NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS
SCHOOL OF SCIENCE
DEPARTMENT OF INFORMATICS AND TELECOMMUNICATIONS
GRADUATE STUDIES PROGRAM

DISSERTATION

Algebraic algorithms for polynomial system solving and applications

Christos Konaxis

ATHENS
JUNE 2010

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Αλγεβρικοί αλγόριθμοι για την επίλυση πολυωνυμικών συστημάτων και εφαρμογές

Χρήστος Σ. Κοναξής

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: Ιωάννης Ζ. Εμίρης, Καθηγητής ΕΚΠΑ

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:

Ιωάννης Ζ. Εμίρης, Καθηγητής ΕΚΠΑ
Ηλίας Κουτσουπιάς, Καθηγητής ΕΚΠΑ
Ευάγγελος Ράπτης, Αναπληρωτής Καθηγητής ΕΚΠΑ

ΕΠΤΑΜΕΛΗΣ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

Ιωάννης Ζ. Εμίρης,
Καθηγητής ΕΚΠΑ

Ηλίας Κουτσουπιάς,
Καθηγητής ΕΚΠΑ

Ευάγγελος Ράπτης,
Αναπλ. Καθηγητής ΕΚΠΑ

Δημήτριος Αχλιόπτας,
Αναπλ. Καθηγητής UC Santa Cruz

Δημήτριος Γουνόπουλος,
Αναπλ. Καθηγητής ΕΚΠΑ

Λεωνίδας Παληός,
Αναπλ. Καθηγητής Παν. Ιωαννίνων

Δημήτριος Πουλάκης,
Καθηγητής ΑΠΘ

Ημερομηνία εξέτασης: 02/06/2010

ABSTRACT

The main object of study in this dissertation is the sparse resultant. Resultants are defined in the sparse (or toric) context in order to exploit the structure of the polynomials as expressed by their Newton polytopes. We consider sparse elimination theory in order to describe the Newton polytope of the sparse resultant of a given overconstrained algebraic system, by enumerating equivalence classes of mixed subdivisions. In particular, we consider specializations of this resultant to a polynomial in a constant number of variables, typically up to 3. We sketch an algorithm that avoids computing the entire secondary polytope; our goal is that it examines only the silhouette of this polytope with respect to an orthogonal projection. Since determinantal formulae are not always possible, the most efficient general method for computing resultants is by rational formulae. This is made possible by Macaulay's seminal result in the dense homogeneous case, extended by D'Andrea to the sparse case. However, the latter requires a lifting of the Newton polytopes, defined recursively on the dimension. We propose a single lifting function of the Newton polytopes, which avoids recursion, and yields a simpler method for computing Macaulay-type formulae of sparse resultants, in the case of generalized unmixed systems, where all Newton polytopes are scaled copies of each other. We fully study a bivariate example and sketch how our approach extends to mixed systems of up to 4 polynomials, and those whose Newton polytopes have a sufficiently different face structure. As another application of sparse elimination, we consider rationally parameterized plane curves, where the polynomials in the parameterization have fixed supports and generic coefficients. We determine the vertex representation of the implicit equation's Newton polygon by considering mixed subdivisions of the input Newton polygons and regular triangulations of point sets defined by Cayley's trick. The implicit polygon is shown to have up to 4, 5, or 6 vertices.

SUBJECT AREA: Computational Algebraic Geometry
KEYWORDS: sparse resultant, mixed subdivision, triangulation,
Macaulay-type formula , implicitization of parametric curves

For my mother, Mariza and Manolis

Ευχαριστίες

Η διατριβή αυτή είναι αποτέλεσμα της συνεχούς στήριξης, έμπνευσης και καθοδήγησης του επιβλέποντα καθηγητή μου Ιωάννη Εμίρη, στον οποίο οφείλω τις θερμότερες ευχαριστίες μου. Υπήρξε ακούραστος καθοδηγητής των ερευνητικών δραστηριοτήτων μου, πηγή γνώσης αλλά και πολύτιμος οδηγός μου στον ακαδημαϊκό κόσμο.

Ακόμα θα ήθελα να ευχαριστήσω τα μέλη της τριμελούς συμβουλευτικής επιτροπής καθ. Ηλία Κουτσουπιά και αναπλ. καθ. Ευάγγελο Ράπτη, καθώς και σε όλα τα υπόλοιπα μέλη της επταμελούς συμβουλευτικής επιτροπής για τις παρατηρήσεις και τα επικοδομητικά τους σχόλια. Ιδιαίτερες ευχαριστίες οφείλω στον Ευάγγελο Ράπτη καθώς με έφερε σε επαφή με το συναρπαστικό κόσμο της Αλγεβρικής Γεωμετρίας και της Υπολογιστικής Άλγεβρας ήδη από τις προπτυχιακές σπουδές μου. Επιπλέον με ενθάρρυνε να συνεχίσω τις σπουδές μου, τόσο σε μεταπτυχιακό, όσο και σε διδακτορικό επίπεδο και συνεχώς μου έδειχνε την εμπιστοσύνη του και την στήριξή του.

Ένα μεγάλο ευχαριστώ είναι το λιγότερο που οφείλω και στον πατέρα μου για την υπομονή του και την υλική και ηθική στήριξή του καθ' όλη τη διάρκεια των σπουδών μου.

Τέλος, θα πρέπει να ευχαριστήσω τους συμφοιτητές μου στο Τμήμα Πληροφορικής, Χρήστο, Γιώργο, Ηλία και Βησσαρίωνα για το ευχάριστο κλίμα που δημιούργησαν στο γραφείο μας, τις εποικοδομητικές συζητήσεις και τις συμβουλές τους.

Η έρευνα που παρουσιάζεται στην εργασία αυτή υποστηρίχθηκε από το πρόγραμμα ΠΕΝΕΔ 2003.

Χρήστος Κοναξής
Αθήνα, Ιούνιος 2010

Contents

1 Introduction **17**
1.1 Sparse elimination . . . 17
1.1.1 Mixed subdivisions . . . 20
1.1.2 Triangulations . . . 21
1.1.3 The Cayley trick . . . 23
1.1.4 Subdivision methods for computing sparse resultants . . . 24
1.2 Thesis structure . . . 24

2 The Newton polytope of the resultant **27**
2.1 Enumeration of mixed cell configurations . . . 27
2.2 Computing silhouettes of $\Sigma(C)$ . . . 30
2.2.1 The projection of $\Sigma(C)$ in dimension one . . . 30
2.2.2 The projection of $\Sigma(C)$ in two and three dimensions . . . 32

3 Single lifting Macaulay-type formulae of unmixed sparse resultants **35**
3.1 Single lifting construction . . . 37
3.2 Recursive construction . . . 41
3.3 Equivalence of constructions . . . 45
3.4 A bivariate example . . . 52
3.5 Conclusion and Further work . . . 58

4 The Newton polygon of the implicit equation **61**
4.1 Rational parameterizations with different denominators . . . 64
4.1.1 The implicit vertices . . . 66
4.2 Rational parameterizations with equal denominators . . . 71
4.2.1 The implicit vertices . . . 77
4.3 Conclusion and Further work . . . 82

Bibliography **87**

List of Figures

1.1 The Minkowski sum of two triangles. 18
1.2 The mixed subdivision of Fig. 1.1 obtained as the projection of the lower hull of the Minkowski sum of the lifted triangles. 21
1.3 Secondary polytope of a pentagon 22
1.4 Application of the Cayley Trick for two triangles. 23

2.1 Lemma 2.1.1: Examples of circuits 29
2.2 Bistellar flips maximizing the coordinate of the volume vector corresponding to the square vertex 31
2.3 Example 2.2.4:A case where every combination of combinatorial criteria fails. 33

3.1 Two scenarios of an application of Def. 3.1.2 for 3 unit squares 39
3.2 Application of Def. 3.1.2 when Q is the unit cube 39
3.3 The mixed subdivisions of 3 unit squares and their Minkowski sum 40
3.4 Input polygons of Exam. 3.2.2 and their subdivisions 43
3.5 Example 3.2.2: 0-step (left) and 1-step of the recursion on secondary cell w.r.t. v_1 (right) of Alg. A 43
3.6 Example 3.3.5: The secondary cell w.r.t. $(-1,-1)$ of the 0-step of Alg. A and its two slices 48
3.7 Example 3.3.7: The two pieces of the secondary cell w.r.t. $(-1,-1)$ of Alg. A and the correspondence between their cells and the cells of the similar secondary cell w.r.t. Alg. B 49
3.8 Input polygons of Exam. 3.4.1 and their subdivisions induced by the lifting of Def. 3.1.3 52
3.9 Exam. 3.4.1: 0-step recursion of Alg. A 53
3.10 Exam. 3.4.1: The mixed subdivision induced by Alg. B 53
3.11 Example 3.4.1: The piece of the secondary cell $\mathcal{F}_{v_1}$ and its mixed subdivision 54
3.12 Example 3.4.1: A slice of the secondary cell $\mathcal{F}_{v_2}$, the corresponding piece and its mixed subdivision w.r.t. Alg. A 56

4.1 The implicit polygons of the curves of Example 4.0.3 63
4.2 The triangulations of C in Thm. 4.1.2 giving vertices $e_1^{max}|_{e_0^{max}}$ and $e_1^{min}|_{e_0^{max}}$. 67
4.3 The triangulations of C in Example 4.1.9, and the corresponding terms . . 71
4.4 Example 4.2.3: polygons C_i, and two mixed subdivisions of C 73
4.5 Second case of Lemma 4.2.7 75
4.6 Lemma 4.2.9: the mixed subdivisions for a certain choice of B_i's. 76

4.7 The implicit polygon in case (2A), in the $e_i e_j$-plane, and the subdivisions of the proof of Thm. 4.2.11 78
4.8 The implicit polygon of a polynomially parameterized curve 80

List of Tables

3.1 Illustration of Cor. 3.3.10 and Cor. 3.3.11 for Example 3.4.1 58

Chapter 1

Introduction

This chapter introduces the basic concepts of this thesis. First, we define the sparse resultant of an overconstrained system of equations with symbolic coefficients. Then, we discuss polytope theory and take a glimpse at the interplay between algebraic geometry and combinatorial geometry and sketch a subdivision-based method to compute sparse resultants.

1.1 Sparse elimination

Elimination theory deals with the following problem: given a set of polynomial equations $f_i(x, y) = 0$, where $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_m)$, find equations $r_j(x) = 0$, which are satisfied, for a given x, if and only if there exists a y such that (x, y) is a common solution of the equations $f_i(x, y) = 0$. It is called elimination theory because we have eliminated the variables y. There are a few symbolic methods for algebraic variable elimination, including Gröbner (or standard) bases, and resultants. Both have exponential complexity in the number of variables, which is expected since the problem is NP-hard; but the latter are preferable in certain situations because they eliminate many variables at one step and can handle symbolic coefficients. Resultants also seem more efficient for solving certain classes of zero-dimensional algebraic systems. In particular, they reduce system solving to linear algebra, via matrix formulae, or to solving univariate polynomials, via the rational univariate representation of all common roots. The resultant generalizes the determinant of the coefficient matrix in the linear case, and the discriminant of a multivariate polynomial. For more information, see [1, 2, 3].

The sparse (or toric) resultant captures the structure of the polynomials by combinatorial means and constitutes the cornerstone of sparse elimination theory [4, 3], [1, chap.7], [2, chap.7]. It is an important tool in deriving new, tighter complexity bounds for system solving, Hilbert's Nullstellensatz, and related problems. These bounds depend on the polynomials' Newton polytopes and their mixed volumes, instead of total degree, which is the only parameter in classical elimination theory. In particular, if d bounds the total degree of each polynomial, the projective resultant has complexity roughly $d^{O(n)}$, whereas the sparse resultant is computed in time roughly proportional to the number of integer lattice points in the Minkowski sum of the Newton polytopes.

The resultant is defined for an overconstrained system of $n+1$ polynomials in n variables over some coefficient ring K. It is the unique, up to sign, integer polynomial over K which vanishes precisely when the system has a root in some variety X. There are two main cases:

- The projective, or classical, resultant expresses solvability of a system of dense polynomials $f_i \in K[x_1, \ldots, x_n]$ in the projective space over the algebraic closure $\overline{K}$ of K.
- The sparse resultant expresses solvability of a system of Laurent polynomials $f_i \in K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ over the toric projective variety X defined by the supports of f_i, in which the torus $(\overline{K})^n$ is a dense subset.

We recall now some crucial notions of sparse elimination theory. Given a polynomial f, its *support* $\mathcal{A}(f)$ is the set of the exponent vectors corresponding to monomials with nonzero coefficients. Its *Newton polytope* $\mathcal{N}(f)$ is the convex hull of $\mathcal{A}(f)$, denoted $\mathrm{CH}(\mathcal{A}(f))$. Newton polytopes are the main tool that allows us to translate algebraic problems into the language of combinatorial geometry. The *Minkowski sum* $A+B$ of $A, B \subset \mathbb{R}^n$ is the set $A+B = \{a+b \mid a \in A, b \in B\} \subset \mathbb{R}^n$. If A, B are convex polytopes, then $A+B$ is also a convex polytope. In what follows we will denote the support of a polynomial f_i as A_i and its Newton polytope as Q_i.

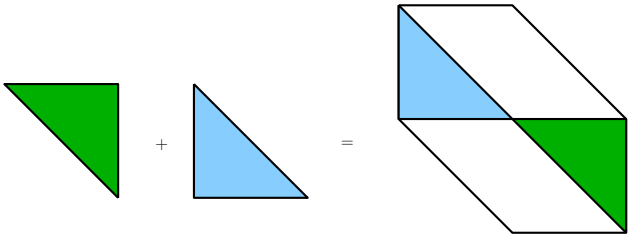

Figure 1.1: The Minkowski sum of two triangles.

Definition 1.1.1. Given convex polytopes $Q_1, \ldots, Q_n \subset \mathbb{R}^n$, their *mixed volume* is the unique integer-valued function $\mathrm{MV}(Q_1, \ldots, Q_n)$, which is symmetric, multilinear with respect to Minkowski addition and scalar multiplication, and satisfies $\mathrm{MV}(Q, \ldots, Q) = n! \mathrm{Vol}(Q)$, for any lattice polytope $Q \subset \mathbb{R}^n$, where $\mathrm{Vol}(\cdot)$ indicates Euclidean volume.

Sometimes the following is taken as the definition of the mixed volume.

Definition 1.1.2. Given convex polytopes $Q_1, \ldots, Q_n \subset \mathbb{R}^n$, their *mixed volume* $\mathrm{MV}(Q_1, \ldots, Q_n)$ is the coefficient of the monomial $\lambda_1 \cdots \lambda_n$ in $\mathrm{Vol}(\lambda_1 Q_1 + \cdots + \lambda_n Q_n)$, considered as a polynomial in $\lambda_1, \ldots, \lambda_n \in \mathbb{R}_+$.

An equivalent but more algorithmic definition of the mixed volume is given in Subsection 1.1.1. We shall abuse notation and denote the mixed volume of a family of supports $A_1, \ldots, A_n$ by $\mathrm{MV}(A_1, \ldots, A_n)$ instead of $\mathrm{MV}(\mathrm{CH}(A_1), \ldots, \mathrm{CH}(A_n))$. The following theorem shows how the geometry of the Newton polytopes can capture the sparseness of a polynomial system of equations and can be used to predict the number of its solutions. The theorem is named after Bernstein but it is also known as BKK bound to emphasize the contribution of Kushnirenko and Khovanskii.

Theorem 1.1.3 (Bernstein). *Given Laurent polynomials $f_1, \ldots, f_n$ over $\mathbb{C}$ with Newton polytopes $Q_1, \ldots, Q_n$, the number of their isolated common roots, counted with multiplicities, is either infinite or does not exceed MV$(Q_1, \ldots, Q_n)$. For almost all specializations of the coefficients of the f_i, the bound is exact.*

The Bernstein bound generalizes the Bézout bound, i.e. the product of the degrees of the polynomials, in the sense that they coincide for a system of dense polynomials. However, for sparse systems the Bernstein bound is significantly lower than Bézout bound.

Let $f_0, \ldots, f_n$ be Laurent polynomials in $\mathbb{C}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ with supports $A_0, \ldots, A_n \subset \mathbb{Z}^n$ and Newton polytopes $Q_0, \ldots, Q_n$. Each polynomial f_i can be written as $f_i = \sum_{a_{ij} \in A_i} c_{ij} x^{a_{ij}}$. We identify each f_i with the vector of its (symbolic) coefficients $c_i = (c_{i0}, c_{i1}, \ldots, c_{in})$ and the system of all polynomials f_i with the vector $\mathbf{c} = (c_0, c_1, \ldots, c_n)$. Let Z_0 be the set of all such vectors for which the polynomials have a common root in $(\bar{\mathbb{C}}^*)^n$ and Z be the Zariski closure of Z. Then Z is an irreducible algebraic variety.

Definition 1.1.4. The sparse resultant $\mathcal{R} = \text{Res}(A_0, A_1, \ldots, A_n)$ of the polynomials f_i is the, unique up to sign, integer polynomial in the coefficients c_{ij}, i.e. $\mathcal{R} \in \mathbb{Z}[\mathbf{c}]$, such that:

1. if Z is of codimension 1, then $\mathcal{R}$ is the defining irreducible polynomial of the hypersurface Z, and
2. if Z has codimension greater than 1, then $\mathcal{R} := 1$.

Corollary 1.1.5. *$\mathcal{R} = Res(A_0, A_1, \ldots, A_n)$ is a homogenous polynomial in the coefficients of each polynomial f_i, of degree MV$_{-i}(Q_0, \ldots, Q_n)$, where MV$_i$ stands for the mixed volume MV$(Q_0, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_n)$. The vanishing of $\mathcal{R}$ is a necessary and sufficient condition for the existence of roots in the toric variety defined by the supports A_i.*

For dense polynomials f_i, i.e. when each Q_i is a Minkowski multiple of the unit simplex in $\mathbb{R}^n$, the sparse resultant coincides with the projective resultant.

Definition 1.1.6. The family of supports A_i of polynomials $f_i,\ i = 0, \ldots, n$, is essential, if for the affine lattice

$$\mathcal{L} := \left\{ \sum_{i=0}^{n} \lambda_i a_i \mid a_i \in A_i,\ \lambda_i \in \mathbb{Z},\ \sum_{i=0}^{n} \lambda_i = 1 \right\}$$

generated by the A_i holds that $\text{rank}(\mathcal{L}) = n$ and $\text{rank}(\mathcal{L}') \geq |J|$ for every $J \subset \{0, 1, \ldots, n\}$, where $\mathcal{L}'$ is the affine lattice generated by the family of supports $\{A_j \mid j \in J\}$.

If every Newton polytope Q_i is n-dimensional, then the family of supports A_i is essential.

Corollary 1.1.7. *[3] Consider the family of supports $\{A_i\}_{i \in I}$, where $I = \{0, \ldots, n\}$. The algebraic variety Z has codimension 1 if and only if there exists a unique subset $\{A_j\}_{j \in J},\ J \subseteq I$ which is essential. Then, the sparse resultant $\mathcal{R} = Res(A_0, \ldots, A_n)$ coincides with the sparse resultant of the equations $\{f_j : j \in J\}$.*

1.1.1 Mixed subdivisions

In this section we introduce our main tool for computing sparse resultants and mixed volumes. Let $Q_0, \ldots, Q_m$ be polytopes in $\mathbb{R}^n$ with $P_i = \mathrm{CH}(A_i)$ and Q their Minkowski sum. We assume that Q is n-dimensional. We are interested in two main cases: $m = n - 1$ (well-constrained systems), when we can define the mixed volume $\mathrm{MV}(Q_0, \ldots, Q_{n-1})$, and $m = n$ (overconstrained systems), when we can define the sparse resultant of polynomials $f_0, \ldots, f_n$ with Newton polytopes $Q_0, \ldots, Q_n$.

A *Minkowski cell* of Q is any full-dimensional convex polytope $B = \sum_{i=0}^{m} B_i$, where each B_i is a convex polytope with vertices in A_i. We say that two Minkowski cells $B = \sum_{i=0}^{m} B_i$ and $B' = \sum_{i=0}^{m} B'_i$ *intersect properly* when the intersection of the polytopes B_i and B'_i is a face of both and their Minkowski sum descriptions are compatible, cf. [5].

Definition 1.1.8. [5, Definition 1.1] A mixed subdivision of Q is any family S of Minkowski cells which partition Q and intersect properly as Minkowski sums. Some Minkowski cells are of particular interest.

- ($m = n - 1$) A cell R is *mixed* if it is the Minkowski sum of n 1-dimensional segments $E_j \subset Q_j$: $R = E_0 + \cdots + E_n$,
- ($m = n$) A cell R is mixed, in particular i-mixed or v_i-mixed, if it is the Minkowski sum of n 1-dimensional segments $E_j \subset Q_j$ and one vertex $v_i \in Q_i$: $R = E_0 + \cdots + v_i + \cdots + E_n$.

