Computing efficiently the non-properness set of polynomial maps on the plane*

Boulos EL HILANY† Elias TSIGARIDAS‡

Abstract

We introduce novel mathematical and computational tools to develop a complete and efficient algorithm for computing the set of non-properness of polynomial maps on the plane. This is a subset of $\mathbb{K}^2$ where a dominant polynomial map $f : \mathbb{K}^2 \to \mathbb{K}^2$ is not proper; $\mathbb{K}$ could be either $\mathbb{C}$ or $\mathbb{R}$. Unlike previously known approaches we make no assumptions on f.

The algorithm takes into account the sparsity of polynomials as it depends on (the Minkowski sum of) the Newton polytopes of f. As a byproduct we provide a finer representation of the set of non-properness as a union of algebraic or semi-algebraic sets, that correspond to edges of the Newton polytope, which is of independent interest. Finally, we present a precise bit complexity analysis of the algorithm and a prototype implementation in MAPLE.

1 Introduction

A simple and powerful approach to model problems in science and engineering is to consider a dominant polynomial map $f : X \to Y$. Then, for an input $y \in Y$, the output is the preimage $f^{-1}(y)$. Typically, X and Y are real, or complex varieties of the same dimension. Namely, for a generic y, that is when y belongs to an open subset of Y, the preimage is a finite subset of X. The various algorithms exploit this property to solve efficiently the problem at hand and their complexity, usually, depends on the hardness of inverting f.

However, if y belongs to a certain lower dimensional subset(s) of Y, then its preimage does not behave "properly" anymore, it has an exceptional behavior; for example it might not even be finite. This exceptional set, which we denote by $\mathcal{B}_f$, is intrinsic to f and contains the critical values of f. When $y \in \mathcal{B}_f$, then the computation of its preimage becomes challenging, if possible at all. Hence, an effective description of $\mathcal{B}_f$ provides important information and insight on f and the problem that encodes.

Such a situation arises in computer vision for the problem of 3D reconstruction where we aim to recover a three dimensional scene from a set of two dimensional images. More specifically, for the point-line minimal problems we consider X to be the set of positions of points and lines in 3D and cameras and Y to be the 2D images containing the 2D arrangements of the points and lines specified by the cameras' view. Also $f : X \to Y$ is a dominant map that sends a point-line arrangement in space and the cameras to the corresponding joint image, e.g. [31, 12].

*MSC: 14R25, 26C05 (Primary), 12D10, 14P10, 52B20 (Secondary). Keywords: Real polynomial maps, Set of non-properness, Maps on the plane, Newton polytopes, Boolean complexity.

†Johann Radon Institute for Computational and Applied Mathematics (RICAM), Austrian Academy of Sciences, Austria (`email:`boulos.hilani@gmail.com)

‡Inria Paris and Institut de Mathématiques de Jussieu-Paris Rive Gauche, Sorbonne Université and Paris Université, France (`email:`elias.tsigaridas@inria.fr)

The cardinality of the preimage of a generic point $y \in Y$ is always the same; it is the degree of the minimal problem. Besides, in many cases of the interest we want to recover only the camera poses. So, roughly speaking, if the 2D image y belongs to $\mathcal{B}_f$, then its preimage corresponds to camera poses that are not uniquely defined. This makes the reconstruction much harder. Even more, we want the (minimal) problems to be stable under perturbations, which is not the case when we are near or in $\mathcal{B}_f$. Consequently, the computation of $\mathcal{B}_f$ provides fundamental information for the reconstruction. We refer the reader to [31] and [12, 11] for further details and important progress on the classification of minimal problems based on computational algebraic geometry tools.

Another application comes for the theory of rigid graphs, where the goal is to compute and classify rigid graphs that correspond to (robotic) mechanisms that can move only as a whole. If a graph is not rigid, then the corresponding mechanism has mobility and some of its parts can move; for example they can rotate around a joint (vertex). We refer the reader to [41] for an overview and to [6] for important recent progress on classification algorithms.

In the planar case, a graph $G = (V, E)$, where V is the set of vertices and E is the set of edges, is rigid if and only if $2|V| - 3 = |E|$; these are the Laman (or Pollaczek-Geiringer) graphs. If $X = \mathbb{R}^{2|V|-3}$ and $Y = \mathbb{R}^{|E|}$, then $f : X \to Y$, for given coordinates of the vertices, computes the edge lengths. If $2|V| - 3 = |E|$, then for a generic $y \in Y$, that is for a generic assignment of edge lengths, there is a finite number of preimages that correspond to rigid graphs in 2D. However, if $y \in \mathcal{B}_f$, which is a lower dimensional subset of $Y = \mathbb{R}^{|E|}$, then $f^{-1}(y)$ is either not finite, or has smaller size than a typical preimage. Consequently, some points in $\mathcal{B}_f$ correspond to mechanisms with mobility.

Similar problems emanate from dynamical systems [33], algebraic statistics [38], and optimization [32], to mentions some further applications.

The setting and related work Let f be the dominant polynomial map $f = (f_1, f_2) : \mathbb{K}^2 \to \mathbb{K}^2$, where $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}\}$. The preimage $f^{-1}(y)$ of a dominant polynomial map f for a generic $y \in \mathbb{K}^2$ consists of finitely many points. The *bifurcation set of* f contains all the points $y \in \mathbb{K}^2$ at which the cardinality of the preimage is not stable over any neighborhood of y. This is the exceptional set of interest and we denote it by $\mathcal{B}_f \subset Y$.

The computation, or even a good approximation, of the bifurcation set for general maps is a difficult problem [5, 37, 40, 42, 15, 50, 14, 10, 28]. Nevertheless, it becomes easier when the domain and the codomain are the same. This is so, because in this case the topological behavior at the vicinity of the bifurcation set is well understood: a point in the preimage either collides with another one and together they form a critical point or it "escapes to infinity". The critical points correspond to the critical values of f which we denote by $\mathcal{K}_f \subset Y$. We denote the set of points "escaping at infinity" by $\mathcal{J}_f$. It holds $\mathcal{B}_f = \mathcal{K}_f \cup \mathcal{J}_f$. There are efficient algorithms to compute the critical points and thus a part of the bifurcation set. Our goal is to compute the points escaping to infinity, $\mathcal{J}_f$, when the domain and the codomain is $\mathbb{K}^2$.

The map f is *proper at* $y \in \mathbb{K}^2$ if there exists an open neighborhood of y, say $\mathcal{U}$, such that $f^{-1}(\overline{\mathcal{U}})$ is compact, where $\overline{\mathcal{U}}$ is the Euclidean closure of $\mathcal{U}$. The set of points in $\mathbb{K}^2$ at which f is *not* proper corresponds to the set of points that escape to infinity. We call this set of non-properness *the Jelonek set* of f, see Definition 2.1, and this is why we denote it by $\mathcal{J}_f$.

The Jelonek set, and its properties, is ubiquitous in computational problems and applications e.g., [33, 38, 32, 12, 31, 41], while it is equally important in theoretical and algorithmic questions in various areas ranging from affine geometry [23] to the study of fibrations [26, 28]. There are efficient algorithms for computing exactly the Jelonek set of polynomial maps, even in a general setting [22, 23, 43, 47]. Unfortunately, they are valid under assumptions; for example, in some cases [22, 24, 43] they require $\mathbb{K}$ to be an algebraically closed field, while in other cases they need the map to be finite [47]. In addition, to our knowledge, there are no precise bit complexity estimates. Even more, the known algorithms rely on black box elimination techniques based on Gröbner basis computations and they do not take into account the structure and sparsity of the input. When $\mathbb{K} = \mathbb{R}$, the situation is more dire. Even though the geometry of the Jelonek set is fairly understood [22, 25, 47, 27], to our knowledge, there are no dedicated algorithms to compute it. Up until now, we had to rely on algorithms that assume $\mathbb{K} = \mathbb{C}$ and compute a superset of the (real) Jelonek set.

1.1 Our contribution

We present a complete and efficient algorithm, SPARSE_JELONEK_2 (Alg. 3), along with its mathematical foundations, complexity analysis, and a prototype implementation, to compute the Jelonek set, $\mathcal{J}_f$, of a dominant polynomial map $f = (f_1, f_2) : \mathbb{K}^2 \to \mathbb{K}^2$, where $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}\}$.

The algorithm makes no assumptions on the input polynomials f. It outputs a partition of the (equations of the) Jelonek set to subsets of semi-algebraic (or algebraic) curves of smaller degree; hence it provides a more accurate picture of the topology and the geometry of the Jelonek set. It does not depend on the total degree of the input polynomials, but on their Newton polytopes; the latter encode the non-zero terms of the polynomials, see Sec. 3.1.1 for the definition and various properties. This feature allows us to exploit the sparsity of the input, provides us with tools from combinatorial and toric geometry, and makes the algorithm input and output sensitive. We present a precise bit complexity analysis of the algorithm, when the input consists of polynomials with rational coefficients, and a (prototype) implementation in MAPLE. To our knowledge this the first dedicated algorithm for computing the Jelonek set when $\mathbb{K} = \mathbb{R}$, under no assumptions.

A key property, for our approach, of the Jelonek set is that it is a finite union of semi-algebraic curves (algebraic if $\mathbb{K} = \mathbb{C}$) in $\mathbb{K}^2$ [22, 23, 25]. Using this property, we compute a partition of the Jelonek into sets of curves; we call the sets in the partition Γ-*multiplicity sets* and we denote them by $\mathcal{M}_f(\Gamma)$, see Definition 5.8. The equations of the curves in each partition set depend on the coefficients of f restricted at some distinguished edge Γ of the polygon $\mathsf{NP}(f)$; the latter is the Minkowski sum of the Newton polytopes of f_1 and f_2, $\mathsf{NP}(f_1)$ and $\mathsf{NP}(f_2)$ respectively. The following theorem summarizes these properties and its proof appears in Sec. 5.2.

Theorem 1.1. *Let $f : \mathbb{K}^2 \to \mathbb{K}^2$ be a dominant polynomial map, where $\mathbb{K} = \mathbb{C}$, or $\mathbb{R}$. Then, the Jelonek set of f is the union of its Γ-multiplicity sets.*

The idea behind this result goes as follows: Parts of the preimage $f^{-1}(y)$ escape to infinity in the vicinity of the Jelonek set. These either add new solutions to $f - y = 0$ at infinity, with respect to some toric compactification of $(\mathbb{K}^*)^2$, or increase the multiplicities of the already existing ones. The direction at which the preimage escapes to infinity is the direction of the normal of an edge Γ of $\mathsf{NP}(f)$ (Proposition 5.10). Consequently, either y contributes to a new solution at infinity or it increases the multiplicity of a critical point of $f^{-1}(0)$ at infinity. A Γ-multiplicity set detects points $y \in \mathbb{K}^2$ that are responsible for one of these two situations.

The bulk of our work is to develop tools to compute the Γ-multiplicity sets of f. We exploit a specific type of change of variables, we call it *toric*, that depends on the edge Γ (see Sections 3.2.1, and 5.1), and a method for computing the multiplicities of the solutions of a bivariate square polynomial system. Several results are already in place for achieving the latter task [7, 17, 18, 20, 36]. For example, Gathmann's version [18] of Fulton's algorithm [36] is an iterative process that takes as input two bivariate polynomials and returns the multiplicity of $(0, 0)$ as a solution of the system. For our purposes, we design two algorithms, MS_FULTON (Alg. 4) and MS_RESULTANT (Alg. 5), for this task.

Theorem 1.2. *Let $f : \mathbb{K}^2 \to \mathbb{K}^2$ be a dominant polynomial map, where $\mathbb{K} = \mathbb{C}$, or $\mathbb{R}$. Then, for any edge Γ of $\mathsf{NP}(f)$,* MS_FULTON *(Alg. 4), or* MS_RESULTANT *(Alg. 5), correctly computes the Γ-multiplicity set.*

MS_FULTON is based on Fulton's approach for computing solution multiplicities and outperforms MS_RESULTANT for maps that are mildly degenerate; alas its has exponential worst case complexity. MS_RESULTANT relies on resultant computations and exploits the property that the multiplicity of a root of the resultant accumulates the multiplicities of the solutions of the system in the corresponding fiber. It is the best choice for maps that are more degenerate and it has polynomial worst case complexity.

In its simplest form, a straightforward method to compute the Jelonek set can be as follows: For all edges Γ of $\mathsf{NP}(f)$ compute the corresponding Γ-multiplicity set. This is exactly the approach of SPARSE_JELONEK_2.

Theorem 1.3. *Let $f : \mathbb{K}^2 \to \mathbb{K}^2$ be a dominant polynomial map, where $\mathbb{K} = \mathbb{C}$, or $\mathbb{R}$. Then,* SPARSE_JELONEK_2 *(Alg. 3) computes the Jelonek set of f.*

Unlike previously known methods for computing $\mathcal{J}_f$, SPARSE_JELONEK_2 depends on the Newton polytopes of f_1 and f_2 and not on their total degree. This ties the complexity bounds with the topology of f. Consequently, SPARSE_JELONEK_2 has an advantage in efficiency, especially for maps with are mildly degenerate; compare Theorem 2.5 and Corollary 4.2.

We propose in Section A more sophisticated variations of SPARSE_JELONEK_2 that can further improve its practical performance. For example, it is enough to compute some of the multiplicity sets to deduce/predict the emptiness of the others. Furthermore, several properties of $\mathcal{J}_f$ and the combinatorics of the Newton polytopes $\mathsf{NP}(f_1), \mathsf{NP}(f_2) \subset \mathbb{R}^2$ can lead to further improvements of SPARSE_JELONEK_2. We leave this for a future work.

1.2 Future directions

Jelonek proved that $\mathcal{J}_f$ is a union of $\mathbb{K}$-uniruled curves, that is, each of the curves is parametrized by a polynomial map [22, 25]. He also proved that for any union Σ of $\mathbb{C}$-uniruled curves in $\mathbb{C}^2$, one can construct a map $f : \mathbb{C}^2 \to \mathbb{C}^2$ such that $\mathcal{J}_f = \Sigma$ [23]. Unfortunately, his technique is not constructive. The theoretical results supporting SPARSE_JELONEK_2 form the first step towards a constructive approach for f given a set of uniruled curves. Nevertheless, we still lack a complete algorithm.

A natural next step is to consider algorithms for computing the Jelonek set in higher dimensions. Partial results are already known. Namely, the first author used the faces of Newton polytopes to describe the Jelonek set of a large family of polynomial maps $\mathbb{K}^n \to \mathbb{K}^n$ (called **T-BG**) [13]); the corresponding computations rely on multivariate resultants that in turn rely on some tuples of polytopes [13, Theorem 1.2]. Based on these results the first author later presented methods [19] to give a good approximation of the set of isolated points in $\mathbb{C}^2 \setminus f(\mathbb{C}^2)$. We plan to extend the results in this paper and [13] to all maps $\mathbb{K}^n \to \mathbb{K}^n$ without any assumptions.

1.3 Notation

For a polynomial $f \in \mathbb{Z}[x]$ or $f \in \mathbb{Z}[x_1, x_2]$ its infinity norm $\|f\|_\infty$ equals the maximum absolute value of its coefficients. We denote by $\mathcal{L}(f)$ the logarithm of its infinity norm. We also call the latter the bitsize of the polynomial, where we mean the maximum bitsize of all its coefficients. A univariate polynomial is of size (d, τ) when its degree is at most d and has bitsize τ. We represent an algebraic number $\alpha \in \mathbb{C}$ by the *isolating interval representation.* If $\alpha \in \mathbb{R}$, it includes a square-free polynomial which vanishes at α and a (rational) interval containing α and no other root. When α is not real, it includes a square-free polynomial which vanishes at α and a (rational) rectangle in the complex plane (Cartesian products of intervals) containing α and no other root. We denote by $\mathcal{O}$, resp. $\mathcal{O}_B$, the arithmetic, resp. bit, complexity and we use $\widetilde{\mathcal{O}}$, respectively $\widetilde{\mathcal{O}}_B$, to ignore (poly-)logarithmic factors.

