal catenary degree.* The *equal catenary degree* of  $m$ ,  $c_{\text{eq}}(m)$ , is the minimum  $N \in \mathbb{N}_0 \cup \{\infty\}$  such that for all  $a, b \in Z(m)$ ,  $|a| = |b|$  and there exist a monotone  $N$ -chain between them (consequently all lengths in the chain coincide). In the same way,  $c_{\text{eq}}(M) = \sup\{c_{\text{eq}}(m) \mid m \in M\}$ .

To compute the equal catenary degree of an element  $m$  we first split the set  $Z(m)$  in layers of factorizations with the same length. Then we compute the catenary degree of each layer, and take the maximum of them. See Listing D.7 for the definition of the function using GAP ([16]).

In order to compute the equal catenary degree of  $M$ , we must obtain the minimal pairs  $(a, b) \in \mathcal{F}(\sim_M)$ , with the additional condition that  $|a| = |b|$ , and then for each  $(a, b)$  of this form we compute the equal catenary degree of  $\phi(a)$  and take the maximum of them (see [37]). This means that we must add one equation to (12) to get:

$$(13) \quad \begin{pmatrix} A & -A \\ \mathbb{1} & -\mathbb{1} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

There are different ways to compute the minimal  $\mathbb{N}$ -solutions of this linear Diophantine system as the method exposed in Section 3 of the first chapter. As well, using the concept of Graver basis, the set of solutions of interest can be computed considering half the number of columns of the matrix in (13):

$$\begin{pmatrix} A \\ \mathbb{1} \end{pmatrix} x = 0.$$

We recall briefly what a Graver basis is, and why it can be used in our setting. A *Graver basis* of the matrix  $A_{m \times k} = (a_{ij})$ , with  $a_{ij} \in \mathbb{Z}$  is the finite set

$$\text{Gv}(A) = \min_{\sqsubseteq} \{x \in \mathbb{Z}^k \setminus \{0\} \mid Ax = 0\},$$

under the partial order  $\sqsubseteq$  on  $\mathbb{Z}^k$  defined as  $x \sqsubseteq y$  when  $x_i y_i \geq 0$  and  $|x_i| \leq |y_i|$  for  $i \in \{1, \dots, k\}$ .

Let  $x = (x_1, \dots, x_k)$ , we denote the tuples

$$x^+ = (\max\{0, x_1\}, \max\{0, x_2\}, \dots, \max\{0, x_k\})$$

and

$$x^- = (-\min\{0, x_1\}, -\min\{0, x_2\}, \dots, -\min\{0, x_k\}).$$

Then  $x = x^+ - x^-$  and  $x \sqsubseteq y$  if and only if  $(x^+, x^-) \leq (y^+, y^-)$ . Let  $x$  denote now a minimal solution of the Graver basis for  $A$ . It is easy to check that this solution corresponds to the pair  $(x^+, x^-)$  which is the minimal nonzero solution with nonnegative integer coefficients of the system of equations:

$$(A \mid -A) \begin{pmatrix} x^+ \\ x^- \end{pmatrix} = 0.$$

Observe that  $(A \mid -A)(x^+, x^-)^T = Ax^+ - Ax^- = A(x^+ - x^-) = Ax$ . This equivalence enables an improvement on the computation of the equal catenary degree based on the corresponding tool of 4ti2 software package to calculate the Graver basis of  $(A \mid \mathbb{1})^T$ . Listing D.8 has 2 functions that are used to perform this computation. The first, named `EqualPrimitiveElementsOfAffineSemigroup` does the Graver basis computation using 4ti2 ([30]) by using our GAP ([16]) package 4ti2gap (see Appendix C). The second function gets the result by finding the maximum catenary degree among the set of the factorizations of the equal primitive elements (primitive elements corresponding to  $M^{\text{eq}}$ , a monoid that we define in Section 7.2).

**4.1.3. Adjacent catenary degree.** Let  $C$  be a set of nonnegative integers, two elements  $p, q \in C$  are *adjacent* if  $C \cap [\min\{p, q\}, \max\{p, q\}] = \{p, q\}$ . The set of factorizations of an element  $m \in M$  with length  $p$  is denoted

$$Z_p(m) = \{a \in Z(m) \mid |a| = p\}.$$

Now we define the *adjacent catenary degree* as

$$c_{\text{adj}}(m) = \sup\{d(Z_p(m), Z_q(m)) \mid p, q \in L(m) \text{ are adjacent}\}.$$

Likewise,  $c_{\text{adj}}(M) = \sup\{c_{\text{adj}}(m) \mid m \in M\}$ . The idea to compute the  $c_{\text{adj}}(m)$  is in Listing D.9.

As we noted previously, for an element  $m \in M$  the monotone catenary degree is the supremum of the adjacent and equal catenary degree values.

**LEMMA 3.6.** *Let  $m \in M$ ,  $c_{\text{mon}}(m) = \max\{c_{\text{eq}}(m), c_{\text{adj}}(m)\}$ .*



PROOF. First we prove that  $c_{\text{mon}}(m) \leq \max\{c_{\text{eq}}(m), c_{\text{adj}}(m)\}$ . Consider the set of lengths of the factorizations of  $m$  ordered as  $l_1 < \dots < l_k$ . For  $i \in \{1, \dots, k-1\}$ , choose  $z_i$  and  $z_{i+1}$  such that  $d(z_i, z_{i+1}) = d(Z_{l_i}(m), Z_{l_{i+1}}(m)) \leq c_{\text{adj}}(m)$ . From any pair of factorizations  $a, a' \in Z(m)$ , to go from the  $a$  to  $a'$ , first we move between factorizations with the same length as  $a$ . We repeat this process until we arrive to the  $Z_{|a'|}(m)$ . Then we have a sequence with  $c_{\text{mon}}(m) \leq \max\{c_{\text{eq}}(m), c_{\text{adj}}(m)\}$ .

To probe  $\max\{c_{\text{eq}}(m), c_{\text{adj}}(m)\} \leq c_{\text{mon}}(m)$ . First consider two factorizations  $a, a' \in Z(m)$  with the same length. By the definition of monotone catenary degree, there is a monotone  $c_{\text{mon}}(m)$ -chain joining  $a$  and  $a'$ . This forces all the factorizations in this sequence to have the same length. Consequently  $c_{\text{eq}}(m) \leq c_{\text{mon}}(m)$ . Now take  $l_i < l_{i+1}$  two consecutive lengths of factorizations of  $m$ , such that  $c_{\text{adj}}(m) = d(Z_{l_i}(m), Z_{l_{i+1}}(m))$ . Take  $z_i$  and  $z_{i+1}$  as above. Again, from the definition of monotone catenary degree, there exists a monotone  $c_{\text{mon}}(m)$ -chain  $u_1, \dots, u_t$  joining  $z_i$  and  $z_{i+1}$ . Hence there exists  $s \in \{1, \dots, t-1\}$  such that  $u_s \in Z_{l_i}(m)$  and  $u_{s+1} \in Z_{l_{i+1}}(m)$ . By definition  $c_{\text{adj}}(m) = d(Z_{l_i}(m), Z_{l_{i+1}}(m)) \leq d(u_s, u_{s+1}) \leq c_{\text{mon}}(m)$ .  $\square$

EXAMPLE 3.7. From Example 3.1 we know that

$$Z(77) = \{(0, 7, 0, 0), (1, 4, 1, 0), (2, 1, 2, 0), (2, 2, 0, 1)\}$$

in  $M = \langle 10, 11, 23, 35 \rangle$ . We have that  $Z(77) = Z_7(77) \cup Z_6(77) \cup Z_5(77)$ , with

$$Z_7(77) = \{(0, 7, 0, 0)\}, Z_6(77) = \{(1, 4, 1, 0)\} \text{ and } Z_5(77) = \{(2, 1, 2, 0), (2, 2, 0, 1)\}.$$

Hence  $c_{\text{eq}}(77) = 2 = d((2, 1, 2, 0), (2, 2, 0, 1))$ .

Also  $d(Z_6(77), Z_7(77)) = 3$  and  $d(Z_5(77), Z_6(77)) = 2$ , and consequently  $c_{\text{adj}}(77) = 3$ . We conclude that  $c_{\text{mon}}(77) = 3$ .

**4.2. Tame degree.** Let  $M$  be an affine semigroup minimally generated by the set  $\{m_1, \dots, m_k\}$ . For  $m \in M$  and  $x \in \mathbb{N}^k$  with  $m - \phi(x) \in M$ , the *tame degree*  $t(m, x)$  is the smallest  $N \in \mathbb{N} \cup \{\infty\}$  such that for all  $a \in Z(m)$ , there exists  $b \in Z(m)$  with  $b \geq x$  and  $d(a, b) \leq N$ . If we take one of the generators  $e_i$  in place of  $x$ , then  $t(m, e_i)$  is a bound of the distance of the factorizations  $z$  of  $m$  with  $i \notin \text{supp}(z)$  to other factorizations where  $i$  appears in the support.

For a subset  $M' \subset M$  and  $X \subset \mathbb{N}^k$ ,  $t(M', X)$  is defined as

$$t(M', X) = \sup\{t(m, x) \mid m \in M', x \in X\} \in \mathbb{N} \cup \{\infty\}.$$

The monoid  $M$  is called *locally tame* when  $t(M, \{m_i\})$  is finite for all  $i \in \{1, \dots, k\}$ .  $M$  is *tame* if  $t(M) = t(M, \{m_1, \dots, m_k\}) < \infty$  (in our setting both definitions coincide since  $M$  is finitely generated). For  $M' = \{m\}$ ,  $t(m, \{m_1, \dots, m_k\})$  is denoted by  $t(m)$ , the tame degree of  $m$ . Notice that with this notation  $t(M) = \sup\{t(m) \mid m \in M\}$ .

EXAMPLE 3.8. In order to illustrate the computation of the tame degree of an element, let us go back to Example 3.1. Recall that

$$Z(77) = \{(0, 7, 0, 0), (1, 4, 1, 0), (2, 1, 2, 0), (2, 2, 0, 1)\}.$$

The worst situation is, taking the factorization  $(0, 7, 0, 0)$ , find another one with non zero last coordinate. The only possibility is  $(2, 2, 0, 1)$ , and the distance between this two factorizations is 5. So  $t(77) = 5$ .

For the computation of  $t(M)$  we need some results.

LEMMA 3.9. *Let  $a \in Z(m_i + M) \setminus \{e_i\}$  be minimal (with respect to  $\leq$ ) for some  $i \in \{1, \dots, k\}$ , and let  $m = \phi(a)$ . Then  $a \cdot b = 0$  for all  $b = (b_1, \dots, b_k) \in Z(m)$  such that  $b_i \neq 0$ .*

PROOF. Observe that given these preconditions if  $a = (a_1, \dots, a_k)$ , then  $a_i = 0$ . Also, since  $a \in Z(m_i + M)$ , there exists  $b = (b_1, \dots, b_k) \in Z(m)$  such that  $b_i \neq 0$ .

Assume that  $a \cdot b \neq 0$ . As  $a_i = 0$  there exists  $j \in \{1, \dots, k\} \setminus \{i\}$  with  $a_j \neq 0 \neq b_j$ . But then  $\phi(b) = m_i + m_j + m'$  for some  $m' \in M$ , and consequently  $\phi(a - e_j) = \phi(b - e_j) \in m_i + M$ , contradicting the minimality of  $a$ .  $\square$

For  $m, m' \in M$ , as usual, we write  $m \leq_M m'$  whenever  $m' - m \in M$ .

PROPOSITION 3.10. *Let  $m \in M$  be minimal (with respect to  $\leq_M$ ) such that  $t(m) = t(M)$ . Then there exists  $\{i, j\} \subseteq \{1, \dots, k\}$  such that  $m - m_i, m - m_j \in M$  and  $m - m_i - m_j \notin M$ .*

PROOF. Let  $i \in \{1, \dots, k\}$  be such that  $t(m) = d(a, b)$  with  $a = (a_1, \dots, a_k)$  and  $b = (b_1, \dots, b_k)$  in  $Z(m)$ ,  $a_i = 0$  and  $b_i \neq 0$ . Then according to [2, Lemma 5.4],  $a$  is minimal (with respect to  $\leq$ ) in  $Z(m_i + M)$  and  $a \neq e_i$ , because  $a_i = 0$ . Take  $j$  such that  $a_j \neq 0$ . In particular, this means that, because of  $b_i \neq 0$ ,  $m - m_i \in M$ , and because of  $a_j \neq 0$ ,  $m - m_j \in M$ . If  $m - m_i - m_j \in M$ , there exists  $c \in Z(m)$  with  $c_i \neq 0 \neq c_j$ . But then  $a \cdot c \neq 0$ , in contradiction with Lemma 3.9.  $\square$

The above result has a nice combinatorial interpretation. Here we recall the description of the associated graph to an element in Section 1.

COROLLARY 3.11. *Let  $m \in M$  be minimal (with respect to  $\leq_M$ ) such that  $t(m) = t(M)$ . Then  $G_m$  is not complete.*

We have already seen that the catenary degree of  $M$  is reached in an element with nonconnected associated graph (that is, a Betti element). Thus in some sense, Corollary 3.11 finds a similar characterization for the tame degree.

We denote  $\text{Prim}(M) = \{\phi(a) \mid (a, b) \in \mathcal{F}(\sim_M), a \neq b\}$ . From [8, Proposition 4.1] we obtain the following result.

COROLLARY 3.12.  $t(M) = \max\{t(m) \mid m \in \text{Prim}(M)\}$ .

Let  $\text{NComp}(M)$  be the set of elements  $m \in M$  such that  $G_m$  is not complete. As a consequence of Corollaries 3.11 and 3.12, we get the following.