For mixed subdivisions see also [4, 6]. When $m = n - 1$ we can easily compute the mixed volume of polytopes P_i.

Theorem 1.1.9. *Given polytopes $Q_1, \ldots, Q_n \subset \mathbb{R}^n$ and a mixed subdivision of $Q = Q_1 + \cdots + Q_n$, the mixed volume $MV(Q_1, \ldots, Q_n)$ is the sum of the volumes of all mixed cells of the mixed subdivision.*

A mixed subdivision is called regular if it is obtained as the projection of the lower hull of the Minkowski sum of lifted polytopes $\widehat{Q_i} := \{(p_i, \omega_i(p_i)) \mid p_i \in Q_i\}$. If the lifting function $\omega := \{\omega_i \ldots, \omega_m\}$ is sufficiently generic, then the induced mixed subdivision is called fine or tight, and $\sum_{i=0}^{m} \dim B_i = \dim \sum_{i=0}^{m} B_i$, for every cell $\sum_{i=0}^{m} B_i$. This construction method ensures that the lower hull facets of the Minkowski sum of the lifted polytopes $\widehat{Q_i}$, are projected bijectively onto Q. Thus, every cell R of the mixed subdivision can be written uniquely as the Minkowski sum

$$R = F_0 + \cdots + F_N \subset \mathbb{R}^n : \quad F_i \text{ is a face of } Q_i,\ i = 0, 1, \ldots, n.$$

Two mixed subdivisions are equivalent if they share the same mixed cells. The equivalence classes are called *mixed cell configurations* [7].

A monomial of the sparse resultant is called extreme if its exponent vector corresponds to a vertex of the Newton polytope $N(\mathcal{R})$ of the resultant. Let ω be a sufficiently generic lifting function. The ω-extreme monomial of $\mathcal{R}$, is the monomial with exponent vector that maximizes the inner product with ω; it corresponds to a vertex of $N(\mathcal{R})$ with outer normal vector ω. The following theorem allows us to compute the extreme monomials of the sparse resultant using regular mixed subdivisions.

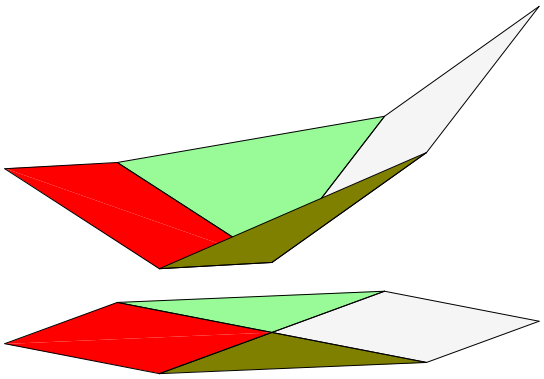

Figure 1.2: The mixed subdivision of Fig. 1.1 obtained as the projection of the lower hull of the Minkowski sum of the lifted triangles.

Proposition 1.1.10. [6]. *For every sufficiently generic lifting function ω, we obtain the ω-extreme monomial of $\mathcal{R}$, of the form*

$$\pm \prod_{i=0}^{n} \prod_{R} c_{i,v_i}^{\mathrm{Vol}(R)}, \tag{1.1}$$

where $\mathrm{Vol}(R)$ *is the Euclidean volume of R, the second product is over all v_i-mixed cells R of the regular tight mixed subdivision of P induced by ω, and c_{i,v_i} is the coefficient of the monomial of f_i corresponding to vertex v_i.*

Corollary 1.1.11. *There exists a surjection from the mixed cell configurations onto the set of extreme monomials of the sparse resultant.*

1.1.2 Triangulations

Another geometric tool we shall use in studying resultants is the set of triangulations of of a point set. This is closely related to the set of mixed subdivisions of a corresponding set of supports, as we shall see in the next subsection.

Let $A \subset \mathbb{R}^d$ be a set of points. A *triangulation* $\mathcal{T}$ of A is a collection of cells $I \subset A$ with cardinality $d+1$ and dimension of $\mathrm{CH}(I) = d$, i.e. I is a simplex in $\mathbb{R}^d$, such that $\bigcup_{I \in \mathcal{T}} \mathrm{CH}(I) = \mathrm{CH}(A)$, and for all $I, J \in \mathcal{T}$, $\mathrm{CH}(I \cap J) = \mathrm{CH}(I) \cap \mathrm{CH}(J)$. A triangulation $\mathcal{T}$ is called *regular* if there exists a lifting vector $\omega \in \mathbb{R}^A$ such that $\mathcal{T}$ is the projection of the lower (equivalently upper) hull of the set $\widehat{A} = \{(a, \omega(a)) \mid a \in A\}$ to $\mathrm{CH}(A)$.

A circuit $Z = \{z_1, \ldots, z_k\}$ is a minimal affinely dependent subset of A, satisfying a unique (up to a constant) affine equation $\lambda_1 z_1 + \ldots + \lambda_k z_k = 0$, where all λ_i are nonzero and $\sum \lambda_i = 0$. Z can be written in the form $Z = (Z_+, Z_-)$, where $Z_+ = \{z_i \mid \lambda_i > 0\}$ and $Z_- = \{z_i \mid \lambda_i < 0\}$. This is usually called Radon's property. The *induced* triangulation $\mathcal{T}^Z$ of Z, is the collection of all simplices in $\mathcal{T}$ with vertices in Z.

A circuit Z has exactly two triangulations $\mathcal{T}_+^Z = \{Z \setminus \{z_i\} \mid z_i \in Z_+\}$ and $\mathcal{T}_-^Z = \{Z \setminus \{z_i\} \mid z_i \in Z_-\}$. The link of a set $\sigma \subset A$ in a triangulation $\mathcal{T}$ of A is defined as

$$\text{link}_{\mathcal{T}}(\sigma) := \{\rho \subset A \mid \rho \cap \sigma = \emptyset, \rho \cup \sigma \in \mathcal{T}\}.$$

Now the bistellar flip on Z can be defined as follows:

Definition 1.1.12. [8] Let $\mathcal{T}_1$ be a triangulation of A that contains one of the two triangulations of Z, say $\mathcal{T}_+^Z$. Suppose that all the cells $\sigma \in \mathcal{T}_+^Z$ have the same link L in $\mathcal{T}_1$. Then the circuit Z *supports a bistellar flip* in $\mathbb{T}_1$ which gives triangulation $\mathcal{T}_2$:

$$\mathcal{T}_2 := \mathcal{T}_1 \setminus \{\rho \cup \sigma \mid \rho \in L, \sigma \in \mathcal{T}_+^Z\} \cup \{\rho \cup \sigma \mid \rho \in L, \sigma \in \mathcal{T}_-^Z\}.$$

A bistellar flip between two regular triangulations $\mathcal{T}_1$ and $\mathcal{T}_2$ can also be understood as a certain regular subdivision T_0 whose only two regular refinements are triangulations T_1 and T_2. The following theorem allows us to explore the set of regular triangulations of a point set using bistellar flips.

Theorem 1.1.13. *[4] For every set A of points affinely spanning $\mathbb{R}^d$ there is a polytope $\Sigma(A)$ in $\mathbb{R}^{|A|-d-1}$, the secondary polytope of A, such that its vertices correspond to the regular triangulations of A and there is an edge between two vertices if and only if the two corresponding triangulations are obtained one from the other by a bistellar flip.*

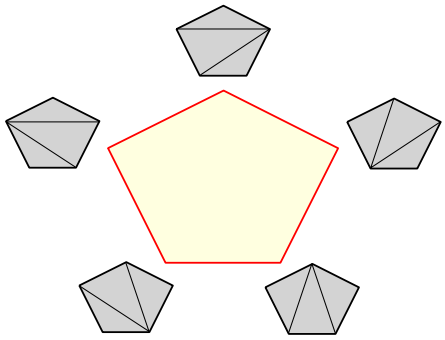

Figure 1.3: Secondary polytope of a pentagon

There are two standard methods to construct the secondary polytope of a point set A. The first one, due to Gelfand, Kapranov and Zelevinskii [4], gives for each vertex $v_{\mathcal{T}}$, corresponding to triangulation $\mathcal{T}$ of A (not necessarily regular), coordinates:

$$(v_{\mathcal{T}})_i = \sum_{\sigma : \sigma \in \mathcal{T}, i \in \text{Vert}(\sigma)} \text{Vol}(\sigma), \quad i = 1, \ldots, |A|.$$

The $|A|$-dimensional vector $v_{\mathcal{T}}$ corresponding to every triangulation $\mathcal{T}$ of A, is called the *volume vector* of $\mathcal{T}$. Then, $\Sigma(A) \subset \mathbb{R}^{|A|}$ is defined as the convex hull of all the volume vectors. Volume vectors of triangulations that are not regular fall into the interior of some face of $\Sigma(A)$ or the interior of $\Sigma(A)$. However, the secondary polytope constructed this way is not full-dimensional but resides in an $(|A| - d - 1)$ - dimensional subspace.

The second method, due to Billera and Sturmfels [9], describes the secondary polytope as the Minkowski integral of the fibers of the affine projection $\pi : \Delta_A \to \text{conv}(A)$, where Δ_A is a simplex with $|A|$ vertices of dimension $|A| - 1$, and π bijects the vertices of Δ_A to A.

1.1.3 The Cayley trick

Given pointsets $A_0, \ldots, A_n$, the Cayley embedding κ introduces a new pointset

$$C := \kappa(A_0, A_1, \ldots, A_n) = \bigcup_{i=0}^{n} (A_i \times \{e_i\}) \subset \mathbb{Z}^{2n+1}, \tag{1.2}$$

where the set of e_i is an affine basis of $\mathbb{R}^n$. The dimension of the convex hull of C is $D \leq 2n$.

Proposition 1.1.14. [The Cayley Trick] [7, 5] *There exists a bijection between the regular tight mixed subdivisions of the Minkowski sum $P = \sum_{i=0}^{n} CHP_i$ and the regular triangulations of C.*

Given a regular triangulation $\mathcal{T}$ of C, we obtain the corresponding regular fine mixed subdivision of polytope P, by intersecting $\mathcal{T}$ with the affine subspace $\mathbb{R}^n \times \{\sum \frac{1}{n+1} e_i\}$ or any other hyperplane in $\mathbb{R}^{2n}$ which is not a supporting hyperplane any (P_i). In particular, the first intersection yields an mixed subdivision of the scaled Minkowski sum $\frac{1}{n+1} \sum P_i$, see Figure 1.4.

Lemma 1.1.15. *A cell R is an n-dimensional cell of a mixed subdivision S of the scaled Minkowski sum $\sum_{i=0}^{n} \frac{1}{n+1} P_i$, if and only if it is the intersection with hyperplane $\mathbb{R}^n \times \{\sum \frac{1}{n+1} e_i\}$, of a $2n$-dimensional cell of a triangulation $\mathcal{T}$ of C, which contains at least one point (a_{ij}, e_i) from every set $A_i \times e_i$.*

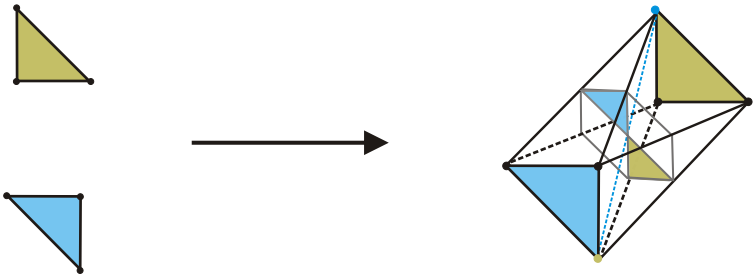

Figure 1.4: Application of the Cayley Trick for two triangles.

An algebraic interpretation of the Cayley trick is the following: given $n+1$ Laurent polynomials f_i in n variables $x_1 \ldots, x_n$ with supports A_i and Newton polytopes P_i, we introduce $n+1$ new variables $y_0, \ldots, y_n$ and form the auxiliary polynomial

$$f = y_0 f_0 + y_1 f_1 + \cdots + y_n f_n.$$

The support of f is the $2n$-dimensional set C of Equation (1.2). Consider the C-discriminant Δ_C of the polynomial f [4].

Proposition 1.1.16. *[4, Prop. 1.3.1] The sparse resultant $\mathcal{R}$ of the polynomials $f_0, \ldots, f_n$ equals the A-discriminant Δ_A of f.*

1.1.4 Subdivision methods for computing sparse resultants

Let us sketch the algorithm of [10, 11] for constructing a sparse resultant matrix, see also [12, 6] for generalizations. It is based on and extends the construction of a mixed subdivision described in Subsection 1.1.1.

Given polynomials $f_0, \ldots, f_n$ with supports $A_0, \ldots, A_n$ and Newton polytopes $Q_0, \ldots, Q_n$, $Q_i = \mathrm{CH}(A_i)$, construct a mixed subdivision of $Q = \sum_{i=0}^{n} Q_i$. Let Z be the integer lattice generated by $\sum_{i=0}^{n} A_i$ and . The algorithm uses the information contained in the mixed subdivision of Q and constructs a square matrix M whose determinant is non-zero if the f_i have generic coefficients, and is divisible by the sparse resultant $\mathrm{Res}(f_0, \ldots, f_n)$.

The mixed subdivision of Q is perturbed by a vector $\delta \in \mathbb{Q}^n$, which is sufficiently small with respect to Z, and in sufficiently generic position with respect to the Q_i. Every lattice point p in $\mathcal{E} := Z \cap (\sum_{i=0}^{n} Q_i + \delta)$ is then associated to a unique maximal cell of the subdivision. This allows us to construct an $|\mathcal{E}| \times |\mathcal{E}|$ matrix M whose rows and columns are indexed by all these points. In particular, polynomial $x^{p-a_{ij}} f_i$ fills in the row indexed by the lattice point p in Definition 1.1.17.

Definition 1.1.17. Let $p \in \mathcal{E}$ lie in a cell $F_0 + \cdots + F_n + \delta$ of the perturbed mixed subdivision, where F_i is a face of Q_i. The *row content (RC)* of p is (i, j), if $i \in \{0, \ldots, n\}$ is the largest integer such that F_i equals a vertex $a_{ij} \in A_i$.

Summarizing, the basic steps of the algorithm are:

1. Pick (affine) liftings $\omega_i : \mathbb{Z}^n \to \mathbb{R} : A_i \to \mathbb{Q}$, $i = 0, \ldots, n$.
2. Construct a regular fine mixed subdivision of the Minkowski sum $\sum_{i=0}^{n} Q_i$ using liftings ω_i.
3. Perturb the Minkowski sum $\sum_{i=0}^{n} Q_i$ by a sufficiently small $\delta \in \mathbb{Q}^n$, so that integer points in $\sum_{i=0}^{n} Q_i + \delta$ belong to a unique cell of the subdivision, and assign *row content* to these points by Definition 1.1.17.
4. Construct resultant matrix M with rows and columns indexed by the previous integer points.

1.2 Thesis structure

The next chapter provides methods for the efficient computation of the resultant polytopes. We exploit the surjection from the set of mixed cell configurations onto the vertices of the resultant polytope and, by means of the Cayley Trick, we reduce the problem to the enumeration of the corresponding equivalence classes of regular triangulations. Then, we characterize the relevant flips that correspond to edges between two such equivalence classes.

In Chapter 3 we offer a single lifting function that allows Canny-Emiris algorithm to construct a Macaulay-type formula for the sparse resultant of polynomial systems with Newton polytopes that are scaled copies of each other. We illustrate our results by

studying a bivariate example, and sketch the the extension of our algorithm to mixed systems.

Finally, Chapter 4 offers a full description of the Newton polygon of the implicit equation of rational parametric curves, under the assumption of generic coefficients. In the case of rationally parameterized curves with different denominators (which includes the case of Laurent polynomial parameterizations), the Cayley trick reduces the problem to computing regular triangulations of point sets in the plane. If the denominators are identical, two-dimensional mixed subdivisions are examined.

Chapter 2

The Newton polytope of the resultant

2.1 Enumeration of mixed cell configurations

In this section we describe algorithms to compute the Newton polytope of the sparse resultant, or resultant polytope, of an overconstrained system of polynomials. We rely on Propositions 1.1.10 and 1.1.14 and following [7] it suffices to enumerate a subset of the vertices of the secondary polytope associated with the input data, corresponding to mixed cell configurations. The resultant polytope allows us to compute a superset of the support of the resultant by considering all integer points contained in it; then we can reduce the computation of the resultant to linear algebra [13].

Several algorithms and implementations enumerate regular triangulations e.g. PUNTOS [14], TOPCOM [15], and the algorithm in [16, 17] which uses reverse search techniques [18] for memory efficiency.

Corollary 1.1.11 establishes a surjection from the set of mixed cell configurations onto the set of vertices of the resultant polytope. Experiments[1] indicate that mixed cell configurations are, depending on the input, much less numerous than mixed subdivisions, hence the computation of the resultant vertices becomes more efficient if we focus on the former. The algorithm in [17], enumerating regular triangulations corresponding to mixed cell configurations, runs in time $O(n^2 s^2 LP(|C| - 2(n+1), s)|M|)$ and space $O(ns)$, where s bounds the number of simplices of any dimension in a triangulation of C, $|M|$ is the number of mixed-cell configurations, and $LP(m, n)$ is the time required to solve a linear programming problem with m variables and n strict inequalities. The same algorithm, enumerating all regular triangulations, runs in time $O(n^2 s^2 LP(|C| - 2(n+1), s)|S|)$, where $|S|$ is the number of all regular triangulations (equivalently, the number of all regular mixed subdivisions) of the set C introduced by the Cayley embedding.

We proceed to characterize the circuits of a triangulation that support bistellar flips that lead from one mixed cell configuration to another. The subgraph of the secondary polytope with vertices regular triangulations corresponding to mixed cell configurations and edges corresponding to these special flips between mixed cell configurations, is con-

[1] See for example the webpage http://ergawiki.di.uoa.gr/index.php/Implicitization

nected.

Consider polynomials $f_0, \dots f_n$, with supports $A_0, \dots, A_n \subset \mathbb{Z}^n$ and Newton polytopes $P_0, \dots, P_n \subset \mathbb{R}^n$. Let $C = \kappa(A_0, \dots, A_n)$ be their image under the Cayley embedding and $d = 2n$ the dimension of C. A mixed subdivision S of $A = A_0 + \dots + A_n$, corresponds, by the Cayley trick, to some triangulation $\mathcal{T} = \kappa(S)$ of C. A set $Z = Z_0 + \dots + Z_n$, $Z_i \subset P_i$ is a circuit of S, if $\kappa(Z) = \kappa(Z_0, \dots, Z_n)$, is a circuit of $\mathcal{T}$. A circuit Z supports a bistellar flip on S if $\kappa(Z)$ supports a bistellar flip on $\mathcal{T}$, and $S' = \text{flip}_Z(S)$ if $\kappa(S') = \text{flip}_{\kappa(Z)}(\kappa(S))$. By abuse of notation, the tuple $(Z_0, \dots, Z_n)$ shall denote both Z and $\kappa(Z)$; every Z_i shall be denoted as $Z_i = \{z_{i,1}, \dots, z_{i,|Z_i|}\}$, where $z_{i,j} \in A_i$ or $z_{i,j} \in A_i \times e_i$, depending on the setting.

Recall that every (maximal) cell of $\mathcal{T} = \kappa(S)$ is a d-dimensional simplex that corresponds to a n-dimensional cell of the mixed subdivision S. A circuit $Z \subset \mathcal{T}$ involves an i-mixed cell if there exist a cell I in $\mathcal{T}$ and a i-mixed cell $R = F_0 + \dots + v_i + \dots + F_n$ in S, such that Z involves I and $I = \kappa(R)$. As above, we shall denote both R and I by the same tuple $(F_0, \dots, F_n)$.

The circuits of interest are those that involve an i-mixed cell. The bistellar flip on every such circuit shall destroy at least one mixed cell and lead to a new mixed cell configuration.