For a polynomial $f \in \mathbb{K}[x_1, x_2]$, where $\mathbb{K}$ is either $\mathbb{R}$ or $\mathbb{C}$, we denote its zero set by $\mathbb{V}_{\mathbb{K}}(f) \subset \mathbb{K}^2$ and $\mathbb{V}_{\mathbb{K}^*}(f) \subset (\mathbb{K}^*)^2$ is its zero set over the corresponding torus. We use the same notation if f is a polynomial system.

1.4 Organization of the paper

Section 2 gives the state of the art of the problem. We present the known methods for computing the Jelonek set for maps $\mathbb{C}^n \to \mathbb{C}^n$ (Algorithms 1, and 2), and deduce their complexity in Theorems 2.4, and 2.5. In Section 3 we give the necessary notations to introduce the algorithm SPARSE_JELONEK_2. This includes a classification of faces of $\mathsf{NP}(f)$ and the introduction of toric change of coordinates. The first half of Section 4 gives a detailed description of the functionality of SPARSE_JELONEK_2, while in the second half we present its complecity analysis (Theorem 4.1) and a detailed example. Sections 5, and 6 concern the correctness of Algorithm SPARSE_JELONEK_2; in particular we define Γ-multiplicity sets in terms of particular toric transformations introduced in Section 5.1. Then, we reformulate Theorem 1.1 as Proposition 5.10 and prove it. The proof of Theorem 1.2 is divided into Propositions 6.2, and 6.2 in Section 6. Finally, Section 7 presents our prototype implementation.

2 The set of points at which a map is non-proper

We start with a definition of the Jelonek set, see [22, 23].

Definition 2.1. *Given two affine varieties, X and Y, and a map $F : X \to Y$, we say that F is* non-proper *at a point $y \in Y$, if there is no neighborhood $U \subset Y$ of y, such that the preimage $F^{-1}(\overline{U})$ is compact, where $\overline{U}$ is the Euclidean closure of U. In other words, F is non-proper at y if there is a sequence of points $\{x_k\}$ in X such that $\|x_k\| \to +\infty$ and $f(x_k) \to y$. The* Jelonek set *of F, $\mathcal{J}_F$, consists of all points $y \in Y$ at which F is non-proper.*

Jelonek proved [22, 25] that for a dominant polynomial map $f = (f_1, \dots, f_n) : \mathbb{K}^n \to \mathbb{K}^n$, $x := (x_1, \dots, x_n) \mapsto f(x)$, the set $\mathcal{J}_f$ is $\mathbb{K}$-*uniruled*. That is, for every point $y \in \mathcal{J}_f$, there exists a non-constant polynomial map $\varphi : \mathbb{K} \to \mathcal{J}_f$ such that $\varphi(0) = y$. Moreover, if $\mathbb{K} = \mathbb{C}$, then $\mathcal{J}_f$ is a hypersurface [22]. These two properties are also valid for maps over algebraically closed fields [44] and when the domain, or the codomain, is an affine variety [27]. In this setting, there are methods for testing properness [23] and computing the Jelonek set [22, 43]. These also lead to an upper bound on degree of $\mathcal{J}_f$ when $\mathbb{K} = \mathbb{C}$ [22],

$$\frac{\prod_{i=1}^n \deg f_i - \mu(f)}{\min_{i=1,\dots,n} \deg f_i},$$

where $\mu(f)$ is the size of a generic preimage under f.

Let $\mathbb{K} = \mathbb{C}$ and for $i = \{1, \dots, n\}$ consider the map $F_i : \mathbb{C}^n \to \mathbb{C}^n \times \mathbb{C}$, such that $F_i(x) := (f(x), x_i)$. Also let

$$\sum_{k=0}^{N_i} A_k^i(f) x_i^{N_i - k} \in \mathbb{C}[f_1, \dots, f_n, x_i],$$

be the polynomial defining the equation of the hypersurface $F_i(\mathbb{C}^n) \subset \mathbb{C}^n \times \mathbb{C}$. Then, $A_0^i(f)$ is the *i-th non-properness polynomial of f*.

Algorithm 1: JELONEK_N$(f_1, \ldots, f_n)$

Input : $f = (f_1, \ldots, f_n) \in \mathbb{Z}[x_1, \ldots, x_n]^n$
Output : The set of non-properness of $f : \mathbb{C}^n \to \mathbb{C}^n$

/* Notice that $F_i \in (\mathbb{C}[y])[x]$ */
$F_1 \leftarrow f_1(x) - y_1, \ldots, F_n \leftarrow f_n(x) - y_n$;
for $i \in [n]$ **do**
  /* Eliminate all the x-variables but x_i. */
  $R_i = \mathtt{res}_{x_i}(F_1, \ldots, F_n) = \sum_{k=0}^{N_i} A_k^i(y) x_i^{N_i - k} \in (\mathbb{C}[y])[x_i]$

RETURN $\prod_{i=1}^{n} A_0^i(y) \in \mathbb{C}[y]$;

Theorem 2.2 ([22, Proposition 7])**.** *The Jelonek set, $\mathcal{J}_f$, of a dominant polynomial map $f : \mathbb{C}^n \to \mathbb{C}^n$, is the zero locus of the polynomial $\prod_{i=1}^{n} A_0^i(y)$, where each A_0^i is the i-th non-properness polynomial of f.*

For the special case $n = 2$, the following theorem holds:

Theorem 2.3 ([24, Theorem 2.2])**.** *Consider a dominant polynomial map $f : \mathbb{C}^2 \to \mathbb{C}^2$, $(x_1, x_2) \mapsto f(x_1, x_2)$. Let $P_i(y_1, y_2, x_i) = \sum_{k=0}^{n_i} P_{ik}(y_1, y_2) x_i^{n_i - k}$ be the resultant of the polynomials $(f_1 - y_1, f_2 - y_2)$ with respect to x_j for distinct $i, j \in \{1, 2\}$. Then, the Jelonek set of f is $\{(y_1, y_2) \in \mathbb{C}^2 \mid P_{1,0} P_{2,0} = 0\}$.*

The computation of the implicit equation of parametrized hypersurfaces $F_i(\mathbb{C}^n)$ requires to eliminate $n-1$ from the variables $x_1, \ldots, x_n$. Thus, to compute the Jelonek set we need effective computations with Gröbner bases and/or resultants. In Alg. 2 and Alg. 1 we present the pseudo-code of the algorithms that realize the computation of Jelonek set supported by Theorems 2.2, and 2.3. The proofs of the following two results are in the appendix.

Theorem 2.4. *Let $f = (f_1, \ldots, f_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be polynomials of degree bounded by d and maximum coefficient bitsize τ. Alg. 1 computes the Jelonek set $\mathcal{J}_f$ in*

$$\widetilde{\mathcal{O}}_B(2^n n^{n(\omega+1)-\omega+1} d^{n^2+(n-1)\omega} (\tau + nd)), \tag{1}$$

where ω is the exponent of matrix multiplication. It consists of polynomials in $\mathbb{Z}[y_1, \ldots, y_n]$ of degree $\mathcal{O}(d^n)$ and maximum coefficient bitsize $\widetilde{\mathcal{O}}((nd)^{n-1}\tau)$.

For the special case of two variables a slightly better bound is possible.

Theorem 2.5. *Let $f_1, f_2 \in \mathbb{Z}[x_1, x_2]$ be polynomials of degree d and maximum coefficient bitsize τ. Alg. 2 computes the Jelonek set $\mathcal{J}_f$ in $\widetilde{\mathcal{O}}_B(d^6\tau)$. It consists of a polynomial in $\mathbb{Z}[y_1, y_2]$ of degree $\mathcal{O}(d)$ and maximum coefficient bitsize $\widetilde{\mathcal{O}}(d\tau)$.*

3 Preliminaries

We present the necessary terminology we need for the following sections.

Algorithm 2: JELONEK_2(f_1, f_2)

Input : $F = (f_1, f_2) \in \mathbb{Z}[x_1, x_2]^2$
Output : The set of non-properness of $F : \mathbb{C}^2 \to \mathbb{C}^2$

$g_1 \leftarrow f_1(x_1, x_2) - y_1$;
$g_2 \leftarrow f_2(x_1, x_2) - y_2$;
$r_1 \leftarrow \texttt{res}_{x_2}(g_1, g_2) \in (\mathbb{Z}[y_1, y_2])[x_1]$;
$r_2 \leftarrow \texttt{res}_{x_1}(g_1, g_2) \in (\mathbb{Z}[y_1, y_2])[x_2]$;
/* Return the leading coefficient wrt to x_1, resp. x_2, of r_1 and r_2 */
$p \leftarrow \texttt{lc}_{x_1}(r_1) \cdot \texttt{lc}_{x_2}(r_2) \in \mathbb{Z}[y_1, y_2]$;
RETURN p ;

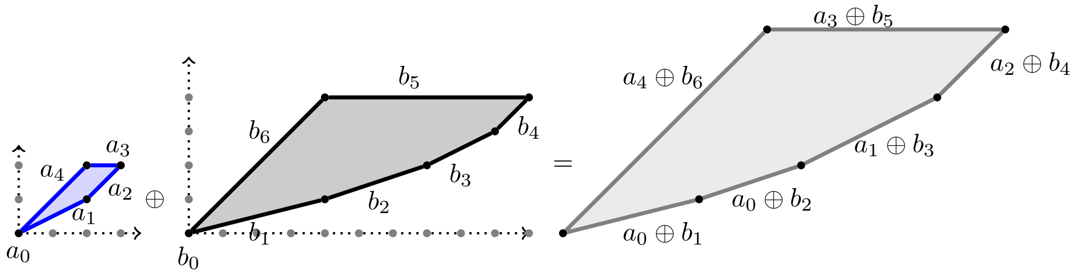

Figure 1: Two Newton polytopes and their Minkowski sum. They correspond to the polynomials of the map in Section 4.4. The edges of the blue, resp. the black, polytope are labeled by a_i, resp. b_j, for $i, j \neq 0$. The vertices that correspond to $(0, 0)$ are a_0, and b_0.

3.1 Polytopes, Minkowksi sums, and mixed volume

A *polytope* Δ in $\mathbb{R}^2$ is a bounded intersection of closed half-spaces of the form $\{a_1 X_1 + a_2 X_2 \geq a_0\} \subset \mathbb{R}^2$, where $a_1, a_2, a_0 \in \mathbb{R}$. The latter are the *supporting half-spaces* of Δ and their boundary intersects the boundary of Δ, $\partial\Delta$, at a connected set of Δ that we call *face*. Thus, any face F of Δ minimizes a function $a^* : \Delta \to \mathbb{R}$, such that $(X_1, X_2) \mapsto a_1 X_1 + a_2 X_2 - a_0$. In this case, we say that $a = (a_1, a_2) \in \mathbb{R}^2$ *supports* F.

The *Minkowski sum* $A \oplus B$ of two subsets $A, B \subset \mathbb{R}^n$ is the set $\{a + b \mid a \in A, b \in B\}$. Let A_1, A_2 denote the convex hull of two finite sets in $\mathbb{Z}^2$ and let their Minkowski sum be $A = A_2 \oplus A_2$. The *summands* of A refers to the pair (A_1, A_2). If Γ is a face of A, that is $\Gamma \prec A$, then the summands of Γ is the pair (Γ_1, Γ_2), such that $\Gamma = \Gamma_1 \oplus \Gamma_2$ and $\Gamma_1 \prec A_1$ and $\Gamma_2 \prec A_2$.

3.1.1 Mixed volume

Given a convex set $\Delta \subset \mathbb{R}^2$, let $\mathrm{Vol}(\Delta)$ be its fixed and translation invariant Lebesgue measure endowed in $\mathbb{R}^2$. Minkowski's *mixed volume* is the unique real-valued multi-linear, with respect to the Minkowski sum, function of two convex sets $\Delta_1, \Delta_2 \subset \mathbb{R}^2$, whose value, if $\Delta_1 = \Delta_2 = \Delta$, equals $2\,\mathrm{Vol}(\Delta)$. We denote the mixed volume by $V(\Delta_1, \Delta_2)$ and we can compute it using the inclusion-exclusion formula

$$\mathrm{Vol}(\Delta_1 + \Delta_2) - \mathrm{Vol}(\Delta_1) - \mathrm{Vol}(\Delta_2).$$

If $\Delta_1 + \Delta_2$ is a line segment or if (one of the) Δ_i is a point, then $V(\Delta_1, \Delta_2) = 0$. The other direction of this statement is also true; it is a particular case of Minkowski's theorem for the higher-dimensional mixed volume, see [30, Section 2].

A pair (Δ_1, Δ_2) is *independent* if $V(\Delta_1, \Delta_2) \neq 0$; or, equivalently, if $\dim(\sum_{i \in I} \Delta_i) \geq |I|$ for all $I \subset \{1, 2\}$. A pair is *dependent* if it is not independent.

3.1.2 Characterization of the faces

For our purposes we need to characterize, actually partition, the edges of the Minkowksi sum of two convex polygons according to their summands. The following definition details the characterization, while Figure 2 gives a pictorial overview.

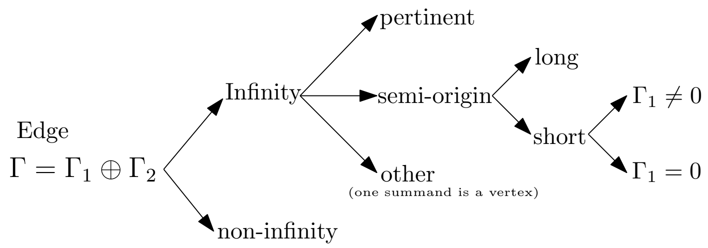

Figure 2: The partition of the edges that SPARSE_JELONEK_2 exploits. Γ is an edge of the Minkowski sum. Its summands are Γ_1 and Γ_2.

Definition 3.1. *Let $A = A_1 \oplus A_2$. A face $\Gamma \prec A$ with summands (Γ_1, Γ_2) is an* edge *if* $\dim(\Gamma) = 1$. *An edge is*

- long *if both of its members have dimension 1, that is if* $\dim(\Gamma_1) = \dim(\Gamma_2) = 1$.
- short *if it is not long.*
- pertinent *if it is long and both of its members do not contain the origin, that is* $(0, 0) \notin \Gamma_1$ *and* $(0, 0) \notin \Gamma_2$.
- semi-origin *if at least one of its members contains the origin, that is* $(0, 0) \in \Gamma_1$ *or* $(0, 0) \in \Gamma_2$.
- *infinity if all of its supporting vectors have a negative coordinate.*

Example 3.2. *Consider the three (Newton) polytopes in Figure 1. The third polytope is the Minkowski sum of the first two and we have the following characterization of its edges:*

- *Semi-origin long edges:* $a_1 \oplus b_3$, $a_4 \oplus b_6$.
- *Origin long edges:* $a_4 \oplus b_6$.
- *Semi-origin short edges:* $a_0 \oplus b_1$, $a_0 \oplus b_2$.
- *Origin short edges:* $a_0 \oplus b_0$, $a_0 \oplus b_1$.
- *Pertinent edges:* $a_2 \oplus b_4$, $a_3 \oplus b_5$.
- *Almost semi-origin edges:* $a_2 \oplus b_4$.
- *All of the edges are infinity edges.*

3.2 Bivariate polynomial systems and toric change of variables

Let $P \in \mathbb{K}[x_1^{\pm 1}, x_2^{\pm 1}]$ be a bivariate Laurent polynomial, that is

$$P(x) = \sum_{a \in \mathbb{Z}^2} c_a \, x^a = \sum_{(a_1,a_2) \in \mathbb{Z}^2} c_a \, x_1^{a_1} x_2^{a_2},$$

where $c_a \in \mathbb{K}$. The *support*, $\mathrm{supp}(P)$, of P is the set $\{a \in \mathbb{Z}^2 \mid c_a \neq 0\}$. The Newton polytope of P is the convex hull of the support, $\mathsf{CH}(\mathrm{supp}(P))$; we denote it by $\mathsf{NP}(P)$.