THEOREM 3.13. *Let  $M$  be a affine semigroup.*

$$t(M) = \max_{m \in \text{Prim}(M) \cap \text{NComp}(M)} t(m).$$

This theorem allows us to reduce drastically the search space. If we know  $\text{NComp}(M)$ , we can remove from this set those elements  $m$  such that

$$\bigcap_{z \in Z(m)} \text{supp}(z) \neq \emptyset.$$

This is because if  $(x, y) \in \mathcal{F}(\sim_M)$ , then  $\text{supp}(x) \cap \text{supp}(y) = \emptyset$  (otherwise if  $i \in \text{supp}(x) \cap \text{supp}(y)$ , then  $(x - e_i, y - e_i) \in \sim_M$ , contradicting the minimality of  $(x, y)$ ).

For the particular case of numerical semigroups, this idea together with the use of `RestrictedPartitions` (instead of `NSGPFactorizationsNC` in previous implementations) produced a significant speed up of the computation of the tame degree in GAP ([16]). In Listing D.11 this idea is implemented, note that if  $G_m$  is not complete then  $m \in \{m_1, \dots, m_k\} + \bigcup_{i=1, \dots, k} \text{Ap}(M, m_i)$ .

For affine semigroups, Listing D.13 shows its computation, based on the function `PrimitiveElementsOfAffineSemigroup`. This last function uses the package `4ti2gap` to compute  $\text{Gv}(A)$ , where  $A$  is the matrix of the generators of a given affine semigroup as an input parameter (see Listing D.12).

EXAMPLE 3.14. Let  $M = \langle 10, 11, 23, 35 \rangle$  as above.

```
gap> TameDegreeOfNumericalSemigroup(NumericalSemigroup(10, 11, 23, 35));
9
```

## 5. Binomials, lengths and distances

From the first chapter, in Section 1.4, recall that  $\mathbb{k}[X] = \mathbb{k}[x_1, \dots, x_k]$  is the polynomial ring on  $k$  variables over a field  $\mathbb{k}$ , and  $X^\alpha = x_1^{\alpha_1} \dots x_k^{\alpha_k}$  is a monomial of  $\mathbb{k}[X]$ . We define the *degree of a monomial*  $X^\alpha$  as  $\deg(X^\alpha) = \sum_{i=1}^k \alpha_i$ .

Recall that the factorization homomorphism for  $M = \mathbb{N}m_1 + \dots + \mathbb{N}m_k$  is

$$\begin{aligned} \phi : \mathbb{N}^k &\longrightarrow M \\ \alpha = (\alpha_1, \dots, \alpha_k) &\longmapsto \sum_{i=1}^k \alpha_i m_i \end{aligned}$$

that defines a homomorphism of semigroup algebras

$$\begin{aligned} \pi : \mathbb{k}[X] &\longrightarrow \mathbb{k}[M] := \bigoplus_{m \in M} \mathbb{k}\chi^m \\ X^\alpha &\longmapsto \chi^{\phi(\alpha)}, \end{aligned}$$

and that the kernel of  $\pi$ ,  $\ker(\pi)$ , is denoted as  $l_M$ .

LEMMA 3.15 (Herzog's correspondence, [32]). *Let  $\sigma \subseteq \mathbb{N}^k \times \mathbb{N}^k$ . Then  $\sigma$  generates  $\ker(\pi)$  if and only if  $l_M = \langle X^\alpha - X^\beta \mid (\alpha, \beta) \in \sigma \rangle$ .*

EXAMPLE 3.16. Let  $M = \langle 3, 5, 7 \rangle$ .

```
gap> s:=NumericalSemigroup(3,5,7);;
gap> MinimalPresentationOfNumericalSemigroup(s);
[ [ [ 0, 2, 0 ], [ 1, 0, 1 ] ], [ [ 3, 1, 0 ], [ 0, 0, 2 ] ],
  [ [ 4, 0, 0 ], [ 0, 1, 1 ] ] ]
```

This computation has been performed by using the Betti elements of  $M$ . An alternative approach is to use  $\pi$  and elimination.

```
gap> x:=X(Rationals,"x");;y:=X(Rationals,"y");;z:=X(Rationals,"z");;
t:=X(Rationals,"t");;
gap> gen:=[x-t^3, y-t^5, z-t^7];
[ -t^3+x, -t^5+y, -t^7+z ]
gap> ReducedGroebnerBasis(gen,EliminationOrdering([t]));
[ x*z-y^2, x^3*y-z^2, x^4-y*z, x^2*y^3-z^3, x*y^5-z^4,
  y^7-z^5, -x*y+z*t, -x^2+y*t, x^2*t-z, x*t^2-y, t^3-x ]
```

According to Herzog's correspondence,

$$\{((1,0,1),(0,2,0)),((3,1,0),(0,0,2)),((4,0,0),(0,1,1)), \\ ((2,3,0),(0,0,3)),((1,5,0),(0,0,4)),((0,7,0),(0,0,5))\}$$

is a presentation of  $M$ , though clearly not minimal. We can then eliminate those pairs not corresponding to Betti elements (and this can be done by  $\mathcal{R}$ -classes computations).

Another possibility is using 4ti2 through our package 4ti2gap.

```
gap> GroebnerBasis4ti2([[3,5,7]]);
[ [ -4, 1, 1 ], [ -3, -1, 2 ], [ -1, 2, -1 ] ]
```

Though in this setting the output corresponds to the differences of the pairs of a minimal presentation, it may happen that we have to filter those that do not correspond to Betti elements.

With this notation, for a factorization  $\alpha = (\alpha_1, \dots, \alpha_k)$  of an element  $m \in M$  its length can be obtained  $|\alpha| = \sum_{i=1}^k \alpha_i = \deg(X^\alpha)$ .

We define the  $M$ -degree of a monomial  $X^\alpha \in \mathbb{k}[X]$ ,

$$\deg_M(X^\alpha) = \sum_{i=1}^k \alpha_i m_i (= \phi(\alpha)).$$

Now the distance between two factorizations  $\alpha$  and  $\beta \in \mathbb{N}^k$  can be defined as follows

$$d(\alpha, \beta) = \max(\deg(X^\alpha), \deg(X^\beta)) - \deg(\gcd(X^\alpha, X^\beta)).$$

## 6. Omega primality

There is still another non-unique factorization invariant that apparently has nothing to do with distances, and measures how far an element is from being a prime.

The  $\omega$ -primality of  $m$ ,  $\omega(m)$ , is the least positive integer such that whenever  $c_1 + \dots + c_r - m \in M$  for some  $c_1, \dots, c_r \in M$ , then  $c_{i_1} + \dots + c_{i_{\omega(m)}} - m \in M$  for some  $\{i_1, \dots, i_{\omega(m)}\} \subseteq \{1, \dots, r\}$ .

$\{1, \dots, r\}$ . We can restrict the search to sums of the form  $c_1 + \dots + c_r$ , with  $c_1, \dots, c_r \in \{m_1, \dots, m_k\}$  (see [2, Lemma 3.2]). In particular,  $\omega(m) = 1$  means that  $m$  is prime<sup>1</sup>.

Given  $m \in M$ ,  $\omega(m)$  can be computed in the following form [2, Proposition 3.3]:

$$(14) \quad \omega(m) = \sup\{|\alpha| : \alpha \text{ minimal in } Z(m+M)\}.$$

In our setting, thanks to Dickson's lemma, this supremum turns out to be a maximum.

The  $\omega$ -primality of  $M$  is defined as  $\omega(M) = \max_{i \in \{1, \dots, k\}} \{\omega(m_i)\}$ .

EXAMPLE 3.17. Let  $M = \langle 3, 5, 7 \rangle$ . Then a minimal presentation for  $M$  is

$$\{((0, 2, 0), (1, 0, 1)), ((3, 1, 0), (0, 0, 2)), ((4, 0, 0), (0, 1, 1))\}.$$

Let us compute  $N$  the set of minimal elements of  $Z(3+M)$ . Trivially  $(1, 0, 0) \in N$ . As  $2 \times 5 = 3 + 7$  we get that  $(0, 2, 0) \in N$  (which is minimal since  $5 \notin 3+M$ ). Analogously  $(0, 0, 2), (0, 1, 1) \in N$ . Hence  $N = \{(1, 0, 0), (0, 2, 0), (0, 0, 2), (0, 1, 1)\}$ .

In the above example the  $\omega$ -primality of 3 can be computed easily due to the shape of the minimal presentation of  $M$ . For an arbitrary numerical semigroup, the  $\omega$ -primality can be calculated with the help of the Apéry sets. This fact together with [2, Remarks 5.9] and the following result by Barron, O'Neil and Pelayo (personal communication), allows a big improvement in computing times.

LEMMA 3.18. *For a numerical semigroup  $M \subset \mathbb{N}$  minimally generated by  $G \subset M$ , we have*

$$\omega(n) = \max \left\{ L(\langle G' \rangle, x+n) \mid G' \subset G, x \in \bigcap_{g \in G'} \text{Ap}(M, g) \right\}$$

where  $L(K, x)$  denotes the maximum factorization length of  $x$  in  $K$ .

For affine semigroups we can compute the set of minimal elements of  $Z(m+M)$  by using [47], which is the idea exploited in [18]. In Listing D.14 is implemented this computation based in 4ti2 ([30]) `zsolve` program with the 4ti2gap (see Appendix C) package for GAP ([16]). It results a more simple approach that finds  $Z(m+M)$  minimals by solving  $Ax = m + Ay$  (this step is explicitly performed by `FactorizationsVectorWRTList` from Listing D.3), or equivalently

$$(A \mid -A) \begin{pmatrix} x \\ y \end{pmatrix} = m,$$

and projecting on the  $x$  part of the solutions, to finally get the minimal elements from this set.

<sup>1</sup>Recall that  $p$  is prime if  $p \mid ab$  then  $p \mid a$  or  $p \mid b$ .

## 7. Invariants in half-factorial affine semigroups

In this section we summarize the adaptation of the invariants presented so far for the half-factorial setting. The results present in this section correspond to our work in [23].

Let  $M$  be the affine semigroup minimally generated by  $m_1, \dots, m_k$  and  $A$  the matrix as in Section 2, with columns  $m_1, m_2, \dots, m_k$ .

LEMMA 3.19. *The monoid  $M$  is half-factorial if and only if there exists  $h \in \mathbb{Q}^n$  such that  $hA = (1, \dots, 1)$ . If this is the case,  $L(m) = \{h \cdot m\}$ , for every  $m \in M$ .*

PROOF. For a half-factorial monoid  $M$ , every  $m \in M$  has  $\sharp L(m) = 1$ . This means that the ideal  $l_M$  is homogeneous. In view of [54, Lema 4.14], there exists  $h \in \mathbb{Q}^n$  such that

$$hA = (1, \dots, 1).$$

The converse is also true because if there exists such an  $h$ , then for any two factorizations  $\alpha, \beta$  of an element  $m \in M$ ,  $m = \phi(\alpha) = \phi(\beta)$ , and thus  $m = A\alpha = A\beta$ . Hence  $h \cdot m = hA\alpha = hA\beta$ , which leads to  $h \cdot m = (1, \dots, 1) \cdot \alpha = (1, \dots, 1) \cdot \beta$ , that is  $h \cdot m = |\alpha| = |\beta|$ .  $\square$

**7.1. Catenary degree in a half factorial monoid.** We will make extensive use of the preceding lemma to rewrite the concept of distance and give alternative characterizations of Betti elements. As we will see, this will have some nice consequences.

LEMMA 3.20. *Let  $h$  be as in Lemma 3.19. For  $\alpha, \beta \in Z(m)$ ,*

$$d(\alpha, \beta) = h \cdot m - |\alpha \wedge \beta|.$$

*In particular,  $d(\alpha, \beta) \leq h \cdot m$ , and the equality holds if and only if  $\alpha \cdot \beta = 0$ .*

PROOF. It is straightforward from Lemma 3.19.  $\square$

Hence, we have that

$$(15) \quad h \cdot m - \max_{\alpha, \beta \in Z(m)} |\alpha \wedge \beta| \leq c(m) \leq h \cdot m,$$

for each  $m \in M$ .

We see now that the second inequality becomes an equality precisely when  $m \in \text{Betti}(M)$ .

PROPOSITION 3.21. *Let  $m \in M$ . Then  $m \in \text{Betti}(M)$  if and only if  $c(m) = h \cdot m$ .*

PROOF. By definition  $m \in \text{Betti}(M)$  if and only if there exists  $\alpha, \beta \in Z(m)$  in different  $\mathcal{R}$ -classes. Equivalently, for every chain,  $\gamma_0, \dots, \gamma_r \in Z(m)$  from  $\alpha$  to  $\beta$ , there exist  $j$  such that  $\gamma_j \cdot \gamma_{j+1} = 0$ ; that is,  $d(\gamma_j, \gamma_{j+1}) = h \cdot m$  by Lemma 3.20. Since  $c(m) \leq h \cdot m$ , we obtain that the equality must hold. Conversely, if  $c(m) = h \cdot m$ , then there exists  $\alpha$  and  $\beta \in Z(m)$  such that  $d(\alpha, \beta) = c(m)$ , and for every chain  $\gamma_0, \dots, \gamma_r \in Z(m)$  from  $\alpha$  to  $\beta$ , there exist  $j$  such that  $d(\gamma_j, \gamma_{j+1}) \geq c(m) = h \cdot m$ . By Lemma 3.20,  $\gamma_j \cdot \gamma_{j+1} = 0$ . So  $\alpha$  and  $\beta$  belong to different connected components of  $G_m$ .  $\square$

Next result shows that all possible catenary degrees in a half-factorial monoid are attained in its Betti elements.

**THEOREM 3.22.** *Let  $M$  be half-factorial, and let  $m \in M$  with  $\sharp Z(m) \geq 2$ . There exists  $t \in \text{Betti}(M)$  such that  $c(m) = c(t)$ .*

**PROOF.** Let  $h \in \mathbb{Q}^n$  as in Lemma 3.19 be such that  $hA = (1, \dots, 1)$ .

There exist  $\alpha, \beta \in Z(m)$  such that  $d(\alpha, \beta) = c(m)$  and for every chain,  $\gamma_0, \dots, \gamma_r \in Z(m)$  from  $\alpha$  to  $\beta$ , there exist  $j$  with  $d(\gamma_j, \gamma_{j+1}) \geq c(m)$ . Thus by Lemma 3.20, for  $j$  we have

$$h \cdot m - |\gamma_j \wedge \gamma_{j+1}| \geq c(m) = h \cdot m - |\alpha \wedge \beta|,$$

this is to say  $|\alpha \wedge \beta| \geq |\gamma_j \wedge \gamma_{j+1}|$ .