Now, consider a triangulation $\mathcal{T}$ of C and a k-dimensional circuit $Z = (Z_0, \dots, Z_n)$ of $\mathcal{T}$, where $k \leq d$. Suppose that $\mathcal{T}$ is supported on Z. Let $X_1, \dots, X_k$ be the k-dimensional simplices of the induced by $\mathcal{T}$ triangulation on Z. Definition 1.1.12 implies that every X_i is a k-dimensional face of a d-dimensional simplex U_i of $\mathcal{T}$. Moreover, there exist $Y_1, \dots, Y_k \subset C \setminus Z$, where every Y_i is $(d-k-1)$-dimensional, such that $U_i = \text{CH}(X_i \cup Y_i)$. If $k = d$, then $Y_i = \emptyset$ και $U_i = X_i$. Circuit Z is the convex hull of $k+2$ affinely dependent vertices, whereas, every X_i is the convex hull of $k+1$ affinely dependent vertices. Hence, Z is the convex hull of $k+1$ vertices of $X_i \subset U_i$ and a vertex $c \notin U_i$ lying on the same k-dimensional hyperplane defined by X_i. This leads to:

Lemma 2.1.1. *Let $\mathcal{T}$ be a triangulation of C, Z a k-dimensional circuit supported on $\mathcal{T}$, and X a cell of $\mathcal{T}^Z$ of Z. There exists a simplex $U = (U_0, \dots, U_r, \dots, U_n)$ of $\mathcal{T}$, such that X is a k-face of U, and Z can be written as*

$$Z = (Z_0, \dots, Z_r \cup \{c\}, \dots, Z_n), \tag{2.1}$$

where each Z_i is a possibly empty subset of U_i and $c \in (A_r \times e_r) \setminus U_r$.

Note that expression (2.1) is not unique, but depends on the simplex X we choose. Lemma 2.1.1 implies that a circuit involving a mixed cell must contain, in its induced triangulation, at least one simplex X that is a k-dimensional face of a simplex $U = \kappa(R)$, where R is a mixed cell. The following theorem extends [7, Thm 5.1] to our setting, i.e. when we have $n+1$ polytopes in $\mathbb{R}^n$. It also provides a combinatorial condition on the circuits that support bistellar flips between mixed cell configurations.

Theorem 2.1.2. *Let $Z = (Z_0, \dots, Z_n)$ be a circuit of the triangulation $\mathcal{T} = \kappa(S)$ of C, and $R = (F_0, \dots, v_s, \dots, F_n)$ an s-mixed cell of the mixed subdivision S, where $F_i = \{f_{i1}, f_{i2}\} \subseteq A_i$, for $i \neq s$, is an edge, and vertex $v_s \in A_s$. If Z involves $\kappa(R)$, then there exist $r \in \mathbb{N}$, $0 \leq r \leq n$,*

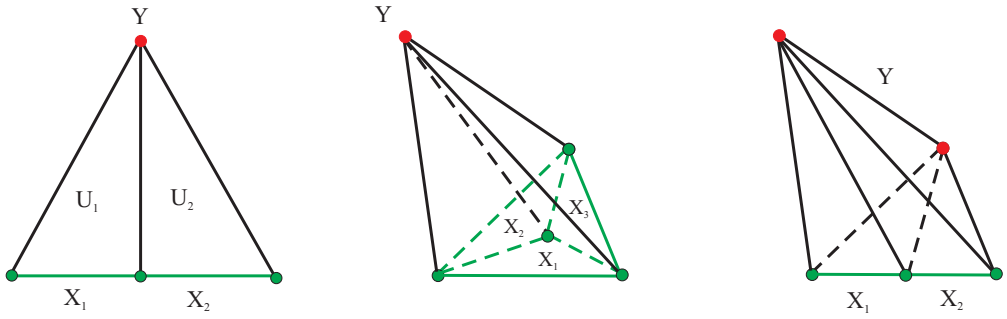

Figure 2.1: Lemma 2.1.1: Examples of circuits (in green color) for $d = 2, 3$ and $k = 1, 2$. The first and third circuits are odd, whereas the second is neither even nor odd

and $c \in A_r \times e_r$, *such that*

$$\begin{array}{ccc} Z_i = F_i \times e_i & \text{or} & Z_i = \emptyset, \ \text{for } i \neq r \\ & \text{and} & \\ Z_r = F_r \times e_r \cup \{c\} & \text{or} & Z_r = \{f_r\} \cup \{c\}, \ f_r \in F_r \times e_r, \ \text{for } i = r. \end{array} \tag{2.2}$$

Proof. Lemma 2.1.1 implies that there exist $r \in \mathbb{N}$ and $c \in A_r \times e_r$, such that Z can be written as

$$Z = (Z_0, \ldots, Z_r \cup \{c\}, \ldots, Z_n), \ Z_i \subseteq F_i \times e_i.$$

Z satisfies a unique (up to a nonzero real multiple) affine relation:

$$\sum_{z \in Z} \lambda_z z = 0, \quad \text{where} \quad \sum_{z \in Z} \lambda_z = 0 \quad \text{and} \quad \lambda_z \neq 0, \ \forall z \in Z. \tag{2.3}$$

Every $z \in Z$ is of the form (z', e_i), $z' \in A_i$. By grouping the summands from each support set A_i, relation (2.3) can be rewritten as:

$$\sum_{i=0}^{d} \left(\sum_{z' \in A_i} \lambda_{z'} (z', e_i) \right) = 0, \tag{2.4}$$

where $\sum_{i=0}^{d} \left(\sum_{z' \in A_i} \lambda_{z'} \right) = 0$ and $\lambda_{z'} \neq 0, \ \forall i \ \forall z' \in A_i$.

Vectors e_i, e_j are linear independent, hence, $< e_i, e_j >= 0$, for every $i \neq j$ and $< e_i, e_i >= 1$. Setting $\vec{0} = (0, \ldots, 0) \in \mathbb{R}^n$ and forming the inner product of (2.4) with every $(\vec{0}, e_i)$, $i = 0, \ldots, n$, we have:

$$\sum_{z' \in A_0} \lambda_{z'} = 0, \ \ldots \ , \sum_{z' \in A_s} \lambda_{z'} = 0, \ \ldots \ , \sum_{z' \in A_s} \lambda_{z'} = 0, \ \ldots \ , \sum_{z' \in A_s} \lambda_{z'} = 0, \tag{2.5}$$

which imply that coefficients λ_z of points z in every Z_i add up to zero. This implies that $|Z_i| \neq 1, \ \forall i = 0, \ldots, n$. Finally, circuit $Z = (Z_0, \ldots, Z_n)$ satisfies:

1. $i \neq r$, then for every Z_i

- $|Z_i| = 0 \iff Z_i = \emptyset$ or
- $|Z_i| = 2 \iff Z_i = F_i \times e_i$.

2. $i = r$, then for Z_r

- $|Z_r| = 2 \iff Z_i = \{f_i\} \cup \{c\},\ f_i \in F_i \times e_i,\ c \in A_r \times e_r$ or
- $|Z_r| = 3 \iff Z_i = F_i \times e_r \cup \{c\},\ c \in A_r \times r$.

□

If $|Z_r| = 2$, the circuit is called even, and if $|Z_r| = 3$, is called odd. Note that Z cannot contain vertex $(v_s, e_s) \in F_s \times e_s$, of the s-mixed cell R, unless $s = r$ and Z_r is of the form $Z_r = F_s \times e_s \cup \{c\} = \{(v_s, e_s), c\}$.

2.2 Computing silhouettes of $\Sigma(C)$

Applications such as the computation of the u-resultant or implicitization of polynomial parametric curves or surfaces call for the computation of the resultant polytope after a specialization of some of its indeterminates, i.e. some of the coefficients of the input polynomials. This reduces to enumerating the vertices lying on the silhouette of the secondary polytope $\Sigma(C)$ with respect to some suitably defined projection. For example, the projection of $\Sigma(C)$ to $\mathbb{R}^2$ solves the problem of implicitization of polynomial curves, the projection to $\mathbb{R}^3$ the one of polynomial surfaces etc. The approach of this section and of Chapter 4 give the same result for the case of polynomial parametric curves with no constant term, although they use different criteria, the first based on volume vectors and the latter on combinatorics. The silhouette can be obtained naively by computing all the vertices of $\Sigma(C)$, then projecting them to the subspace of smaller dimension. For efficiency we want to enumerate only the vertices lying on a silhouette of $\Sigma(C)$ with respect to a projection to be defined by the problem, without computing $\Sigma(C)$.

In short, we have the following polytope theory problem: We have a high dimensional polytope $\Sigma(C)$ which we know only locally. By this we mean that from every vertex we have an oracle to find the coordinates of all of its neighbours. We want an algorithm to compute, for a certain projection π to some lower dimension, the projection $\pi(\Sigma(C))$.

2.2.1 The projection of $\Sigma(C)$ in dimension one

Suppose that we project $\Sigma(C)$, of dimension D, to a line by deleting all coordinates except the first one, in every volume vector. Then, the projection of $\Sigma(C)$ is the convex hull of the vertices $\Phi_{\mathcal{T}_{\max}}, \Phi_{\mathcal{T}_{\min}}$ of the secondary polytope corresponding to the triangulations $\mathcal{T}_{\max}$ and $\mathcal{T}_{\min}$, which maximize and minimize respectively the first coordinate φ_1 of the volume vectors. Translating the problem to its algebraic counterpart, we wish to specialize all but one coefficient appearing in the input polynomials. The Newton polytope of the specialized resultant is a (possibly degenerate) segment.

Starting from an arbitrary regular triangulation $\mathcal{T}$ corresponding to the vertex $\Phi_{\mathcal{T}}$ of the secondary polytope, we want to flip monotonically towards the vertices $\Phi_{\mathcal{T}_{\max}}, \Phi_{\mathcal{T}_{\min}}$.

For this we can use any algorithm that enumerates regular triangulations modified so as to apply the criteria described bellow.

Definition 2.2.1. A simplicial complex K in $\mathbb{R}^D$ is a collection of simplices in $\mathbb{R}^D$ such that: (1) the empty set is in K, (2) for any σ in K, all faces of σ are in K and (3) the intersection of any two simplices in K is a face of both.

The join $K \star L$ of two simplicial complexes K, L is defined as

$$K \star L = \{\sigma \cup \tau : \sigma \in K \text{ and } \tau \in L\}.$$

The volume of a simplicial complex is defined as the sum of the volumes of its simplices.

Lemma 2.2.2. *Let $\mathcal{T}_1$ be a regular triangulation of C, $Z \subset C$ a circuit of $\mathcal{T}_1$ supporting a bistellar flip which gives triangulation $\mathcal{T}_2$, $a_1 \in C$, and $\varphi_1^{\mathcal{T}_1}, \varphi_1^{\mathcal{T}_2}$ the coordinates of the volume vectors of $\mathcal{T}_1$ and $\mathcal{T}_2$ respectively, corresponding to point a_1. Suppose that the simplices of the induced triangulation $\mathcal{T}_1^Z$ of Z are $\sigma_i,\ i \in I$. Then a_1 is a vertex of every simplex σ_i, for $i \in I$, if and only if $\varphi_1^{\mathcal{T}_1} > \varphi_1^{\mathcal{T}_2}$.*

Proof. Let $\mathcal{T}_1^Z, \mathcal{T}_2^Z$ be the triangulations of Z induced by $\mathcal{T}_1$ and $\mathcal{T}_2$ respectively, L the common link of all simplices $\sigma_{1i} \in \mathcal{T}_1^Z$, and $\sigma_{2j},\ j \in J$ the simplices of $\mathcal{T}_2^Z$.

Suppose that a_1 is a vertex of every simplex $\sigma_{1i}, i \in I$. This implies that a_1 is a vertex of every $\sigma_{1i} \star \rho,\ \rho \in L$. Thus, $(\varphi^{\mathcal{T}_1})_1 = \sum_{\forall i \in I, \rho \in L} \mathrm{Vol}(\sigma_{1i} \star \rho) = \mathrm{Vol}(Z \star L)$. Since there is a unique triangulation of Z, such that a_1 is a vertex of all its simplices, the conclusion follows.

For the opposite direction, suppose that there exists a simplex $\sigma_{1k},\ k \in I$ such that a_1 is not one of its vertices. Then a_1 is not a vertex of $\sigma_{1k} \star \rho,\ \rho \in L$ and $\varphi_1^{\mathcal{T}_1} = \sum_{\forall i \in I \setminus k, \rho \in L} \mathrm{Vol}(\sigma_{1i} \star \rho) < \mathrm{Vol}(Z \star L)) = \varphi_1^{\mathcal{T}_2}$. □

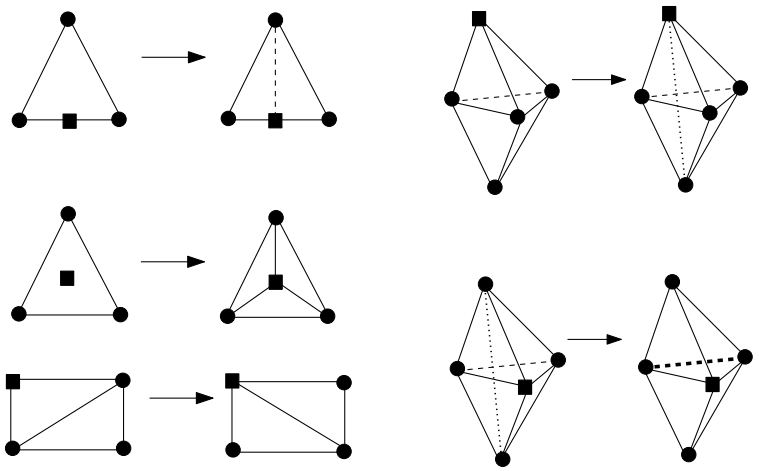

Figure 2.2: Bistellar flips maximizing the coordinate of the volume vector corresponding to the square vertex

The previous lemma allows us to compute a set of candidate circuits with the property that flipping on each one of them increases coordinate φ_1 of the volume vector. Now, we wish to choose among the candidate circuits the one that gives the triangulation $\mathcal{T}_r$ having volume vector with the maximum φ_1 coordinate.

Lemma 2.2.3. *Let $\mathcal{T}$ be a triangulation of C, $Z_1, \ldots, Z_s$ be a set of circuits that increase coordinate φ_1 of the volume vector, $L_1, \ldots, L_s$ their links respectively, and $\mathcal{T}_1, \ldots, \mathcal{T}_s$ the corresponding triangulations obtained by performing a bistellar flip on them. If $\sigma_i \in \mathcal{T}^{Z_i}$ is the unique simplex, of the same dimension as Z_i, not containing vertex a_1, then we obtain the triangulation $\mathcal{T}_r$ such that $\varphi_1^{\mathcal{T}_r} = \max\{\varphi_1^{\mathcal{T}_j} \mid j = 1, \ldots, s\}$, by performing a bistellar flip on circuit Z_r, $r \in \{1, \ldots, s\}$ satisfying*

$$\mathrm{Vol}(\sigma_r \star L_r) = \max\{\mathrm{Vol}(\sigma_j \star L_j) \mid j = 1, \ldots, s\}.$$

Proof. A bistellar flip on each of the candidate circuits Z_i in $\mathcal{T}$ yields triangulation $\mathcal{T}_i$, in which point a_1 is a vertex of all the simplices in the induced triangulation $\mathcal{T}_i^{Z_i}$ of Z_i. Then , $\varphi_1^{\mathcal{T}_i}$ equals the volume of $\sigma_i \star L_i$. □

The previous results can be modified accordingly to provide the triangulation with minimum φ_1-coordinate among all the bistellar neighbours of triangulation $\mathcal{T}$.

In order to compute vertices $\mathcal{T}_{\max}$ and $\mathcal{T}_{\min}$, we start with an initial triangulation $\mathcal{T}$. A regularity check should follow the application of any of the previous criteria. Depending on the setting, the output of these criteria might be the empty set, i.e. there does not always exists a triangulation adjacent to $\mathcal{T}$, which has strictly greater (or smaller) φ_1-coordinate. In such a case, the next vertex to be enumerated is decided by the criteria of the algorithm of Section 2.1 and the path computed is not strictly monotonic or the shortest. When there exists a path from $\mathcal{T}$ to $\mathcal{T}_{\max}$ (or $\mathcal{T}_{\min}$), consisting of vertices with a strictly monotonic sequence of φ_1-coordinates, then our algorithm provides the shortest path. The algorithm described has the same space and time complexities as the algorithm of Section 2.1 in the worst case, but should be more efficient on average.

2.2.2 The projection of $\Sigma(C)$ in two and three dimensions

Suppose that we project $\Sigma(C)$, to the plane defined by the first two coordinates φ_1, φ_2 of the volume vectors. Initially we apply the criteria of the previous section in order to find the vertices of $\Sigma(C)$ that are extreme with respect to each coordinate. Thus, we compute triangulations $\mathcal{T}_{\max}^{\varphi_1}, \mathcal{T}_{\min}^{\varphi_1}, \mathcal{T}_{\max}^{\phi_2}$ and $\mathcal{T}_{\min}^{\varphi_2}$. Now we have to compute the vertices that fill the rest of the silhouette of $\Sigma(C)$. Every combination of our criteria above is not sufficient for this, as it is illustrated by the following example:

Example 2.2.4. Consider the setting shown in Figure 2.3, where $\mathcal{T}_1, \ldots, \mathcal{T}_5$ are the triangulations corresponding to the vertices of the convex hull of the projection of $\Sigma(C)$ to the (φ_1, φ_2)-plane. Suppose that given vertex $\mathcal{T}_1$, we want to flip towards vertex $\mathcal{T}_3$ with maximum φ_1-coordinate, while staying on the silhouette. Using the criteria developed for 1-dimensional projections, we can compute only the bistellar neighbors of $\mathcal{T}_1$: $\mathcal{T}_6 = \max_{\varphi_2}\{\mathcal{T} \mid \varphi_1^{\mathcal{T}} > \varphi_1^{\mathcal{T}_1}\}$ and $\mathcal{T}_7 = \min_{\varphi_2}\{\mathcal{T} \mid \varphi_1^{\mathcal{T}} > \varphi_1^{\mathcal{T}_1}\}$, thus, failing to compute vertex $\mathcal{T}_2$.

We can overcome this by switching from combinatorial to geometric criteria. In particular, we utilize the well known CCW (or Orientation) determinant [19], which decides the relative orientation of any three points in a plane. Let $\pi : \mathbb{R}^D \mapsto \mathbb{R}^2$, be the projection to the (φ_1, φ_2)-plane. Suppose that $\mathcal{T}_1, \ldots, \mathcal{T}_k$ are the bistellar neighbours, with greater φ_1

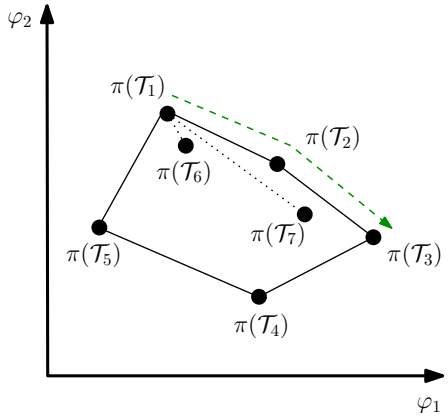

Figure 2.3: Example 2.2.4:A case where every combination of combinatorial criteria fails.

coordinate, of triangulation $\mathcal{T}^{\varphi_2}_{\max}$. A vertex $\mathcal{T}_i$ for which $\mathrm{CCW}(\pi(\mathcal{T}^{\varphi_2}_{\max}), \pi(\mathcal{T}_i), \pi(\mathcal{T}_j))$ holds, for some $\mathcal{T}_j \in \{\mathcal{T}_1, \ldots, \mathcal{T}_k\}$, cannot lie on the silhouette of $\Sigma(C)$ with respect to the projection π. This is essentially Jarvis' algorithm for computing the Convex Hull of points in the plane; it is an instance of the gift-wrapping paradigm [19]. A careful asymptotic analysis would exploit the local behavior of the CCW.

This discussion can be generalized for the case where we project to a subspace of dimension three. For this, we use the gift-wrapping algorithm. This is a well-known algorithm with output sensitive complexity. We can also use reverse search to minimize memory consumption as in [17].

Chapter 3

Single-lifting Macaulay-type formulae of generalized unmixed sparse resultants

A resultant is most efficiently expressed by a *matrix formula:* this is a generically nonsingular matrix, whose specialized determinant is a multiple of the resultant. Its degree in the coefficients of one polynomial equals the corresponding degree of the resultant. For $n = 1$ there are matrix formulae named after Sylvester and Bézout, whose determinant equals the resultant. Unfortunately, such determinantal formulae do not generally exist for $n > 1$, except for specific cases, e.g. [20, 21, 22, 23, 24, 25]. Macaulay's seminal result [26] expresses the extraneous factor as a minor of the matrix formula, for projective resultants of (dense) homogeneous systems, thus yielding the most efficient general method for computing such resultants. There exists a method which, given a Macaulay-type formula of the resultant, constructs a determinant which equals the resultant [27].

Matrix formulae for the sparse resultant were first constructed in [28]. The construction relies on a lifting of the given polynomial supports, which defines a mixed subdivision of their Minkowski sum into mixed and non-mixed cells, then applies a perturbation δ so as to define the integer points that index the matrix. The algorithm was extended in [10, 12, 6]. In the case of dense systems, the matrix coincides with Macaulay's numerator matrix. As a corollary of this construction, one obtains a limited version of a toric effective Nullstellensatz [10, Sec.8].