Consider the pair of polynomials $f := (f_1, f_2) \in \mathbb{K}[x_1^{\pm 1}, x_2^{\pm 1}]^2$, such that

$$f_1 = \sum\nolimits_{a \in S_1} c_{1,a} x^a \quad \text{and} \quad f_2 = \sum\nolimits_{b \in S_2} c_{2,a} x^b, \tag{2}$$

where $S_i = \mathrm{supp}(f_i) \subset \mathbb{Z}^2$ and $\mathrm{supp}(f) = (\mathrm{supp}(f_1), \mathrm{supp}(f_2)$. The corresponding Newton polytopes (in our case polygons) are $A_i = \mathsf{NP}(f_i) = \mathsf{CH}(\mathrm{supp}(f_i))$, for $i \in \{1,2\}$. Also let $\mathsf{NP}(f) := A = A_1 \oplus A_2$. For any face $\Gamma \prec A$ with summands (Γ_1, Γ_2), we denote by $f_{1,\Gamma}$ the restriction of f_1 to those monomial terms $c_{1,a} x^a$ for which $a \in \Gamma_1 \cap \mathbb{Z}^2$. Similarly for $f_{2,\Gamma}$. We also write f_Γ for the pair $(f_{1,\Gamma}, f_{2,\Gamma}) \in \mathbb{K}[x_1^{\pm 1}, x_2^{\pm 1}]^2$.

3.2.1 Toric change of coordinates and dominant maps

Let $f = (f_1, f_2) : \mathbb{K}^2 \to \mathbb{K}^2$, $x = (x_1, x_2) \mapsto f(x)$ be a *dominant* polynomial map. For any $y = (y_1, y_2) \in \mathbb{K}^2$ we consider $f - y = (f_1 - y_1, f_2 - y_2)$ to be a pair of translated polynomials in $\mathbb{K}[x_1, x_2]$.

Remark 3.3. *The previous assumption imply that if either $A_1 = \{(0,0)\}$ or $A_2 = \{(0,0)\}$, then f maps $\mathbb{K}^2$ onto a line. Also, if $\dim(A) = 1$, then f maps $\mathbb{K}^2$ onto a (general) curve. Therefore, the independence of A is a necessary condition for f to be dominant. In fact, there is an equivalence, but we will not illustrate its proof here.*

Following [2], a *unimodular toric* (or simply *toric* for brevity) change of variables that acts on $x = (x_1, x_2)$ is a map $(\mathbb{K}^*)^2 \to (\mathbb{K}^*)^2$, such that

$$(x_1, x_2) \mapsto (z_1^{u_{11}} z_2^{u_{21}}, z_1^{u_{12}} z_2^{u_{22}}),$$

where $U = \left(\begin{smallmatrix} u_{11} & u_{1,2} \\ u_{2,1} & u_{2,2} \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z})$. It induces an isomorphism between polynomials, which by abuse of notation, we also denote by U; it is

$$U : \mathbb{K}[x_1, x_2] \to \mathbb{K}[z_1^{\pm 1}, z_2^{\pm 1}],$$

that maps the monomial x^a to $z^{U a^\top}$, where $a = (a_1, a_2)$. Hence, for any polynomial, say $P \in \mathbb{K}[x_1, x_2]$, we have

$$\mathrm{supp}(UP) = U(\mathrm{supp}(P)),$$

and the zero locus $\mathbb{V}_{\mathbb{K}^*}(P)$ is isomorphic to $\mathbb{V}_{\mathbb{K}^*}(UP)$.

Remark 3.4. *If $f = (f_1, f_2)$ is a pair of bivariate polynomials and $Uf = (Uf_1, Uf_2)$, then $\mathbb{V}_{\mathbb{K}^*}(f)$ has the same number of isolated points as $\mathbb{V}_{\mathbb{K}^*}(Uf)$.*

If Uf consists of Laurent polynomials, then there might be monomials with negative exponents. We transform them to polynomials by multiplying them by suitable monomials. We denote this transformation by $\overline{U}f$ which is the map $(Ux^{r_1} f_1, Ux^{r_2} f_2)$, for suitable $r_1, r_2 \in \mathbb{Z}^2$; in other words we multiply with suitable monomials to clear the denominators.

4 Computing the Jelonek set

In what follows $f = (f_1, f_2) : \mathbb{K}^2 \to \mathbb{K}^2$, where $f_1, f_2 \in \mathbb{Z}[x_1, x_2]$ and are as in (2). Also, let $A_1 = \mathsf{NP}(f_1)$, $A_2 = \mathsf{NP}(A_2)$ and $A = A_1 \oplus A_2$.

We describe in detail how the algorithm SPARSE_JELONEK_2 computes the Jelonek set.

The input consists of a pair of polynomials $f_1, f_2 \in \mathbb{Z}[x_1, x_2]$ and a flag $\mathbb{K}$ that takes the values $\mathbb{R}$ or $\mathbb{C}$ and indicates if we want to compute the Jelonek set over the real or the complex numbers. We consider polynomials with integer coefficients to study the bit complexity of the algorithm.

As a preproccessing step we can translate both polynomials, that is $(f_1 + a_1, f_2 + a_2)$, where $a := (a_1, a_2) \in \mathbb{Z}^2$ is a random point. This is to ensure that they both have a constant term, or in other words both their Newton polytopes contain the origin. Additionally, this implies that $f(0,0)+a \notin f\big(\mathbb{K}^2 \setminus (\mathbb{K}^*)^2\big)$, see Lemma 5.7. If $c_{1,0}$, resp. $c_{2,0}$, is the constant term of f_1, resp. f_2, then it suffices to choose $a_1 \neq -c_{1,0}$ and $a_2 \neq -c_{2,0}$. Thus, the translation does not increase the bitsize of the polynomials. In what follows we assume that polynomials have a constant term.

The algorithm has two phases. During the first phase, which we detail in Sec. 4.1, we compute the Minkowski sum of the Newton polytopes of the input polynomials and we characterize its edges. The partition of the edges with respect to the various types appears in Fig. 2. At the second phase, which we detail in Sec. 4.2, for each edge of interest, we compute with a restricted polynomial system. For each, real or complex depending on $\mathbb{K}$, solution of this system, we exploit its multiplicity to compute the corresponding multiplicity set, see Sec. 5. The union of the multiplicity sets is the Jelonek set.

4.1 Characterizing the edges

The first phase of SPARSE_JELONEK_2 characterizes the edges (and the corresponding summands) of the Minkowski sum. The Newton polytopes of (f_1, f_2) are (A_1, A_2). We compute their Minkowski sum, that is $A = A_1 \oplus A_2$, using Alg. 7, MINKOWSKI_SUM. The algorithm, besides computing the Minkowski sum it also characterizes the edges according to the various types, see Sec. 3.1.2. In particular it identifies the edges $\Gamma \prec A$ which are infinity edges and also either semi-origin or pertinent. The characterization relies on the summands of Γ, say (Γ_1, Γ_2). Alg. 7 checks whether $\dim(\Gamma_i)$ is zero or not and if Γ_i contains $\{0\}$ or not, for $i \in \{1, 2\}$, see Def. 3.1.

We consider the pertinent edges only when the number of isolated solutions, counted with multiplicities, of the system $f = 0$, say N, is smaller than the mixed volume $V(A)$. We decide this using Alg. 6, TEST_NUMBER_OF_ROOTS. The reason we can ignore pertinent edges when $N = V(A)$ is the following observation: Bernstein's Theorem B [2] states that $N < V(A)$ if and only if $f_\Gamma = 0$ has a solution in $(\mathbb{K}^*)^2$ for some $\Gamma \prec A$. This face has to be pertinent since the pair of polynomials f_Γ can be written in terms of one variable (see Remark 5.2), and a is generic.

4.2 Computing the multiplicity sets

After characterizing the edges of A we consider only the semi-origin and the pertinent ones. For each one them, say Γ with summands (Γ_1, Γ_2), the algorithm computes the Γ-*multiplicity* set. Recall that this is the set of points $y \in \mathbb{K}^2$ for which there exists a particular transformation $U \in \mathrm{SL}(2, \mathbb{Z})$ (see Section 5.1) such that $\overline{U}(f - y) = 0$ has more isolated solutions (counted with multiplicities) in $\mathbb{K}^* \times \{0\}$ than $\overline{U} f = 0$ in the same locus (see Definition 5.3, and Lemma 5.8).

First, we compute the multiplicity set of the semi-origin edges, Line 4 in SPARSE_JELONEK_2. For each such Γ, after we restrict f to Γ, the multiplicity set $\mathcal{M}_f(\Gamma)$ is the solution set of a triangular system of two equations in three variables. Proposition 5.6, item (2) implies that in this

Algorithm 3: SPARSE_JELONEK_2($f = (f_1, f_2), \mathbb{K}$)

Input : $f_1, f_2 \in \mathbb{Z}[x_1, x_2]$, $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}\}$
Require: Both f_1 and f_2 have a non-zero constant term.
Output : The Jelonek set $\mathcal{J}$.

$\mathcal{J} \leftarrow \varnothing$;
$A_1 \leftarrow \mathsf{NP}(f_1)$; $A_2 \leftarrow \mathsf{NP}(f_2)$;
$A \leftarrow$ MINKOWSKI_SUM_2(A_1, A_2) ;
forall *semi-origin edges* $\Gamma \prec A$ **do**
    `/*` It holds $\Gamma = \Gamma_1 \oplus \Gamma_2$ `*/`
    $f_1|_{\Gamma_1} \leftarrow x^u \cdot \sum_{i=0}^{|\Gamma_1 \cap \mathbb{N}^2|} a_i (x_1^k x_2^l)^i$; $f_2|_{\Gamma_2} \leftarrow x^v \cdot \sum_{j=0}^{|\Gamma_2 \cap \mathbb{N}^2|} b_j (x_1^k x_2^l)^j$;
    if $0 \notin \Gamma_1$ **then** $\mathcal{J} \leftarrow \mathcal{J} \cup \left\{ (y_1, y_2) \in \mathbb{K}^2 \mid y_2 = \sum_j b_j t^j, \text{ with } P_1(t) = \sum_i a_i t^i = 0 \right\}$;
    if $0 \notin \Gamma_2$ **then** $\mathcal{J} \leftarrow \mathcal{J} \cup \left\{ (y_1, y_2) \in \mathbb{K}^2 \mid y_1 = \sum_i a_i t^i, \text{ with } P_2(t) = \sum_j b_j t^j = 0 \right\}$;
    if $0 \in \Gamma_1$ *and* $0 \in \Gamma_2$ **then** $\mathcal{J} \leftarrow \mathcal{J} \cup \left\{ (y_1, y_2) \in \mathbb{K}^2 \mid y_1 = \sum_i a_i t^i, y_2 = \sum_j b_j t^j, \text{ where } t \in \mathbb{K} \right\}$;

forall *pertinent edges* $\Gamma \in A$ *such that* $f|_\Gamma = 0$ *has solutions in* $(\mathbb{K}^*)^2$ **do**
    `/*` Let a_1 be the vertex of Γ closer to the origin. Let v be a primitive vector on Γ starting from a_1. We compute a basis for the lattice $\mathbb{Z}^2$, (v, w) that spans positively the polytope $A - a_1$. `*/`
    $(v, w) \leftarrow$ COMPUTE_LATTICE_BASIS ;
    `/*` It holds $T = \left(\begin{smallmatrix} v_1 & v_2 \\ w_1 & w_2 \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z})$ and $D = \det(T)$. `*/`
    `/*` We perform the change of variables $x_1 \leftarrow z_1^{w_2/D} z_2^{-v_2/D}, x_2 \leftarrow z_1^{-w_1/D} z_2^{v_1/D}$. `*/`
    $D \leftarrow \det(T) = v_1 w_2 - v_2 w_1$ `/*` Notice that $D = \pm 1$, because v, w is a unimodal basis. `*/`
    $g_1 \leftarrow \mathtt{numer}(f_1(z_1^{w_2/D} z_2^{-v_2/D}, z_1^{-w_1/D} z_2^{v_1/D}) - y_1) \in \mathbb{Z}[y_1, z_1, z_2]$;
    $g_2 \leftarrow \mathtt{numer}(f_2(z_1^{w_2/D} z_2^{-v_2/D}, z_1^{-w_1/D} z_2^{v_1/D}) - y_2) \in \mathbb{Z}[y_2, z_1, z_2]$;
    $g \leftarrow \gcd(g_1(y_1, z_1, 0), g_2(y_2, z_1, 0)) \in \mathbb{Z}[z_1]$;
    $h \leftarrow \det(\mathtt{Jac}_z(g_1, g_2)) \in \mathbb{Z}[y_1, y_2][z_1, z_2]$;
    foreach *complex (or real depending on* $\mathbb{K}$*) root* ρ *of* g **do**
        if $h(\rho, 0) \neq 0$ **then**
            `/*` If the Jacobian is not zero, then the multiplicity is one. `*/`
            `/*` It holds $h(\rho, 0) \in \mathbb{Z}[\rho][y_1, y_2]$. `*/`
            $\mathcal{J} \leftarrow \mathcal{J} \cup \{h(\rho, 0)\}$;
        else
            `/*` The Jacobian is zero; the solution $(\rho, 0)$ has multiplicity > 1. `*/`
            $\mathcal{J} \leftarrow \mathcal{J} \cup$ CIM_BY_RESULTANT$(g_1, g_2, (\rho, 0))$;
            `/*` Alternatively, we could use CIM$(g_1, g_2, (\rho, 0))$. `*/`

RETURN $\mathcal{J}$;

case $\mathcal{M}_f(\Gamma)$ is a point, a parametrized curve, or a union of lines. We obtain the corresponding equations from $\overline{U}(f-y)_\Gamma = 0$, see Lines 6, 7, and 8 of SPARSE_JELONEK_2.

Next, we consider the pertinent edges, Line 9 of SPARSE_JELONEK_2. Assume that $N < V(A)$ and let $\Gamma \prec A$ be pertinent. First, we transform the polynomials $f - y$, using a toric change of variables, to $g = (g_1, g_2) \in \mathbb{Q}[y_1, y_2][z_1, z_2]$, Lines 12 and 13. The change of variables corresponds to a basis of the lattice $\mathbb{Z}^2$, Line 10. This new basis spans positively the lattice points of the Minkowski sum, $A + \{-a_1\}$ and has as one of its basis elements the primitive vector in the direction of Γ; a_1 is the vertex of Γ closer to the origin. We detail this procedure in Sec. 5.1.

Following Remarks 3.4, 5.2, and Lemma 5.9, the change of basis preserves the number of the 0-dimensional solutions and leads to a simpler system to solve; actually a univariate one, Line 14.

We consider Γ only if $\overline{U}f_\Gamma = 0$ has solutions in $\mathbb{K}^* \times \{0\}$; this is so because if there no solutions in $\mathbb{K}^* \times \{0\}$ for any $y \in \mathbb{K}^2$, then $\mathcal{M}_f(\Gamma)$ is empty (see Lemma 5.8).