Let  $t = m - \phi(\alpha \wedge \beta)$ . We take the factorizations  $\alpha' = \alpha - (\alpha \wedge \beta)$  and  $\beta' = \beta - (\alpha \wedge \beta)$  of  $t$ . As  $\alpha' \cdot \beta' = 0$  by Lemma 3.20:  $d(\alpha', \beta') = h \cdot t - 0$ .

By Lemma 3.19,  $h \cdot \phi(\alpha \wedge \beta) = |\alpha \wedge \beta|$ , and from this we can write

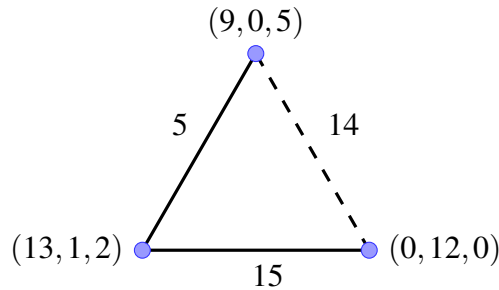
$$d(\alpha', \beta') = h \cdot t = h \cdot m - |\alpha \wedge \beta| = c(m).$$

Now, we prove that  $t \in \text{Betti}(M)$ . Every chain  $\gamma'_0, \dots, \gamma'_r \in Z(t)$  from  $\alpha'$  to  $\beta'$  lifts to a chain  $\gamma_0, \dots, \gamma_r \in Z(m)$  from  $\alpha$  to  $\beta$  (indeed, it suffices to take  $\gamma_i = (\alpha \wedge \beta) + \gamma'_i$ , for all  $i$ ), and  $d(\gamma_j, \gamma_{j+1}) = d(\gamma'_j, \gamma'_{j+1})$ . By the above argument, there exists  $j$  such that  $|\alpha \wedge \beta| \geq |\gamma_j \wedge \gamma_{j+1}|$ . Notice that by construction  $\alpha \wedge \beta \leq \gamma_j \wedge \gamma_{j+1}$ , and this forces  $\alpha \wedge \beta = \gamma_j \wedge \gamma_{j+1}$ . We conclude that  $\gamma'_j \wedge \gamma'_{j+1} = 0$  for some  $j$ .

Therefore, it follows that  $t$  is a Betti degree (because  $\alpha'$  and  $\beta'$  are in different  $\mathcal{R}$ -classes), and by Proposition 3.21,  $c(t) = h \cdot t = c(m)$ .  $\square$

This result does not hold for non half-factorial monoids.

**EXAMPLE 3.23.** Let  $M = \langle 31, 47, 57 \rangle \subseteq \mathbb{N}$ . Then  $\text{Betti}(M) = \{171, 517, 527\}$ , and  $c(171) = 5$ ,  $c(517) = 15$  and  $c(527) = 17$ . However,  $c(564) = 14 \notin \{5, 15, 17\}$ .



From Lemma 3.15, the above theorem can be restated as saying that the catenary degrees of  $M$  are the total degrees of the minimal binomial generators of  $\mathfrak{l}_M$ .

**COROLLARY 3.24.** *The catenary degree of  $M$  is the maximum of the total degrees of a minimal system of binomial generators of  $\mathfrak{l}_M$ .*

As we mentioned above the catenary degree of  $M$  is attained in the catenary degree of one of its Betti elements. This last corollary gives an alternative proof of this fact in the half-factorial setting.

**7.2. The equal catenary degree revisited.** Given  $\{m_1, \dots, m_k\} \subset \mathbb{N}^n$ , and the matrix  $A = (m_1 | \dots | m_k)$ , we construct a half-factorial monoid whose catenary degree agrees with the equal catenary degree of the original monoid  $M$ . We also define the matrix  $A^{\text{eq}} = ((1, m_1)^T | \dots | (1, m_k)^T) \in \mathbb{N}^{n+1} \times \mathbb{N}^k$  whose columns are generators of a monoid that we denote by  $M^{\text{eq}}$ . Notice that  $(i, m) \in M^{\text{eq}}$  if and only if  $m \in M$  and  $i \in L(m)$ . Also, taking  $h = (1, 0, \dots, 0)$  by Lemma 3.19,  $M^{\text{eq}}$  is a half-factorial monoid.

**PROPOSITION 3.25.** *Let  $M$  be an affine semigroup. Then  $c_{\text{eq}}(M) = c(M^{\text{eq}})$ .*

**PROOF.** Just notice that as observed above, the factorizations of  $(i, m)$  in  $M^{\text{eq}}$  correspond to factorizations of  $M$  with length  $i$ .  $\square$

**EXAMPLE 3.26.** Let  $M = \langle 3, 5, 7 \rangle$ . Then  $M^{\text{eq}} = \langle (1, 3), (1, 5), (1, 7) \rangle$ . A presentation for  $M^{\text{eq}}$  can be computed for instance as in Example 3.16, from  $\pi$  and elimination, or just using the appropriate command in `numericalsgps`.

```
gap> a:=AffineSemigroup([[1,3],[1,5],[1,7]]);
<Affine semigroup in 2 dimensional space, with 3 generators>
gap> MinimalPresentationOfAffineSemigroup(a);
[[ [ 1, 0, 1 ], [ 0, 2, 0 ] ]]
```

Hence a presentation for  $M^{\text{eq}}$  is  $\{(1, 0, 1), (0, 2, 0)\}$ . It follows that  $c(M^{\text{eq}}) = 2$ , and we deduce that  $c_{\text{eq}}(M) = 2$ . Also, from the minimal presentation we obtained in Example 3.16,  $c(M) = 4$ .

As a consequence of Corollary 3.24 and Section 5, we obtain the following.

**COROLLARY 3.27.** *The equal catenary degree of  $M$  is the maximum of the total degrees of a minimal system of binomial generators of  $M^{\text{eq}}$ .*

**7.3. The homogeneous catenary degree.** The *homogeneous catenary degree* of an element  $m \in M$ , denoted by  $c_{\text{hom}}(m)$ , is the least  $N \in \mathbb{N}$  such that for any  $\alpha, \beta \in Z(m)$  there exists a  $N$ -chain from  $\alpha$  to  $\beta$  in  $Z(m) \cap \{v \mid |v| \leq \max\{|\alpha|, |\beta|\}\}$ . If no such  $N \in \mathbb{N}$  does exist, we define  $c_{\text{hom}}(m) = \infty$ .

The computation of  $c_{\text{hom}}(m)$  is performed as  $c(m)$ , but previously from the complete graph we eliminate the edges with weight greater than  $\max\{|\alpha|, |\beta|\}$ .

Now we construct a half-factorial monoid  $M^{\text{hom}}$  given by the set of generators

$$\{e_0, (1, m_1), \dots, (1, m_k)\} \subseteq \mathbb{N} \times \mathbb{N}^n$$

with  $e_0 = (1, 0, \dots, 0)$ . This is also a half-factorial monoid for  $h = (1, 0, \dots, 0)$ . First, we see the relationship between the factorization on  $M$  and  $M^{\text{hom}}$ .



LEMMA 3.28. *Under the standing hypothesis,  $Z((i, m)) = \{(j, \alpha) \in \mathbb{N} \times Z(m) \mid j = i - |\alpha|\}$ .*

PROOF. Let  $(\alpha_0, \dots, \alpha_k) \in Z((i, m))$ , then  $\alpha_0 e_0 + \alpha_1(1, m_1) + \dots + \alpha_k(1, m_k) = (i, m)$ . This implies that  $m = \alpha_1 m_1 + \dots + \alpha_k m_k$  and  $i = \alpha_0 + \alpha_1 + \dots + \alpha_k$ . Take  $j = \alpha_0$  and  $\alpha = (\alpha_1, \dots, \alpha_k)$ .

The other inclusion is also straightforward. Let  $\alpha \in Z(m)$  for  $m \in M$ , taking  $j \in \mathbb{N}$  with  $|\alpha| \leq j$  then  $i = j - |\alpha|$  and  $(i, m) = i \cdot e_0 + \sum_{l=1}^k \alpha_l m_l$ .  $\square$

Now we see that the distances of factorizations of an element in  $M^{\text{hom}}$  are ruled by the factorizations of the corresponding one in  $M$ .

LEMMA 3.29. *Let  $(i, m) \in M^{\text{hom}}$ , and let  $(j_\alpha, \alpha), (j_\beta, \beta) \in Z((i, m))$ . Then*

$$d((j_\alpha, \alpha), (j_\beta, \beta)) = d(\alpha, \beta).$$

PROOF. From Lemma 3.28,  $i = |\alpha| + j_\alpha = |\beta| + j_\beta$ . Assume without loss of generality that  $|\beta| \geq |\alpha|$  and in consequence  $j_\beta \leq j_\alpha$ . Set  $\gamma = \alpha \wedge \beta$ . Then  $(j_\alpha, \alpha) \wedge (j_\beta, \beta) = (j_\beta, \gamma)$ , and using Lemma 3.20:

$$\begin{aligned} d((j_\alpha, \alpha), (j_\beta, \beta)) &= h \cdot (i, m) - |(j_\beta, \gamma)| \\ &= i - (j_\beta + |\gamma|) = |\beta| - |\gamma| \\ &= \sum_{i=1}^k \beta_i - \sum_{i=1}^k \gamma_i \\ &= \sum_{i=1}^k \beta_i - \gamma_i = |\beta - \gamma|. \end{aligned}$$

We supposed that  $|\beta| \geq |\alpha|$ , then  $d(\alpha, \beta) = \max\{|\alpha - \gamma|, |\beta - \gamma|\} = |\beta - \gamma|$ .  $\square$

PROPOSITION 3.30. *Let  $M$  be an affine semigroup. Then  $c_{\text{hom}}(M) = c(M^{\text{hom}})$ .*

PROOF. Let  $\alpha, \beta \in Z(m)$ , for some  $m \in M$ . Assume without loss of generality that  $j_\alpha = |\alpha| \leq |\beta| = j_\beta$ . Then by Lemma 3.28,  $(j_\beta - j_\alpha, \alpha), (0, \beta)$  are factorizations of  $(j_\beta, m)$  and there exists a  $c(M^{\text{hom}})$ -chain  $(j_1, \gamma_1), \dots, (j_r, \gamma_r)$  joining them. For every factorization of this chain it is true that for  $q \in \{1, \dots, r\}$ ,  $j_q = j_\beta - |\gamma_q|$ , as a consequence  $|\gamma_q| \leq |\beta|$ , and thus  $\gamma_1, \dots, \gamma_r$  is a  $c(M^{\text{hom}})$ -chain joining  $\alpha$  and  $\beta$  with  $|\gamma_q| \leq \max\{|\alpha|, |\beta|\}$ . This proves  $c_{\text{hom}}(M) \leq c(M^{\text{hom}})$ .

Conversely, let  $(j_\alpha, \alpha), (j_\beta, \beta)$  be factorizations of  $(i, m) \in M^{\text{hom}}$ . In view of Lemma 3.28,  $j_\alpha + |\alpha| = j_\beta + |\beta| = i$ . Assume without loss of generality that  $|\alpha| \leq |\beta|$ . Let  $\gamma_1, \dots, \gamma_r$  be a  $c_{\text{hom}}(M)$ -chain from  $\alpha$  to  $\beta$ . By definition, for  $q \in \{1, \dots, r\}$ ,  $|\gamma_q| \leq |\beta| \leq i$ . Set  $j_q = i - |\gamma_q|$ , then  $(j_1, \gamma_1), \dots, (j_r, \gamma_r)$  is a  $c_{\text{hom}}(M)$ -chain joining  $(j_\alpha, \alpha), (j_\beta, \beta)$ . Thus  $c(M^{\text{hom}}) \leq c_{\text{hom}}(M)$ , and this completes the proof.  $\square$

As a consequence of Corollary 3.24 we obtain the following.

**COROLLARY 3.31.** *The homogeneous catenary degree of  $M$  is the maximum of the total degrees of a minimal system of binomial generators of  $\mathsf{l}_{M^{\text{hom}}}$ .*

This corollary allows us to compute the homogeneous catenary degree of  $M$  once we know any of its presentations (see Listing D.15).

We prove that this new catenary degree is an upper bound for the usual catenary degree.

**PROPOSITION 3.32.** *Let  $M$  be an affine semigroup. Then  $c(M) \leq c_{\text{hom}}(M)$ .*

**PROOF.** Let  $m \in M$  and  $\alpha, \beta \in Z(m)$  with  $|\alpha| \leq |\beta|$ . We show that there exists a  $c_{\text{hom}}(M)$ -chain joining  $\alpha$  and  $\beta$ . Set  $j_\alpha = |\alpha| \leq |\beta| = j_\beta$ , then  $(j_\beta - j_\alpha, \alpha)$  and  $(0, \beta) \in Z((j_\beta, m))$ . From the definition of homogeneous catenary degree, there exists a  $c(M^{\text{hom}})$ -chain  $(j_1, \gamma_1), \dots, (j_r, \gamma_r)$  of factorizations of  $(j_\beta, m)$  from  $(j_\beta - j_\alpha, \alpha)$  and  $(0, \beta)$  and  $d((j_q, \gamma_q), (j_{q+1}, \gamma_{q+1})) \leq c(M^{\text{hom}})$ . Besides  $d((j_q, \gamma_q), (j_{q+1}, \gamma_{q+1})) = d(\gamma_q, \gamma_{q+1})$  from Lemma 3.29, where  $\gamma_1, \dots, \gamma_r$  is a  $c(M^{\text{hom}})$ -chain joining  $\alpha$  and  $\beta$ .  $\square$

The catenary degree might be strictly smaller than the homogeneous catenary degree.