Extending the Macaulay formula to sparse resultants had been conjectured in [10, 1, 11, 4, 6]; it was a major open problem in elimination theory. We cite [6, p.219], where $P_{\omega,\delta}$ is the extraneous factor, and ω denotes the lifting: *"It is an important open problem to find a more explicit formula for $P_{\omega,\delta}$ in the general toric case. Does there exist such a formula in terms of some smaller resultants? This problem is closely related to the following empirical observation. For suitable choice of δ and ω, the matrix $\mathcal{M}_{\delta,\omega}$ seems to have a block structure which allows to extract the resultant from a proper submatrix. This leads to faster algorithms for computing the sparse mixed resultant."*

D'Andrea's result [29] answers the conjecture by a *recursive* definition of a Macaulay-type formula, see Section 3.2. But this approach does not offer a global lifting, in order to address the stronger original Conjecture 3.0.5. Let M be a matrix formula, also known

as Newton matrix, and $M^{(nm)}$ its submatrix indexed by points in non-mixed cells of the mixed subdivision.

Conjecture 3.0.5. [11, Conj. 3.1.19] [10, Conj. 13.1] *There exist perturbation vector δ and $n+1$ lifting functions for which the determinant of matrix $M^{(nm)}$ divides exactly the determinant of Newton matrix M and, hence, the sparse resultant of the given polynomial system is* $\det M / \det M^{(nm)}$.

We give an affirmative answer to this stronger conjecture by presenting a single lifting which constructs Macaulay-type formulae for generalized unmixed systems, i.e. when all Newton polytopes are scaled copies of each other. We state our main result, to be proven in Section 3.3:

Theorem 3.0.6. *Algorithm B of Section 3.1 constructs a Macaulay-type formula for the sparse resultant of an overconstrained generalized unmixed algebraic system, by means of the lifting function of Definition 3.1.3.*

Our method is generalized, in Section 3.5, to certain mixed systems: those with $n \leq 3$, as well as reduced systems, defined in [30] to possess sufficiently different Newton polytopes. Most of these cases have been studied: reduced systems were settled in [31], and bivariate systems ($n = 2$) in [32], by directly establishing the extraneous factor. We expect that our approach should make the single-lifting algorithm applicable to the fully general case.

A single lifting algorithm is conceptually simpler and also easier to implement. In [33], the authors argue for the advantages of a single lifting over a recursive one in the context of polyhedral homotopy methods for solving algebraic systems. Using a unique global lifting function means that we consider a deformed system, defined by adding a new variable t so that each input monomial x^a gets multiplied by $y^{H(a)}$, where $H(a) \in \mathbb{Q}$ is the lifting value of $a \in \mathbb{Z}^n$. Such deformations capture the system's behavior at toric infinity, hence lie at the heart of most theorems in sparse elimination, such as sparse homotopies, sparse resultants, and the sparse Nullstellensatz [34, 10, 1, 4, 35, 6]. Having a unique deformed system in defining the Macaulay-type formula may allow for further applications of this formula.

Our method belongs to the family of combinatorial methods, which use a row content function for computing sparse resultant formulae, like e.g., [10, 1, 36, 6]. This is the more direct of the two main classes of constructive methods for sparse resultants, the other relying on Koszul and Weyman complexes and their variations, see e.g., [21, 23, 25, 20, 24].

D'Andrea's [29] recursive construction requires one to associate integer points with cells of every dimension from n to 1. Our method constructs the matrix formula directly, without recursion, by examining only n-dimensional cells. These are more numerous than the n-dimensional cells in [29] but our algorithm defines significantly fewer cells totally. The weakness of our method is to consider extra points besides the input supports. Related implementations have been undertaken in Maple, but cover only the original Canny-Emiris method [10], either standalone[1] or as part of library Multires[2]. We expect

[1] http://www.di.uoa.gr/∼emiris/soft_alg.html
[2] http://www-sop.inria.fr/galaad/logiciels/multires.html

that our algorithm shall lead to an efficient implementation of Macaulay-type formulae. The work presented in this section has been submitted for publication in [37].

3.1 Single lifting construction

For any polytopes or point sets A, B, let $\langle A \rangle$ denote the affine span (or hull) of A over $\mathbb{R}$ and $\langle A, B \rangle$ the affine span of $A \cup B$ over $\mathbb{R}$. Let $f_0, \ldots, f_n$ be polynomials with supports $A_0, \ldots, A_n \subset \mathbb{Z}^n$ and Newton polytopes

$$Q_0, \ldots, Q_n \subset \mathbb{R}^n,\ Q_i = \mathrm{CH}(A_i),$$

where $\mathrm{CH}(\cdot)$ denotes convex hull. A monomial with exponent $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ shall be denoted as x^a, where $x := x_1 \cdots x_n$.

Our lifting shall induce a regular and fine (or tight) mixed subdivision of the Minkowski sum $\sum_{i=0}^n Q_i$.Regularity implies the subdivision is in bijective correspondence with the face structure of the upper (or lower) hull of the Minkowski sum of $Q_0, \ldots, Q_n$ after they are lifted to $\mathbb{R}^{n+1}$. Each cell in $\mathbb{R}^n$ is written uniquely as the Minkowski sum of faces F_i of the Q_i. A fine subdivision is characterized by an equality between cell dimension and the sum of the faces' dimensions. We focus on cells of maximal dimension n, and call them maximal or, simply, cells. We distinguish them as mixed and non-mixed: the former are the Minkowski sum of n edges and a vertex. Mixed cells are i-mixed if this vertex lies in A_i. The *type* of a cell is either i-mixed or non-mixed.

Let Z be the integer lattice generated by $\sum_{i=0}^n A_i$. The Minkowski sum $\sum_{i=0}^n Q_i$ is perturbed by a vector $\delta \in \mathbb{Q}^n$, which is sufficiently small with respect to Z, and in sufficiently generic position with respect to the Q_i. The lattice points in $\mathcal{E} = Z \cap (\sum_{i=0}^n Q_i + \delta)$ are associated to a unique maximal cell of the subdivision, and this allows us to construct a matrix formula M whose rows and columns are indexed by these points. In particular, polynomial $x^{p-a_{ij}} f_i$ fills in the row indexed by the lattice point p in Definition 1.1.17.

Our method is based on the matrix construction algorithm of [10, 11], see Section 1.1.4. Below, we modify step 1 of this algorithm to use the lifting function of Definition 3.1.3, and shall extend the last step to produce additionally the denominator matrix. We shall refer to the modified algorithm as Alg. B.

The main idea of both our and D'Andrea's methods is that one point, say $b_{01} \in Q_0$, is lifted significantly higher. Then, the 0-summand of all maximal cells is either b_{01} or a face not containing it. In D'Andrea's case, facets not containing b_{01} correspond to different subsystems where the algorithm recurses (each time on the integer lattice specified by that subsystem). In designing a unique lifting, the issue is that points appearing in two of these subsystems may be lifted differently in different recursions. To overcome this, we introduce several points c_{ijs}, each lying in a suitable face of Q_i indexed by s, very close (with respect to Z) to every b_{ij}, which is lifted very high at recursion i by D'Andrea's method. This captures the multiple roles b_{ij} may assume in every recursion step.

Algorithm B. Our algorithm directly generalizes the one given in [10, 11], and is based on the 4 steps described in Section 1.1.4. We modify step (1) and define a new lifting function; moreover, we describe necessary adjustments to the matrix construction and

extend step (4) so as to produce the denominator matrix of the Macaulay-type formula. The following three definitions suffice to specify our algorithm.

We shall use $\mathcal{E}$ to index the rows (and columns) of the numerator matrix M, whereas the denominator shall be indexed by points lying in non-mixed cells. We focus on generalized unmixed systems, where

$$Q_i = k_i Q \subset \mathbb{R}^n,$$

for some n-dimensional lattice polytope Q and $k_i \in \mathbb{N}^*, i = 0, \ldots, n$. Let the vertices of Q be $b_0, \ldots, b_{|\mathcal{A}|}$, where $Q = \mathrm{CH}(A)$. We shall denote the vertices of each $Q_i = k_i Q$, for $i = 0, \ldots, n$, as $b_{i1}, \ldots, b_{i|\mathcal{A}|}$. Obviously, $b_{ij} := k_i b_j$.

Definition 3.1.1. For $i = 0, \ldots, n-2$, consider any $(n-i)$-dimensional face $F_s^{(i)} \subset Q$, where integer s indexes all such faces. Take any vertex $b_{ij} \in k_i F_s^{(i)}$, for any valid $j \in \mathbb{N}$. Let $\delta_{ijs} \in \mathbb{Q}^n$ denote a *perturbation* vector such that:

1. $b_{ij} + \delta_{ijs}$ lie in the relative interior of $k_i F_s^{(i)}$,
2. It is sufficiently small compared to lattice Z, and $\|\delta_{ijs}\| \ll \|\delta\|$, where $\|\cdot\|$ is the Euclidean norm and δ as above, and
3. It is sufficiently generic to avoid all edges in the mixed subdivision of $\sum_{i=0}^n Q_i$.

For an example of Definition 3.1.1 see Figures 3.1, 3.2, where the (appropriately translated) δ_{ijs}'s are depicted by arrows. We shall use the perturbation vectors of Definition 3.1.1 to define extra points *not* contained in the input supports. Condition (2) of Definition 3.1.1 implies that, in the mixed subdivision induced by the single lifting function β bellow, the cells created by the introduction of the extra points will not contain integer points after we perturb the mixed subdivision by δ. This can be checked at the end of the construction of the mixed subdivision.

Definition 3.1.2. We define points $c_{ijs} \in Q_i \cap \mathbb{Q}^n$, for $i = 0, \ldots, n-2$. Firstly, set $c_{011} := b_{01} + \delta_{011} \in Q_0 \cap \mathbb{Q}^n$ where δ_{011} satisfies Definition 3.1.1. Now let $\{c_{ijs} \in k_i F_s^{(i)}\}$ be the set of points defined in Q_i, where s ranges over all $(n-i)$-dimensional faces $F_s^{(i)} \subset Q$ and j over the set of indices of points in Q_i. Then, let $F_u^{(i+1)}$ be a facet of $F_s^{(i)}$ such that:

1. $k_i F_u^{(i+1)}$ does *not* contain any of the b_{ij}'s corresponding to the already defined c_{ijs}'s, and
2. $k_{i+1} F_u^{(i+1)}$ does *not* contain any of the already defined $c_{(i+1)l}$'s.

For each such facet choose a vertex $b_{(i+1)j} \in A_{i+1}$, for some j, and a suitable perturbation vector $\delta_{(i+1)ju}$ satisfying Definition 3.1.1, and set $c_{(i+1)ju} := b_{(i+1)j} + \delta_{(i+1)ju} \in Q_{i+1} \cap \mathbb{Q}^n$.

The previous definition implies a many-to-one mapping from the set of c_{ijs}'s to that of b_{ij}'s; it reduces to a bijection when restricted to a fixed face $k_i F_s^{(i)} \subset Q_i$ containing b_{ij}. Condition 1 of Definition 3.1.1 implies that c_{ijs} does not lie on a face of dimension $< n-i$ and lies in the interior of $(n-i)$-dimensional $F_s^{(i)}$. We can reduce the number of the c_{ijs}'s in Alg. B, but this would complicate the subsequent proofs.

For an application of Definition 3.1.2 for $n = 2$ see Figure 3.1 where Q is the unit square, and also Figure 3.7 where Q is a pentagon. In both examples, for illustration purposes, we define points c_{ijs} also on edges of polytope Q_1. See also Figure 3.2, where Q is the unit cube.

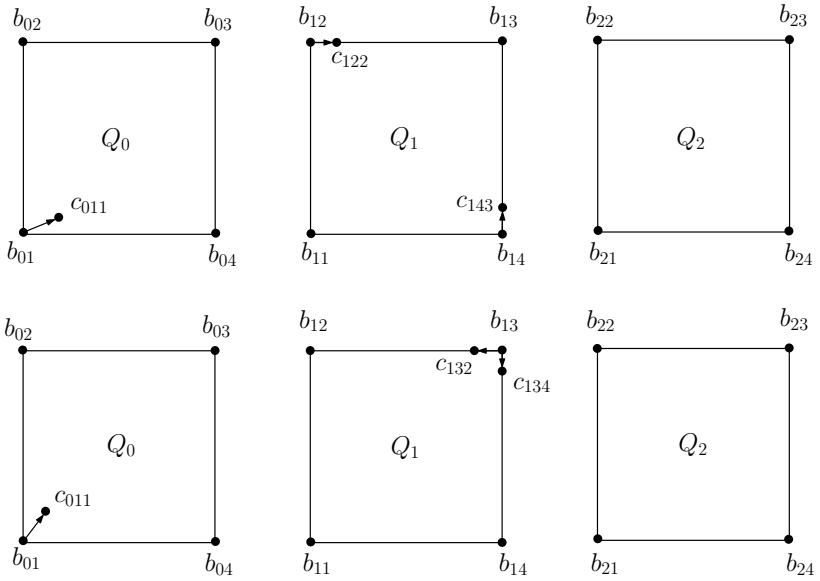

Figure 3.1: Two scenarios of an application of Def. 3.1.2 for 3 unit squares. Facets are numbered clockwise starting from the left vertical edge

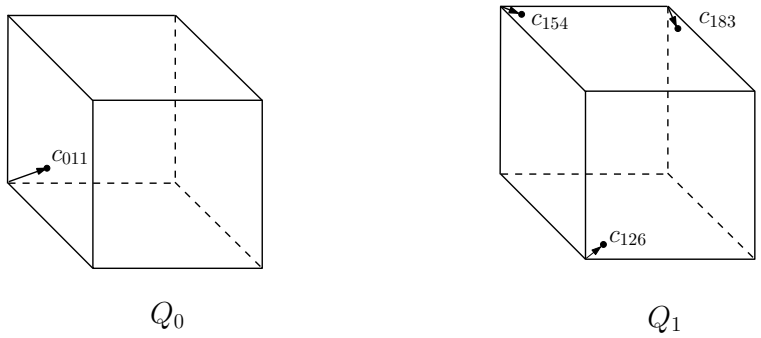

Figure 3.2: Application of Def. 3.1.2 when Q is the unit cube. Alg. B defines additional points only in polytopes Q_0 and Q_1

Definition 3.1.3. Let $h_0 \gg h_1 \gg \ldots \gg h_{n-1} \gg 1$. Alg. B uses sufficiently random linear functions $H_i, i = 0, \ldots, n$, such that:

$$1 \gg H_i(a_{ij}) > 0, \text{ and } H_i \gg H_t,\ i < t,$$

where $a_{ij} \in A_i$ and $i, t = 0, \ldots, n,\ j = 1, \ldots, |A_i|$. Alg. B defines global lifting β as follows:

1. $c_{ijs} \mapsto h_i,\ c_{ijs} \in k_i F_s^{(i)} \subset Q_i,\ i = 0, \ldots, n-1$; this is called primary lifting.
2. $a_{ij} \mapsto H_i(a_{ij}),\ a_{ij} \in A_i, i = 0, \ldots, n.$

Let F^β denote face F lifted under β. Now c^β_{tjs}, for all valid j, s, is much higher, respectively lower, than any c^β_{ijs}, for $i > t$, respectively $i < t$. The β-induced subdivision contains edges with one or two vertices among the c_{ijs}, and edges from the Q_i. The vertex set of the upper hull of Q_i^β contains some or all of the c^β_{ijs} and the lifted vertices of Q_i.

When all Q_i are simplices, as in the classical dense case, it suffices to apply a primary lifting to one point of every Q_i as in Definition 3.1.2. Thus our scheme generalizes the approach by Macaulay [26].

Figure 3.3 shows the mixed subdivisions of three unit squares and their Minkowski sum, induced by lifting β. Here, the perturbation vectors are not sufficiently small compared to $\mathbb{Z}^2$ for illustration purposes.

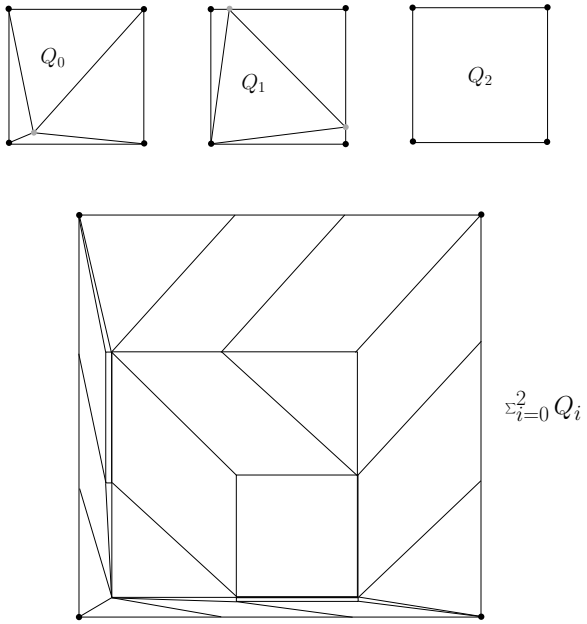

Figure 3.3: The mixed subdivisions of 3 unit squares and their Minkowski sum induced by lifting β

The matrix formula M constructed by Alg. B is indexed by all lattice points in $\mathcal{E}$. To decide the content of each row, every point is associated to a unique (maximal) cell of the mixed subdivision according to Definition 1.1.17. The t-mixed cells contain lattice points as follows:

$$p \in k_0E_0 + \cdots + k_{t-1}E_{t-1} + c_{tjs} + k_{t+1}E_{t+1} + \cdots + k_nE_n \cap Z,$$

for edges $E_i \subset Q$ spanning $\mathbb{R}^n$. This gives unique writing

$$p = p_0 + \cdots + p_{t-1} + (b_{tj} + \delta_{tjs}) + p_{t+1} + \cdots + p_n,\ p_i \in A_i \cap E_i.$$

Hence, the row indexed by p, as with matrix constructions in [10, 29], contains a multiple of $f_t(x)$:

$$x^{p_0+\cdots+p_{t-1}+p_{t+1}+\cdots+p_n} f_t(x),$$

and the diagonal element is the coefficient of the monomial with exponent b_{tj} in $f_t(x)$. Similarly, for the rows corresponding to lattice points in non-mixed cells. The extraneous

factor $\det M/\mathrm{Res}(f_0,\ldots,f_n)$ is the minor of M indexed by points in $\mathcal{E}$ lying in non-mixed cells.

Let us sketch the asymptotic complexity of our algorithm. Alg. B, implemented by the direct approach of [10], comprises of two main steps. First, the computation of the vertices of each Q_i which is typically dominated. Second, we compute RC for all $p \in \mathcal{E}$, which includes the matrix construction. Both steps can be reduced to linear programming with C constraints in V variables, and coefficient bitsize B. If we use a poly-time algorithm such as Karmarkar's [38], the bit complexity is $C^{5.5}V^2B^2$, where B depends on the bitsize of the input coordinates and of δ, δ_{ijs}. It is related to the probability that the chosen perturbations are not sufficiently generic; see [10] for the full analysis.

Let m be the maximum number of vertices of the Q_i, r the total number of c_{ijs}'s, and let $O^*(\cdot)$ indicate that we ignore polylog factors. The linear programs have complexity $O^*(r^2B^2) = O^*(m^nB^2)$ because r is bounded by the total number $O(m^{\lfloor n/2 \rfloor})$ of faces in Q, which is quite pessimistic. In an output sensitive manner, $r = O(|\mathcal{E}|)$, because the addition of every c_{ijs} is made in order to handle at least one distinct point in $\mathcal{E}$. Hence, the complexity of constructing the Macaulay-type formula is $O^*(|\mathcal{E}|^3B^2)$. This holds for matrices in sparse and dense representation. For generalized unmixed systems, one can use $|\mathcal{E}| = O(k^n e^n D)$ from [10, thm.3.10], where $k = \max_i\{k_i\}$, D is the total degree of the sparse resultant as a polynomial in the input coefficients, and e the basis of natural logarithms.

A better implementation finds RC for one point in a maximal cell, then enumerates all points in this cell in time proportional to their cardinality multiplied by a polynomial in m, n, B [39, thm.16]. The neighbours of these points which lie outside the cell will yield new cells, so as to explore the entire Minkowski sum; detecting new cells does not increase the overall complexity. If $S \leq |\mathcal{E}|$ is the number of maximal cells containing at least one lattice point, Alg. B has complexity $O^*(Sr^2B^2 + |\mathcal{E}|) = O^*(S|\mathcal{E}|^2B^2)$, where typically, $S \ll |\mathcal{E}|$. This may be compared to the complexity of Alg. A at the end of the next section.

3.2 Recursive construction

We recall D'Andrea's recursive construction of a Macaulay-type formula [29]. There are certain free parameters in the algorithm which we specify so as to obtain a version very similar to our approach.