If $\mathcal{M}_f(\Gamma)$ is not empty, then $\overline{U}(f-y) = 0$, or $g = 0$, has solutions $(\rho, 0) \in \mathbb{K}^* \times \{0\}$, (Definition 5.3), whose multiplicity changes depending on whether y belongs to $\mathcal{M}_f(\Gamma)$, or not. Each such solution, real or complex depending on $\mathbb{K}$, corresponds to a subset of the multiplicity set $\mathcal{M}_f(\Gamma)$ and their union give us $\mathcal{M}_f(\Gamma)$. Therefore, the multiplicity of $(\rho, 0)$ as a solution of the bivariate polynomial system $g = 0$ is important for the computation of $\mathcal{M}_f(\Gamma)$.

If the multiplicity of $(\rho, 0)$ is one, then the Jacobian of g, with respect to the variables z_1 and z_2, is non-zero and we can use it to compute the multiplicity set, Lines 17 in SPARSE_JELONEK_2. The Jacobian, say h, is a polynomial in $\mathbb{Z}[y_1, y_2][z_1, z_2]$ and the multiplicity set is the evaluation of h at $(\rho, 0)$, that is $\mathcal{M}_f(\Gamma) = h(\rho, 0) \in \mathbb{Z}[\rho][y_1, y_2]$, Line 17. If the Jacobian is zero, then the multiplicity of $(\rho, 0)$ is greater than one, Line 19 in SPARSE_JELONEK_2.

We present two methods for computing the multiplicity of a solution to a bivariate system (Sections 6.1 and 6.2). We modify them to also compute the multiplicity sets; MS_FULTON (Alg. 4) and MS_RESULTANT (Alg. 5) are the corresponding algorithms.

4.3 Complexity and representation of the output

Let $f_1, f_2 \in \mathbb{Z}[x_1, x_2]$ be polynomials of degree d and bitsize τ. Also, assume that their Newton polytopes have at most n edges.

Initially we compute the Minkowski sum, Line 3. This costs $\widetilde{\mathcal{O}}(n)$ and results a polygon with at most $\mathcal{O}(n)$ edges at its convex hull. This is Alg. 7 which is a slight modification of the well known optimal algorithm [9, Sec. 13.3] for computing the Minkonwski sum of two polygons. The modifications consists in characterizing, within the same complexity bound, the edges, $\Gamma \prec A$ and the summands (Γ_1, Γ_2).

The fist phase of the algorithm considers the semi-origin edges of the Minkowski sum, Line 4 to 8. The most computational expensive operation is the computation of the roots (real or complex) of univariate polynomials; these are the polynomials $P_1(t)$ and $P_2(t)$ appearing at Lines 6 and 7. These polynomials come from the restriction of f_1 or f_2 on Γ and so they have degree at most d and bitsize at most τ. The computation of their roots (real or complex) costs $\widetilde{\mathcal{O}}_B(d^3 + d^2\tau)$ [39]. As there are at most $\mathcal{O}(n)$ semi-origin edges, the total cost of the first phase is $\widetilde{\mathcal{O}}_B(n(d^3 + d^2\tau))$.

Regarding the output of the first phase, first we assume that $\mathbb{K} = \mathbb{R}$. When $0 \notin \Gamma_2$, then if the real roots of $P_1 \in \mathbb{Z}[t]$ are $\gamma_1, \ldots, \gamma_r$, the output is a union of horizontal lines defined by numbers in $\mathbb{Z}[\gamma_i]$, for $i \in [r]$. Similarly for the case $0 \notin \Gamma_1$. When both Γ_1 and Γ_2 contain zero (Line 8), the Jelonek set is a parametrized polynomial curve, defined by polynomials in $\mathbb{Z}[t]$ of degree at most d and bitsize at most τ. Its implicit representation, when $\mathbb{K} = \mathbb{C}$, consists of a polynomial in $\mathbb{Z}[y_1, y_2]$ of degree at most d and maximum coefficient bitsize $\widetilde{\mathcal{O}}(d\tau)$. We compute it in $\widetilde{\mathcal{O}}_B(d^3\tau)$. If $\mathbb{K} = \mathbb{C}$, then when $0 \in \Gamma_1$ we represent the union of lines in a more unified way by considering the resultant $R_2(y) = \texttt{res}(y_2 - \sum_j b_j t^j, P_1(t), t) \in \mathbb{Z}[y_2]$. Then the representation is $(y_1, R_2(y))$.

The second phase of the algorithm deals with pertinent edges. Then, the first task consists in computing a unimodular basis that fits our needs Line 10. The most costly part of this procedure is the computation of the Smith Normal Form (SNF) of matrix. As the degree of the input polynomials is $\mathcal{O}(d)$, this also bounds the dimension of the matrices. The cost of SNF is $\widetilde{\mathcal{O}}_B(d^{\omega+1})$ [45], where ω is the exponent of matrix multiplication.

After the toric change of variables we obtain a univariate polynomials and we compute its roots. Then, we compute the multiplicity sets by exploiting the multiplicities of the roots of the corresponding bivariate polynomial system. The worst case corresponds to consider that all the roots have multiplicities. Then, for all the roots we use MS_RESULTANT (Alg. 5) to compute the corresponding multiplicity set. This costs $\widetilde{\mathcal{O}}_B(d^9\tau)$ (Theorem 6.3). As there at most n pertinent edges the total cost is $\widetilde{\mathcal{O}}_B(nd^9\tau)$, that also dominates the cost of the algorithm.

Theorem 4.1. *Let $f = (f_1, f_2) : \mathbb{K}^2 \to \mathbb{K}^2$ be a dominant polynomial, where $f_1, f_2 \in \mathbb{Z}[x_1, x_2]$ are polynomials of degree at most d and bitsize τ and their Newton polytopes have at most n edges.* SPARSE_JELONEK_2 *computes the Jelonek set of f in $\widetilde{\mathcal{O}}_B(n\,d^9\tau)$.*

Corollary 4.2. *Let $f = (f_1, f_2) : \mathbb{K}^2 \to \mathbb{K}^2$ be a dominant polynomial, where $f_1, f_2 \in \mathbb{Z}[x_1, x_2]$ are polynomial of degree at most d and bitsize τ and their Newton polytopes have at most n edges. If f_1 and f_2 are generic, then* SPARSE_JELONEK_2 *computes the Jelonek set of f in $\widetilde{\mathcal{O}}_B(n(d^3 + d^2\tau))$.*

Proof. When the input polynomials are generic, then the Minkowski sum of their Newton polytopes does contain a pertinent edge with probability 1. Therefore, the complexity of the algorithm depends on the computation of the Minkowksi sum and the manipulation of the semi-origin edges. The latter dominates the complexity bound. Its complexity is $\widetilde{\mathcal{O}}_B(n(d^3 + d^2\tau))$, as we have to solve n times a univariate polynomial. □

Remark 4.3. *The genericity property of the polynomials in Cor. 4.2 is wrt fixed Newton polytopes and wrt non-fixed ones. Even more, if we fix the degree, then a generic polynomial has a simplex as Newton polytope and thus the Corollary still holds.*

4.4 An example

Let $A := A_1 \oplus A_2$, where A_1, and A_2 are integer polytopes in $(\mathbb{R}_{\geq 0})^2$; they appear at the l.h.s of Figure 1. The r.h.s. illustrates A.

We want to compute the Jelonek set $\mathcal{J}_f$ of the map $f = (f_1, f_2) : \mathbb{K}^2_{u,v} \to \mathbb{K}^2_{r,s}$, where

$$\begin{aligned} f_1 &= 1 + uv + 2u^2v^2 - \tfrac{7}{10}u^2v - 3u^3v^2, \\ f_2 &= 1 + 3uv - 4u^2v^2 + 5u^3v^3 - 6u^4v^4 + \tfrac{3^7}{2^5}u^{10}v^4 - 54u^6v^3 + \tfrac{5103}{320}u^9v^3 - u^7v^2 + u^4v. \end{aligned}$$

Figure 1 shows that $\mathsf{NP}(f) = A$ has exactly six infinity edges, that are either pertinent or semi-origin (see Definition 3.1). Let $S_{01}, S_{02}, S_{13}, S_{24}, S_{35}, S_{46} \subset \mathbb{K}^2$, denote the corresponding multiplicity sets multiplicity sets in $\mathbb{K}^2$ (see Definition 5.3) where

$$S_{ij} := \mathcal{M}_f(a_i \oplus b_j).$$

By Proposition 5.10 their union is $\mathcal{J}_f$. We apply SPARSE_JELONEK_2 to compute $\mathcal{J}_f$.

- Edges $a_0 \oplus b_1$, $a_0 \oplus b_2$, and $a_1 \oplus b_3$ are infinity semi-origin and only a_0 contains $(0,0)$. Therefore, Lines 7 and 8 of SPARSE_JELONEK_2 results

$$\begin{aligned} S_{01} =& \{(r,s) \in \mathbb{K}^2 \mid r = 1,\ 1 + t = 0\} = \{r = 1\}, \\ S_{02} =& \{(r,s) \in \mathbb{K}^2 \mid r = 1,\ 1 - t = 0\} = \{r = 1\}, \\ S_{13} =& \{(r,s) \in \mathbb{K}^2 \mid r = 1 - 7t/10,\ 320 + 5163t = 0\} = \{r - 761/729 = 0\}. \end{aligned}$$

- The edge $a_4 \oplus b_6$ is origin, where $(0,0) \in a_4$ and $(0,0) \in b_6$. Then, Line 8 resylts

$$S_{46} = \{(r,s) \in \mathbb{K}^2 \mid r = 1 + t + 2t^2,\ s = 1 + 3t - 4t^2 + 5t^3 - 6t^4\}.$$

- Edges $a_2 \oplus b_4$, and $a_3 \oplus b_5$ are pertinent. Moreover, the systems $f_{a_2 \oplus b_4} = 0$ and $f_{a_3 \oplus b_5} = 0$ have solutions in $(\mathbb{K}^*)^2$. Then, we first apply Lines $10 - 15$ to f for both edges, next Line 17 for $a_2 \oplus b_4$, and Line 19 for $a_3 \oplus b_5$. Therefore, the algorithm outputs

$$S_{24} = \{r + 1468/18225 = 0\} \text{ and } S_{35} = \{r + 6238/10935 = 0\}.$$

5 Jelonek set and critical points at infinity

The main goal of this section is to describe the Jelonek set in terms of multiplicities and the existence of solutions of some transformed systems. This consist of a substantial part of the correctness proof of the main algorithm in Section 6. We start by introducing several notations and technical results.

5.1 Toric change of variables using the edges

We introduce a toric change of coordinates $U \in \mathrm{SL}(2, \mathbb{Z})$, Sec. 3.2.1, that will help us to deduce a useful description of points in the preimage, under f, that escape to infinity. It turns out that the best choice of U is the one whose entries depend on an edge of $A = A_1 \oplus A_2$ (Prop. 5.10).

Consider an edge, say $\Gamma \prec A$ with summands (Γ_1, Γ_2), along which we want to perform a change of basis. Let a_1 be the vertex of Γ that is closest to the origin. Also let v be the primitive vector starting from a_1 along the direction of Γ. Let Γ' be the edge adjacent to Γ at a_1 and let v' be the corresponding primitive vector. We refer to Figure 3 for a depict of this setting.

Our goal is to compute a pair of vectors, $\tilde{e} := (\tilde{e}_1, \tilde{e}_2)$ where $e_i \in \mathbb{Z}^2$, such that

(Π1) $\tilde{e}$ is a basis of the lattice $\mathbb{Z}^2$, and

(Π2) the Minkowski sum $A + \{-a_1\}$ is contained in the cone $\{b_1\tilde{e}_1 + b_2\tilde{e}_2 \mid b_1, b_2 \in \mathbb{R}_{\geq 0}\}$. Or in other words the basis $\tilde{e}$ spans positively the lattice points of $A - a_1$.

Using the new basis $\tilde{e}$ we can define a linear transformation $U : \mathbb{Z}^2 \to \mathbb{Z}^2$ that maps $\tilde{e}$ to the canonical basis of $\mathbb{Z}^2$.

To compute $\tilde{e}$ we proceed as follows: We enumerate all the the lattice points inside the fundamental parallelepiped that v and v' define. To enumerate the lattice points inside a (fundamental) parallelepiped we use the algorithm from [4, Theorem 3.4 and Algorithm 7]. Then, we find the lattice point that is closest to Γ, say c. Next, we consider a line, say ℓ, through c that is parallel to Γ. Finally, we find the lattice point on ℓ that is closest to a_1 but does not belong to the interior of the polygon. This point and a_1 define the second vector in the new basis. If we call this vector w, then $\tilde{e} = (v, w)$. We refer the reader to Figure 3 for an illustration of the various points and vectors.

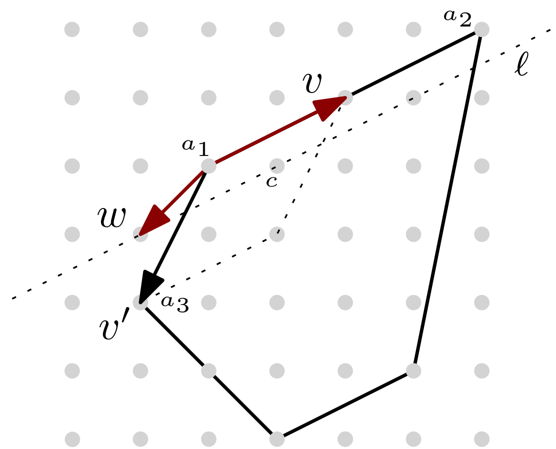

Figure 3: Toric change of basis. Γ is the edge delimited by a_1 and a_2, while Γ' is delimited by a_1 and a_3. The corresponding primitive vectors are v and v', respectively. The vectors v and w consist a basis of $\mathbb{Z}^2$. In addition they define a cone that contains all the lattice points of the polygon. Thus, the toric change of basis is defined by the vectors v and w and $\tilde{e} = (v, w)$.

We consider the matrix T, where

$$T = \left(\begin{smallmatrix} t_{11} & t_{1,2} \\ t_{2,1} & t_{2,2} \end{smallmatrix}\right) = \left(\begin{smallmatrix} v_1 & v_2 \\ w_1 & w_2 \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z}).$$

Then, T corresponds to the following change of variables $z = x^{T\binom{1}{1}}$. Thus, the transformation U that we are looking for is the inverse of this map, that is

$$x_1 \mapsto z_1^{w_2/D} z_2^{-v_2/D}, x_2 \mapsto z_1^{-w_1/D} z_2^{v_1/D},$$

where $D = \det(T) = \pm 1$ is the determinant of T. From the properties (Π1) and (Π2) of $T \in \mathrm{SL}(2, \mathbb{Z})$, we deduce that T, and thus also U, depends on Γ and A. We denote the subset of $\mathrm{SL}(2, \mathbb{Z})$ of all such U by $\mathsf{TM}_\Gamma(\mathbb{Z}^2)$. We also have the following immediate consequence.

Lemma 5.1. *Let $\alpha \in \mathbb{Z}^2$ be the primitive integer vector supporting an edge $\Gamma \prec A$. Then, for any $U \in \mathsf{TM}_\Gamma(\mathbb{Z}^2)$, $U\Gamma$ is an edge of UA. Moreover, the vector $(U^{-1})^\top \cdot \alpha$ is equal to $(0, 1)$ and it supports $U\Gamma$.*

Let $r_1, r_2 \in \mathbb{N}^2$ be the respective points in Γ_1, Γ_2 whose Minkowski sum $r_1 \oplus r_2$ results the point $a_1 \in \Gamma$ (see Figure 3). Property (Π1) implies that if $\varphi \in \mathbb{K}[x_1, x_2]^2$; $\mathrm{supp}(\varphi) = A$, then

$$(Ux^{r_1}\varphi_1, Ux^{r_2}\varphi_2) = \left(\overline{U}\varphi_1, \overline{U}\varphi_2\right) \tag{3}$$

consists of two polynomials in $\mathbb{K}[z_1, z_2]$. Note that this is not necessarily true for $U\varphi$, as the latter pair might have negative exponents.