**EXAMPLE 3.33.** Let  $M = \langle 10, 11, 14, 19 \rangle \subseteq \mathbb{N}$ . One can check that  $c(m) = 4$ . Since a minimal system of binomial generators of  $\mathsf{l}_{M^{\text{hom}}} \subseteq \mathbb{k}[x_0, \dots, x_4]$  is  $\{x_2x_3^2 - x_1^2x_4, x_1x_3^2 - x_0x_4^2, x_2^3 - x_0x_3x_4, x_1^3 - x_0x_2x_4, x_1^2x_2^2 - x_0x_3^3, x_3^5 - x_1x_2^2x_4^2\}$ , we may conclude by Corollary 3.31 that  $c_{\text{hom}}(M) = 5$ .

```
gap> s:=NumericalSemigroup(10,11,14,19);
<Numerical semigroup with 4 generators>
gap> HomogeneousCatenaryDegreeOfNumericalSemigroup(s);
5
gap> CatenaryDegreeOfNumericalSemigroup(s);
4
```

We now compare the homogeneous catenary degree with the widely studied monotone catenary degree.

**PROPOSITION 3.34.** *Let  $M$  be an affine semigroup. Then  $c_{\text{hom}}(M) \leq c_{\text{mon}}(M)$ .*

**PROOF.** Let  $(i, m) \in M^{\text{hom}}$  and  $(j_\alpha, \alpha), (j_\beta, \beta) \in Z((i, m))$ . Assume for instance that  $i - j_\alpha = |\alpha| \leq |\beta| = i - j_\beta$ . From the definition of  $c_{\text{mon}}(M)$ , there exist  $\gamma_1, \dots, \gamma_r \in Z(m)$  with  $\gamma_1 = \alpha$ ,  $\gamma_r = \beta$ , and for  $q \in \{1, \dots, r\}$ ,  $d(\gamma_q, \gamma_{q+1}) \leq c_{\text{mon}}(M)$  and  $|\gamma_q| \leq |\gamma_{q+1}|$ . Set  $j_q = i - |\gamma_q|$ , then  $(j_1, \gamma_1), \dots, (j_r, \gamma_r)$  is a  $c_{\text{mon}}(M)$ -chain joining  $(j_\alpha, \alpha)$  and  $(j_\beta, \beta)$ . Thus  $c(M^{\text{hom}}) \leq c_{\text{mon}}(M)$ .  $\square$

In some cases the homogeneous catenary degree is sharper than the monotone catenary degree.

**EXAMPLE 3.35.** Let  $M = \langle 11, 19, 32 \rangle$ . Then

$$c_{\text{eq}}(M) = 3 < c(M) = c_{\text{hom}}(M) = c_{\text{mon}}(M) = 9.$$

For embedding dimension 3 numerical semigroups, the homogeneous catenary degree (together with the homogeneous Betti elements) have been deeply studied in [1].

7.3.1. *Computing the monotone catenary degree by homogenization.* To compute the monotone catenary degree of  $M$  we recall the procedure exposed for the equal catenary degree, but with the condition:  $|a| \leq |b|$ , where  $a$  and  $b \in Z(m)$ . We add a new variable to express conveniently the inequality as an equality:  $|a| - |b| + c = 0$  with  $c \in \mathbb{N}_0$ . This leads us to the following system of equations, by assigning a corresponding unknown to each factorization and the scalar:

$$(16) \quad \begin{pmatrix} A & -A & 0 \\ \mathbb{1} & -\mathbb{1} & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0.$$

In order to exploit the speed of Graver basis computing with 4ti2, we homogenize:

$$(17) \quad \begin{pmatrix} A & 0 & -A & 0 \\ \mathbb{1} & 1 & -\mathbb{1} & -1 \end{pmatrix} \begin{pmatrix} x \\ z \\ y \\ t \end{pmatrix} = 0.$$

The solutions of (17) are equivalent to those of (16), in other words, the set of irreducibles of  $\sim_M$  (11) for the homogeneous generating set of  $M^{\text{hom}}$  is equivalent to the set of irreducibles of  $\sim_M$  with the monotony condition  $|a| \leq |b|$ . Let  $X$  be the set of minimal solutions of (16), and  $Y$  the set of minimal solutions of (17), with  $(x, z, y, t) \in Y$ :

- If  $z \cdot t = 0$ , then we have 2 cases:
  - (1) If  $(x, z, y, 0) \in Y$ , then  $(A \mid -A)(x \mid y)^T = 0$  and  $|x| + z - |y| = 0$ , thus  $(x, y, z) \in X$ .
  - (2) If  $(x, 0, y, t) \in Y$ , then  $|y| = |x| + t$  and we can write  $(A \mid -A)(y \mid x)^T = 0$ , thus  $(y, x, t) \in X$ .
- If  $z \cdot t \neq 0$ , assume without loss of generality that  $z > t$ . Then for some  $l \in \mathbb{N}$ ,  $z = t + l$ . As  $(x, z, y, t) \in Y$ ,  $|x| + t + l = |y| + t$ , we deduce  $(x, l, y, 0)$  is a nontrivial solution of (17), and  $(x, l, y, 0) < (x, z, y, t)$ , contradicting that  $(x, z, y, t) \in Y$ . So this setting never occurs.

As for the equal catenary degree, now the Graver basis elements of

$$(18) \quad \begin{pmatrix} A & 0 \\ \mathbb{1} & 1 \end{pmatrix}$$

are the irreducibles of  $\sim_M$  for  $M^{\text{hom}}$ ,  $(x, z) \in \mathbb{Z}^k \times \mathbb{Z}$  (but now with the homogenization term written as the last component). With the notation of  $x = x^+ - x^-$  and using the same arguments for the equal catenary degree, for every  $(x, z)$  in the Graver basis of (18):

- if  $z \geq 0$  then  $(x^+, z, x^-, 0)$  is a solution of (17) and  $(x^+, x^-, z)$  is solution of (16), and
- for  $z < 0$   $(x^+, 0, x^-, z)$  is a solution of (17) and  $(x^-, x^+, -z)$  is solution of (16).

Listing D.16 uses this procedure by computing the Graver basis with the `4ti2gap` ([25]) package for the GAP system ([16]), in the affine semigroups setting.

**7.4. The tame degree in half-factorial monoids.** We assume that  $\{m_1, \dots, m_k\} \subseteq \mathbb{Z}^n$  is a minimal system of generators of  $M$ , and we introduce this notation: given  $m, m'$  in  $\mathbb{Z}^n$ , recall that we write  $m \leq_M m'$  if  $m' - m \in M$ , and given  $c, c'$  in  $\mathbb{Z}^k$ , we write  $c \leq c'$  if  $c' - c \in \mathbb{N}^k$ .

**PROPOSITION 3.36.** *Let  $M$  be an affine semigroup. Then  $t(M) \leq t(M^{\text{hom}})$ .*

**PROOF.** Let  $m \in M$  and select  $i \in \{1, \dots, k\}$  such that  $m_i \leq_M m$ , and let  $m' = m - m_i$ . Assume that there exists  $\alpha = (\alpha_1, \dots, \alpha_k) \in Z(m)$  with  $\alpha_i = 0$  (for  $\alpha_i \neq 0$  it suffices to take  $\alpha = \alpha'$  in the definition of tame degree;  $d(\alpha, \alpha') = 0$  in this case). Let  $j = \max L(m)$ ,  $j' = \max L(m')$ , and  $l_\alpha = j - |\alpha|$ . Let  $\beta \in Z(m')$  be such that  $|\beta| = j'$ . As  $\beta + e_i \in Z(m)$ , we deduce that  $j' + 1 \leq j$ . Then  $(j, m)$  and  $(j - 1, m - m_i) = (j, m) - (1, m_i)$  are elements of  $M^{\text{hom}}$ , and  $(l_\alpha, \alpha) \in Z((j, m))$ . So by definition of  $t(M^{\text{hom}})$ , there exists  $(l_\gamma, \gamma) \in Z((j, m))$  with  $\gamma \cdot e_i \neq 0$  and  $d((l_\alpha, \alpha), (l_\gamma, \gamma)) \leq t(M^{\text{hom}})$ . From Lemma 3.29 we deduce that  $d(\alpha, \gamma) \leq t(M^{\text{hom}})$ . This proves that  $t(M) \leq t(M^{\text{hom}})$ .  $\square$

**7.5. Omega primality for half-factorial monoids.** In the half-factorial case, both tame degree and  $\omega$ -primality coincide.

**PROPOSITION 3.37.** *Let  $M$  be an affine semigroup. Assume that  $M$  is half-factorial. Then*

$$\omega(M) = t(M).$$

**PROOF.** It is well known that  $\omega(m) \leq t(M)$  (see [27, Theorem 3.6]). So we only have to prove the other inequality. Let  $m \in M$  be minimal with respect to  $\leq_M$  fulfilling that  $t(m) = t(M)$ . Then according to [2, Lemma 5.4] and Lemma 3.9, there exists  $\alpha, \beta \in Z(m)$  such that  $t(m) = d(\alpha, \beta)$  with  $\alpha$  minimal (with respect to  $\leq$ ) in  $Z(m_i + M)$ ,  $\alpha \cdot e_i = 0$  and  $\beta \cdot e_i \neq 0$ . In light of the last result,  $\alpha \cdot \beta = 0$ , whence  $d(\alpha, \beta) = \max\{|\alpha|, |\beta|\}$ . As  $M$  is half-factorial we obtain  $\max\{|\alpha|, |\beta|\} = |\alpha| = |\beta|$ . Hence  $t(m) = |\alpha|$ . From (14) we conclude that  $|\alpha| \leq \omega(m_i) \leq \omega(M)$ .  $\square$

**EXAMPLE 3.38.** It is well known that  $c(m) \leq \omega(M)$  (see [27, Sec. 3]). In the half-factorial case, this inequality might be strict. For instance, let the affine semigroup  $M = \langle (1, 0), (1, 3), (1, 5), (1, 7) \rangle$ , then  $c(M) = 4 < 7 = \omega(M)$ .

## Results, conclusions and future work

Throughout the manuscript we have been listing the results obtained, which are more than we expected initially.

Our software `DPSolve` has in general worst performance than `Normaliz` and `4ti2`. We have not been able to characterize families of systems of equations in which `DPSolve` runs faster, nor any heuristics suitable to discriminate which software to use for a given system of equations. We are now testing parallel implementations of our algorithm, which seem to fit with the structure of the algorithm.

The lack of satisfactory results encouraged us to develop the package `4ti2gap`, to deal with factorizations and presentations of affine semigroups in `GAP`.

The results on affine convex body semigroups, apart from generalizing the concept of proportionally modular numerical semigroups, had an unexpected and gratifying consequence: the possibility of building in an easy way, families of Buchsbaum affine semigroups. We are now trying to generalize this ideas to higher dimensions.

Our study of nonunique factorization invariants started due to the interconnection with linear integer programming. We wanted to determine the range of possible catenary degrees, and we were able to achieve this for half-factorial monoids. Also we introduced a new promising invariant, and were able to relate equal catenary degree and this new catenary degree with catenary degree in auxiliary half-factorial monoids, that are inspired in classical constructions.

After implementing algorithms for the calculation of these invariants in `GAP`, we discovered that some could be improved. New results have appeared then for the computation of the tame degree, and in the future we should focus in better options to calculate monotone catenary degree. We are also doing experiments with alpha release of the parallel version on `GAP`, named `hpc-gap`. We expect to take advantage of its programming interface to gain in performance when the hardware architecture is available. At the present time, in the context of the `numericalsgps` ([13]) package there is an effort testing `hpc-gap` in this sense, to parallelize the calculations of catenary degrees, tame degree and  $\omega$ -primality. Many work is still to be done in `hpc-gap`.



## APPENDIX A



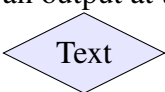


### CircleSG

CircleSG ([19]) is a set of routines included in a Mathematica<sup>1</sup> package. Those routines are very specific to support the main routine called also CircleSG, for this reason we do not explain them in detail. In this appendix we show a block diagram describing the main routine steps.

#### 1. Notes about the implementation

Figures 1 and 2 show the computation path of the main function in CircleSG package. It takes the center and radius of a circle, all positive values, as the necessary input parameters.

The elements in the figures of the block diagram have these meanings.

- , denotes a processing step. The initial block is drawn with a thick edge.
- , denotes an input at the starting block or, if it has a thick edge, it denotes an output at the end of processing.
- , denotes a decision.
- , data transfer and process flow.
- , data transfer and process flow between different pages.

The implementation takes into account the fact that the sequence of circles can intersect with the  $x$  and  $y$  axes. In this case, they turn into the rays of the cone that encloses the affine semigroup. With this in mind, in Figure 1 the blocks labelled as [1a] and [1b] give the generators of the affine semigroup elements on the rays. These will be used to replace those of the cone in block [2], one at a time. Although it is not made explicit, the resulting set,  $B$ , is checked to discard non-minimal elements inserted by applying Lemma 2.5. This requires the resolution of a system of linear Diophantine equations, in order to find one particular solution to know that a given element can be expressed as a linear combination of other elements. Initially we used an implementation in Mathematica of the algorithm of Contejean and Devie[10] modified for our purposes by doing an external call from Mathematica framework. The actual version of CircleSG uses FindInstance included in Mathematica, resulting more convenient by speed and portability.

---

<sup>1</sup>Every reference to the term Mathematica in this document, is referred to the set of programs of Wolfram Research, except where it is otherwise stated. Mathematica is a registered trademark of Wolfram Research Inc.

Using  $d$  in Block [4] of Figure 2 we find the index,  $i$ , of the circle such that, every element in any of the circles after the  $i$ th in the sequence, is in the affine semigroup  $\mathcal{S}$ . Next we collect those elements outside of the circles up to the  $i$ th and inside the cone, and apply the loop steps defined by Blocks [5] and [6]. This loop appends the minimal generators needed to replace those outside of the circles, inside of the cone. As in Block [2], every new element is discarded in case it is not minimal. Clearly, the loop on Blocks [5] and [6] can be very time consuming due to the distance  $d$ , which determines the number of elements in  $E$ .