At the input of the 0-step the algorithm may use an additional polytope mQ, for any $m \in \mathbb{R}$, which we omit by setting $m = 0$. We describe the t-th recursive step, for $t = 0, 1, \ldots, n-1$.

Algorithm A. The input are polytopes

$$l_0P^{(t)}, \ldots, l_{t-1}P^{(t)}, k_tP^{(t)}, \ldots, k_nP^{(t)} \subset \mathbb{R}^{n-t},\ l_i \in [0, k_i] \cap \mathbb{Q},$$

the integer lattice $L^{(t)}$ spanned by $\sum_{i=t}^n A_i \cap k_iP^{(t)}$, and perturbation vector $\delta_t \in \mathbb{Q}^{n-t}$. Here, $k_iP^{(t)},\ i \geq t$, is an $(n-t)$-dimensional face of k_iQ, thus $P^{(0)} = Q$. Also, $P^{(t)}$ is a facet of $P^{(t-1)}$, and $l_iP^{(t)},\ i < t$, is homothetic to $k_iP^{(t)}$. These constructions shall be specified at the Recursion Phase. Also, $L^{(0)} = Z$ and $\delta_0 = \delta$.

Construction Phase: Vertex $b_{tj} \in k_t P^{(t)} \cap A_t$ is lifted to 1. We require that $b_{tj} = c_{tjs} - \delta_{tjs}$, where s is determined by the face $k_t P^{(t)}$. All other vertices of all input polytopes are lifted to 0. This is the primary lifting which partitions the Minkowski sum of the input polytopes into a primary cell

$$l_0 P^{(t)} + \cdots + l_{t-1} P^{(t)} + b_{tj} + k_{t+1} P^{(t)} + \cdots + k_n P^{(t)} + \delta_t, \tag{3.1}$$

of dimension $n-t$, and several secondary cells. Each secondary cell is defined by an inner normal $v \in \mathbb{Q}^{n-t}$ to a facet of $k_t P^{(t)}$ not containing b_{tj}.

Polytopes $\sum_{i=0}^{t-1} l_i P^{(t)}, k_{t+1} P^{(t)}, \ldots, k_n P^{(t)}$ are lifted by applying the restriction of β on them. We consider β fixed throughout the algorithm. The upper hull of the Minkowski sum of the lifted polytopes induces a mixed subdivision of $\sum_{i=0}^{t-1} P^{(t)} + k_{t+1} P^{(t)} + \cdots + k_n P^{(t)}$, which is then perturbed by δ_t. The lattice points p of $L^{(t)}$ contained in the perturbed subdivision are assigned RC by Definition 1.1.17. This also assigns RC to points $p + b_{tj}$ contained in the intersection of (3.1) with $L^{(t)}$. Let us take care of the c_{ijs}. If point p lies in

$$(F + F_{t+1} + \cdots + F_n + \delta_t) \cap L^{(t)}, \tag{3.2}$$

where $F_i \subset k_i Q_i,\ i > t,\ F \subset \sum_{i=0}^{t-1} l_i P^{(t)}$, having $\mathrm{RC}(p) = (h, j)$, where $F_h = c_{hjs} = b_{hj} + \delta_{hjs}$, then the corresponding matrix row is filled in by $x^{p - b_{hj}} f_h$.

Face $F \subset \sum_{i=0}^{t-1} P^{(t)}$ in (3.2), can be written as $F = l_0 F_0 + \cdots + l_{t-1} F_{t-1}$, where $F_i \subset P^{(t)}$ for $i < t$. Moreover, every cell in (3.1) is the Minkowski sum of b_{tj} and the cell in (3.2).

Mixed cells of type 0 are defined here as in Section 3.1. A t-mixed cell with respect to Alg. A, for $t > 0$, shall have $n - t$ linear summands from polytopes $k_{t+1} P^{(t)}, \ldots, k_n P^{(t)}$ and a zero-dimensional summand from polytope $\sum_{i=0}^{t-1} l_i P^{(t)}$. This summand can be written as $l_0 p_0 + \cdots + l_{t-1} p_{t-1}$, where $p_i \in P^{(t)}$, for $i = 0, \ldots, t-1$ and $l_i p_i$ stands for a scalar multiple of p_i, seen as a vector. This leads to:

Lemma 3.2.1. *The maximal cells at step t of Alg. A are, for some j and $l_i \in [0, k_i]$, of the form:*

$$l_0 F_0 + \cdots + l_{t-1} F_{t-1} + b_{tj} + k_{t+1} F_{t+1} + \cdots + k_n F_n + \delta_t, \tag{3.3}$$

where F_i is the projection of a face of the upper hull of $P^{(t)}$ lifted by β, and

$$\dim(\langle F_0, \ldots, F_{t-1}, F_{t+1}, F_n \rangle) = n - t.$$

Specifically, the t-mixed cells in Alg. A are:

$$l_0 p_0 + \cdots + l_{t-1} p_{t-1} + b_{tj} + k_{t+1} E_{t+1} + \cdots + k_n E_n + \delta_t, \tag{3.4}$$

where $E_{t+1}, \ldots, E_n$ are projections of edges on the upper hull of $P^{(t)}$ lifted by β, $\dim(\langle E_{t+1}, \ldots, E_n \rangle) = n - t$, and points $p_i \in P^{(t)}$, for $i = 0, \ldots, t-1$.

Throughout the paper we shall use a running example to illustrate the Lemmas and Corollaries. The example shall be detailed in Section 3.4.

Example 3.2.2 (Running example)**.** Let $n = 2$, Q be the pentagon with vertices $\{(1,0), (0,1), (0,2), (1,2), (3,0)\}$, $k_0 = k_2 = 1$, $k_1 = 2$. The input polygons are $Q_i = k_i Q$, $i = 0, 1, 2$ and the input supports are $A_0 = A_2 = \{(1,0), (0,1), (0,2), (1,2), (3,0)\}$, and $A_1 = \{(2,0), (0,2),$

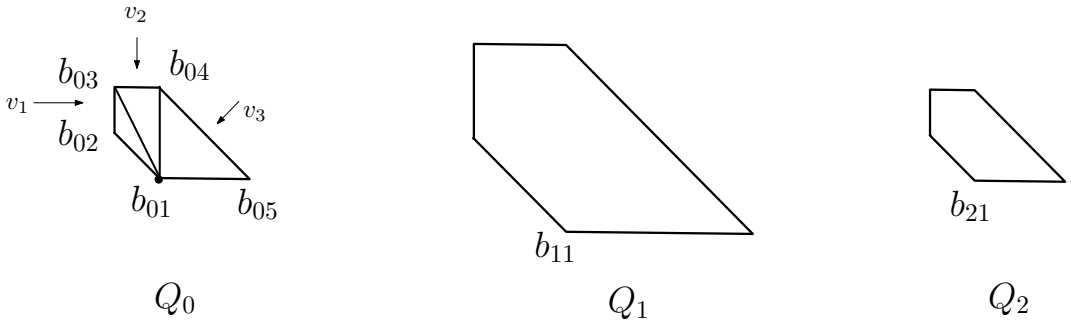

Figure 3.4: Input polygons of Exam. 3.2.2 and their subdivisions induced by the lifting of Def. 3.1.3

$(0,4),(2,4),(6,0)\}$. The lattice generated by $\sum_{i=0}^{2} A_i$ is $\mathbb{Z}^2$. The normals to the facets of Q not containing vertex $b_{01} = (1,0)$ are $v_1 = (-1,0)$, $v_2 = (0,-1)$, $v_3 = (-1,-1)$. Let $\delta = (-1/30, -1/30)$ be the global perturbation vector. See Figure 3.4.

In the 0 step of the recursion, b_{01} is lifted to 1, while all other vertices of all polygons

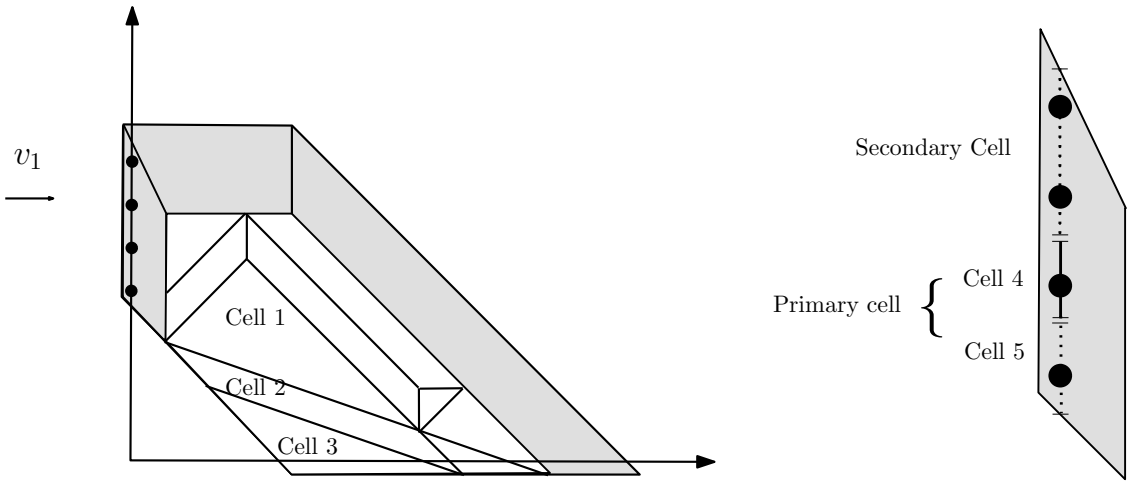

Figure 3.5: Example 3.2.2: 0-step (left) and 1-step of the recursion on secondary cell w.r.t. v_1 (right) of Alg. A

are lifted to 0. Then, the primary cell is subdivided using lifting β. The primary and secondary cells are shown in Figure 3.5, left, in white and grey color respectively (also in Figure 3.8). To illustrate Lemma 3.2.1, consider cells 1,2 and 3 of the primary cell. They can be written as

Cell 1: $b_{01} + \mathrm{CH}(c_{122}, c_{143}, c_{154}) + b_{21}$, non-mixed.

Cell 2: $b_{01} + (c_{122}, c_{154}) + (b_{21}, b_{21})$, 1-mixed.

Cell 3: $b_{01} + \mathrm{CH}(c_{122}, b_{11}, c_{154}) + b_{21}$, non-mixed.

Now, consider the recursion step of Alg. A at the secondary cell of step 0 with respect to vector $(1,0)$ shown in Figure 3.5, right. In this cell the algorithm recurses on a segment containing points $(0,4),(0,5),(0,6),(0,7)$. This segment is partitioned into new primary and secondary cells and the new primary cell is subdivided again using β. The cells are:

Secondary cell: $\frac{29}{30}b_{03} + (b_{12}, b_{13}) + b_{23}$, 2-mixed.

Cell 4: $\frac{29}{30}(b_{02}, b_{03}) + b_{11} + b_{22}$, non-mixed.

Cell 5: $\frac{29}{30}b_{02} + b_{11} + (b_{22}, b_{23})$, 1-mixed.

For details see Example 3.4.1.

Recursion Phase: When $t = n - 1$, the algorithm terminates, since it has reached the Sylvester case. Otherwise, it recurses: let $P^{(t+1)}$ be the facet of $P^{(t)}$ supported by v. The (perturbed) secondary cell corresponding to v is

$$\begin{aligned}\mathcal{F}_v = l_0P^{(t+1)} + \cdots + l_{t-1}P^{(t+1)} + \mathrm{CH}(b_{tj}, k_tP^{(t+1)}) \\ + k_{t+1}P^{(t+1)} + \cdots + k_nP^{(t+1)} + \delta_t.\end{aligned} \tag{3.5}$$

Its associated diameter is

$$d_v = b_{tj} \cdot v - \min_{p \in \mathrm{CH}(b_{tj}, k_tF)} \{p \cdot v\} \in \mathbb{N}^*,$$

where $\cdot$ stands for inner product. We define two sublattices of $L^{(t)}$: $L^{(t)}_+$ is spanned by $\sum_{i=t+1}^{n} A_i \cap k_iP^{(t+1)}$ and $L^{(t)}_v$ is the sublattice orthogonal to v. They have the same dimension, so we define the (finite) index $\mathrm{ind}_v = [L^{(t)}_v : L^{(t)}_+]$, equal to the quotient of the volumes of their base cells. Let q range over the ind_v coset representatives for $L^{(t)}_+$ in $L^{(t)}_v$.

Let $l_t \in [0, k_t]$ take d_v distinct values corresponding to different values of $p \cdot v$ for all $p \in (\mathrm{CH}(b_{tj}, k_tP^{(t+1)}) + \delta_t) \cap L^{(t)}$. Note that $l_tP^{(t+1)}$ is homothetic to $k_tP^{(t+1)}$. Let $\delta'_t \in \mathbb{Q}^{n-t}$ be a translation vector such that $l_tP^{(t+1)} + \delta'_t$ contains at least one point in $(\mathrm{CH}(b_{tj}, k_tP^{(t+1)}) + \delta_t) \cap L^{(t)}$.

In particular, $l_tP^{(t+1)} + \delta'_t$ equals $k_tP^{(t+1)}$ if and only if $l_t = k_t$, and vertex b_{tj} if and only if $l_t = 0$, otherwise it equals $(\mathrm{CH}(b_{tj}, k_tP^{(t+1)}) + \delta_t) \cap H$, where H is a hyperplane parallel to a supporting hyperplane of $k_tP^{(t+1)}$; see [29, Lem.3.3]. By abuse of notation, in the rest of this paper we shall denote H, and the supporting hyperplanes of faces $k_tP^{(t+1)}$ and b_{tj} of the previous convex hull, as $\langle l_tP^{(t+1)} \rangle$.

Points in $(\mathcal{F}_v + \delta_t) \cap L^{(t)}$ are partitioned into d_v subsets (one per value of l_t), called *slices*, of the form

$$l_0P^{(t+1)} + \cdots + l_{t-1}P^{(t+1)} + (l_tP^{(t+1)} + \delta'_t) + k_{t+1}P^{(t+1)} + \cdots + k_nP^{(t+1)} + \delta_t \cap L^{(t)}, \tag{3.6}$$

which can be rearranged as

$$l_0P^{(t+1)} + \cdots + l_tP^{(t+1)} + k_{t+1}P^{(t+1)} + \cdots + k_nP^{(t+1)} + \delta_\lambda \cap L^{(t)}, \tag{3.7}$$

where $\delta_\lambda = \delta_t + \delta'_t$. Moreover, δ_λ can be decomposed as $\delta^v_\lambda + \delta_{\lambda v}$, where $\delta^v_\lambda \in \mathbb{Q}v$ and $\delta_{\lambda v} \in L^{(t)}_+ \otimes \mathbb{Q}$. Now, every point in (3.7) corresponds to a point in

$$l_0P^{(t+1)} + \cdots + l_tP^{(t+1)} + k_{t+1}P^{(t+1)} + \cdots + k_nP^{(t+1)} + \delta_{\lambda v} \cap (q + L^{(t)}_+),$$

for some coset representative q. Set $\delta_{t+1} := \delta_{\lambda v} - q$, $L^{(t+1)} := L_+^{(t)}$, and observe that point p belongs to (3.7) if and only if point

$$p' := p - \delta_\lambda^v - q \tag{3.8}$$

belongs to

$$l_0 P^{(t+1)} + \cdots + l_t P^{(t+1)} + k_{t+1} P^{(t+1)} + \cdots + k_n P^{(t+1)} + \delta_{t+1} \cap L^{(t+1)}. \tag{3.9}$$

We call this set a *piece*; δ_{t+1} carries the information to define the piece from the input polytopes and $L^{(t+1)}$. The algorithm recurses on each of the ind_v such pieces. The set

$$l_0 P^{(t+1)}, \ldots, l_t P^{(t+1)}, k_{t+1} P^{(t+1)}, \ldots, k_n P^{(t+1)},\ \delta_{t+1}$$

over $L^{(t+1)}$ is exactly like the original input, only one dimension lower. This completes the algorithm.

Remark 3.2.3. Since every point p' in a piece corresponds bijectively to a point p in a slice via the monomial bijection (3.8), we shall often consider a piece as a subset of a slice and omit the translation.

At the end of the recursion, RC is defined on $\mathcal{E}$. Alg. A defines a partition of $\mathcal{E}$ in the form of a collection of mixed subdivisions of primary cells (of decreasing dimension). The edges of the cells of this partition, coming from polytope Q_i, are defined by any point in A_i or among the c_{ijs}, for all valid j, s, and may be multiplied by a rational number in $(0, k_i]$.

D'Andrea's algorithm uses at every construction step the matrix construction algorithm of [10], so its complexity is dominated by $O(|\mathcal{E}|n)$ linear programs, since every $p \in \mathcal{E}$ may require $O(n)$ of them for its image under RC to be determined. Each linear program has bit complexity $O(n^{7.5} m^2 B^2)$, by Karmarkar's algorithm, where m is the maximum number of vertices of the Q_i, and B is the bitsize of the input coordinates. This process essentially decides in which slice of which secondary cell lies p. Although this subdivision contains much more cells than Alg. B, the asymptotic analysis indicates that the latter is competitive for large n; see the end of section 3.1 for comparing with Alg. A.

3.3 Equivalence of constructions

Intuitively, the single-lifting algorithm (Alg. B) has an overall effect very similar to that of Alg. A, since they both use β. The former partitions $\mathcal{E}$ into sets of points in n-dimensional cells and assigns RC, whereas Alg. A partitions $\mathcal{E}$ into subsets which, at step t, lie on the intersection of a $(n-t)$-dimensional hyperplane with an n-dimensional cell of β. Note that the intersection itself, as a subset of $\mathbb{R}^{n-t}$, does not coincide with the cell of Alg. A. However, their set difference is of infinitesimal volume and thus contains no lattice points. Although both algorithms use β to subdivide their input polytopes, they do so in a distinct fashion; Alg. B applies β to every Q_i, whereas Alg. A does so recursively to a different set of polytopes at every step.

In the rest of the chapter, for simplicity, we shall omit the translation vectors δ_t. Moreover, unless otherwise stated, we shall treat every slice and piece as a polytope and not

as the set of points in the intersection of this polytope with an appropriate lattice. In particular, we shall be interested only on the form of a slice or piece as a Minkowski sum of polytopes. The existence of a translation vector, for this polytope to contain integer points in the considered lattice, shall be implied.

We now establish the correspondence between the two algorithms for $t = 0$, then generalize to $t > 0$. We introduce the notation $pr.cell_i^{(X)}, sec.cell_i^{(X)}$, where i indicates the recursion step of Alg. A and $X \in \{A, B\}$ indicates the algorithm under consideration. At step 0 of Alg. A, b_{01} is lifted to 1, while every other vertex of all input polytopes to 0; this creates a primary cell

$$pr.cell_0^{(A)} := b_{01} + k_1 Q + \cdots + k_n Q,$$

and several secondary cells of the form

$$sec.cell_0^{(A)} := \mathrm{CH}(b_{01}, k_0 P^{(1)}) + k_1 P^{(1)} + \cdots + k_n P^{(1)},$$

each corresponding to a facet $P^{(1)}$ of Q not containing b_{01}. In Alg. B, c_{011} plays the role of b_{01} and this leads to a group of cells covering the corresponding primary cell

$$pr.cell_0^{(B)} := c_{011} + k_1 Q + \cdots + k_n Q,$$

and several groups of cells, each group covering

$$sec.cell_0^{(B)} := \mathrm{CH}(c_{011}, k_0 P^{(1)}) + k_1 P^{(1)} + \cdots + k_n P^{(1)},$$

which is a typical n-dimensional secondary cell with respect to Alg. B. Not all cells in $sec.cell_0^{(B)}$ may have $k_i P^{(1)}$ as a summand. Those who do not, have a summand where some or all of the vertices of $k_i P^{(1)}$ are replaced by the corresponding additional points c_{ijs} from Definition 3.1.2.

Remark 3.3.1. All cells within $pr.cell_0^{(A)}$ and $pr.cell_0^{(B)}$ differ only at their first summand; the former are of the form $b_{01} + F_1 + \cdots + F_n$, whereas the latter are $c_{011} + F_1 + \cdots + F_n$, where F_i is a face of Q_i, since β is used by both algorithms to subdivide $Q_1 + \cdots + Q_n$, and $c_{011} = b_{01} + \delta_{011}$.