For the rest of the paper, we will us the notation $\overline{U}\varphi$ for reference to the pair in (3).

Remark 5.2. *For any $\varphi \in \mathbb{K}[x_1, x_2]^2$, where $A = \mathsf{NP}(\varphi)$, the following hold: (i) For any $U \in \mathsf{TM}_\Gamma(\mathbb{Z}^2)$, the system $\overline{U}\varphi_\Gamma = 0$ is univariate, and $\overline{U}\varphi = 0$ is bivariate, and (ii) $\overline{U}\varphi_\Gamma = 0$ has a solution $\rho \in \mathbb{K}^*$ iff $\overline{U}\varphi = 0$ has a solution $(\rho, 0) \in \mathbb{K}^* \times \{0\}$ iff $\varphi_\Gamma = 0$ has a solution in $(\mathbb{K}^*)^2$.*

5.2 Jelonek set is the union of multiplicity sets

Let $f : \mathbb{K}^2 \to \mathbb{K}^2$ be a dominant polynomial map. We will describe in Proposition 5.6 the multiplicity set $\mathcal{M}_f(\Gamma)$ that corresponds to a semi-origin or pertinent edge Γ. Afterwards, we show that the union of all multiplicity sets form the Jelonek set (Prop. 5.10). Let Γ be an edge of A and consider a matrix U in $\mathsf{TM}_\Gamma(\mathbb{Z}^2)$.

Definition 5.3. *The* Γ-multiplicity set $\mathcal{M}_f(\Gamma)$ *is the closure of the set consisting of points* $y \in \mathbb{K}^2$ *for which* $\overline{U}(f-y) = 0$ *has a solution* $\varrho \in \mathbb{K}^* \times \{0\}$ *of multiplicity* m*, and there exists* $\tilde{y} \in \mathbb{K}^2$*, different from* y*, for which* $\overline{U}(f-\tilde{y}) = 0$ *has a solution* ϱ *of multiplicity* $\tilde{m}$ *and* $0 \leq \tilde{m} < m$*.*

Example 5.4. *Let* $f - y = 0$ *denote the polynomial system*

$$\begin{aligned} 1 + 2uv - u^2v^3 - y_1 &= 0, \\ 5 + 12uv - 10u^2v^3 + 2u^3v^5 - y_2 &= 0. \end{aligned}$$

The corresponding Newton polytopes and their Minkowski sum are in in Figure . If Γ *denotes the only pertinent face of* $\mathsf{NP}(f)$ *(i.e., the one supported by* $(-2,1)$*), then we have* $U = \left(\begin{smallmatrix} -1 & 1 \\ -2 & 1 \end{smallmatrix}\right) \in \mathsf{TM}_\Gamma(\mathbb{Z}^2)$*. The system* $\overline{U}(f-y) = 0$ *can be written as*

$$\begin{aligned} 2 - s + t(1 - y_1) &= 0, \\ 12 - 10s + 2s^2 + t(5 - y_2) &= 0, \end{aligned}$$

and has only two solutions in $\mathbb{K}^2$ *that are simple for any generic* $y \in \mathbb{K}^2$*. One of them is* $(2,0)$*.*

The Jacobian of $\overline{U}(f-y)$*, with respect to the variables* (s,t)*, evaluated at* $(2,0) \leftarrow (s,t)$ *is the matrix* $\left|\begin{smallmatrix} -1 & -2 \\ 1-y_1 & 5-y_2 \end{smallmatrix}\right|$*. Therefore, the solution* $(2,0)$ *of the system* $\overline{U}(f-y) = 0$ *has multiplicity two if and only if* $-3 - 2y_1 + y_2 = 0$*. Consequently, this forms the* Γ*-multiplicity set of* f*.*

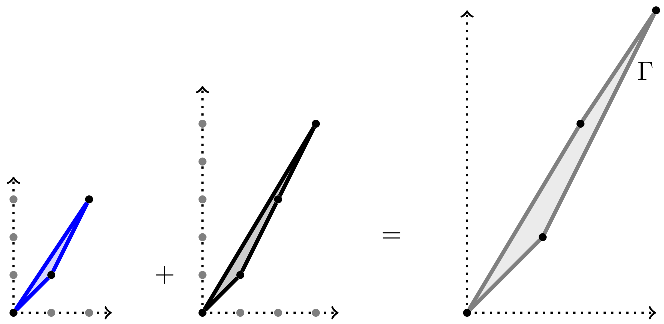

Figure 4: The Newton polytopes, with their Minkowski sum, corresponding to the map in Example 5.4.

Lemma 5.5. *The set* $\mathcal{M}_f(\Gamma)$ *does not depend on the choice of the element in* $\mathsf{TM}_\Gamma(\mathbb{Z}^2)$*.*

Proof. The unimodularity of matrices in $\mathsf{TM}_\Gamma(\mathbb{Z}^2)$ implies that the number of solutions of the transformed systems, as well as their multiplicities, is preserved. Moreover, all transformed systems under U are equal when restricted to Γ. Therefore, any transformation of $f - y$ under U gives a unique number of solutions in $\mathbb{K}^* \times \{0\}$, together with multiplicities. $\square$

The proof of this next result is at the end of the section.

Proposition 5.6. *Let Γ be an edge of A, and let $U \in \mathsf{TM}_\Gamma(\mathbb{Z}^2)$. The following hold:*

(1) If Γ is short and not semi-origin, then $\mathcal{M}_f(\Gamma) = \varnothing$.

(2) If Γ is semi-origin, then $\mathcal{M}_f(\Gamma)$ is either a point, a semi-algebraic curve, or a finite union of lines.

(3) If $\mathcal{M}_f(\Gamma) \neq \varnothing$, then

(3.1) $\mathcal{M}_f(\Gamma)$ has Lebesgue measure zero.

(3.2) Consider any $y \in \mathcal{M}_f(\Gamma)$ and let $\varrho \in \mathbb{K}^* \times \{0\}$ be a solution of $\overline{U}(f-y) = 0$. Then for any open neighborhood $\mathcal{U} \subset \mathbb{K}^2$ of ϱ, there exists $\tilde{y} \in \mathbb{K}^2 \setminus \mathcal{M}_f(\Gamma)$ (close enough to y) such that $\overline{U}(f-\tilde{y}) = 0$ has a solution $\tilde{\varrho} \in \mathcal{U} \cap (\mathbb{K}^*)^2$.

We denote by $\mathcal{D}_f$ the *discriminant* of f. If $C_f := \{x \in \mathbb{K}^2 \mid \det(\mathtt{Jac}_x(f)) = 0\}$, then this is the set $f(C_f)$. Since f is a dominant map, the following observation is straightforward.

Lemma 5.7. *The set $\mathcal{D}_f \cup f\big(\mathbb{K}^2 \setminus (\mathbb{K}^*)^2\big)$ is a finite union of curves.*

The map f is said to be *typical* (or, equivalently *typically dominant*) if $f(0,0)$ is a generic point in $(\mathbb{K}^*)^2$. Note that, thanks to Lemma 5.7 and Proposition 5.6, one can always find a point $a \in (\mathbb{K}^*)^2$ such that the map $f - a$ is typical. This operation preserves the Jelonek set up to translations. Therefore, in what follows, we assume that f is a typical map. The discussion leads to the following consequence.

Lemma 5.8. *With the same notation as in Definition 5.3, the Γ-multiplicity set $\mathcal{M}_f(\Gamma)$ is the closure of the set of points $y \in \mathbb{K}^2$ for which $\varrho \in \mathbb{K}^* \times \{0\}$ is a solution of $\overline{U}(f-y) = 0$ of multiplicity m, whereas ϱ is a solution of $\overline{U}f = 0$ of multiplicity $< m$.*

The following technical lemma is needed to prove our main result in this section.

Lemma 5.9. *If Γ is a short face that is not semi-origin (see Definition 3.1), then for any $y \in \mathbb{K}^2$, the system $(f-y)_\Gamma = 0$ has no solutions in $(\mathbb{K}^*)^2$.*

Proof. We have $(f-y)_\Gamma = f_\Gamma$. Moreover, since one of the summands of Γ is a vertex, the system $f_\Gamma = 0$ consists of two equations in which one of the polynomials is a unique monomial $c_w x^w$; $c_w \in \mathbb{K}^*$. Therefore, it has no solutions in $(\mathbb{K}^*)^2$. ☐

Proposition 5.10. *Let $f : \mathbb{K}^2 \to \mathbb{K}^2$ be a typical polynomial map. It holds*

$$\mathcal{J}_f = \bigcup_{\Gamma} \mathcal{M}_f(\Gamma), \tag{4}$$

where Γ runs over all edges of A that are either semi-origin or pertinent.

Proof. Consider the subset $\mathcal{J}_f^\bullet$ of points $y \in \mathcal{J}_f$ for which $f^{-1}(y)$ is finite (e.g., $\mathcal{J}_f^\bullet = \{(0, y_2) \mid y_2 \in \mathbb{K}^*\}$ if f is the blowup $(u,\ v) \mapsto (u,\ uv)$). Since preimages of $\mathcal{J}_f \setminus \mathcal{J}_f^\bullet$ are components of the set of critical points C_f, we have $f\big(\mathcal{J}_f \setminus \mathcal{J}_f^\bullet\big)$ is finite.

Let $\mathcal{M}_f^\circ(\Gamma)$ be the subset of points $y \in \mathcal{M}_f^\circ(\Gamma)$ as in Definition 5.3, but without taking the closure. Then, since $\mathcal{J}_f$ is a union of curves in $\mathbb{K}^2$ [25], it is enough to show

$$\mathcal{J}_f^\bullet \setminus f(0,0) = \bigcup_{\Gamma} \mathcal{M}_f^\circ(\Gamma) \setminus f(0,0), \tag{5}$$

where the faces Γ are as in the statement. For the first inclusion, we proceed using similar arguments as in the proof of [2, Theorem B]. Lemma 5.7 and Proposition 5.6 (3.1) show that for any $y \in \mathcal{J}_f^\bullet$, one can choose a point $p \in \mathbb{K}^2$, and a line segment $\lambda(]0,1])$ outside

$$\bigcup_{\Gamma} \mathcal{M}_f(\Gamma) \cup \mathcal{D}_f \cup \mathcal{J}_f^\bullet \cup f\big(\mathbb{K}^2 \setminus (\mathbb{K}^*)^2\big),$$

where $\lambda := (\lambda_1, \lambda_2) :\ [0,1] \to \mathbb{K}^2,\ t \mapsto (1-t)y + tp$.

Consider the parametrized polynomial system

$$f - \lambda(t) = 0. \tag{6}$$

Our assumptions on λ show that all solutions $x(t) \in \mathbb{K}^2$ to (6) are simple, and contained in $(\mathbb{K}^*)^2$. Moreover, any one such solution can be represented as a function in t, in which the i-th coordinate is written as the Puiseux series

$$a_i t^{\alpha_i} + \text{ higher order terms in } t, \text{ for } i \in \{1,2\}, \tag{7}$$

where $a_i \in \mathbb{K}^*$, and $\alpha_i \in \mathbb{Q}$. Those are solutions to the system (6), where we extend the field of coefficients to the field of Puiseux series defined over $\mathbb{K}$.

Now, substituting $x(t)$ into $f_i + \lambda_i(t)$, and setting to zero the coefficient q of the smallest power of t, we obtain $(f_i - y_i)_\Gamma(a_1, a_2) = 0$ for some $\Gamma \prec \mathsf{NP}(f)$. Indeed, the value q is the minimum $\min(\langle \alpha, w\rangle \mid w \in \mathsf{NP}(f_i))$, which is reached only for points w in the face of $\mathsf{NP}(f_i)$ supported by the vector $\alpha = (\alpha_1, \alpha_2)$. Therefore, the point $a = (a_1, a_2) \in (\mathbb{K}^*)^2$ is a solution to $(f - y)_\Gamma = 0$.

To describe the obtained Γ, recall that $y \in \mathcal{J}_f^\bullet$. Then, there exists a sequence $\{x_k\}$ of isolated solutions to $f - f(x_k) = 0$, converging to infinity, while $f(x_k) \to y$. Such a sequence can be chosen so that $f(x_k) \in \lambda([0,1])\ \forall k$. The curve selection Lemma implies that one of the solutions $x(t)$ to (6) converges to infinity as $t \to 0$. Then, the value α_i. appearing in (7) is negative for some i. The negativity of α_i and Lemma 5.9 imply that Γ is as in the statement.

To prove that $y \in \mathcal{M}_f^\circ(\Gamma)$, we combine the above description with toric change of coordinates. The vector $(\beta_1, \beta_2) := \big(U^{-1}\big)^\top \cdot \alpha$ supporting the edge $\Xi := U\Gamma$ of the transformed polytope $U\mathsf{NP}(f)$ is equal to $(0,1)$ (Lemma 5.1). The point $z(t)$, satisfying $z^U(t) = x(t)$, is a solution to

$$\overline{U}(f - \lambda(t)) = 0, \tag{8}$$

and we have

$$z_i(t) = b_i t^{\beta_i} + \text{ higher order terms in } t,\ i = 1,2, \tag{9}$$

for some $b = (b_1, b_2) \in (\mathbb{K}^*)^2$. Therefore, as $t \to 0$, $z(t)$ converges to a point $\varrho \in \mathbb{K}^* \times \{0\}$, that is a solution to $\overline{U}(f - y) = 0$. This shows that the multiplicity of ϱ is higher for $\overline{U}(f - y) = 0$, than for $\overline{U}(f - p) = 0$.

To prove the second inclusion, let $\Gamma \prec \mathsf{NP}(f)$ be an edge that is either infinity semi-origin, or pertinent. Assume that $\mathcal{M}_f^\circ(\Gamma) \neq \varnothing$ for some matrix $U \in \mathsf{TM}_\Gamma(\mathbb{Z}^2)$. For any $y \in \mathcal{M}_f^\circ(\Gamma)$, let $\tilde{y}$ be close enough to y, producing a solution $\tilde{\varrho} \in (\mathbb{K}^*)^2$ to $\overline{U}(f - \tilde{y}) = 0$ as in Proposition 5.6 (3.2).

As $\tilde{y}$ converges to y, the second coordinate of $\tilde{\varrho}$ converges to 0, while the first one remains close to a non-zero constant. Then, we can approximate $\tilde{\varrho}$ by a Puiseux series of the form (9), with $\beta = (0,1)$. Any choice of the matrix $U \in \mathsf{TM}_\Gamma(\mathbb{Z}^2)$ transforms the point $\tilde{\varrho}$ to a solution $\tilde{\varrho}^U$ to the system $\overline{U}(f - \tilde{y})$, whose coordinates are expressed as in (7). The assumptions on Γ imply that one of the α_i appearing in (7) is negative. Then, the solution $\tilde{\varrho}^U$ converges to infinity as $\tilde{\varrho} \to \varrho$, and $\tilde{y} \to y$. This proves that $y \in \mathcal{J}_f^\bullet$. □

Proof of Proposition 5.6. (1) follows from Lemma 5.9. To prove (2), assume first that both members of Γ contain $(0,0)$. Remark 5.2 shows that $\overline{U}(f-y)_\Gamma = 0$ is written as

$$g_1(t) - y_1 = g_2(t) - y_2 = 0, \tag{10}$$

for some $y \in \mathcal{M}_f(\Gamma)$, and $g_1, g_2 \in \mathbb{K}[t]$. Then, the set $\mathcal{M}_f(\Gamma)$ coincides with points in $\mathbb{K}^2$ such that (10) satisfies $t \in \mathbb{K}^*$. If g_i is not a constant for some $i \in \{1,2\}$, then all such points y define a parametric semi-algebraic curve in $\mathbb{K}^2$. Otherwise, we have $\mathcal{M}_f(\Gamma) = (g_1(0), g_2(0)) = (f_1(0,0), f_2(0,0))$.