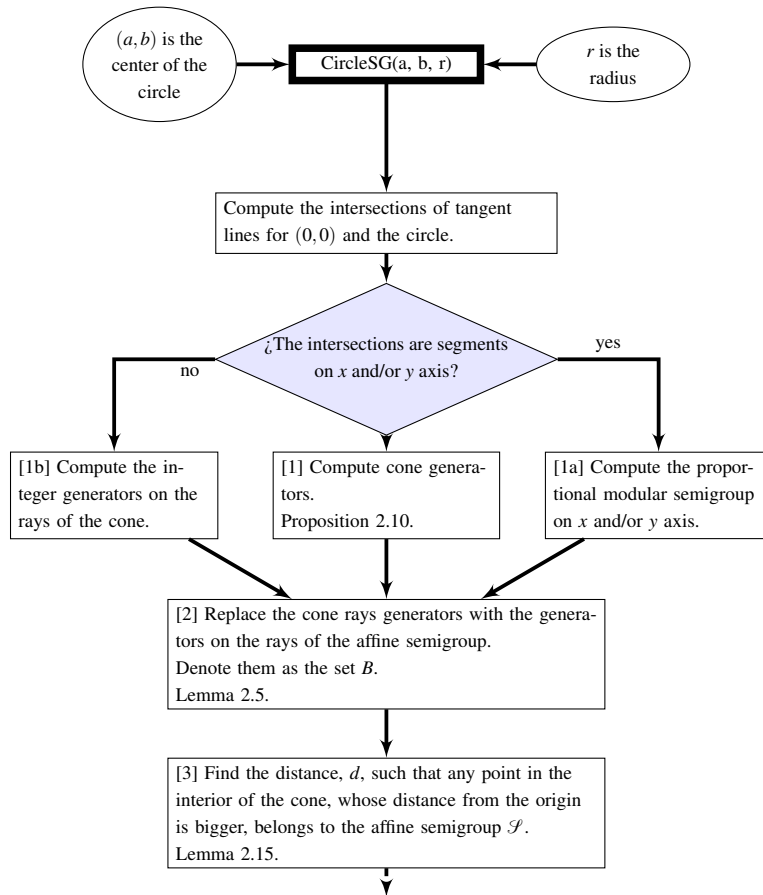


FIGURE 1. CircleSG processing diagram.



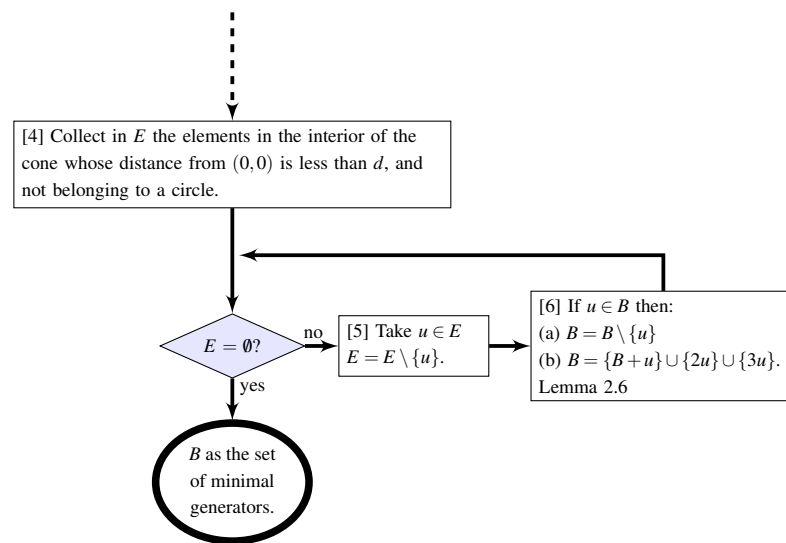


FIGURE 2. CircleSG processing diagram cotinuation.



## APPENDIX B

### PSGIsBuchsbaumQ

This is the name of the routine that implements in Mathematica<sup>1</sup> the test to the Buchsbaum property of an affine convex polygonal semigroup. It is part of a package named PolySGTools ([20]). This package also offers routines to test the membership of an element to this kind of affine semigroups, and to compute the minimal generating set of a segment in  $\mathbb{Q}^2$ , and for an affine polygonal semigroup in  $\mathbb{N}^2$ .

#### 1. Notes about the implementation

PSGIsBuchsbaumQ is heavily supported by other routines in the package PolySGTools. In special for testing when an element belongs to the closure of the affine polygonal semigroup,  $\mathcal{P}$ . Besides, it is a quite self-contained by design. In this sense it is not complex because of its dependencies, but it is because of the large number of test, although some are symmetric with a similar structure. The path of computation has been designed to take advantage of the computations needed in various points of decision.

The blocks diagram elements have the same meaning as in Appendix A.

---

<sup>1</sup>Every reference to the term Mathematica in this document, is referred to the set of programs of Wolfram Research, except where it is otherwise stated. Mathematica is a registered trademark of Wolfram Research Inc.

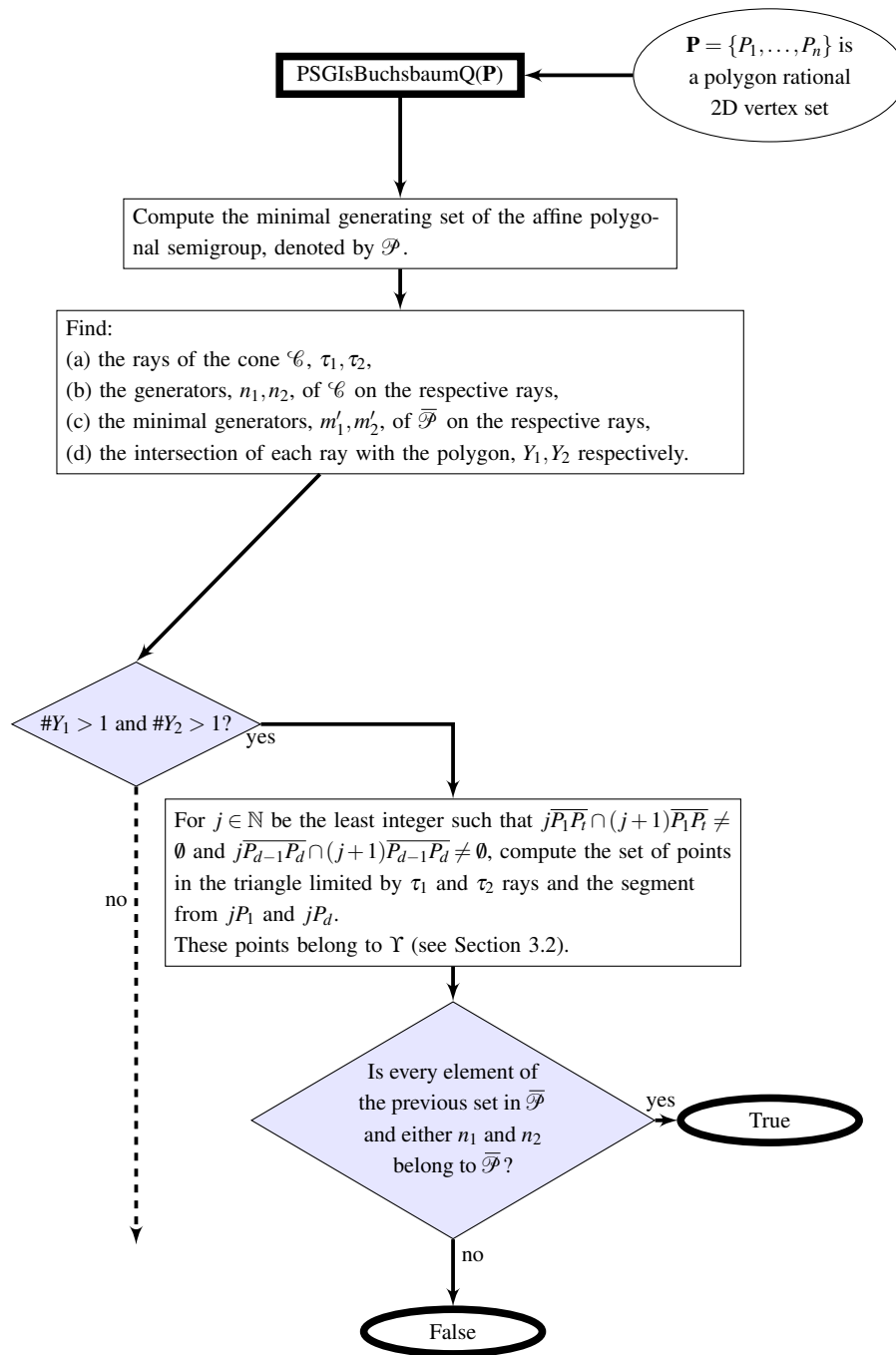


FIGURE 1. PSGISBuchsbauMQ processing diagram (I).

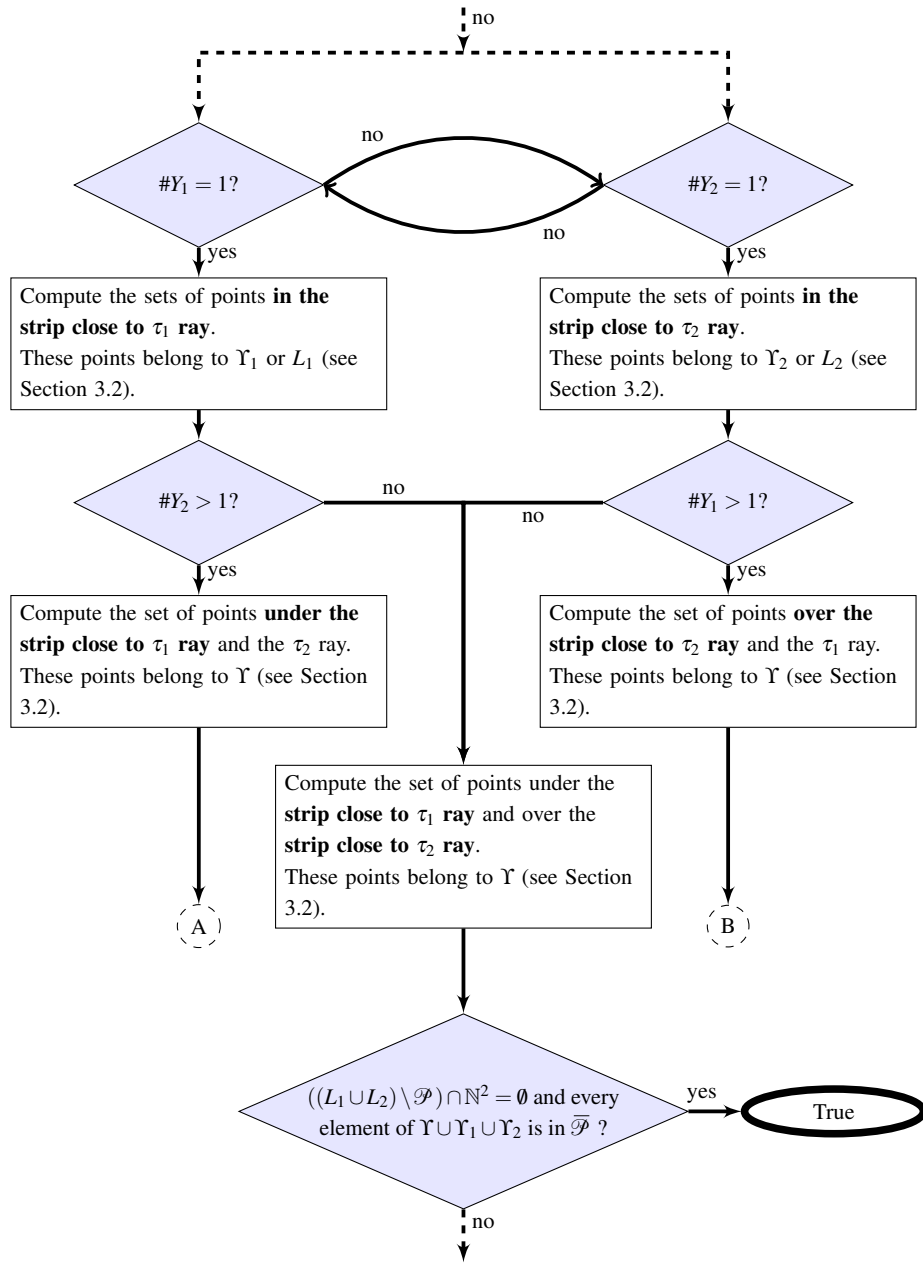


FIGURE 2. PSGIsBuchsbauMQ processing diagram (II).