Lemma 3.3.2. *$pr.cell_0^{(A)} \cap \mathcal{E} = pr.cell_0^{(B)} \cap \mathcal{E}$, and points in this set are assigned the same RC under both algorithms.*

Proof. Recall that $\delta_0 = \delta$ and consider the subdivision of $\sum_{i=0}^{n} Q_i$ induced by β and compare $pr.cell_0^{(A)} + \delta$ and $c_{011} + Q_1 + \cdots + Q_n + \delta = b_{01} + \delta_{011} + Q_1 + \cdots + Q_n + \delta$. These polytopes differ by δ_{011}, which is very small. Moreover, by the choice of δ, the boundary of $pr.cell_0^{(A)} + \delta$ has no points in Z. Since, by Definition 3.1.1, $\|\delta\| \gg \|\delta_{011}\|$, the two polytopes contain the same Z-points. This settles the first claim. The second claim follows from Remark 3.3.1 and the fact that the two subdivisions may only differ in cells having vertex b_{01} instead of c_{011}. Since $c_{011} - b_{01} = \delta_{011}$ is very small compared to Z, even these cells contain the same Z-points. □

Example 3.3.3 (Running example (cont'd))**.** Let us return to our running example. It holds that $pr.cell_0^{(A)} \cap \mathcal{E} = pr.cell_0^{(B)} \cap \mathcal{E}$. Now, consider points $(8, 1), (7, 2)$ and $(4, 4)$, see Figures 3.9 and 3.10. They belong to cells of $pr.cell_0^{(A)}$ and $pr.cell_0^{(B)}$ as in the following table:

point	cell in $pr.cell_0^{(A)}$	cell in $pr.cell_0^{(B)}$	type	RC
$(8,1)$	$b_{01} + c_{154} + \mathrm{CH}(b_{22}, b_{24}, b_{25})$	$c_{011} + c_{154} + \mathrm{CH}(b_{22}, b_{24}, b_{25})$	non-mixed	$(1,5)$
$(7,2)$	$b_{01} + (c_{143}, c_{154}) + (b_{23}, b_{24})$	$c_{011} + (c_{143}, c_{154}) + (b_{23}, b_{24})$	0-mixed	$(0,1)$
$(4,4)$	$b_{01} + (c_{143}, c_{154}) + (b_{22}, b_{23})$	$c_{011} + (c_{143}, c_{154}) + (b_{22}, b_{23})$	0-mixed	$(0,1)$

Note that, for simplicity, we have omitted the global perturbation vector δ.

Each $sec.cell_0^{(A)}$ is divided by Alg. A into slices

$$l_0P^{(1)} + k_1P^{(1)} + \cdots + k_nP^{(1)},$$

one for each value of $l_0 \in [0, k_0]$. Each slice is partitioned into pieces on which Alg. A recurses producing $(n-1)$-dimensional primary cell

$$pr.cell_1^{(A)} := l_0P^{(1)} + b_{1j} + k_2P^{(1)} + \cdots + k_nP^{(1)}, \tag{3.10}$$

and secondary cells

$$sec.cell_1^{(A)} := l_0P^{(2)} + CH(b_{1j}, k_1P^{(2)}) + k_2P^{(2)} + \cdots + k_nP^{(2)}. \tag{3.11}$$

Every piece of a given slice lies on lattice $L^{(1)}$ and can be thought of as the intersection of a translation of that slice, regarded as a polytope, with $L^{(1)}$. Recall that, by Remark 3.2.3, we shall consider a piece as subset of a slice.

Similarly to Alg. A, we can partition the corresponding $sec.cell_0^{(B)}$ into slices:

$$l_0'P^{(1)} + k_1P^{(1)} + \cdots + k_nP^{(1)},$$

by intersecting $\mathrm{CH}(c_{011}, k_0P^{(1)})$ with a hyperplane parallel to (a supporting hyperplane of) $k_0P^{(1)}$. Recall that we denote this hyperplane as $\langle l_0'P^{(1)}\rangle$.

Remark 3.3.4. Observe that each slice of $sec.cell_0^{(B)}$ (resp. $sec.cell_0^{(A)}$) parameterized by l_0' (resp. l_0), is homothetic to a facet of this secondary cell, supported by $\langle k_0'P^{(1)}\rangle$ (resp. $\langle k_0P^{(1)}\rangle$). Moreover, this homothecy is defined by a homothecy only on the first summand $k_0P^{(1)}$ of this facet.

Example 3.3.5 (Running example (cont'd))**.** To illustrate Remark 3.3.4, consider in our running example the secondary cell with respect to Alg. A

$$\mathcal{F}_{v_3} = \mathrm{CH}(b_{01}, k_0F_{v_3}) + k_1F_{v_3} + k_2F_{v_3} + \delta,$$

defined by the facet $F_{v_3} = ((3,0),(1,2))$ of Q supported by $v_3 = (-1,-1)$, and its slice

$$(l_0F_{v_3} + \delta') + k_1F_{v_3} + k_2F_{v_3} + \delta, \tag{3.12}$$

where $l_0 = \frac{32}{60}$ and $\delta' = (\frac{7}{15}, 0)$. This slice contains the integer points $(11,0), (10,1), (9,2), (8,3), (7,4), (6,5), (5,6), (4,7)$ and is the dashed segment in Figure 3.6. It is homothetic to the facet

$$k_0F_{v_3} + k_1F_{v_3} + k_2F_{v_3} + \delta \tag{3.13}$$

of $\mathcal{F}_{v_3}$ and the homothecy is defined by the homothecy $l_0F_{v_3}+\delta'$ of the 0-summand $k_0F_{v_3}$ of the facet, see Figure 3.6. The second slice of $\mathcal{F}_{v_3}$ is

$$\left(\frac{1}{30}F_{v_3}+(\frac{29}{30},0)\right)+k_1F_{v_3}+k_2F_{v_3}+\delta \tag{3.14}$$

and contains integer points $(10,0),(9,1),(8,2),(7,3),(6,4),(5,5),(4,6)$. It is homothetic to the facet (3.13) of $\mathcal{F}_{v_3}$ and the homothecy is defined by the homothecy $\frac{1}{30}F_{v_3}+(\frac{29}{30},0)$ of the 0-summand $k_0F_{v_3}$ of the facet, see Figure 3.6 (dotted segment).

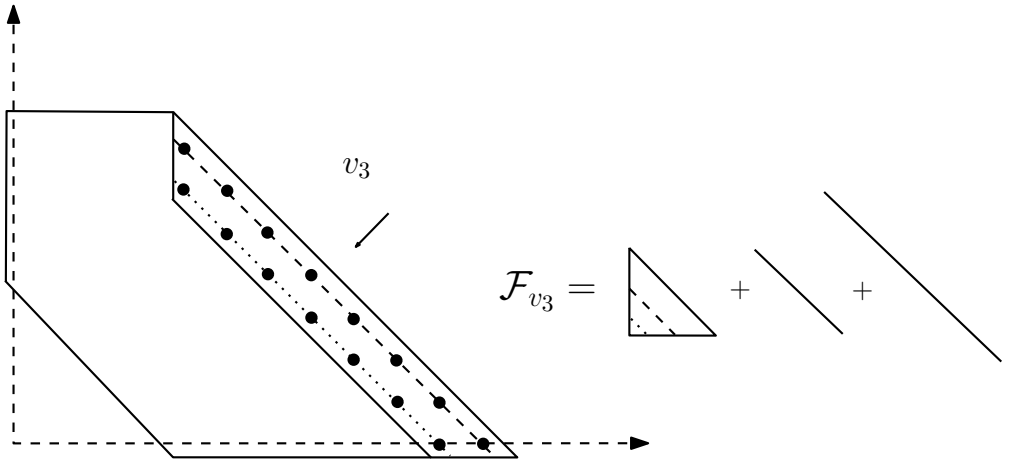

Figure 3.6: Example 3.3.5: The secondary cell w.r.t. $(-1,-1)$ of the 0-step of Alg. A and its two slices

Hyperplanes $\langle l_0'P^{(1)}\rangle$ and $\langle l_0P^{(1)}\rangle$ are identical; they differ only on the homothecy on $k_0P^{(1)}$ expressed by l_0' and l_0 respectively. Obviously, $l_0'\approx l_0$ because $c_{011}\approx b_{01}$. Note that we omit the translation vector so that the slice lies in $sec.cell_0^{(B)}$. Thus, corresponding slices contain the same points in the lattice $L^{(0)}=Z$. This, moreover, leads to the following extension of Lemma 3.3.2.

Lemma 3.3.6. *Every maximal cell of the subdivision induced by β on $pr.cell_1^{(A)}$ corresponds to the intersection of a unique maximal cell of the same type in $sec.cell_0^{(B)}$, with a slice defined by hyperplane $\langle l_0'P^{(1)}\rangle$, for some l_0'. The cells contain the same points in $L^{(1)}$, with the same image under RC.*

Proof. Any maximal cell in $pr.cell_1^{(A)}$ has the form $l_0F_0+b_{1j}+k_2F_2+\cdots+k_nF_n$, where faces $F_i\subset P^{(1)}, i=0,2,\ldots,n$, have dimensions adding up to $n-1$. Recall $pr.cell_1^{(A)}$ lies on a slice of $sec.cell_0^{(A)}$ parameterized by the value of l_0 hence, when β is employed, it gives rise to the same subdivision in every such primary cell. By construction, subspace $\langle b_{01},F_0\rangle$ is orthogonal and complementary to $\langle P^{(1)}\rangle$.

In $k_1P^{(1)}$, point c_{1js} is lifted sufficiently higher than any other, so there exist maximal cells in $sec.cell_0^{(B)}$ that has it as summand. The other summands are induced by β on $\mathrm{CH}(c_{011},k_0P^{(1)})$, $k_2P^{(1)},\ldots,k_nP^{(1)}$. These n-dimensional cells of Alg. B correspond, when intersected with the slice parameterized by $\langle l_0'P^{(1)}\rangle$, to $(n-1)$-dimensional cells in $pr.cell_1^{(A)}$. It is straightforward to show that, for $l_0'\in[0,k_0]$ and any β-induced cell in this Minkowski

sum, its intersection with the slice defined by $\langle l_0' P^{(1)} \rangle$ is a β-induced cell in $l_0' P^{(1)} + k_2 P^{(1)} + \cdots + k_n P^{(1)}$

There exists $l_0' \approx l_0$ that establishes the Lemma, because β is applied to $(n-1)$-dimensional Minkowski sums which are almost identical, and the effect of b_{1j} and c_{1js} is the same in what concerns the lattice points in corresponding cells, following the proof of Lemma 3.3.2. □

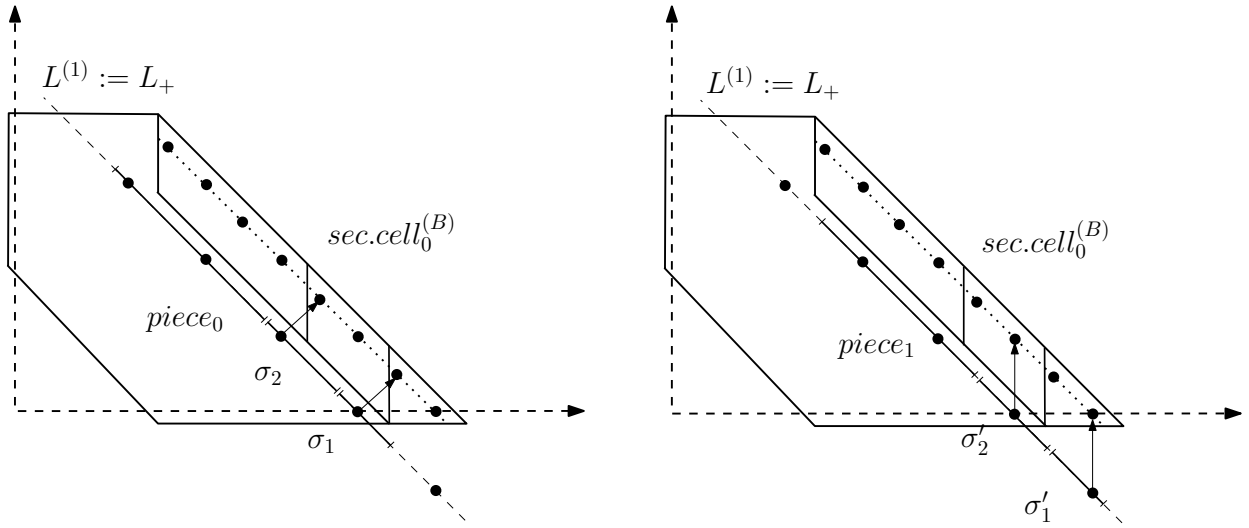

Figure 3.7: Example 3.3.7: The two pieces of the secondary cell w.r.t. $(-1,-1)$ of Alg. A and the correspondence between their cells and the cells of the similar secondary cell w.r.t. Alg. B

Example 3.3.7 (Running example (cont'd))**.** We shall return to our running example to illustrate Lemma 3.3.6. Consider the slice

$$(l_0 F_{v_3} + \delta') + k_1 F_{v_3} + k_2 F_{v_3} + \delta \tag{3.15}$$

of the secondary cell with respect to Alg. A

$$sec.cell_0^{(A)} = \mathrm{CH}(b_{01}, k_0 F_{v_3}) + k_1 F_{v_3} + k_2 F_{v_3} + \delta,$$

where $l_0 = \frac{32}{60},\ \delta' = (\frac{7}{15}, 0),\ \delta = (-\frac{1}{30}, -\frac{1}{30})$, see also equation (3.27). This slice is obtained by intersecting $\mathrm{CH}(b_{01}, b_{04}, b_{05})$ with the hyperplane $\langle l_0 F_{v_3} \rangle := \langle \frac{32}{60} F_{v_3} + (\frac{7}{15}, 0) \rangle$, and contains integer points $(11,0), (10,1), (9,2), (8,3), (7,4), (6,5), (5,6), (4,7)$ in L. The corresponding slice of $sec.cell_0^{(B)}$ is obtained by intersecting $\mathrm{CH}(c_{011},\ b_{04}, b_{05})$ with the hyperplane $\langle l_0' F_{v_3} \rangle := \langle \frac{639}{1199} F_{v_3} + (\frac{1274}{2725}, \frac{28}{89925}) \rangle$, see Figure 3.6 (dotted segment). It contains the same points in L.

Slice (3.15) of $sec.cell_0^{(A)}$ contains two pieces in $L^{(1)} := L_+ = \langle (9,0), (7,2) \rangle \cong 2\mathbb{Z}$:

$$piece_0 := \frac{32}{60} F_{v_3} + k_1 F_{v_3} + k_2 F_{v_3} + (-\frac{17}{30}, -\frac{31}{30}), \tag{3.16}$$

$$piece_1 := \frac{32}{60} F_{v_3} + k_1 F_{v_3} + k_2 F_{v_3} + (\frac{13}{30}, -\frac{61}{30}). \tag{3.17}$$

Piece (3.16) is partitioned into a primary cell $\frac{32}{60} F_{v_3} + b_{15} + k_2 F_{v_3} + (-\frac{17}{30}, -\frac{31}{30})$ and a secondary cell $\frac{32}{60} b_{04} + k_1 F_{v_3} + b_{24} + (-\frac{17}{30}, -\frac{31}{30})$. Then, lifting β induces a mixed subdivision

on the primary cell consisting of the cells

$$\sigma_1 = \frac{32}{60}F_{v_3} + b_{15} + b_{25} + (-\frac{17}{30}, -\frac{31}{30}) \text{ and } \sigma_2 = \frac{32}{60}b_{04} + b_{15} + k_2F_{v_3} + (-\frac{17}{30}, -\frac{31}{30}).$$

Cell σ_1 is non-mixed and contains point $(9,0) \in L_+$, which translates to point $(10,1) \in L$. This cell corresponds to the intersection of the slice of $sec.cell_0^{(B)}$, defined by hyperplane $\langle l_0'F_{v_3}\rangle$, with its non-mixed cell $\text{CH}(c_{011}, b_{04}, b_{05})+c_{15}+b_{25}+\delta$. Cell σ_2 is 1-mixed and contains the point $(7,2) \in L_+$ which translates to the point $(8,3) \in L$. This cell corresponds to the intersection of the slice of $sec.cell_0^{(B)}$, defined by hyperplane $\langle l_0'F_{v_3}\rangle$, with the 1-mixed cell with respect to Alg. B $(c_{011}, b_{04}) + c_{154} + (b_{24} + b_{25}) + \delta$, see Figure 3.7,(left).

The second piece (3.17) is partitioned into a primary cell $\frac{32}{60}F_{v_3} + b_{15} + k_2F_{v_3} + (\frac{13}{60}, -\frac{61}{30})$ and a secondary cell $\frac{32}{60}b_{04} + k_1F_{v_3} + b_{24} + (\frac{13}{60}, -\frac{61}{30})$. Lifting β induces a mixed subdivision on the primary cell consisting of the cells

$$\sigma_1' = \frac{32}{60}F_{v_3} + b_{15} + b_{25} + (\frac{13}{60}, -\frac{61}{30}) \text{ and } \sigma_2' = \frac{32}{60}b_{04} + b_{15} + k_2F_{v_3} + (\frac{13}{60}, -\frac{61}{30}).$$

The former is non-mixed and contains point $(11,-2) \in L_+$ corresponding to $(11,0) \in L$. It corresponds to the intersection of the slice cell of $sec.cell_0^{(B)}$, defined by hyperplane $\langle l_0'F_{v_3}\rangle$, with its non-mixed cell $\text{CH}(c_{011}, b_{04}, b_{05}) + c_{154} + b_{25} + \delta$. Cell σ_2' is 1-mixed and contains the integer point $(9,0) \in L_+$ corresponding to point $(9,2) \in L$. It corresponds to the intersection of the slice defined by hyperplane $\langle l_0'F_{v_3}\rangle$ with the 1-mixed cell of $sec.cell_0^{(B)}$ $(c_{011}, b_{04}) + c_{154} + (b_{24} + b_{25}) + \delta$, see Figure 3.7, (right).

In each $sec.cell_0^{(B)}$ we distinguish 2 types of cells: cells in

$$pr.cell_1^{(B)} := \text{CH}(c_{011}, k_0P^{(1)}) + c_{1js} + k_2P^{(1)} + \cdots + k_nP^{(1)}, \tag{3.18}$$

which, by Lemma 3.3.6, contains exactly the integer points in all primary cells of Alg. A of the form (3.10) (for each slice/coset), and for each facet $P^{(2)}$ of $P^{(1)}$, cells in

$$sec.cell_1^{(B)} := \text{CH}(c_{011}, k_0P^{(2)}) + \text{CH}(c_{1js}, k_1P^{(2)}) + k_2P^{(2)} + \cdots + k_nP^{(2)}. \tag{3.19}$$

Note that both $pr.cell_1^{(B)}$ and $sec.cell_1^{(B)}$ are n-dimensional, whereas $pr.cell_1^{(A)}$ and $sec.cell_1^{(A)}$ are $(n-1)$-dimensional.

Remark 3.3.8. Every maximal cell in $sec.cell_1^{(B)}$ must have summands $F_0 = \text{CH}(c_{011}, G_0)$, $F_1 = \text{CH}(c_{1js}, G_1)$, for some $G_0 \subset k_0P^{(2)}$ and $G_1 \subset k_1P^{(2)}$.

A similar argument as in Lemma 3.3.6, implies that (3.19) contains exactly the integer points in the union of all secondary cells (3.11) defined over the various values of $l_0 \in [0, k_0]$, for a given j. The recursion steps of Alg. A, for $t \geq 2$ are defined over a chain of facets $P^{(2)} \supset P^{(3)} \supset \cdots \supset P^{(n-1)}$. Hence, every $pr.cell_t^{(A)}$, for $t > 1$, contains integer points in $sec.cell_1^{(B)} \cap Z$. Therefore, we generalize the correspondence between the two algorithms by focusing on $sec.cell_1^{(B)}$.

Lemma 3.3.9. (Main) *Every maximal cell of the subdivision induced by β on $pr.cell_t^{(A)}$, for $t \geq 2$, corresponds to the intersection of hyperplane $\langle l_{t-1}'P^{(t)}\rangle$, for some $l_{t-1}' \approx l_{t-1} \in [0, k_{t-1}] \cap \mathbb{Q}$, with a unique maximal cell in $sec.cell_1^{(B)}$, of the same type. The cells contain the same points in lattice $L^{(t)}$ with the same image under RC.*

Proof. Primary cells of step t lie on $(n-t)$-dimensional slices of the $(n-t+1)$-dimensional $sec.cell_{t-1}^{(A)}$, parameterized by the value of $l_{t-1} \in [0, k_{t-1}]$:

$$l_0P^{(t)} + \cdots + l_{t-1}P^{(t)} + k_tP^{(t)} + \cdots + k_nP^{(t)}. \tag{3.20}$$

Similarly to Remark 3.3.4, let $l_0, \ldots, l_{t-1},\ l_i \in [0, k_i] \cap \mathbb{Q}$, define the homothecies on the first t summands of (3.20) and the corresponding hyperplanes $\langle l_0P^{(t)}\rangle, \ldots, \langle l_{t-1}P^{(t)}\rangle$. Note, that $pr.cell_t^{(A)}$ is a subset of (3.20) and is subdivided by β into maximal cells of the form (3.3).