Assume now that one of the members, say Γ_1, of Γ does not contain the point $(0,0)$. Then, the system (10) is instead expressed as

$$g_1(t) = g_{2,0}(t) - y_2 = 0, \tag{11}$$

where $g_i = \overline{U}f_{i,\Gamma}$. Similarly as above, the set of solutions in (11) give rise to a finite union of lines $\big\{(y_1, y_2) \in \mathbb{K}^2 \mid y_2 = g_2(t),\ g_1(t) = 0\big\} = \mathcal{M}_f(\Gamma)$.

To prove (3), we assume that Γ is pertinent, and $\mathcal{M}_f(\Gamma) \neq \varnothing$. We associate to the pair of polynomials $\overline{U}f \in \mathbb{K}[z_1, z_2]^2$, a graph-like set

$$G := \left\{ (z,y) \in \mathbb{K}^2 \times \mathbb{K}^2 \;\middle|\; \overline{U}(f-y)(z) = 0 \right\}.$$

We consider the restrictions $p_1 : G \to \pi_1(G)$, and $p_2 : G \to \pi_2(G)$ to G, of the respective first, and second projections $\pi_1, \pi_2 : \mathbb{K}^4 \to \mathbb{K}^2$, $(z,y) \mapsto z$, and $(z,y) \mapsto y$.

One can check that for any $z \in (\mathbb{K}^*)^2$ there exists a unique $y \in \mathbb{K}^2$, such that $\overline{U}(f-y)(z) = 0$. Then, p_1 is an unramified covering of $(\mathbb{K}^*)^2$ of degree 1.

To prove item (3.2), consider points $y \in \mathcal{M}_f(\Gamma)$, $\varrho \in \mathbb{K}^* \times \{0\}$ as in Definition 5.3, let $\mathcal{V}$ be any small neighborhood of $(\varrho, y) \in \mathbb{K}^2 \times \mathbb{K}^2$, and let $\mathcal{V}_G$ denote the set

$$\mathcal{V}_G^\circ := \mathcal{V} \cap G \cap \big((\mathbb{K}^*)^2 \times \mathbb{K}^2\big).$$

From p_1 being a local covering, we deduce the same for the map

$$F := p_{2|\overline{\mathcal{V}_G^\circ}} : \overline{\mathcal{V}_G^\circ} \to p_2\big(\overline{\mathcal{V}_G^\circ}\big).$$

This yields (3.2). To finish the proof, we show (3.1). Note that the multiplicity of the solution ϱ to $\overline{U}(f-y)(z) = 0$ in $p_1\big(\overline{\mathcal{V}_G^\circ}\big)$ can increase only outside the set of points in $F\big(\overline{\mathcal{V}_G^\circ}\big)$ at which F is a locally trivial fibration. Then, the set of critical values of F contains $\mathcal{M}_f(\Gamma) \cap F\big(\overline{\mathcal{V}_G^\circ}\big)$. We obtain (3.1) by applying the Sard theorem to F. ☐

6 Computing multiplicity sets in presence of multiplicities

Let $f : \mathbb{K}^2 \to \mathbb{K}^2$ be a typical polynomial map and let $A := \mathsf{NP}(f)$. In this section we present how to compute the multiplicity set $\mathcal{M}_f(\Gamma)$ that corresponds to a pertinent edge $\Gamma \prec A$.

After we perform a toric change of variables, we obtain a bivariate polynomial system that has solutions of the form $(\rho, 0)$, for some complex (or real) ρ. When the multiplicity of the solution is one, then we can obtain the multiplicity set using the Jacobian of the system. If the multiplicity is greater than one, then it is more complicated to obtain $\mathcal{M}_f(\Gamma)$.

We present two methods to compute $\mathcal{M}_f(\Gamma)$ in presense of multiplicities. The first one, MS_FULTON, is based on Fulton's algorithm for computing the intersection multiplicity of two plane curves and its worst case complexity is exponential. However, because of its simplicity, if the multiplicity is a small constant, then it outperforms other approaches. The second one, MS_RESULTANT, exploits resultant computations and its worst case complexity is polynomial.

6.1 Computing multiplicity sets à la Fulton

The first part of this section follows closely [18]. It presents a recursive algorithm, introduced by Fulton [17], to compute the intersection multiplicity of two planar curves. We modify it to also compute the multiplicity set $\mathcal{M}_f(\Gamma)$.

6.1.1 Gathmann's presentation

Let $F, G \in K[x_1, x_2]$, for some field K, and assume that $(0,0)$ is a solution to $F = G = 0$. The following is an algorithm described in [18] to compute $\mu_0(F, G)$. It is based on Fulton's algorithm [17]; see also [36, 20] for other variants that compute the intersection multiplicities of two planar curves based on Euclid algorithm. Let us also mention a recent algorithm [7] that exploits blowups.

1. If F and G both contain a monomial independent of x_2, we write

$$\begin{aligned} F = & \quad a x_1^m + \quad \text{(terms involving } x_2 \text{ or lower degree of } x_1\text{)},\\ G = & \quad b x_1^n + \quad \text{(terms involving } x_2 \text{ or lower degree of } x_1\text{)}. \end{aligned}$$

   for some $a, b \in K^*$ and $m, n \in \mathbb{N}$, where we may assume that $m \geq n$. We then set

$$F' := F - \frac{a}{b} x_1^{m-n} G, \tag{12}$$

   to cancel the x_1^m-term in F. Then, $\mu_0(F, G) = \mu_0(F', G)$. As $F'(0) = G(0) = 0$ we can repeat the algorithm recursively with F' and G to compute $\mu_0(F', G)$.

2. If one of the polynomials F and G, say F, does not contain a monomial independent of x_2, we can factor it as $F = x_2 F'$. Then

$$\mu_0(F, G) = \mu_0(x_2, G) + \mu_0(F', G). \tag{13}$$

   We can compute directly the multiplicity $\mu_0(x_2, G)$. By [18, Example 2.10], it equals the smallest power of x_1 in a term of G independent of x_2 (or ∞ if G contains x_2 as a factor).

   To compute $\mu_0(F', G)$, if F' does not vanish at $(0,0)$, then $\mu_0(F', G) = 0$ (see [18, Lemma 2.5 (a)]. So we have computed $\mu_0(F, G)$, and the algorithm terminates. Otherwise, it holds $F'(0,0) = G(0,0) = 0$ and we repeat the procedure for F' and G to compute $\mu_0(F', G)$.

Let $\mathbb{K}[[y]]$ denote the field of all fractions $\frac{f}{g}$, where $f, g \in \mathbb{K}[y_1, y_2]$.

Proposition 6.1. MS_FULTON *(Alg. 4) correctly computes the multiplicity set* $\mathcal{M}_f(\Gamma)$ *that corresponds to a* pertinent *edge* $\Gamma \prec A$*. The multiplicity set is a (possibly empty) union* $\bigcup C_i$ *of finitely-many curves* C_i *that are zero loci of polynomials in* $\mathbb{K}[y_1, y_2]$*, where* $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ *and* i *runs over all solutions to the system* $g_1 = g_2 = 0$ *in* $\mathbb{K}^* \times \{0\}$*.*

Proof. Assume that for some $y \in \mathbb{K}^2$, and $U \in \mathsf{TM}_\Gamma(\mathbb{Z}^2)$, the system $\overline{U}(f - y) = 0$ has a solution $(\rho, 0) \in \mathbb{K}^* \times \{0\}$ of multiplicity $m > 0$. Then, the system $g = 0$; $g_i := \overline{U}(f_i - y_i)(z_1 - \rho, z_2)$, $i = 1, 2$, has $(0,0)$ as a solution of multiplicity $\mu_0(g) = m$.

In what follows, we run the Algorithm MS_FULTON on g with $\rho = 0$, and $1 \leq d_1 \leq d_2$. For $i = 1, 2$, the coefficient $f_i(0,0) - y_i$ is a polynomial in y_i of degree 1, whereas all other coefficients of $f_i - y_i$ have values in $\mathbb{K}$. Since Γ is pertinent, we get

$$g_i(z_1, 0) \in \mathbb{K}[z_1] \quad \text{and} \quad g_i(z_1, z_2) \in \mathbb{K}[y_i][z_1, z_2]. \tag{14}$$

Therefore, as long as condition in Line 12 is satisfied, applying lines 12– 14 any number of times, we obtain a pair $\tilde{g} := (\tilde{g}_1, \tilde{g}_2)$; $\mu_0(\tilde{g}) = \mu_0(g)$, and $\tilde{g}_i$ satisfies (14).

Now, assume that we have applied those lines enough times until Line 7 is satisfied. We abuse notation by letting g (instead of $\tilde{g}$) refer to the resulting pair of polynomials. We assume furthermore without loss of generality that $g_i(z_1, 0) \equiv 0$ for $i = 1$. Thus, we have

$$\mu_0(g) = \mu_0(z_2, g_2) + \mu_0(g_1', h_2), \tag{15}$$

where $g_1 = z_2 g_1'$. One can check that

$$g_2(z_1, 0) = \sum\nolimits_{j \in J} c_j(y) z_1^j, \tag{16}$$

where J is a non-empty finite subset of $\mathbb{N}^*$, and $c_j : \mathbb{K}^2 \to \mathbb{K}$, $y \mapsto c_j(y)$, are non-zero (possibly constant) functions.

We proceed as follows. First, [18, Example 2.10] shows that $\mu_0(z_2, g_2)$ is either greater, or equal to $j_0 := \min(j,\ j \in J)$. This is determined by whether or not y is a solution to $c_{j_0} = 0$. Therefore, the set $\{c_{j_0} = 0\}$ (empty if c_{j_0} is constant) is a component of $\mathcal{M}_f(\Gamma)$. This is the output in Line 2. Regarding g_1', we distinguish two cases.

(I) $g_1'(0, 0)$ is a non-zero (possibly constant) function $F : \mathbb{K}^2 \to \mathbb{K}$, $y \mapsto F(y)$. These are the conditions of Line 7. Then, $\mu_0(g_1', g_2) = 0$ if $y \notin \{F = 0\}$, and $\mu_0(g_1', g_2) > 0$ otherwise. Therefore, Line 14 adds $\{F = 0\}$ to $\{c_{i_0} = 0\}$.

(II) $g_1'(0, 0)$ is equal to zero independently of y. Then, condition of Line 7 is satisfied, and Algorithm MS_FULTON applies again lines 7– 11 until Outcome (I) above is satisfied.

Outcome (I) will eventually be reached giving the output $\{F = 0\} \cup \{c_{i_0} = 0\}$. According to (15), this output describes exactly points $y \in \mathbb{K}^2$ at which $\mu_0(g)$ increases. This finishes the proof of the first statement.

Finally, we show that all zero loci of the form $\{c_{i_0} = 0\}$ or $\{F = 0\}$ are algebraic curves defined over $\mathbb{K}$. It suffices to note that at each iteration a pair (g_1, g_2) has coefficients in $\mathbb{K}[[y_1, y_2]]$. □

6.2 Multiplicity set using resultants

Proposition 6.2. MS_RESULTANT*, Alg. 5, correctly computes the multiplicity set* $\mathcal{M}_f(\Gamma)$ *that corresponds to a* pertinent *edge* $\Gamma \prec A$. *The multiplicity set is a (possibly empty) union* $\bigcup C_i$ *of finitely-many curves* C_i *that are zero loci of polynomials in* $\mathbb{K}[y_1, y_2]$, *where* $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ *and* i *runs over all solutions to the system* $g_1 = g_2 = 0$ *in* $\mathbb{K}^* \times \{0\}$.

Proof. Let $(\rho, 0)$ be a solution to the system $g_1 = g_2 = 0$, say of multiplicity μ. We will exploit the fact that if we project on z_1, then ρ is a root of the resultant of multiplicity at least μ.

We consider the resultant of g_1 and g_2 with respect to z_2. This results a polynomial $R_1 \in \mathbb{Z}[y_1, y_2][z_1]$. Obviously ρ is a root of g of multiplicity at least μ, say μ_1; thus $\mu_1 \geq \mu$. We also know that R_1 factors as $R_1 = R_{11} R_{12}$, where $R_{11} \in \mathbb{Z}[z_1]$ and $R_{12} \in \mathbb{Z}[y_1, y_2][z_1]$. The factor R_{11} is guaranteed because the system has solutions of the form $(\rho, 0)$. We divide out the factors of R_1 that depend only on z_1, that is R_{11} and we end up with the polynomial R_{12}. If we do the substitution $z_1 = \rho$ to R_{12}, then the resulting polynomial J_1 is in $\mathbb{Z}[\rho][y_1, y_2]$ and it is non-zero. If we want ρ to be of higher multiplicity as a root of R_1, then J_1 should be zero. Thus, J_1 is a superset of the part of the multiplicity set $\mathcal{M}_f(\Gamma)$ emanating from $(\rho, 0)$. Then, we consider the resultant of g_1 and g_2 with respect to z_1. We proceed as before, mutatis muntadis, where now

Algorithm 4: MS_FULTON$(g_1, g_2, \varrho, mult, \mathcal{J})$

Input : $(g_1, g_2) \in (\mathbb{Z}[y_1 y_2])[z_1, z_2]$, $\varrho = (\rho, 0) \in \mathbb{C}^2$
Require: $g_1(\rho, 0) = g_2(\rho, 0) = 0$
The algebraic number ρ is given in isolating interval representation, $\rho \cong (A(x_1), I)$.
We also assume that initially $mult = 0$ and $\mathcal{J} = \varnothing$.
Output : The multiplicity of $(\varrho, 0)$, $mult$ and the Jelonek set, $\mathcal{J}_f$.

/* Check if $\varrho = (\rho, 0)$ is a solution of the system. If not the multiplicity is 0. */
if $g_1(\rho, 0)\, g_2(\rho, 0) \neq 0$ **then**
  /* tcoeff returns the tailing coeff of a polynomial wrt z_1. */
  RETURN tcoeff$(g_1(z_1, 0)) \cup$ tcoeff$(g_2(z_1, 0))$;

$d_1 \leftarrow \deg(g_1(z_1, 0))$;
$d_2 \leftarrow \deg(g_2(z_1, 0))$;
/* Ensure that g_1 has always the smallest degree. */
if $d_1 > d_2$ **then**
  RETURN MS_FULTON$(g_2, g_1, \varrho, mult, \mathcal{J})$;

/* If $d_1 = \infty$, then $g_1(z_1, 0) \equiv 0$, thus z_2 divides $g_1(z_1, z_2)$. */
if $d_1 = -\infty$ **then**
  Write g_2 as $g_2(z_1, 0) = (z_1 - \rho)^m (a_0 + (z_1 - \rho) a_1 + \cdots)$;
  In other words, find the multiplicity of ρ in $g_2(z_1, 0)$ by estimating how many times $(z_1 - \rho)$ divides $g_2(z_1, 0)$;
  $mult \leftarrow mult + m$;
  RETURN MS_FULTON$(\mathrm{quo}(g_1, z_2), g_2, \varrho, mult, \mathcal{J})$;

if $d_1 \leq d_2$ **then**
  $g_2 \leftarrow g_2 - z_1^{d_2 - d_1} \frac{\mathtt{lc}(g_2(z_1,0))}{\mathtt{lc}(g_1(z_1,0))} g_1$; // Decrease the degree of g_2.
  RETURN MS_FULTON$(g_2, g_1, \varrho, mult, \mathcal{J})$;

the R_{21} is a power of z_2. At the end we compute a superset of the part of the multiplicity set $\mathcal{M}_f(\Gamma)$ emanating from $(\rho, 0)$.

If we want the solution $(\rho, 0)$ to have multiplicity higher than m as a solution to the system $g_1 = g_2 = 0$, then both ρ and 0 should be roots of higher multiplicity of the corresponding resultants, that is R_1 and R_2, respectively. Thus, the gcd of J_1 and J_2 should be zero. This the subset of the multiplicity set $\mathcal{M}_f(\Gamma)$ that corresponds to $(\rho, 0)$.