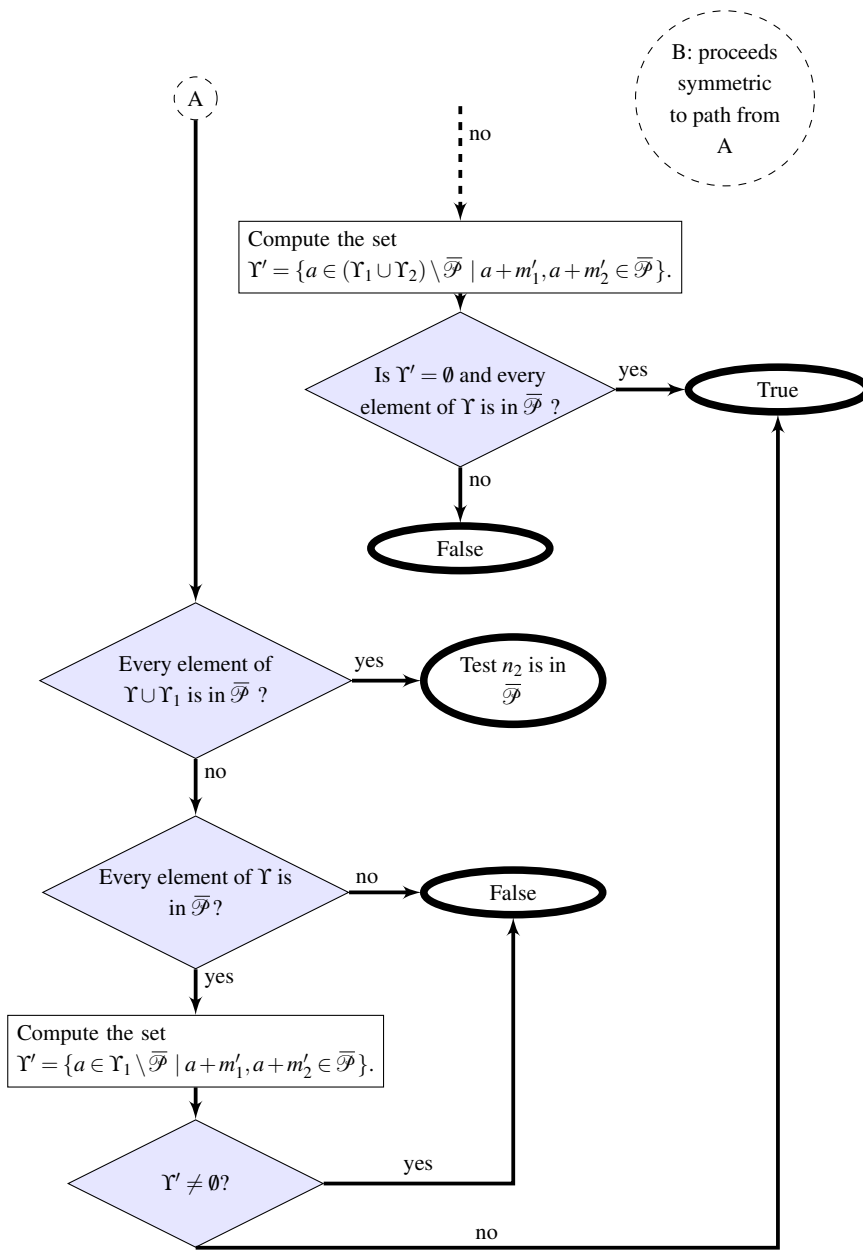


FIGURE 3. PSGISBUCHSBAUMQ processing diagram (III).

## APPENDIX C

### 4ti2gap

#### 1. Introduction

The package `4ti2gap` ([25]) is a GAP ([16]) wrapper for the algebraic software `4ti2` (see [30]). It was produced mainly due to the fact that presentations for affine and numerical semigroups are in correspondence with binomial ideals, and `4ti2` makes fast computations with these. Also factorizations of elements in affine semigroups are solutions of systems of Diophantine linear equations, which can be computed with its `zsolve` component.

`4ti2gap` uses direct linking with the shared libraries of `4ti2`. For this reason, some overhead in the routines calling is avoided, saving the necessary transformation of the data structures between both programs.

#### 2. Design

The set of tools included in `4ti2` are arranged into two separated programs. They group the different functions we are interested in.

- `4ti2`, which gives the name to the package, embeds the computations of the programs `groebner`, `minimize`, `markov`, among others. It has versions for 32 and 64 bits processor architectures, and multiple precision as an option, in the case that the GNU MP library is installed in the system. So there exist `4ti2int32`, `4ti2int64` and if it is the case, `4ti2gmp`. Also, the respective library files are provided.
- `zsolve` offers `hilbert`, `graver`, and also itself, which can be used to compute the solutions over  $\mathbb{Z}$  of a linear system of equations. In this case all the options of arithmetic precision are included in `zsolve`.

Indeed, one of the tasks to accomplish is the adaptation of data representation between GAP and `4ti2`. To this end, at the lowest fine-grain level, the conversion of data is based on the corresponding code of `NormalizInterface` package (see [28]).

The first approach that we developed, was designed to provide separated functions according to the arithmetic precision needed, as in `4ti2`. From this we placed the offered functions in two files `4ti2gap.so` and `4ti2gapgmp.so`, respectively for the processor architecture word size setting and GNU MP library, if available for `4ti2`.

Unfortunately, this caused a bad behavior (segmentation fault errors) in GNU/Linux systems, specifically when computing Gröbner bases. It also caused memory access errors

after finishing a GAP session. This was not detected in the OSX installation, which was our main platform of development.

In consequence, we redesigned the structure of the code, and adapted it to the characteristics of the interface to groebner (`4ti2[int32 | int64 | gmp]`) and `zsolve` components. Now, there is only one dynamic library that supports all of them, called `4ti2gap.so`.

The source code has 3 main component files: `4ti2gap.cc`, `4ti2groebner.cc` and `4ti2zsolve.cc`. The code in `4ti2gap.cc` does initialization task for GAP. We briefly describe the other files in the next sections.

**2.1. `4ti2zsolve.cc`.** In this file we implement the components that use the interface of `zsolve` defined in `ZSolveAPI.hpp`. This is performed by linking its object code to the corresponding dynamic library of the `4ti2` package. The class `_4ti2_zsolve_::ZSolveAPI<T>` has different methods. We use the next:

- `create_matrix(std::istream& in, const char* name)`, to provide input data. The parameter `name` is used to distinguish between the types of inputs. This creates a `_4ti2_zsolve_::VectorArray<T>` component.
- `set_options(int argc, char** argv)`, to select precision and verbosity.
- `compute()` performs the computations given the setting selected using the two previous methods.
- `get_matrix(const char* name)` gives access to the results stored in `_4ti2\_-\-zsol\-ve_::VectorArray<T>` specific matrices.

In this source file we have the following library callable functions from a GAP session. Those whose name ends in `GMP`, are the corresponding versions with multiple precision support.

```
Obj _4ti2zsolve_Hilbert( Obj self, Obj list );
Obj _4ti2zsolve_HilbertGMP( Obj self, Obj list );
Obj _4ti2zsolve_Graver( Obj self, Obj list );
Obj _4ti2zsolve_GraverGMP( Obj self, Obj list );
Obj _4ti2zsolve_ZSolve( Obj self, Obj list );
Obj _4ti2zsolve_ZSolveGMP( Obj self, Obj list );
```

All of them take a list as an argument, which must be a sequence of “string” and matrix, as in the example below.

EXAMPLE C.1. Consider the following system of linear Diophantine inequalities:

$$\begin{aligned} x - y &\leq 2, \\ -3x + y &\leq 1, \\ x + y &\geq 1, \\ y &\geq 0, \end{aligned}$$

```
gap> problem:=["mat", [[1, -1], [-3, 1], [1, 1]],
```



```

"rel", ["<", "<", ">"],
"rhs", [[2, 1, 1]], "sign", [0, 1]]];
gap> _4ti2zsolve_ZSolve( problem );
[ [ [ 2, 0 ], [ 0, 1 ], [ 1, 0 ], [ 1, 1 ] ],
  [ [ 1, 3 ], [ 1, 1 ], [ 1, 2 ] ] ]

```

The string designates the type of input matrix that follows, which depends on the input supported by `4ti2`. For more details, see the package documentation ([30]).

There are defined also GAP functions to access these library functions. They do some checks and adaptations if necessary, before calling the corresponding library module.

- `HilbertBasis4ti2(arg)`
- `HilbertBasis4ti2gmp(arg)`
- `GraverBasis4ti2(arg)`
- `GraverBasis4ti2gmp(arg)`
- `ZSolve4ti2(arg)`
- `ZSolve4ti2gmp(arg)`

EXAMPLE C.2. This is the same example as before. The main difference is that the output is accessible as a `rec`.

```

gap> ZSolve4ti2( problem );
rec( zhom := [ [ 1, 3 ], [ 1, 1 ], [ 1, 2 ] ],
      zinhom := [ [ 2, 0 ], [ 0, 1 ], [ 1, 0 ], [ 1, 1 ] ] )

```

This output means that the set of solutions of the above system is

$$\{(2,0), (0,1), (1,0), (1,1)\} + \langle (1,3), (1,1), (1,2) \rangle.$$

**2.2. `4ti2groebner.cc`.** This file has the adaptations to use `4ti2`'s Gröbner computations. Its object code links to the GNU MP library if available, and if not, it is compiled using the corresponding processor word size. The `4ti2` component library does not offer an API as `zsolve`, neither a C++ template interface. For this fact, we had coded a sequence of instructions following those in `groebner_main.cpp`.

In `4ti2groebner.cc` we have the following library callable functions from a GAP session.

```

Obj _4ti2groebner_GroebnerBasisOrder( Obj self, Obj listA,
                                      Obj list0 );
Obj _4ti2groebner_GroebnerBasis( Obj self, Obj listA );

```

The parameter `listA` is a matrix, usually its columns are the generating elements of a monoid. The list `list0` is also a matrix used to set the order to compute the Gröbner basis. As for the previous functions in `zsolve`, the package provides a GAP function to access these library functions. It does some checks and allow us to specify as an option

the order identified by the proper string: “lex”, “grlex” and “grevlex”. The order can also be directly specified by a matrix.

- `GroebnerBasis4ti2(matrix[,order])`

EXAMPLE C.3. Compute a Gröbner basis of the ideal  $l_M \subset \mathbb{k}[x, y, z, t, u]$ , associated to the monoid

$$M = \left\langle \begin{pmatrix} 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 5 \\ 8 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 7 \end{pmatrix}, \begin{pmatrix} 17 \\ 85 \end{pmatrix} \right\rangle$$

```
gap> GroebnerBasis4ti2([[2, 5, 1, 3, 17], [3, 8, 2, 7, 85]],
"grevlex");
```

```
[ [ -21, -3, 2, 24, -1 ], [ -14, -6, 0, 25, -1 ],
  [ -3, 1, 4, -1, 0 ], [ -1, 0, 5, -1, 0 ],
  [ 2, -1, 1, 0, 0 ], [ 5, -2, -3, 1, 0 ],
  [ 23, 2, -1, -24, 1 ], [ 25, 1, 0, -24, 1 ],
  [ 28, 0, -4, -23, 1 ] ]
```

This output says that

$$l_M = \langle z^2 t^{24} - x^{21} y^3 u, t^{25} - x^{14} y^6 u, z^4 t - x^3 y, z^5 t - x, x^2 z - y, x^5 t - y^2 z^3, \\ x^{23} y^2 u - z t^{24}, x^{25} y u - t^{24}, x^{28} u - z^4 t^2 3 \rangle.$$

Recall that thanks to Herzog’s correspondence, we can obtain a (minimal) presentation of  $M$  from the exponents of the binomials generating  $l_M$  (or directly by taking  $(x^+, x^-)$  from the output of `GroebnerBasis4ti2`).

**2.3. Applications to affine semigroups.** See in Appendix D some examples of the application of `4ti2gap` to methods implemented in the `numericalsgps` ([13]) package. In particular, the functions:

- `FactorizationsVectorWRTList` in Listing D.3
- `MinimalPresentationOfAffineSemigroup` in Listing D.4
- `EqualPrimitiveElementsOfAffineSemigroup` a function that gives supports to the computation of `EqualCatenaryDegreeOfAffineSemigroup` in Listing D.8.
- `PrimitiveElementsOfAffineSemigroup` in Listing D.12.
- `MonotonePrimitiveElementsOfAffineSemigroup` a function that gives supports to the computation of `MonotoneCatenaryDegreeOfAffineSemigroup` in Listing D.16.
- `OmegaPrimaltyOfElementInFullAffineSemigroup` in Listing D.17.

## APPENDIX D

### GAP functions

The next functions are written without input error checking code for shortness. They form an almost self-contained set by using some local functions, and in a global sense, referencing to others in this appendix. Even so, the next functions included in the numericalsgps ([13]) are used:

- `GeneratorsOfAffineSemigroup`, to get the generators of an affine semigroup.
- `MinimalGeneratingSystemOfNumericalSemigroup`, returns the minimal set of generators of a numerical semigroup.
- `ApéryListOfNumericalSemigroupWRTElement`, computes the Apéry list of a numerical semigroup with respect to an element.
- `RClassesOfSetOfFactorizations`, return the set of  $\mathcal{R}$ -classes of a set of factorizations.

LISTING D.1. Code for the distance between two factorization. This is an auxiliary function used by the other functions that we expose after this.

---

```
distance:=function(x,y)
  local p,n,i,z;

  p:=0; n:=0; z:=x-y;
  for i in [1..Length(z)] do
    if z[i]>0 then p:=p+z[i]; else n:=n+z[i]; fi;
  od;
  return Maximum(p,-n);
end;
```

---

LISTING D.2. Code for the catenary degree of a set of factorizations.

---

```

CatenaryDegreeOfSetOfFactorizations:=function(fact)
  local len, V, underlyinggraph, i, weights, weightedgraph, j, dd, d,
    w;

  V := Length(fact);
  if V = 1 then return 0;
  elif V = 2 then return distance(fact[1],fact[2]); fi;
  # compute the directed weighted graph
  underlyinggraph := [];
  for i in [2 .. V] do Add(underlyinggraph, [i..V]); od;
  Add(underlyinggraph, []);
  weights := [];
  weightedgraph := StructuralCopy(underlyinggraph);
  for i in [1..Length(weightedgraph)] do
    for j in [1..Length(weightedgraph[i])] do
      dd := distance(fact[i],fact[weightedgraph[i][j]]);
      Add(weights,dd);
      weightedgraph[i][j] := [weightedgraph[i][j],dd];
    od;
  od;
  weights:=Set(weights);
  d := 0;
  while IsConnectedGraphNCForNumericalSemigroups(underlyinggraph) do
    w := weights[Length(weights)-d];
    d := d+1;
    for i in weightedgraph do
      for j in i do
        if IsBound(j[2]) and j[2]= w then Unbind(i[Position(i,j)]);
          fi;
        od;
      od;
    for i in [1..Length(weightedgraph)] do
      weightedgraph[i] := Compacted(weightedgraph[i]);
    od;
    underlyinggraph := [];
    for i in weightedgraph do
      if i <> [] then Add(underlyinggraph, TransposedMatMutable(i)
        [1]);
      else Add(underlyinggraph, []); fi;
    od;
  od;
end;

```

```

    od;
  od;
  return(weights[Length(weights)-d+1]);
end;

```

---

LISTING D.3. Code to compute the factorizations of  $v$  in terms of the elements in list  $l$ .