Intersecting $sec.cell_1^{(B)}$ with the above hyperplanes, yields a $(n-t)$-dimensional subset:

$$l'_0P^{(t)} + \cdots + l'_{t-1}P^{(t)} + k_tP^{(t)} + \cdots + k_nP^{(t)}. \tag{3.21}$$

This subset can also be obtained by directly intersecting $sec.cell_1^{(B)}$ with $\langle l_{t-1}P^{(t)}\rangle$. Now, $l'_i \approx l_i$, for $i = 0, 1, \ldots, t-1$ because $c_{ijs} \approx b_{ij}$. For $i = 0, \ldots, t-1$, each l'_i defines a hyperplane $\langle l'_iP^{(t)}\rangle$ identical to $\langle l_iP^{(t)}\rangle$, except on the homothecy on the i-th summand. Hence, (3.21) is very similar to (3.20) in the sense that they contain the same integer points in $L^{(t)}$ and their volumes differ infinitesimally.

By Definition 3.1.2 there exist n-dimensional cells in $sec.cell_1^{(B)}$ which have c_{tjs} as a summand. The intersection of each of these cells with (3.21) shall also have c_{tjs} as a summand, because this is the only point lifted highest in $P^{(t)}$. These cells correspond to the primary cell with respect to Alg. A of the slice (3.20). Moreover, this intersection is a β-induced cell in (3.21):

$$l'_0F_0 + \cdots + l'_{t-1}F_{t-1} + c_{tjs} + k_{t+1}F_{t+1} + \cdots + k_nF_n, \tag{3.22}$$

which contains the same integer points as (3.3). Since β is applied on $(n-t)$-dimensional polytopes which are almost identical, both (3.3) and (3.22) are of the same type. □

Corollary 3.3.10. *Using the notation of Lemma 3.2.1, in particular for t-mixed cells of Alg. A in the form of (3.4), a t-mixed cell of Alg. B is of the form:*

$$k_0E_0 + \cdots + k_{t-1}E_{t-1} + c_{tjs} + k_{t+1}E_{t+1} + \cdots + k_nE_n + \delta_t\ \cap L,$$

where E_i is the projection of an edge of Q^β,

(a) $\langle E_0, \ldots, E_{t-1}\rangle$ is a t-dimensional space complementary to $\langle P^{(t)}\rangle$, and for $i < t$, $k_iE_i = (c_{ijs}, k_ip_i)$, where $p_i \in P^{(i)}$ in Lemma 3.2.1, and

(b) edges $E_{t+1}, \ldots, E_n$ are the same as in (3.4) at Lemma 3.2.1.

Proof. For $t = 0$, the Corollary follows from Remark 3.3.1.

All 1-mixed cells with respect to Alg. B lie in (3.18), since every maximal cell in it has c_{1js} as a summand. By Lemma 3.3.6, edges $k_2E_2, \ldots, k_nE_n$ span the $(n-1)$-dimensional space $\langle P^{(1)}\rangle$. Hence, edge k_0E_0 has to be of the form (c_{011}, k_0p_0), where $p_0 \in P^{(1)}$, by Lemma 3.3.6, is as in Lemma 3.2.1,(3.4).

Similarly, Lemma 3.3.9 implies that for $t > 1$, the last $(n-t)$ edges of any t-mixed cell with respect to Alg. B span the $(n-t)$-dimensional space $\langle P^{(t)}\rangle$, because β induces the same subdivision on the last $n-t$ summands of (3.20) and (3.21). For the cell to be maximal, $\langle k_0E_0, \ldots, k_{t-1}E_{t-1}\rangle$ must be a t-dimensional space complementary to $\langle P^{(t)}\rangle$. By construction (see proof of Lemma 3.3.9), each k_iE_i, for $i < t$, is an edge in $\mathrm{CH}(c_{ijs}, k_iP^{(t)})$ of the form (c_{ijs}, k_ip_i), where $p_i \in P^{(t)}$ is as in Lemma 3.2.1,(3.4). □

We now consider non-mixed cells, by extending Corollary 3.3.10:

Corollary 3.3.11. *Consider any non-mixed cell of Alg. A, which has the form of (3.3) in Lemma 3.2.1. It corresponds to cell:*

$$CH(c_{011}, k_0F_0) + \cdots + CH(c_{(t-1)js}, k_{t-1}F_{t-1}) + c_{tjs} + k_{t+1}F_{t+1} + \cdots + k_nF_n,$$

which is a non-mixed cell defined by β, where

(a) the $F_0, \ldots, F_{t-1}$ are projections of faces in Q^β, for $i < t$, and

$$\langle CH(c_{011}, k_0F_0), \ldots, CH(c_{(t-1)js}, k_{t-1}F_{t-1})\rangle$$

is a t-dimensional space complementary to $\langle F_{t+1}, \ldots, F_n\rangle$,

(b) $F_0, \ldots, F_{t-1}, F_{t+1}, \ldots, F_n$ are the same in both cells.

For an illustration of Corollaries 3.3.10, 3.3.11 see Table 3.1 in our running Example 3.4.1. We have shown that each row of the constructed matrices, indexed by points of $\mathcal{E}$ lying in a mixed or non-mixed cell, is identical for both algorithms, where $\mathcal{E}$ is the same pointset for both algorithms.

Theorem 3.3.12. *The Macaulay-type formula for the sparse resultant of generalized unmixed systems constructed by Alg. B and that constructed by Alg. A, implementing D'Andrea's approach [29], are identical.*

Proof. We have shown that pointset $\mathcal{E}$ indexing the matrices is the same for both algorithms. Moreover, the previous lemmas and corollaries imply that each row of the constructed matrices, indexed by points of $\mathcal{E}$ lying in a mixed or non-mixed cell, is identical for both algorithms. □

As a consequence of Theorem 3.3.12 and [29, Thm. 3.8], follows Theorem 3.0.6.

3.4 A bivariate example

This section details the running example.

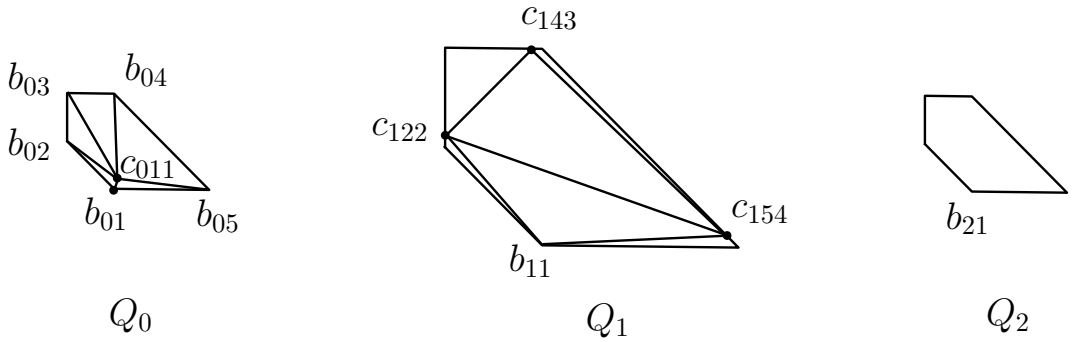

Figure 3.8: Input polygons of Exam. 3.4.1 and their subdivisions induced by the lifting of Def. 3.1.3

Example 3.4.1. Let $n = 2$, Q be the pentagon with vertices $\{(1,0),(0,1),(0,2),(1,2),(3,0)\}$, $k_0 = k_2 = 1$, $k_1 = 2$. The input polygons are $Q_i = k_i Q$, $i = 0,1,2$ and the input supports are $A_0 = A_2 = \{(1,0),(0,1),(0,2),(1,2),(3,0)\}$, and $A_1 = \{(2,0),(0,2),(0,4),(2,4),(6,0)\}$. The lattice generated by $\sum_{i=0}^{2} A_i$ is $\mathbb{Z}^2$. The normals to the facets of Q not containing vertex $(1,0)$ are $v_1 = (-1,0)$, $v_2 = (0,-1)$, $v_3 = (-1,-1)$. Let $\delta = (-1/30, -1/30)$ be the global perturbation vector. See Figure 3.4.

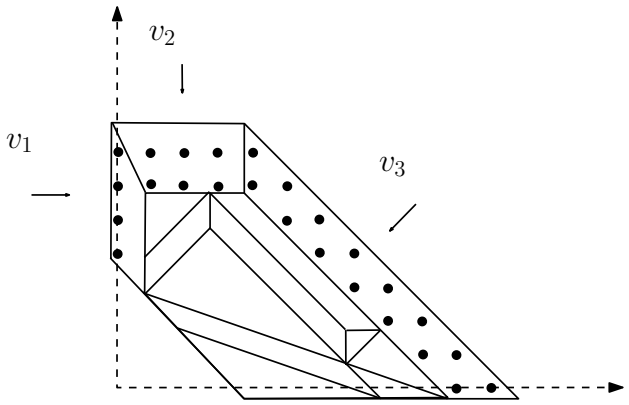

Figure 3.9: Exam. 3.4.1: 0-step recursion of Alg. A

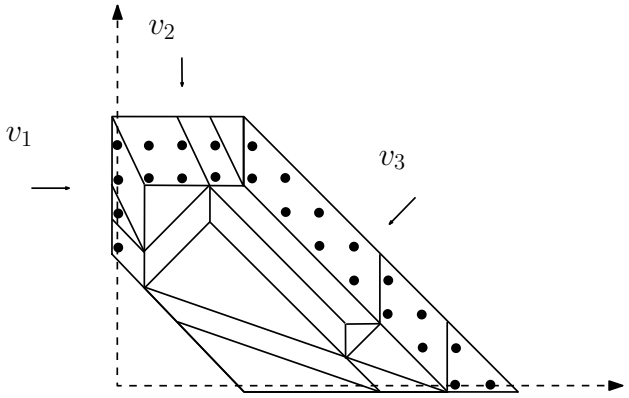

Figure 3.10: Exam. 3.4.1: The mixed subdivision induced by Alg. B

Alg. B: We fix vertices of the input polygons in order to define the additional points required by Definition 3.1.3. Let $b_{01} := (1,0) \in Q_0$, $b_{12} := (0,2)$, $b_{14} := (2,4)$, $b_{15} := (6,0) \in Q_1$, and perturbation vectors $\delta_{011} = (\frac{1}{1000}, \frac{1}{1500})$, $\delta_{122} = (0, \frac{1}{2000})$, $\delta_{143} = (-\frac{1}{3000}, 0)$, $\delta_{154} = (-\frac{1}{2000}, \frac{1}{2000})$, see Figure 3.8. In the subdivision of $\sum_{i=0}^{2} Q_i$, consider the integer points and their cells (Figure 3.10):

point	cell in secondary cell w.r.t. v_2 under Alg. B	type
$(1,7),(2,7)$	$(c_{011},(0,2)) + ((0,4),c_{143}) + (0,2) + \delta$	2-mixed
$(3,7)$	$(c_{011},(0,2)) + c_{143} + ((0,2),(1,2)) + \delta$	1-mixed

where summands come from Q_0, Q_1, Q_2 respectively. These cells together with cell

$$\sigma = \mathrm{CH}(c_{011},(0,2),(1,2)) + c_{143} + (1,2) + \delta,$$

and some infinitesimal cells which do not contain any integer points, correspond to the secondary cell with respect to v_2 of Alg. A, which contains the same integer points. Points $(1,7),(2,7),(3,7)$ correspond (via an appropriate translation) to points of a piece of the secondary cell on which Alg. A recurses. Cell σ does not contain any integer points because of the choice of δ_{ijs}, δ.

Now, consider the points corresponding to a piece of the secondary cell with respect to v_3, of Alg. A, and their cells in the subdivision induced by β under Alg. B:

point	cell in secondary cell w.r.t. v_3 under Alg. B	type
$(4,7),(5,6)$, $(6,5),(7,4)$	$(c_{011},(1,2)) + (c_{154},c_{143}) + (1,2) + \delta$	2-mixed
$(8,3),(9,2)$	$(c_{011},(1,2)) + c_{154} + ((3,0),(1,2)) + \delta$	1-mixed
$(10,1),(11,0)$	$\mathrm{CH}(c_{011},(3,0),(1,2)) + c_{154} + (3,0) + \delta$	non-mixed

Consider the piece of the secondary cell with respect to v_1, of Alg. A. Points in it lie in the following cells of Alg. B:

point	cell in secondary cell w.r.t. v_1 under Alg. B	type
$(0,4)$	$(c_{011},(0,1))+c_{122}+((0,1),(0,2))+\delta$	1-mixed
$(0,5)$	$\mathrm{CH}(c_{011},(0,1),(0,2))+c_{122}+(0,2)+\delta$	non-mixed
$(0,6),(0,7)$	$(c_{011},(0,3))+(c_{122},(0,4))+(0,2)+\delta$	2-mixed

Alg. A: b_{01} is lifted to 1, all other vertices of all polygons are lifted to 0. This partitions $Q_0+Q_1+Q_2$ into a primary cell $b_{01}+Q_1+Q_2$ and 3 secondary cells corresponding to v_1, v_2, v_3, normals to the facets of Q_0 not containing b_{01}. The Q_1, Q_2 are lifted using β, which subdivides the primary cell (Figure 3.9). This subdivision "coincides" with the restriction in $c_{01}+Q_1+Q_2$ of the subdivision by β, except that the latter uses c_{011} whereas the former uses b_{01}, i.e. the integer points in both subdivisions are the same and are assigned the same RC.

- We study the Recursion Phase on secondary cell:

$$\mathcal{F}_{v_1}=\mathrm{CH}(b_{01},k_0F_{v_1})+k_1F_{v_1}+k_2F_{v_1},$$

defined by facet $F_{v_1}=((0,1),(0,2))\subset Q$ supported by v_1, see Figure 3.11. Now,

$$A_{1v_1}=\{(0,2),(0,4)\},\ A_{2v_1}=\{(0,1),(0,2)\},$$

and the lattice generated by $A_{1v_1}+A_{2v_1}$ is $L_+:=\langle(0,3),(0,4)\rangle\cong L_{v_1}\cong\mathbb{Z}$. The index of L_+ in L_{v_1} is $\mathrm{ind}_{v_1}=1$ and the coset representative for L_+ in L_{v_1} is $q_0=(0,0)$. The v_1-*lattice diameter* is

$$d_{v_1}:=b_{01}\cdot v_1-\min_{p\in\mathrm{CH}(b_{01},k_0F_{v_1})}p\cdot v_1=1.$$

Hence, there is one slice corresponding to one piece. We describe the recursion step on

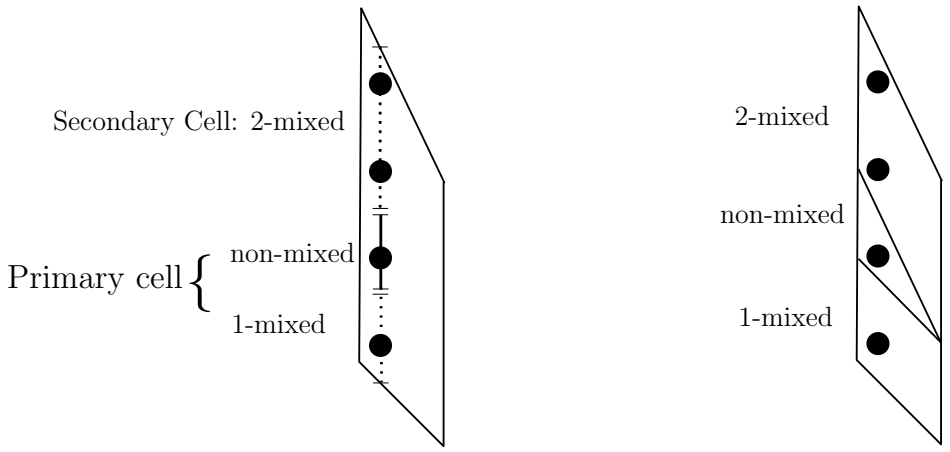

Figure 3.11: Example 3.4.1: The piece of the secondary cell $\mathcal{F}_{v_1}$ w.r.t. vector $v_1=(1,0)$ and its mixed subdivision (left). Also drawn is the corresponding secondary cell and its mixed subdivision w.r.t Alg. B (right)

this piece. It contains points corresponding to $(0,4),(0,5),(0,6),(0,7)$ lying on the slice of $\mathcal{F}_{v_1}+\delta$ of the form

$$(\tilde{\lambda}k_0F_{v_1}+\delta')+k_1F_{v_1}+k_2F_{v_1}+\lambda F_{v_1}+\delta.$$

To define the piece, following notation in [29], the scalar multiple of F_{v_1} is $\tilde{\lambda}F_{v_1}=\frac{29}{30}F_{v_1}$ and the translation vector is $\delta':=(\frac{1}{30},0)$. Since we do not use an initial additional polytope, $\lambda=0$ and $\lambda_{v_1}:=\lambda+\tilde{\lambda}=\frac{29}{30}$.

Let $\delta_\lambda:=\delta+\delta'=(0,-\frac{1}{30})$, and $\delta_\lambda=\delta_\lambda^{v_1}+\delta_{\lambda v_1}$, where $\delta_\lambda^{v_1}=(0,0)\in\mathbb{Q}v_1$ and $\delta_{\lambda v_1}=(0,-\frac{1}{30})\in L_+\otimes\mathbb{Q}$, hence $\delta_{0v_1}:=\delta_{\lambda v_1}-q_0=(0,-\frac{1}{30})$. So, the slice of $\mathcal{F}_{v_1}+\delta$ is

$$k_1F_{v_1}+k_2F_{v_1}+\lambda_{v_1}k_0F_{v_1}+\delta_\lambda, \tag{3.23}$$

and the corresponding piece in L_+ is

$$k_1F_{v_1}+k_2F_{v_1}+\lambda_{v_1}k_0F_{v_1}+\delta_{0v_1}. \tag{3.24}$$

The bijection between points in (3.23) and (3.24) is

$$p=\bar{p}+\delta_\lambda^{v_1}+q_0=\bar{p},$$

where $p\in(3.23)$ and $\bar{p}\in(3.24)$. After re-indexing, the input of the recursion step is:
- the polygons $\overline{Q_0}:=k_1F_{v_1}$, $\overline{Q_1}:=k_2F_{v_1}$, and $\overline{Q_2}:=\frac{29}{30}k_0F_{v_1}$ which is the additional polytope,
- the lattice $L^{(1)}:=L_+=\langle(0,3),(0,4)\rangle$ and
- the perturbation vector $\overline{\delta_0}:=\delta_{0v_1}=(0,-\frac{1}{30})$.

In order to be compatible with β, we choose $\overline{b_{01}}=b_{12}=(0,2)$ and apply the primary lifting. This partitions $\overline{Q_0}+\overline{Q_1}+\overline{Q_2}+\overline{\delta_0}$ into a primary $\overline{b_{01}}+\overline{Q_1}+\overline{Q_2}+\overline{\delta_0}$ and a secondary cell $\overline{Q_0}+(0,2)+\frac{29}{30}(0,2)+\overline{\delta_0}$. Lifting β induces a mixed subdivision on the primary cell consisting of the cells $\overline{b_{01}}+(0,1)+\overline{Q_2}+\overline{\delta_0}$ and $\overline{b_{01}}+\overline{Q_1}+\frac{29}{30}(0,1)+\overline{\delta_0}$. The former is non-mixed and contains point $(0,5)$, corresponding to the same point on the slice, which is also non-mixed under Alg. B. The latter cell is $\overline{0}$-mixed, hence 1-mixed and contains point $(0,4)$, corresponding to the same point on the slice, which is also 1-mixed under Alg. B. The secondary cell $\overline{Q_0}+(0,2)+\frac{29}{30}(0,2)+\overline{\delta_0}$ is $\overline{1}$-mixed, hence 2-mixed and contains the integer points $(0,6),(0,7)$ corresponding to the same points on the slice. They are also 2-mixed under Alg. B.

- We apply recursion on secondary cell:

$$\mathcal{F}_{v_2}=\mathrm{CH}(b_{01},k_0F_{v_2})+k_1F_{v_2}+k_2F_{v_2},$$

defined by the facet $F_{v_2}=((0,2),(1,2))$ of Q supported by v_2, see Figure 3.11. Now,

$$A_{1v_2}=\{(0,4),(2,4)\},\ A_{2v_2}=\{(0,2),(1,2)\}$$

and the lattice generated by $A_{1v_2}+A_{2v_2}$ is $L_+:=\langle(0,6),(1,6)\rangle\cong L_{v_2}\cong\mathbb{Z}$. The index of L_+ in L_{v_2} is $\mathrm{ind}_{v_2}=1$ and the coset representative for L_+ in L_{v_2} is $q_0=(0,0)$. The v_2-*lattice diameter* is

$$d_{v_2}:=b_{01}\cdot v_2-\min_{p\in\mathrm{CH}(b_{01},k_0F_{v_2})}p\cdot v_2=2.$$

Hence, there are two slices, each containing one piece, and the algorithm recurses on each such piece.