If we repeat the same procedure over all solutions $(\rho, 0)$ of the system $g_1 = g_2 = 0$, then we obtain the multiplicity set $\mathcal{M}_f(\Gamma)$. □

Theorem 6.3 (Complexity)**.** *Consider the polynomials $g_1, g_2 \in \mathbb{Z}[y_1, y_2][z_1, z_2]$ which are of degree d wrt to z_1 and z_2 and of degree 1 wrt to y_1 and y_2. Let $g \in \mathbb{Z}[z_1]$ be of degree d and bitsize τ. The bit complexity of* MS_RESULTANT$(g_1, g_2, g, \mathbb{K})$*, Alg. 5, is $\widetilde{\mathcal{O}}_B(d^9 \tau)$.*

Proof. The resultant R_1 is a polynomial in (z_1, y_1, y_2) of degree $(\mathcal{O}(d^2), \mathcal{O}(d), \mathcal{O}(d))$ respectively [1, Prop. 8.49], and bitsize $\widetilde{\mathcal{O}}(d\tau)$ [1, Prop. 8.50]. To compute R_1 we employ fast subresultant algorithms, e.g., [34]. We perform $\widetilde{\mathcal{O}}(d)$ operations. Each operation consists of multiplying two trivariate polynomials in z_1, y_1, y_2; with degrees and bitsize as mentioned before. Each multiplications costs $\widetilde{\mathcal{O}}_B(d^5\tau)$ and so the overall costs for computing R_1 is $\widetilde{\mathcal{O}}_B(d^6\tau)$.

To compute R_{12} we consider R_1 as a bivariate polynomial in y_1 and y_2 with coefficients in $\mathbb{Z}[z_1]$ and we compute its primitive part; that is to compute the gcd of all the coefficients and then divide all of them with it. The coefficients are polynomials in z_1 of degree $\widetilde{\mathcal{O}}(d^2)$ and bitsize $\widetilde{\mathcal{O}}_B(d\tau)$. We can compute their common gcd in $\widetilde{\mathcal{O}}_B(d^6 + d^5\tau)$ with Las Vegas algorithm [29, Lemma 2.2]. The cost of the exact division is dominated by the cost of this operation.

The same complexity bounds hold for the computation of R_2 and R_{22}.

This is of degree d and bitsize τ and so the cost for solving is $\widetilde{\mathcal{O}}_B(d^3 + d^2\tau)$ [39]. Then, for each root of g, say ρ, we make the substituion $(z_1, z_2) \leftarrow (\rho, 0)$ to obtain the polynomials. Finally we compute their gcd in $\mathbb{Z}[\rho][y_1, y_2]$. We use the algorithm by [48], see also [49], by modifying it to employ fast polynomial multiplication algorithns. The cost is $\widetilde{\mathcal{O}}_B(d^8\tau)$. As we have to do this at most d times in the worst case, which corresponds to the different roots of g, the bounds follows. ☐

Algorithm 5: MS_RESULTANT$(g_1, g_2, g, \mathbb{K})$

Input : $(g_1, g_2) \in (\mathbb{Z}[y_1 y_2])[z_1, z_2]$, $g \in \mathbb{Z}[z_1]$, $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$

Require: The g_1, g_2 are the polynomials we obtain after we apply a toric change of variables to f_1, f_2, that corresponds to a pertinent edge Γ of the Minkowski sum $\mathsf{NP}(f_1) \oplus \mathsf{NP}(f_2)$.
The distinct roots of g are $\rho_1, \dots, \rho_r$, and $(\rho_i, 0)$ is a solution to the system $g_1 = g_2 = 0$, for all $i \in [r]$. Notice that $g(z_1) = c\prod_{i=1}^{r}(z_1 - \rho_i)^{\mu_i}$, where $c \in \mathbb{Z}$.

Output : The multiplicity set $\mathcal{M}_f(\Gamma)$.

$R_1 \leftarrow \texttt{res}(g_1, g_2, z_2)$;
/* It holds $R_1 = R_{11}R_{12}$, $R_{11} \in \mathbb{Z}[z_1]$, $R_{12} \in \mathbb{Z}[y_1, y_2][z_1]$ */
/* In particular $R_{11}(z_1) = c_1\prod_{i=1}^{m}(z_1 - \rho_i)^{\mu_{1,i}}$ and $c_1 \in \mathbb{Z}$. */

$R_2 \leftarrow \texttt{res}(g_1, g_2, z_1)$;
/* It holds $R_2 = R_{21}R_{22}$, $R_{21} \in \mathbb{Z}[z_2]$, $R_{22} \in \mathbb{Z}[y_1, y_2][z_2]$ */
/* In particular, $R_{21} = z_2^{\mu_2}$, for some $\delta_2 \in \mathbb{N}$. */

$\mathcal{M}_f(\Gamma) \leftarrow \varnothing$;
for $1 \le i \le r$ **do**
  $J_1 \leftarrow subs(z_1 = \rho_i, R_{12})$;
  $J_2 \leftarrow subs(z_2 = 0, R_{22})$;
  $\mathcal{M}_f(\Gamma) \leftarrow \mathcal{M}_f(\Gamma) \bigcup \gcd(J_1, J_2)$;

RETURN $\mathcal{M}_f(\Gamma)$;

7 Implementation

We have implemented in MAPLE a prototype version of our algorithm for computing the Jelonek set, SPARSE_JELONEK_2 (Alg. 3). We have also implemented Jelonek's algorithm [24] (Alg. 2). Our code also uses CONVEX [16] to perform some polyhedral computations and to MULTIRES[1] to perform some polynomial manipulations.

[1] http://www-sop.inria.fr/members/Bernard.Mourrain/multires.html

A sample use of our software to compute the Jelonek set of the polynomials $(f_1, f_2) = 1 + xy + 2x^2y^2 - 7x^2y/10 - 3x^3y^2, g := 1 + 3xy - 4x^2y^2 + 5x^3y^3 - 6x^4y^4 + 3^7x^{10}y^4/2^5 - 54x^6y^3 + 5103x^9y^3/320 + x^7y^2 + x^4y)$ is as follows:

```
restart;
libname := "path to convex library", libname:
with(convex):
read("/path to/multires.mpl"):
read("/path to/Jelonek.mpl"):
f := 1 + x*y+2*x^2*y^2 -7*x^2 *y/10 - 3*x^3*y^2;
g := 1+3*x*y-4*x^2*y^2+5*x^3*y^3-6*x^4*y^4+3^7*x^(10)*y^4/2^5
     -54*x^(6)*y^3+5103*x^(9)*y^3/320+x^7*y^2+x^4*y;
SJ := Sparse_Jelonek_2:
SJ:-init([f, g]);
SJ:-compute();
```

The output is

$$-150304 + 349920y_1 = 32(10935\,u - 4697)$$

To compute using Jelonek's algorithm, we type

```
Jelonek_2([f, g], u, v);
```

The output is

$$-\frac{1}{64000}(4428675\,y_1 - 4071951)(729\,y_1 - 761)(y_1 - 1)^2(10935\,y_1 - 4697)$$
$$(9\,{y_1}^4 - 32\,{y_1}^3 + 12\,{y_1}^2y_2 + 5\,{y_1}^2 + 19\,y_1y_2 + 4\,{y_2}^2 - 35\,y_1 - 25\,y_2 + 43)$$

As we can see, it contains a superset of the Jelonek set.

Acknowledgments BEH is supported by the Austrian Science Fund (FWF): P33003. Part of this work was done during his stay at the Institute of Mathematics at the Polish Academy of Sciences in Warsaw. Thanks to Zbigniew Jelonek for presenting the problem and to Piotr Migus for fruitful discussions. ET is supported by the ANR JCJC GALOP (ANR-17-CE40-0009), the PGMO grant ALMA, and the PHC GRAPE.

References

[1] S. Basu, R. Pollack, and M-F.Roy. *Algorithms in Real Algebraic Geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, 2003.

[2] D. N. Bernstein. The number of roots of a system of equations. *Funkcional. Anal. i Priložen.*, 9(3):1–4, 1975.

[3] C. Brand and M. Sagraloff. On the complexity of solving zero-dimensional polynomial systems via projection. In *Proc. ACM on International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 151–158, 2016.

[4] F. Breuer and Z. Zafeirakopoulos. Polyhedral omega: A new algorithm for solving linear diophantine systems. *Annals of Combinatorics*, 21(2):211–280, 2017.

[5] S. A. Broughton. Milnor numbers and the topology of polynomial hypersurfaces. *Inventiones mathematicae*, 92(2):217–241, 1988.

[6] J. Capco, M. Gallet, G. Grasegger, C. Koutschan, N. Lubbes, and J. Schicho. The number of realizations of a laman graph. *SIAM Journal on Applied Algebra and Geometry*, 2(1):94–125, 2018.

[7] J. Chalmovianská and P. Chalmovianskỳ. Computing local intersection multiplicity of plane curves via blowup. *arXiv preprint arXiv:1905.00701*, 2019.

[8] D. A. Cox, J. Little, and D. O'shea. *Using algebraic geometry*, volume 185. Springer, 2006.

[9] M. de Berg, O. Cheong, M. Van Kreveld, and M. Overmars. *Computational geometry algorithms and applications*. Springer, 3rd edition, 2008.

[10] L. R. G. Dias, S. Tanabé, and M. Tibăr. Toward effective detection of the bifurcation locus of real polynomial maps. *Foundations of Computational Mathematics*, 17(3):837–849, 2017.

[11] T. Duff, K. Kohn, A. Leykin, and T. Pajdla. Plmp-point-line minimal problems in complete multi-view visibility. In *Proceedings of the IEEE International Conference on Computer Vision*, pages 1675–1684, 2019.

[12] T. Duff, K. Kohn, A. Leykin, and T. Pajdla. PL1P–point-line minimal problems under partial visibility in three views. *arXiv preprint arXiv:2003.05015*, 2020.

[13] B. El Hilany. Describing the Jelonek set of polynomial maps via newton polytopes. *arXiv preprint arXiv:1909.07016*, 2019.

[14] A. Esterov. The discriminant of a system of equations. *Advances in Mathematics*, 245:534–572, 2013.

[15] L. Fourrier. Topologie d'un polynôme de deux variables complexes au voisinage de l'infini. In *Annales de l'institut Fourier*, volume 46, pages 645–687, 1996.

[16] M. Franz. Convex (1.2.0), 2016.

[17] W. Fulton. *Algebraic curves: an introduction to algebraic geometry.* Addison Wesley, Reading, MA, 1974.

[18] A. Gathmann. Plane Algebraic Curves. 2018.

[19] B. E. Hilany. Counting isolated points outside the image of a polynomial map. *arXiv preprint arXiv:1909.08339*, 2019.

[20] J. Hilmar and C. Smyth. Euclid meets Bézout: intersecting algebraic plane curves with the Euclidean algorithm. *The American Mathematical Monthly*, 117(3):250–260, 2010.

[21] J. v. d. Hoeven and É. Schost. Multi-point evaluation in higher dimensions. *AAECC*, 24(1):37–52, 2013.

[22] Z. Jelonek. The set of points at which a polynomial map is not proper. In *Annales Polonici Mathematici*, volume 58, pages 259–266. Instytut Matematyczny Polskiej Akademii Nauk, 1993.

[23] Z. Jelonek. Testing sets for properness of polynomial mappings. *Mathematische Annalen*, 315(1):1–35, 1999.

[24] Z. Jelonek. Note about the set S_f for a polynomial mapping $f\colon \mathbb{C}^2 \to \mathbb{C}^2$. *Bull. Polish Acad. Sci. Math.*, 49(1):67–72, 2001.

[25] Z. Jelonek. Geometry of real polynomial mappings. *Mathematische Zeitschrift*, 239(2):321–333, 2002.

[26] Z. Jelonek and K. Kurdyka. On asymptotic critical values of a complex polynomial. *J. Reine Angew. Math.*, 565:1–11, 2003.

[27] Z. Jelonek and M. Lasoń. Quantitative properties of the non-properness set of a polynomial map. *Manuscripta Mathematica*, 156(3-4):383–397, 2018.

[28] Z. Jelonek and M. Tibăr. Detecting asymptotic non-regular values by polar curves. *International Mathematics Research Notices*, 2017(3):809–829, 2017.

[29] C. Katsamaki, F. Rouillier, E. P. Tsigaridas, and Z. Zafeirakopoulos. On the geometry and the topology of parametric curves. In I. Z. Emiris and L. Zhi, editors, *ISSAC '20: International Symposium on Symbolic and Algebraic Computation, Kalamata, Greece, July 20-23, 2020*, pages 281–288. ACM, 2020.

[30] A. G. Khovanskii. Newton polytopes and irreducible components of complete intersections. *Izvestiya: Mathematics*, 80(1):263, 2016.

[31] J. Kileel. Minimal problems for the calibrated trifocal variety. *SIAM Journal on Applied Algebra and Geometry*, 1(1):575–598, 2017.

[32] J. B. Lasserre. *An introduction to polynomial and semi-algebraic optimization*. Cambridge Texts in Applied Mathematics. Cambridge University Press, Cambridge, 2015.

[33] M. Le Borgne, A. Benveniste, and P. Le Guernic. Polynomial dynamical systems over finite fields. In *Algebraic computing in control (Paris, 1991)*, volume 165 of *Lect. Notes Control Inf. Sci.*, pages 212–222. Springer, Berlin, 1991.

[34] T. Lickteig and M.-F. Roy. Sylvester–Habicht sequences and fast Cauchy index computation. *J. Symb. Comput.*, 31(3):315–341, Mar. 2001.

[35] A. Mantzaflaris, É. Schost, and E. Tsigaridas. Sparse rational univariate representation. In *Proc. ACM on International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 301–308, 2017.

[36] S. Marcus, M. M. Maza, and P. Vrbik. On Fulton's algorithm for computing intersection multiplicities. In *International Workshop on Computer Algebra in Scientific Computing*, pages 198–211. Springer, 2012.

[37] A. Némethi and A. Zaharia. On the bifurcation set of a polynomial function and newton boundary. *Publications of the Research Institute for Mathematical Sciences*, 26(4):681–689, 1990.

[38] L. Pachter and B. Sturmfels, editors. *Algebraic statistics for computational biology*. Cambridge University Press, New York, 2005.

[39] V. Y. Pan. Univariate polynomials: nearly optimal algorithms for numerical factorization and root-finding. *Journal of Symbolic Computation*, 33(5):701–733, 2002.

[40] A. Parusiński. On the bifurcation set of complex polynomial with isolated singularities at infinity. *Compositio mathematica*, 97(3):369–384, 1995.

[41] J. Schicho. And yet it moves: Paradoxically moving linkages in kinematics. *arXiv preprint arXiv:2004.12635*, 2020.

[42] D. Siersma and M. Tibar. Singularities at infinity and their vanishing cycles. *Duke Mathematical Journal*, 80(3):771–784, 1995.

[43] A. Stasica. An effective description of the Jelonek set. *Journal of Pure and Applied Algebra*, 169(2-3):321–326, 2002.

[44] A. Stasica. Geometry of the Jelonek set. *Journal of Pure and Applied Algebra*, 198(1-3):317–327, 2005.

[45] A. Storjohann. Near optimal algorithms for computing smith normal forms of integer matrices. In *Proceedings of the 1996 international symposium on Symbolic and algebraic computation*, pages 267–274, 1996.

[46] A. Storjohann. The shifted number system for fast linear algebra on integer matrices. *Journal of Complexity*, 21(4):609–650, 2005.

[47] A. Valette-Stasica. Asymptotic values of polynomial mappings of the real plane. *Topology Appl.*, 154(2):443–448, 2007.