---

```

FactorizationsVectorWRTList:=function(v,l)
  local matrix,mat,rhs,sign,problem, n;

  sign:=[List(l,_->>1)];
  rhs:=[v];
  problem:=["mat",TransposedMat(l),"sign",sign,"rhs",rhs];
  matrix := ZSolve4ti2(problem);
  return matrix.zinhom;
end;

```

---

LISTING D.4. Code to compute the minimal presentation of an affine semigroup.

---

```

MinimalPresentationOfAffineSemigroup:=function(a)
  local gens, positive, gr, candidates, pres, rclass,exps, c;

  positive:=function(x)
    local p,i;

    p:=[];
    for i in [1..Length(x)] do p[i]:=Maximum(x[i],0); od;
    return p;
  end;

  gens:=GeneratorsOfAffineSemigroup(a);
  gr:=GroebnerBasis4ti2(TransposedMat(gens));

  candidates:=Set(gr,q->positive(q));
  candidates:=Set(candidates,c->c*gens);
  pres:=[];
  for c in candidates do
    exps:=FactorizationsVectorWRTList(c,gens);
    rclass:=RClassesOfSetOfFactorizations(exps);
  end;
end;

```

```

if Length(rclass)>1 then
  pres:=Concatenation(pres,List([2..Length(rclass)],
    i->[rclass[1][1],rclass[i][1]]));
fi;
od;
return pres;
end;

```

---

LISTING D.5. Code for the catenary degree of an affine semigroup.

```

CatenaryDegreeOfAffineSemigroup := function(a)
  local betti, minpre, b, max, c, gens;

  gens:=GeneratorsOfAffineSemigroup(a);
  minpre:=MinimalPresentationOfAffineSemigroup(a);
  betti:=Set(minpre, p->p[1]*gens);
  max:=0;
  for b in betti do
    c:=CatenaryDegreeOfSetOfFactorizations(
      FactorizationsVectorWRTList(b,gens));
    if c>max then max:=c; fi;
  od;
  return max;
end;

```

---

LISTING D.6. Code for the monotone catenary degree of a set of factorizations.

```

MonotoneCatenaryDegreeOfSetOfFactorizations:=function(fact)
  local boolTo01, isConnected, adjmat, adjmatdis, pivfact, dis,
    maxdis, maxdisrow, i, j;

  boolTo01:=function(bv)
    if bv then return 1; else return 0; fi;
  end;

  isConnected:=function(adjmat)
    local i, j, k, aa, c;

    k := Length(adjmat); c := IdentityMat(k); aa := IdentityMat(k);
    for i in [1..k-1] do
      aa := aa*adjmat; c := c+aa;
    end;
  end;

```

```

od;
for i in [2..k] do
  for j in [1..i-1] do
    if c[i][j]=0 then return false; fi;
  od;
od;
return true;
end;

pivfact := fact{[1..Length(fact)]};
Sort(pivfact, function(a, b) return Sum(a)>=Sum(b); end);

adjmat := NullMat(Length(fact),Length(fact));
adjmatdis := NullMat(Length(fact),Length(fact));
for i in [1..Length(fact)] do
  adjmat[i] := List( [1..Length(pivfact)], y->boolTo01( pivfact[i
    ]<>pivfact[y] and
                    Sum(pivfact[i])<=Sum(pivfact[y]) ) );
  adjmatdis[i] := List( [1..Length(pivfact)],
    y->adjmat[i][y]*distance(pivfact[i], pivfact
    [y]) );
od;

dis := Set(Flat(Flat(adjmatdis)));
Sort(dis,function(a,b) return a>=b; end);
maxdis := dis[1];
while maxdis > 0 do
  maxdisrow := First(adjmatdis, x->maxdis in x);
  if maxdisrow<>fail then
    i := Position(adjmatdis, maxdisrow);
    j := Position(adjmatdis[i], First(adjmatdis[i], x->x=maxdis));
    adjmat[i][j] := 0; adjmatdis[i][j] := 0;
    if not isConnected( adjmat ) then return maxdis; fi;
  else
    Remove(dis, 1);
    if Length(dis)>0 then maxdis := dis[1]; else return 0; fi;
  fi;
od;
return 0;
end;

```

---

LISTING D.7. Code for the equal catenary degree of a set of factorizations using GAP.

---

```

EqualCatenaryDegreeOfSetOfFactorizations:=function(fact)
  local distance, lFni;

  lFni:=Set( fact, t->Sum( t ) );
  return Maximum( List( lFni, y->
    CatenaryDegreeOfSetOfFactorizations( Filtered( fact, x->Sum( x
      )=y ) ) ) );
end;

```

---

LISTING D.8. Code for the equal catenary degree of a affine semigroup using GAP.

---

```

EqualPrimitiveElementsOfAffineSemigroup:=function(s)
  local l, n, facs, mat, ones, trunc;

  l:=GeneratorsOfAffineSemigroup(s);
  n:=Length(l);
  ones:=List([1..n],_->1);
  mat:=List(TransposedMat(l));
  Add(mat, ones);
  facs:=GraverBasis4ti2(["mat", mat]);

  trunc:=function(ls)
    return List(ls, y->Maximum(y,0));
  end;

  facs:=Set(facs,trunc);
  return Set(List(facs, f->f*l));
end;

EqualCatenaryDegreeOfAffineSemigroup:=function(a)
  local gens, primeq;

  primeq:=EqualPrimitiveElementsOfAffineSemigroup(a);
  gens:=GeneratorsOfAffineSemigroup(a);

  return Maximum(Set(primeq, x->
    EqualCatenaryDegreeOfSetOfFactorizations(

```



```

FactorizationsVectorWRTList(x, gens)))));
end;

```

---

LISTING D.9. Code for the adjacent catenary degree of a set of factorizations.

```

AdjacentCatenaryDegreeOfSetOfFactorizations:=function(fact)
  local Fn, lenset, Zi, facti, i;

  Fn:=Set(ShallowCopy(fact));
  lenset:=Set( fact, Sum );
  if Length(lenset)=1 then
    return 0;
  fi;
  Zi:=[];
  for i in lenset do
    facti:=Filtered( Fn, x->Sum(x)=i );
    SubtractSet( Fn, facti );
    Add( Zi, facti );
  od;
  return Maximum( List( [2..Length( Zi )], t->Minimum( List( Zi[t-1],
    x->Minimum( List( Zi[t], y->distance( x, y ) ) ) ) ) ) );
Iend;

```

---

LISTING D.10. Code for the tame degree of a set of factorizations.

```

TameDegreeOfSetOfFactorizations:=function(fact)
  local i, max, mtemp, candidates, rest, len;

  max:=0;
  len := Length(fact[1]);
  for i in [1..len] do
    candidates:=Filtered(fact, x->x[i]=0);
    rest:=Filtered(fact,x->x[i]<>0);
    if (rest=[] or candidates=[]) then
      mtemp:=0;
    else
      mtemp:=Maximum(List(candidates,x->Minimum(List(rest, z->
        distance(x,z))))));
    fi;
    if mtemp>max then
      max:=mtemp;
    fi;
  od;

```

```

    fi;
  od;
  return max;
end;

```

---

LISTING D.11. Code for the tame degree of a numerical semigroup.

---

```

TameDegreeOfNumericalSemigroup:=function(s)
  local msg, ap, candidates, rp, facts, translate;

  translate:=function(l) #translates partitions to factorizations
    return List(msg, x-> Length(Positions(l,x)));
  end;

  msg:=MinimalGeneratingSystemOfNumericalSemigroup(s);
  if(msg[1]=1) then
    return 0;
  fi;

  ap:=Difference(Union(Set(msg,n->
    AperyListOfNumericalSemigroupWRTElement(s,n))),[0]);

  candidates:=Set(Cartesian(ap,msg),Sum);

  rp:=List(candidates, x->RestrictedPartitions(x, msg));
  # remove elements having in all its factorizations a common atom
  rp:=Filtered(rp, x->Intersection(x)=[]);
  facts:=List(rp, x->List(x, translate));
  if facts=[] then
    return 0;
  fi;
  return Maximum(Set(facts,n->TameDegreeOfSetOfFactorizations(n)));
end;

```

---

LISTING D.12. Code to compute the set of primitive elements of an affine semigroup.

---

```

PrimitiveElementsOfAffineSemigroup:=function(a)
  local matrix, facts, mat, trunc, ls;

  trunc:=function(ls)
    return List(ls, y->Maximum(y,0));
  end;

  gens:=GeneratorsOfAffineSemigroup(a);
  mat:=TransposedMat(gens);
  matrix := GraverBasis4ti2(["mat",mat]);

  matrix:=Set(matrix,trunc);
  return Set(matrix, x->x*gens);
end;

```

---

LISTING D.13. Code to compute the tame degree of an affine semigroup.

---

```

TameDegreeOfAffineSemigroup:=function(a)
  local prim, tams, p, max, gens;

  gens:=GeneratorsOfAffineSemigroup(a);
  prim:=PrimitiveElementsOfAffineSemigroup(a);
  max:=0;
  for p in prim do
    tams:=TameDegreeOfSetOfFactorizations(
      FactorizationsVectorWRTList(p,gens));
    if tams>max then max:=tams; fi;
  od;
  return max;
end;

```

---

LISTING D.14. Code to compute the omega-primality of an element in a affine semigroup.

---

```

OmegaPrimalityOfElementInAffineSemigroup:=function(m,a)
  local ls, n, mat,extfact,par,tot,le;

  le:=function(a,b) #ordinary partial order
    return ForAll(b-a,x-> x>=0);
  end;

  gens:=GeneratorsOfAffineSemigroup(a);
  n:=Length(gens);
  mat:=TransposedMat(Concatenation(gens,-gens,[-m]));

  extfact:=FactorizationsVectorWRTList(m,Concatenation(gens,-gens));

  par:=Set(extfact, f->f{[1..n]});
  tot:=Filtered(par, f-> Filtered(par, g-> le(g,f))=[f]);
  if tot=[] then return 0; fi;
  return Maximum(Set(tot, Sum));
end;

```

---

LISTING D.15. Code to compute the homogeneous catenary degree of an affine semigroup.

---

```

HomogeneousCatenaryDegreeOfAffineSemigroup:=function(a)
  local gens, gensh, ah, minpre, primeq, one;

  gens:=GeneratorsOfAffineSemigroup(a);
  if gens=[] then return 0; fi;

  gensh:=List(ls, x-> Concatenation(x,[1]));
  one:=List(gens[1],_>0);
  Add(one,1);
  Add(gensh,one);

  ah:=AffineSemigroup(gensh);

  # Get the Betti elements
  minpre:=MinimalPresentationOfAffineSemigroup(ah);
  primeq:=Set(minpre, p->p[1]*gens);

```

```

return Maximum(Set(primeq, x->CatenaryDegreeOfSetOfFactorizations(
    FactorizationsVectorWRTList(x, gensh))));
end;

```

---

LISTING D.16. Code for the monotone catenary degree of a set of factorizations.

---

```

MonotonePrimitiveElementsOfAffineSemigroup:=function(s)
  local l, n, facs, mat, ones, trunc;

  l:=GeneratorsOfAffineSemigroup(s);
  n:=Length(l);
  ones:=List([1..n+1],_->1);
  mat:=List(TransposedMat(l),x->Concatenation(x, [0]));
  Add(mat, ones);
  facs:=GraverBasis4ti2(["mat", mat]);

  trunc:=function(ls)
    return List(ls, y->Maximum(y,0));
  end;
  facs:=Set(facs, trunc);
  return Set(List(facs, f->f*l));
end;

MonotoneCatenaryDegreeOfAffineSemigroup:=function(a)
  local prim, gens;

  prim:=MonotonePrimitiveElementsOfAffineSemigroup(a);
  gens:=GeneratorsOfAffineSemigroup(a);

  return Maximum(Set(prim, n->
    MonotoneCatenaryDegreeOfSetOfFactorizations(
      FactorizationsVectorWRTList(n, gens))));
end

```

---

LISTING D.17. Code to compute the omega-primality of  $m$  in the full affine semigroup  $a$ .

---

```

OmegaPrimalityOfElementInFullAffineSemigroup:=function(m,a)
  local gens, n, extfact, par, tot, le;

  le:=function(a,b) #ordinary partial order
    return ForAll(b-a,x-> x>=0);
  end;

  gens:=GeneratorsOfAffineSemigroup(a);
  n:=Length(gens);
  extfact:=ZSolve4ti2(["mat",TransposedMat(gens),"rel",List(v,_->>1),
    "sign",List([1..n],_->>1),"rhs",m]);
  tot:=extfact.zinhom;
  if tot=[] then return 0; fi;
  return Maximum(Set(tot, Sum));
end;

```

---

## Bibliography

- [1] S. Abdelnaby Taha and P. A. García-Sánchez. Homogenization of a nonsymmetric embedding-dimension-three numerical semigroup. *Involve*, 7(1):77–96, 2014.
- [2] V. Blanco, P. A. García-Sánchez, and A. Geroldinger. Semigroup-theoretical characterizations of arithmetical invariants with applications to numerical monoids and Krull monoids. *Illinois J. Math.*, 55(4):1385–1414 (2013), 2011.
- [3] H. Bresinsky. Monomial Buchsbaum ideals in  $\mathbf{P}^r$ . *Manuscripta Math.*, 47(1-3):105–132, 1984.
- [4] W. Bruns, J. Gubeladze, and N. V. Trung. Problems and algorithms for affine semigroups. *Semigroup Forum*, 64(2):180–212, 2002.
- [5] W. Bruns and B. Ichim. Normaliz: algorithms for affine monoids and rational cones. *J. Algebra*, 324(5):1098–1113, 2010.
- [6] W. Bruns, B. Ichim, T. Römer, and C. Söger. Normaliz 2.11. <http://www.math.uos.de/normaliz>, 2014.
- [7] S. T. Chapman, P. A. García-Sánchez, D. Llena, A. Malyshev, and D. Steinberg. On the delta set and the Betti elements of a BF-monoid. *Arab. J. Math. (Springer)*, 1(1):53–61, 2012.
- [8] S. T. Chapman, P. A. García-Sánchez, D. Llena, V. Ponomarenko, and J. C. Rosales. The catenary and tame degree in finitely generated commutative cancellative monoids. *Manuscripta Math.*, 120(3):253–264, 2006.
- [9] S. T. Chapman, P. A. García-Sánchez, D. Llena, and J. C. Rosales. Presentations of finitely generated cancellative monoids and natural solutions of linear systems of equations. In *Fifth Conference on Discrete Mathematics and Computer Science (Spanish)*, volume 23 of *Ciencias (Valladolid)*, pages 217–224. Univ. Valladolid, Secr. Publ. Intercamb. Ed., Valladolid, 2006.
- [10] E. Contejean and H. Devie. An efficient incremental algorithm for solving systems of linear Diophantine equations. *Inform. and Comput.*, 113(1):143–172, 1994.
- [11] P. Conti and C. Traverso. Buchberger algorithm and integer programming. In *Applied algebra, algebraic algorithms and error-correcting codes (New Orleans, LA, 1991)*, volume 539 of *Lecture Notes in Comput. Sci.*, pages 130–139. Springer, Berlin, 1991.
- [12] D. Cox, J. Little, and D. O’Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.
- [13] M. Delgado, P. A. García-Sánchez, and J. Morais. NumericalSgps, a package for numerical semigroups. <https://bitbucket.org/gap-system/numericalsgps>, 2015. Accessed: 2015-03-24.
- [14] F. Di Biase and R. Urbanke. An algorithm to calculate the kernel of certain polynomial ring homomorphisms. *Experiment. Math.*, 4(3):227–234, 1995.
- [15] D. Eisenbud and B. Sturmfels. Binomial ideals. *Duke Math. J.*, 84(1):1–45, 1996.
- [16] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.7.7*, 2015.
- [17] J. I. García-García, M. A. Moreno-Frías, A. Sánchez-R.-Navarro, and A. Vigneron-Tenorio. Affine convex body semigroups. *Semigroup Forum*, 87(2):331–350, 2013.
- [18] J. I. García-García, M. A. Moreno-Frías, and A. Vigneron-Tenorio. Computation of the w-primality and asymptotic w-primality with applications to numerical semigroups. *ArXiv e-prints*, July 2013.

- [19] J. I. García-García, M.A. Moreno-Frías, A. Sánchez-R.-Navarro, and A. Vigneron-Tenorio. Implementation of algorithms to compute the generating set of affine convex body semigroups (Wolfram Mathematica 7). <http://hdl.handle.net/10498/15832>, 2013.
- [20] J. I. García-García, A. Sánchez-R.-Navarro, and A. Vigneron-Tenorio. The PolySGTools package. <http://departamentos.uca.es/C101/pags-personales/alberto.vigneron/PolySGTools.zip>, 2014. Accessed: 2015-03-24.
- [21] J. I. García-García and A. Vigneron-Tenorio. Computing families of Cohen-Macaulay and Gorenstein rings. *Semigroup Forum*, 88(3):610–620, 2014.
- [22] P. A. García-Sánchez, D. Llena, A.M. Robles-Pérez, and J.C. Rosales. Hilbert bases of two dimensional integral pointed cones. 2008.
- [23] P. A. García Sánchez, I. Ojeda, and A. Sánchez-R.-Navarro. Factorization invariants in half-factorial affine semigroups. *Internat. J. Algebra Comput.*, 23(1):111–122, 2013.
- [24] P. A. García-Sánchez and J. C. Rosales. On Buchsbaum simplicial affine semigroups. *Pacific J. Math.*, 202(2):329–339, 2002.
- [25] P. A. García-Sánchez and A. Sánchez-R.-Navarro. 4ti2gap, GAP wrapper for 4ti2. <https://bitbucket.org/gap-system/4ti2gap>, 2014. Accessed: 2015-03-24.
- [26] A. Geroldinger and F. Halter-Koch. *Non-unique factorizations*, volume 278 of *Pure and Applied Mathematics (Boca Raton)*. Chapman & Hall/CRC, Boca Raton, FL, 2006. Algebraic, combinatorial and analytic theory.
- [27] A. Geroldinger and F. Kainrath. On the arithmetic of tame monoids with applications to Krull monoids and Mori domains. *J. Pure Appl. Algebra*, 214(12):2199–2218, 2010.
- [28] S. Gusche, M. Horn, and C. Sger. NormalizInterface for GAP. <https://github.com/fingolfin/NormalizInterface>, 2014. Accessed: 2015-03-24.
- [29] R. Hemmecke. On the computation of Hilbert bases of cones. In *Mathematical software (Beijing, 2002)*, pages 307–317. World Sci. Publ., River Edge, NJ, 2002.
- [30] R. Hemmecke, R. Hemmecke, M. Koeppe, P. Malkin, and M. Walter. 4ti2 version 1.6.2. <http://www.4ti2.de/>, 2014.
- [31] R. Hemmecke and P. N. Malkin. Computing generating sets of lattice ideals and Markov bases of lattices. *J. Symbolic Comput.*, 44(10):1463–1476, 2009.
- [32] J. Herzog. Generators and relations of abelian semigroups and semigroup rings. *Manuscripta Math.*, 3:175–193, 1970.
- [33] S. Hoşten and B. Sturmfels. GRIN: an implementation of Gröbner bases for integer programming. In *Integer programming and combinatorial optimization (Copenhagen, 1995)*, volume 920 of *Lecture Notes in Comput. Sci.*, pages 267–276. Springer, Berlin, 1995.
- [34] Y. Kamoi. Defining ideals of Buchsbaum semigroup rings. *Nagoya Math. J.*, 136:115–131, 1994.
- [35] E. W. Mayr. Some complexity results for polynomial ideals. *J. Complexity*, 13(3):303–325, 1997.
- [36] T. Oda. *Convex bodies and algebraic geometry*. Springer-Verlag, Berlin, 1988.
- [37] A. Philip. *Non-unique factorizations - A semigroup-theoretic algorithmic approach with applications to non-principal orders in algebraic number fields*. PhD thesis, Karl-Franzens Universität Graz - Institut für Mathematik und Wissenschaftliches Rechnen, 2010.
- [38] P. Pisón-Casares and A. Vigneron-Tenorio. First syzygies of toric varieties and Diophantine equations in congruence. *Comm. Algebra*, 29(4):1445–1466, 2001.
- [39] P. Pisón-Casares and A. Vigneron-Tenorio.  $\mathbb{N}$ -solutions to linear systems over  $\mathbb{Z}$ . *Linear Algebra Appl.*, 384:135–154, 2004.
- [40] L. Pottier. Minimal solutions of linear Diophantine systems: bounds and algorithms. In *Rewriting techniques and applications (Como, 1991)*, volume 488 of *Lecture Notes in Comput. Sci.*, pages 162–173. Springer, Berlin, 1991.



- [41] L. Pottier. The euclide algorithm in dimension  $n$ . In *ISSAC '96 Proceedings of the 1996 international symposium on Symbolic and algebraic computation*, pages 40 – 42, 1996.
- [42] GNU Project. Gnu multiple precision arithmetic library. <http://gmp.lib.org/>, 2014. Last version: 6.0.0 (2014-03-24).
- [43] J. C. Rosales and P. A. García-Sánchez. Nonnegative elements of subgroups of  $\mathbf{Z}^n$ . *Linear Algebra Appl.*, 270:351–357, 1998.
- [44] J. C. Rosales and P. A. García-Sánchez. On Cohen-Macaulay and Gorenstein simplicial affine semi-groups. *Proc. Edinburgh Math. Soc. (2)*, 41(3):517–537, 1998.
- [45] J. C. Rosales and P. A. García-Sánchez. *Finitely generated commutative monoids*. Nova Science Publishers Inc., Commack, NY, 1999.
- [46] J. C. Rosales and P. A. García-Sánchez. *Numerical semigroups*, volume 20 of *Developments in Mathematics*. Springer, New York, 2009.
- [47] J. C. Rosales, P. A. García-Sánchez, and J. I. García-García. Irreducible ideals of finitely generated commutative monoids. *J. Algebra*, 238(1):328–344, 2001.
- [48] J. C. Rosales, P. A. García-Sánchez, and J. I. García-García. Atomic commutative monoids and their elasticity. *Semigroup Forum*, 68(1):64–86, 2004.
- [49] J. C. Rosales, P. A. García-Sánchez, J. I. García-García, and J. M. Urbano-Blanco. Proportionally modular Diophantine inequalities. *J. Number Theory*, 103(2):281–294, 2003.
- [50] J. C. Rosales, P. A. García-Sánchez, and J. M. Urbano-Blanco. On presentations of commutative monoids. *Internat. J. Algebra Comput.*, 9(5):539–553, 1999.
- [51] J. C. Rosales, P. A. García-Sánchez, and J. M. Urbano-Blanco. The set of solutions of a proportionally modular Diophantine inequality. *J. Number Theory*, 128(3):453–467, 2008.
- [52] A. Schrijver. *Theory of linear and integer programming*. Wiley-Interscience Series in Discrete Mathematics. John Wiley & Sons Ltd., Chichester, 1986. A Wiley-Interscience Publication.
- [53] J. Stückrad and W. Vogel. *Buchsbaum rings and applications*. Springer-Verlag, Berlin, 1986. An interaction between algebra, geometry and topology.
- [54] B. Sturmfels. *Gröbner bases and convex polytopes*, volume 8 of *University Lecture Series*. American Mathematical Society, Providence, RI, 1996.
- [55] N. V. Trung. Classification of the double projections of Veronese varieties. *J. Math. Kyoto Univ.*, 22(4):567–581, 1982/83.
- [56] A. Vigneron-Tenorio. Semigroup ideals and linear Diophantine equations. *Linear Algebra Appl.*, 295(1-3):133–144, 1999.



## List of Symbols

$\sqcup$	a disjoint union
$\mathbf{F}$	the convex body monoid generated by a convex body $F$
$d(a, b)$	measure of the distance between the factorizations $a, b \in Z(m)$
$d(P, Q)$	the Euclidean distance between two elements $P, Q \in \mathbb{R}^2$
$\mathcal{C}$	the positive integer cone $L_{\mathbb{Q}_{\geq}}(F) \cap \mathbb{N}^2$
$\mathcal{P}$	the affine convex polygonal semigroup
$\mathcal{S}$	the affine circle semigroup
$\langle m_1, \dots, m_k \rangle$	the monoid generated by $\{m_1, \dots, m_k\}$
$\leq_M$	the order induced by $M$ , that is, $m \leq_M m'$ whenever $m' - m \in M$
$G(S)$	the group generated by $S$ , whose elements are linear combinations of elements from $S$ with integer coefficients
$L_{\mathbb{Q}_{\geq}}(F)$	the cone generated by a convex body $F$
$\text{Ap}(M, m)$	the Apéry set of $m$ in a numerical monoid $M$
$\text{int}(\mathbf{F})$	the interior of $\mathbf{F}$
$\text{Gv}(A)$	the Graver basis of the matrix $A$
$\max\{\dots\}$	the maximum of a set
$\mathbb{N}$	the set of natural numbers
$\omega(m)$	the omega primality of $m$
$\overline{PQ}$	the segment joining $P$ and $Q$
$\phi$	the factorization homomorphism
$\mathbb{Q}$	the set of rational numbers
$\mathbb{R}$	the set of real numbers
$c(\cdot)$	the catenary degree (can be referred to an element or a monoid)
$t(\dots)$	the tame degree (can be expressed with respect to different arguments)
$Z(m)$	the set of factorizations of $m$ in a monoid
$Z_p(m)$	the set of factorizations of $m$ with length $p$
$\sharp S$	the cardinality of a set $S$
$\text{supp}(a)$	the set $\{i \in \{1, \dots, k\} \mid a_i \neq 0\}$ for vector $a$
$\tau_1, \tau_2$	the extremal rays of a cone in $\mathbb{N}^2$
$\mathbb{1}$	the vector whose entries are all 1
$\overline{M}$	the closure of $M$ , $\{a \in \mathbb{N}^2 \mid a + M \subseteq M\}$
$\mathbb{Z}$	the set of integer numbers
$e_i$	the vector with every component equal 0, and 1 at the $i$ -th



## Index

- adjacency, 62
- adjacent catenary degree, 62
- affine semigroup, 5
  - full, 26
- Apéry set, 57
- atom, 55
  
- Bézout sequence, 31
- Betti element, 55
- binomial, 5
- Buchsbaum semigroup, 44
  
- catenary degree, 60
- circuit, 59
- Cohen-Macaulay semigroup, 44
- cone, 25
- convex body, 25
- convex body monoid, 26
- convex body semigroup, 26
  
- Delta set, 58
- distance between factorizations, *see* factorization
  
- elasticity, 59
- equal catenary degree, 61
  
- factorization, 55
  - distance, 59
  - length, 58
  - set of lengths, 58
- full affine semigroup, *see* affine semigroup
  
- Gröbner basis, 9
- Graver basis, 62
  
- half-factorial monoid, 59
- Hilbert basis, 12
- homogeneous catenary degree, 70
  
- irreducible, *see* atom
  
- kernel congruence, 55
  
- $M$ -degree, *see* monomial
- monoid, 5
  - intervals (defined by), 26
  - reduced, 5
  - torsion free, 55
- monomial, 5
  - $M$ -degree, 66
  - degree, 65
- monotone catenary degree, 61
  
- numerical monoid, 57
- numerical semigroup, 43
  
- $\omega$ -primality, 66
  
- presentation, 55
  
- ray, 25
  
- semigroup, 5
  - closure of, 44
- simplicial semigroup, 44
- support, 59
  
- tame degree, 63
- torsion free monoid, *see* monoid
  
- unit, 55