[48] M. Van Hoeij and M. Monagan. A modular gcd algorithm over number fields presented with multiple extensions. In *Proc. International Symposium on Symbolic and Algebraic Computation*, pages 109–116, 2002.

[49] M. Van Hoeij and M. Monagan. Algorithms for polynomial gcd computation over algebraic function fields. In *Proc. of International Symposium on Symbolic and Algebraic Computation*, pages 297–304, 2004.

[50] A. Zaharia. On the bifurcation set of a polynomial function and Newton boundary. II. *Kodai Math. J.*, 19(2):218–233, 1996.

A On optimizing Algorithm SPARSE_JELONEK_2

Several properties of the multiplicity set can be exploited in order to make Algorithm SPARSE_JELONEK_2 skip unnecessary steps. We discuss here two observations which one can take advantage of for this purpose. The formal proofs of some claims will be be omitted, for the improvement of Algorithm SPARSE_JELONEK_2 and its generalizations is left for a future work.

Let $f = (f_1, f_2) : \mathbb{K}^2 \to \mathbb{K}^2$ be a dominant polynomial map, and let $A := \mathsf{NP}(f)$.

A.1 Integer distance and multiplicities of solutions

We start with the following definition.

Definition A.1. *The* integer distance $\text{i-dis}_a(\sigma)$ *of an integer line segment* $\sigma \subset \mathbb{R}^2$*, to a point* $a \in \mathbb{Z}^2$ *is twice the volume of the triangle* $\operatorname{conv}(abc)$*, where* $b, c \in \mathbb{Z}^2$ *are any two consecutive integer points in* σ*.*

Claim A.2. *Let* $\Gamma \prec A$ *be a pertinent edge such that* $\mathcal{M}_f(\Gamma) \neq \emptyset$*. Then,* $\overline{U}f = 0$ *has a solution in* $\mathbb{K}^* \times \{0\}$ *of multiplicity bigger than*

$$\text{i-dis}_0\,\Gamma := \min\left(\text{i-dis}_{(0,0)}(\Gamma_i) \mid i = 1, 2\right). \tag{17}$$

Sketch of Proof. We count the number N of times Algorithm MS_FULTON applies Line 11 on $\overline{U}(f-y)$ (i.e. removing a factor of z_2 from g_1, or g_2) before it terminates. The existence of a non-empty $\mathcal{M}_f(\Gamma)$ shows that N is greater than the smallest d, at which $-y_i z_1^c z_2^d$ is the only monomial appearing $\overline{U}(f_i - y_i)$ that involves y for some $i \in \{1,2\}$. One can then check that d equals to $\text{i-dis}_0\,\Gamma$. Finally, Equation (13) shows that N is not greater than the multiplicity of the solution in the claim. □

The computational time of Algorithm SPARSE_JELONEK_2 can be decreased in the following way.

Proposition A.3 ([19])**.** *Consider a couple of polynomials $\varphi \in \mathbb{C}[x_1, x_2]$, such that* $\operatorname{supp}\varphi = A$. *Let $\mathcal{S}$ denote the set of edges $\Gamma \prec A$ for which there exists $U \in \mathsf{TM}_\Gamma(\mathbb{Z}^2)$, such that $\overline{U}\varphi = 0$ has $m_\Gamma > 0$ solutions, counted with multiplicities in $\mathbb{C}^* \times \{0\}$. Then, the number of isolated points in $\mathcal{Z}^\circ(\varphi)$, counted with multiplicities equals*

$$V(A) - \sum_{\Gamma \in \mathcal{S}} m_\Gamma. \tag{18}$$

Recall that

$$\mu(f) := \mathbb{C}f^{-1}(y) \cap (\mathbb{C}^*)^2$$

is constant for a generic choice of $y \in \mathbb{K}^2$, and $\mu(f) \leq V(A)$ (see Section 4.1). Then, in the notations of Proposition A.3, we get

$$V(A) - \mu(f) = \sum_{\Gamma} m_\Gamma, \tag{19}$$

where Γ runs over all pertinent edges of A. Therefore, Claim A.2 shows that

$$V(A) - \mu(f) \geq \sum_{\Gamma} \text{i-dis}_0\,\Gamma$$

for all above edges Γ at which $\mathcal{M}_f(\Gamma)$ is not empty.

Let $\Gamma(1), \ldots, \Gamma(r)$ be the above edges enumerated according to the order in which they appear in Algorithm SPARSE_JELONEK_2. Then, it suffices to apply Line 19 to only those edges $\Gamma(k)$ that are close enough to the origin. That is

$$V(A) - \mu(f) - \sum_{i=1}^{k-1} \text{i-dis}_0\,\Gamma(i) \geq \text{i-dis}_0\,\Gamma(k).$$

A.2 Real vs Complex Jelonek set

In this part, we propose an approach to speed up Algorithm SPARSE_JELONEK_2 for the case $\mathbb{K} = \mathbb{R}$. Let $\mathbb{C}f$ denote the canonical extension of f to a map from the complex plane to itself. Let $\Gamma \prec A$ be a pertinent edge such that $\mathcal{M}_f(\Gamma) \neq \emptyset$. Let $\{\rho_1, \ldots, \rho_k\}$ denote the set of all solutions to

$$\overline{U}(f-y) = 0$$

in $\mathbb{C}^* \times \{0\}$ that contribute to $\mathcal{M}_f(\Gamma)$ as in Proposition 6.1, or Proposition 6.2.

Recall that each such ρ_i gives rise to one (possibly reducible) component C_i of $\mathcal{M}_f(\Gamma)$. Note that this correspondence $\rho_i \mapsto C_i$ may not be injective. Lemma 6.1 also shows that only the subset of real points $\{\rho_i\}_{i\in I}$ (for some $I \subset \{1, \ldots, k\}$) of $\{\rho_1, \ldots, \rho_k\}$ contributes to $\mathcal{M}_f(\Gamma) \subset \mathbb{R}^2$. Therefore, we have

$$\mathcal{M}_f(\Gamma) = \bigcup_{i \in I} C_i.$$

Fact A.4. *If the curve C_i is not real for some i (i.e. the defining polynomial is not real), then ρ_i is not a real value.*

Several examples indicate that the converse of Fact A.4 is true.

Conjecture A.5. *Let $P_\Gamma \in \mathbb{C}[y_1, y_2]$ be the polynomial defining $\mathcal{M}_{\mathbb{C}f}(\Gamma)$. Then, the real polynomials in the factorization of P_Γ over $\mathbb{C}$ define $\mathcal{M}_f(\Gamma)$.*

If this conjecture is true, then for each pertinent edge Γ, we get

$$\mathcal{M}_f(\Gamma) = \mathcal{M}_{\mathbb{C}f}(\Gamma) \cap \mathbb{R}^2.$$

This unified picture of the Jelonek set can (and should) be exploited for faster algorithms.

B Various subalgorithms

Alg. 7 computes the Minkowski sum of the Newton polytopes of two bivariate polynomials. In addition, it characterizes the edges of the resulting polygon if they are pertinent of infinite semi-origin.

Algorithm 6: TEST_NUMBER_OF_ROOTS($F = (f_1, f_2), \{Q_1, Q_2\}$)

Input : Two bivariate polynomial $f_1, f_2 \in \mathbb{K}[x_1, x_2]$ and the corresponding Newton polygons Q_1, Q_2 with vertex sets $\{v_1, \ldots, v_n\} \subset \mathbb{Z}^2$ and $\{w_1, \ldots, w_m\} \subset \mathbb{Z}^2$.

Require:

Output : `TRUE` if `MV` $= \#\{\text{roots in}\mathbb{C}\}$, `FALSE` otherwise

$v_{n+1} \leftarrow v_1$; $w_{m+1} \leftarrow w_1$;

$Q \leftarrow$ MINKOWKSI_SUM_2(Q_1, Q_2) ;

/* Let the vertex set of Q be $\{q_1, \ldots, q_\ell\}$. */

$\texttt{vol}(Q_1) \leftarrow \frac{1}{2}\sum_{i=1}^{n} \begin{vmatrix} v_{i,1} & v_{i,2} \\ v_{i+1,1} & v_{i+1,2} \end{vmatrix}$; $\texttt{vol}(Q_1) \leftarrow \frac{1}{2}\sum_{j=1}^{m} \begin{vmatrix} w_{j,1} & w_{j,2} \\ w_{j+1,1} & w_{j+1,2} \end{vmatrix}$;

$\texttt{vol}(Q) \leftarrow \frac{1}{2}\sum_{k=1}^{\ell} \begin{vmatrix} q_{k,1} & q_{k,2} \\ q_{k+1,1} & q_{k+1,2} \end{vmatrix}$;

$\texttt{MV} \leftarrow \texttt{vol}(Q) - \texttt{vol}(Q_1) - \texttt{vol}(Q_2)$;

$R \leftarrow \texttt{res}_{x_2}(f_1, f_2) \in \mathbb{K}[x_1]$;

if $\deg(R) = $ `MV` **then** RETURN `TRUE` ;

;

RETURN `FALSE` ;

For the infinity semi-origin edges. Let $\{p_1, \ldots, p_r\}$ be the lattice points on Γ_1. Then the restriction of f_1 on Γ_1 is $\{q_1, \ldots, q_r\}$, then the restriction of f_2 on Γ_2 is

$$f_2 = \sum_{j=1} a_{q_j} x^{q_i} = \sum_{j=1} s a_{q_j} x_1^{q_{j,1}} x_2^{q_{j,2}} = x^v \sum_{j=1}^{s} b_{q_i} (x_1^k x_2^l)^{j-1}$$

C Appendix for Section 2

Proof of Theorem 2.4. We estimate the Boolean cost for computing the Jelonek set using Alg. 1. We follow the approach from [3].

Algorithm 7: MINKOWKSI_SUM(Q_1, Q_2)

Input : Two (Newton) polygons Q_1, Q_2 with vertex sets $\{v_1, \ldots, v_n\} \subset \mathbb{Z}^2$ and $\{w_1, \ldots, w_m\} \subset \mathbb{Z}^2$.

Require: The vertex sets are in counter-clockwise order, starting from the lowest y-coordinate.

Output : The Minkowski sum $Q = Q_1 \oplus Q_2$, as an ordered vertex set, $\{q_1, \ldots, q_\ell\}$, and the characterization of the faces (edges).

$i \leftarrow 1$; $j \leftarrow 1$; $k \leftarrow 1$; `flag` $\leftarrow$ `FALSE` ;
$v_{n+1} \leftarrow v_1$; $v_{n+2} \leftarrow v_2$; $w_{m+1} \leftarrow w_1$; $w_{m+2} \leftarrow w_2$;
repeat
  $q_k \leftarrow v_i \oplus w_j$;
  if `flag` = `TRUE` **then**
    if $0 \notin q_{k-1}$ *and* $0 \notin q_k$ **then** $\overline{q_{k-1}q_k}$ is pertinent;
    if $0 \in$ `summands`(q_{k-1}) *or* `summands`(q_k) **then** $\overline{q_{k-1}q_k}$ is infinite semi-origin;
    `flag` $\leftarrow$ `FALSE` ;
  if $(0 \in$ `summands`(q_{k-1}) *or* `summands`$(q_k))$ *and* $\overline{q_{k-1}q_k}$ *is not a coordinate axis* **then**
    $\overline{q_{k-1}q_k}$ is infinite semi-origin
  $k \leftarrow k + 1$;
  if `Angle`$(v_i, v_{i+1}) <$ `Angle`(w_j, w_{j+1}) **then** $i \leftarrow i + 1$;
  ;
  if `Angle`$(v_i, v_{i+1}) <$ `Angle`(w_j, w_{j+1}) **then** $j \leftarrow j + 1$;
  ;
  if `Angle`$(v_i, v_{i+1}) =$ `Angle`(w_j, w_{j+1}) **then**
    $i \leftarrow i + 1$; $j \leftarrow j + 1$;
    `flag` $\leftarrow$ `TRUE` ;
until $i = (n + 1)$ *and* $j = (m + 1)$;
RETURN $Q = \{q_1, \ldots, q_\ell\}$;

To compute the Jelonek set we perform n (multivariate) resultant computations. It suffices to estimate the cost for R_1. We compute R_1, from the exact division $\det(M(y, x_1))/\det(M_1(y, x_1))$ where $M(x_1, y)$ is the Macaulay matrix, the elements of which are polynomials in $\mathbb{Z}[y][x_1]$, and $M_1(y, x_1)$ is a square submatrix of $M(y, x_1)$. We refer to [8, Chapter 3] for details on the Macaulay matrix and the computation of the resultant.

The matrix M has dimension $\mathcal{O}((nd)^{n-1}) \times \mathcal{O}((nd)^{n-1})$. The resultant R_1 has degree $\mathcal{O}(d^n)$ with respect to x_1 and d with respect to y_i; the bitsize of its coefficients is $\widetilde{\mathcal{O}}((nd)^{n-1}\tau)$ [35]. It has at most $(2n)^n d^{n^2}$ monomials.

We interpret R_1 as a polynomial in $n+1$ variables. We compute its value at $\mathcal{O}(n^n d^{n^2})$ points, say $p = (p_1, p_2, \ldots, p_n, p_{n+1}) \in \mathbb{Z}^{n+1}$. The bitsize of the coordinates of the points is $\widetilde{\mathcal{O}}(n \lg(d))$. Then, using interpolation we recover R_1.

We obtain the evaluation $R_1(p)$ by specializing M, that is $R_1(p) = \det(M(p))/\det(M_1(p))$. The matrix M has dimension $\mathcal{O}((nd)^{n-1}) \times \mathcal{O}((nd)^{n-1})$ and after the specialization its (integer) entries have bitsize $\widetilde{\mathcal{O}}(nd + \tau)$. We compute the determinant in $\widetilde{\mathcal{O}}_B((nd)^{(n-1)\omega}(\tau + nd))$ [46]. We perform this computation $\mathcal{O}(n^n d^{n^2})$ times. This results a total cost of $\widetilde{\mathcal{O}}_B(2^n n^{n(\omega+1)-\omega} d^{n^2+(n-1)\omega}(\tau + nd))$.

The cost of interpolation is almost linear in the size of the output [21] and its costs is dominated. Finally, we multiply the previous bound by n as we have to perform n resultant computations.

$\square$

Proofs of Theorem 2.5. The computation of the polynomials g_1 and g_2 is computationally negligible. The core of the algorithm is the computation of the resultants r_1 and r_2.

Using fast subresultant algorithms [34], the computation of r_1 involves $\widetilde{\mathcal{O}}(d)$ multiplications of polynomials in $\mathbb{Z}[y_1, y_2, x_2]$ of degree $\mathcal{O}(d)$, $\mathcal{O}(d)$, and $\mathcal{O}(d^2)$ respectively, and bitsize $\widetilde{\mathcal{O}}(d\tau)$, in the worst case. Each such multiplication costs $\widetilde{\mathcal{O}}_B(d^5\tau)$, and so the overall cost is $\widetilde{\mathcal{O}}_B(d^6\tau)$ bit operations.

Thus if we consider r_1 as a univariate polynomial in x_1 with coefficients in y_1 and y_2, then its leading coefficient is a polynomial in $\mathbb{Z}[y_1, y_2]$ of bi-degree $(\mathcal{O}(d), \mathcal{O}(d))$ and bitsize $\widetilde{\mathcal{O}}(d\tau)$.

Similar estimates apply for r_2 and its leading coefficient.

Overall, with $\widetilde{\mathcal{O}}_B(d^6\tau)$ bit operations we compute p, that is the complex Jelonek set, which is a polynomial in $\mathbb{Z}[y_1, y_2]$ of of bi-degree $(\mathcal{O}(d), \mathcal{O}(d))$ and bitsize $\widetilde{\mathcal{O}}(d\tau)$. $\square$