We analyze the recursion step on the piece of the shifted secondary cell $\mathcal{F}_{v_2}+\delta$, which contains the integer points corresponding to the points $(1,7),(2,7),(3,7)$ lying on a slice of the shifted secondary cell $\mathcal{F}_{v_2}+\delta$ of the form

$$(\tilde{\lambda}k_0F_{v_2}+\delta')+k_1F_{v_2}+k_2F_{v_2}+\lambda F_{v_2}+\delta.$$

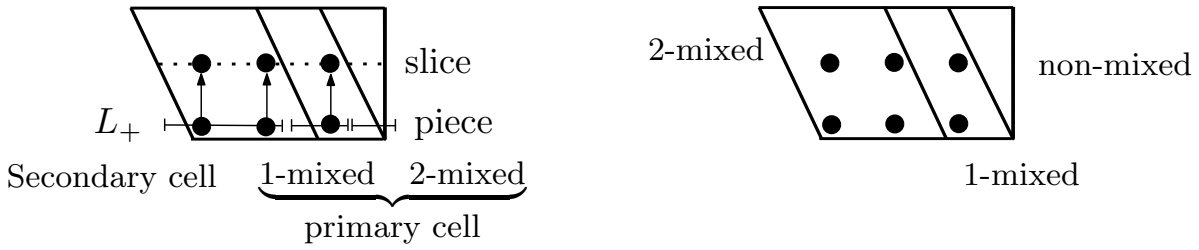

Figure 3.12: Example 3.4.1: A slice of the secondary cell $\mathcal{F}_{v_2}$ w.r.t. vector $v_2=(0,-1)$ containing points $(1,7),(2,7),(3,7)$ (dotted segment, left subfigure), the corresponding piece and its mixed subdivision w.r.t. Alg. A. The arrows show the correspondence between points on the slice and points on the piece. Also depicted is the mixed subdivision of the corresponding secondary cell w.r.t. Alg. B (right subfigure)

To define this piece we have that F_{v_2} is $\tilde{\lambda}F_{v_2}=\frac{31}{60}F_{v_2}$ and the translation vector $\delta':=(\frac{29}{60},0)$. Now $\lambda=0$ and hence $\lambda_{v_2}:=\lambda+\tilde{\lambda}=\frac{31}{60}$. Let $\delta_\lambda:=\delta+\delta'=(\frac{9}{29},-\frac{1}{30})$. Then, δ_λ can be written as $\delta_\lambda=\delta_\lambda^{v_2}+\delta_{\lambda v_2}$, where $\delta_\lambda^{v_2}=(0,1)\in\mathbb{Q}v_2$ and $\delta_{\lambda v_2}=(\frac{9}{20},-\frac{31}{30})\in L_+\otimes\mathbb{Q}$, hence $\delta_{0v_2}:=\delta_{\lambda v_2}-q_0=(\frac{9}{20},-\frac{31}{30})$.

So, the slice of $\mathcal{F}_{v_2}+\delta$ is

$$k_1F_{v_2}+k_2F_{v_2}+\lambda_{v_2}k_0F_{v_2}+\delta_\lambda, \tag{3.25}$$

and the corresponding piece in L_+ is

$$k_1F_{v_2}+k_2F_{v_2}+\lambda_{v_2}k_0F_{v_2}+\delta_{0v_2}. \tag{3.26}$$

The bijection between points in (3.25) and points in (3.26) is

$$p=\bar{p}+\delta_\lambda^{v_2}+q=\bar{p}+(0,1),$$

where $p\in(3.25)$ and $\bar{p}\in(3.26)$.

After re-indexing, the input of the recursion step is:
- the polygons $\overline{Q_0}:=k_1F_{v_2}$, $\overline{Q_1}:=k_2F_{v_2}$, and $\overline{Q_2}:=\frac{31}{60}k_0F_{v_2}$ which is the additional polytope,
- the lattice $L^{(1)}:=L_+=\langle(0,6),(1,6)\rangle$ and
- the perturbation vector $\bar{\delta}:=\delta_{0v_2}=(\frac{9}{20},-\frac{31}{30})$.

To be compatible with β, we choose $\overline{b_{01}}=b_{14}=(2,4)$ and apply the primary lifting; this partitions the Minkowski sum $\overline{Q_0}+\overline{Q_1}+\overline{Q_2}+\bar{\delta}$ into a primary $\overline{b_{01}}+\overline{Q_1}+\overline{Q_2}+\bar{\delta}$ and a secondary cell $\overline{Q_0}+(0,2)+\frac{31}{60}(0,2)+\bar{\delta}$. Lifting β induces a mixed subdivision of the primary cell consisting of the cells $\overline{b_{01}}+(1,2)+\overline{Q_2}+\bar{\delta}$ and $\overline{b_{01}}+\overline{Q_1}+\frac{31}{60}(0,2)+\bar{\delta}$. The latter is $\bar{0}$-mixed, hence 1-mixed and contains the integer point $(3,6)$ corresponding to point $(3,7)$ on the slice which is also 1-mixed under Alg. B. The former is non-mixed and does not contain any integer points.

The secondary cell $\overline{Q_0} + (0,2) + \frac{31}{60}(0,2) + \bar{\delta}$ is $\bar{1}$-mixed, hence 2-mixed and contains the integer points $(1,6),(2,6)$ corresponding to the points $(1,7),(2,7)$ of the slice respectively; they are also 2-mixed under Alg. B.

• The last secondary cell is

$$\mathcal{F}_{v_3} = \mathrm{CH}(b_{01}, k_0 F_{v_3}) + k_1 F_{v_3} + k_2 F_{v_3},$$

defined by the facet $F_{v_3} = ((3,0),(1,2))$ of Q supported by $v_3 = (-1,-1)$, see Figure 3.7 and Example 3.3.7. Now,

$$A_{1v_3} = \{(6,0),(2,4)\}, A_{2v_3} = \{(3,0),(1,2)\},$$

the lattice generated by $A_{1v_3} + A_{2v_3}$ is $L_+ := \langle (9,0),(7,2)\rangle \cong 2\mathbb{Z}$ and $L_{v_3} \cong \mathbb{Z}$. The index of L_+ in L_{v_3} is $\mathrm{ind}_{v_3} = 2$ and the cosets representatives for L_+ in L_{v_3} are $q_0 = (0,0)$ and $q_1 = (-1,1)$. The v_3-*lattice diameter* is

$$d_{v_3} := b_{01} \cdot v_3 - \min_{p \in \mathrm{CH}(b_{01}, k_0 F_{v_3})} p \cdot v_3 = 2.$$

Hence there are two slices, each corresponding to two pieces, and the algorithm recurses on each such piece.

We analyze the recursion step on the two pieces that contain integer points corresponding to points $(11,0),(10,1),(9,2),\ (8,3),(7,4),\ (6,5),(5,6),\ (4,7)$ lying on a slice of the shifted secondary cell $\mathcal{F}_{v_3} + \delta$ of the form

$$(\tilde{\lambda} k_0 F_{v_3} + \delta') + k_1 F_{v_3} + k_2 F_{v_3} + \lambda F_{v_3} + \delta.$$

To define these pieces, we have that the scalar multiple of F_{v_3} is $\tilde{\lambda} F_{v_3} = \frac{32}{60} F_{v_3}$ and the translation vector is $\delta' := (\frac{7}{15}, 0)$. Now, $\lambda = 0$ and hence $\lambda_{v_3} := \lambda + \tilde{\lambda} = \frac{32}{60}$; Let $\delta_\lambda := \delta + \delta' = (\frac{13}{30}, -\frac{1}{30})$.

Then, δ_λ can be written as $\delta_\lambda = \delta_\lambda^{v_3} + \delta_{\lambda v_3}$, where $\delta_\lambda^{v_3} = (1,1) \in \mathbb{Q}v_3$ and $\delta_{\lambda v_3} = (-\frac{17}{30}, -\frac{31}{30}) \in L_+ \otimes \mathbb{Q}$, hence $\delta_{0v_3} := \delta_{\lambda v_3} - q_0 = (-\frac{17}{30}, -\frac{31}{30})$ and $\delta_{1v_3} := \delta_{\lambda v_3} - q_1 = (\frac{13}{30}, -\frac{61}{30})$.

So, the slice of $\mathcal{F}_{v_3} + \delta$ is

$$k_1 F_{v_3} + k_2 F_{v_3} + \lambda_{v_3} k_0 F_{v_3} + \delta_\lambda, \tag{3.27}$$

and the corresponding pieces in L_+ are

$$k_1 F_{v_3} + k_2 F_{v_3} + \lambda_{v_3} k_0 F_{v_3} + \delta_{0v_3}, \tag{3.28}$$

$$k_1 F_{v_3} + k_2 F_{v_3} + \lambda_{v_3} k_0 F_{v_3} + \delta_{1v_3}, \tag{3.29}$$

The correspondences between points in the slice and points in the pieces are

$$p = \bar{p} + \delta_\lambda^{v_3} + q_0 = \bar{p} + (1,1),$$

where $p \in (3.27)$ and $\bar{p} \in (3.28)$, and

$$p = \bar{p} + \delta_\lambda^{v_3} + q_1 = \bar{p} + (0,2),$$

where $p \in (3.27)$ and $\bar{p} \in (3.29)$.

After re-indexing, the input of the recursion step is:
- the polygons $\overline{Q_0} := k_1 F_{v_3}$, $\overline{Q_1} := k_2 F_{v_3}$, and $\overline{Q_2} := \frac{32}{60} k_0 F_{v_3}$ which is the additional polytope,
- the lattice $L^{(1)} := L_+ = \langle (9,0), (7,2) \rangle$ and
- the perturbation vectors $\overline{\delta_0} := \delta_{0v_3} = (-\frac{17}{30}, -\frac{31}{30})$ and $\overline{\delta_1} := \delta_{1v_3} = (\frac{13}{60}, -\frac{61}{30})$.

As β indicates, we choose $\overline{b_{01}} = b_{15} = (6,0)$ and apply the primary lifting.

For the first piece, the lifting partitions the Minkowski sum $\overline{Q_0} + \overline{Q_1} + \overline{Q_2} + \overline{\delta_0}$ into a primary $\overline{b_{01}} + \overline{Q_1} + \overline{Q_2} + \overline{\delta_0}$ and a secondary cell $\overline{Q_0} + (1,2) + \frac{32}{60}(1,2) + \overline{\delta_0}$. Lifting β induces a mixed subdivision on the primary cell consisting of the cells $\overline{b_{01}} + (3,0) + \overline{Q_2} + \overline{\delta_0}$ and $\overline{b_{01}} + \overline{Q_1} + \frac{32}{60}(1,2) + \overline{\delta_0}$. The former is non-mixed and contains point $(9,0)$, which corresponds to $(10,1)$ on the slice which is also non-mixed under Alg. B. The latter is $\overline{0}$-mixed, hence 1-mixed and contains the point $(7,2)$ corresponding to the point $(8,3)$ in the slice which is also 1-mixed under Alg. B.

The secondary cell $\overline{Q_0} + (1,2) + \frac{32}{60}(1,2) + \overline{\delta_0}$ is $\overline{1}$-mixed, hence 2-mixed and contains the integer points $(3,6), (5,4)$ corresponding to the points $(4,7), (6,5)$ of the slice respectively which are also 2-mixed under Alg. B.

For the second piece, the lifting partitions the Minkowski sum $\overline{Q_0} + \overline{Q_1} + \overline{Q_2} + \overline{\delta_1}$ into a primary $\overline{b_{01}} + \overline{Q_1} + \overline{Q_2} + \overline{\delta_1}$ and a secondary cell $\overline{Q_0} + (1,2) + \frac{32}{60}(1,2) + \overline{\delta_1}$. Lifting β induces a mixed subdivision on the primary cell consisting of the cells $\overline{b_{01}} + (3,0) + \overline{Q_2} + \overline{\delta_1}$ and $\overline{b_{01}} + \overline{Q_1} + \frac{32}{60}(1,2) + \overline{\delta_1}$. The former is non-mixed and contains point $(11,-2)$ corresponding to $(11,0)$ on the slice which is also non-mixed under Alg. B, whereas the latter cell is $\overline{0}$-mixed, hence 1-mixed and contains the integer point $(9,0)$ corresponding to point $(9,2)$ on the slice which is also 1-mixed under Alg. B.

The secondary cell $\overline{Q_0} + (1,2) + \frac{32}{60}(1,2) + \overline{\delta_1}$ is $\overline{1}$-mixed, hence 2-mixed and contains the integer points $(7,2), (5,4)$ corresponding to the points $(7,4), (5,6)$ of the slice respectively. These are also 2-mixed under Alg. B.

The second slice of $\mathcal{F}_{v_3} + \delta$ is $\left(\frac{1}{30} F_{v_3} + (\frac{29}{30}, 0)\right) + k_1 F_{v_3} + k_2 F_{v_3} + (-\frac{1}{30}, -\frac{1}{30})$, and contains integer points $(10,0), (9,1), (8,2), (7,3), (6,4), (5,5), (4,6)$.

Table 3.1 illustrates corollaries 3.3.10 and 3.3.11, where the summands come from Q_0, Q_1 and Q_2 respectively. Recall that $c_{011} := (1,0) + \delta_{011}$, $c_{143} := (2,4) + \delta_{143}$ and $c_{154} := (6,0) + \delta_{154}$.

Table 3.1: Illustration of Cor. 3.3.10 and Cor. 3.3.11 for Example 3.4.1

Cell w.r.t. Alg. A	Corresponding cell w.r.t. Alg. B	Type of cell
$\tilde{\lambda}(1,2) + (6,0) + ((3,0),(1,2)) + \delta_{0v3}$	$(c_{011}, (1,2)) + c_{154} + ((3,0),(1,2)) + \delta$	1-mixed
$\tilde{\lambda}((3,0),(1,2)) + (6,0) + (3,0) + \delta_{0v3}$	$\mathrm{CH}(c_{011}, (1,2), (3,0)) + c_{154} + (3,0) + \delta$	non-mixed
$\tilde{\lambda}(1,2) + (6,0) + ((3,0),(1,2)) + \delta_{1v3}$	$(c_{011}, (1,2)) + c_{154} + ((3,0),(1,2)) + \delta$	1-mixed
$\tilde{\lambda}((3,0),(1,2)) + (6,0) + (3,0) + \delta_{1v3}$	$\mathrm{CH}(c_{011}, (1,2), (3,0)) + c_{154} + (3,0) + \delta$	non-mixed
$\tilde{\lambda}(0,2) + (2,4) + ((0,2),(1,2)) + \delta_{0v2}$	$(c_{011}, (0,2)) + c_{143} + ((0,2),(1,2)) + \delta$	1-mixed
$\tilde{\lambda}((0,2),(1,2)) + (2,4) + (1,2) + \delta_{0v2}$	$\mathrm{CH}(c_{011}, (1,2), (0,2)) + c_{143} + (1,2) + \delta$	non-mixed

3.5 Conclusion and Further work

Let us conclude with some preliminary results on mixed algebraic systems.

The sparse resultant is well defined only for essential sets of Newton polytopes, see Definition 1.1.6. An essential set defines a Minkowski sum of dimension $h-1$ but the converse is not always true.

Alg. A admits one main modification in the mixed case: At the Recursion Phase, the faces $F_i \subset Q_i$ supported by vector v are not always the same. Let the input be $n+1$ polytopes; we describe the 0-th iteration for simplicity. Consider the n-dimensional secondary cell:

$$\mathrm{CH}(b_{01}, F_0) + F_1 + \cdots + F_n \subset \mathbb{R}^n,$$

where $F_i \subset \mathbb{R}^{n-1}$. Without loss of generality, let $\{F_1, \ldots, F_k\}$ be an essential subset and let $L_+(k)$ be the integer lattice it defines. The algorithm recurses on lattice $L_+(k)$ and polytope set (representing a piece)

$$\mathrm{CH}(b_{01}, F_0) \cap \Lambda_+(k), F_1, \ldots, F_k, F_{k+1} \cap \Lambda_+(k), \ldots, F_n \cap \Lambda_+(k), \tag{3.30}$$

where $\Lambda_+(k)$ ranges over all possible homothetic copies of $L_+(k)$ defined by the different cosets of $L_+(k)$ in its saturation, and the different slices that can be defined as intersections with $\mathrm{CH}(b_{01}, F_0)$. Alg. A distinguishes two cases, according to whether there is one or more essential subsets of $\{F_1, \ldots, F_n\}$. In the former case, v and the corresponding secondary cell are called *admissible*. For non-admissible cells, all integer points are considered as non-mixed, i.e. treated as if they lied in non-mixed cells. For admissible cells, integer d_{F_v} is defined [29, Sec.4] (cf. [36]), and d_{F_v} pieces of the form (3.30) are (arbitrarily) selected. Lattice points labeled as mixed in these pieces by the recursive application of Alg. A are labeled as mixed overall, the rest are non-mixed.

Before sketching the extension of our algorithm to the mixed case, let us consider some special cases. Reduced systems are such that, for any vector $v \in \mathbb{R}^n$, there is some $i \in \{1, \ldots, n\}$ so that the face supported by v in Q_i is a vertex. For us, it suffices that this holds for any vector v associated with secondary cells at the 0-th recursion step of Alg. A. Reduced systems were settled by D'Andrea (personal communication) by directly establishing the extraneous factor. For reduced systems, as well as for arbitrary systems of three bivariate polynomials, the lifting function (3.31), specified by D'Andrea and Emiris (personal communication), produces a Macaulay-type formula:

$$\begin{array}{lrcll} l_0: & A_0 & \to & \{0,1\} & \\ & b_{01} & \mapsto & 1, & \\ & b_{0j} & \mapsto & 0, & \text{if } j \neq 0, \end{array} \qquad \begin{array}{lrcll} l_i: & A_i & \to & \mathbb{R} & (i \geq 1) \\ & p & \mapsto & 0, & \text{if } p \notin \cup_{\forall v} A_{i,v} \\ & p & \mapsto & r_p & \text{otherwise.} \end{array} \tag{3.31}$$

Here, $A_{i,v} := A_i \cap Q_{i,v}$, where $Q_{i,v}$ is the face of Q_i supported by v, and r_p is a positive random number satisfying $0 < r_p \ll 1$. It is not difficult to see that our lifting β has an overall effect similar to that of lifting (3.31), therefore it also produces a Macaulay-type formula for the previous systems. For bivariate systems, the idea of the proof is subsumed by that for $n = 3$ at the end of this section.

For extending Alg. B to the mixed case, we must modify it so that Definition 3.1.2 applies to different polytopes and also up to $i = n-1$. We sketch a proof that it produces the same matrix as Alg. A, by extending the correlation between maximal cells, established in the unmixed case. Our proof might extend to $n > 3$, but seems complicated; we hope that a more elegant approach is possible.

In non-admissible secondary cells of Alg. A, for any n, we show that both algorithms behave in the same way, namely that the corresponding lattice points lie in non-mixed cells of Alg. B. We demonstrate the contrapositive by focusing on a mixed cell of Alg. B and a corresponding secondary cell of Alg. A, following Lemma 3.3.9.

Lemma 3.5.1. *Every t-mixed cell by Alg. B, when intersected with a $(n-t)$-di-mensional hyperplane as in Lemma 3.3.9, is contained in an admissible secondary cell of step $t-1$ of Alg. A.*

Proof. Any t-mixed cell of Alg. B is of the form $E_0+\cdots+E_{t-1}+a_{tj}+E_{t+1}+\cdots+E_n$, where a_{tj} is either a vertex of Q_i or some c_{tjs} in the interior of an $(n-t)$-dimensional face, and edges $E_{t+1},\ldots,E_n$ span an $(n-t)$-dimensional space. This cell is intersected by a $(n-t)$-dimensional hyperplane, similarly to Lemma 3.3.9. The intersection is contained in a t-primary cell of Alg. A with t-summand b_{tj}; it lies in a piece of $(t-1)$-secondary cell

$$F_0+\cdots+F_{t-2}+\mathrm{CH}(b_{(t-1)h},F_{t-1})+F_t+\cdots+F_n,$$

where the F_i are faces of the Q_i, $i=1,\ldots,n$, supported by the same vector, with $\dim F_i \leq n-t$. We claim $\{F_t,\ldots,F_n\}$ contains a unique essential set, with cardinality $r+1$, spanning an r-dimensional space, which is defined as follows: F_t and $r\leq n-t$ faces, denoted without loss of generality $F_{t+1},\ldots,F_{t+r}$, where r is minimal so that $\dim H=r$, for $H=\langle F_t,\ldots,F_{t+r}\rangle$.

By hypothesis, $\dim\langle F_{t+1},\ldots,F_n\rangle = n-t$, since a subspace is spanned by the E_i and has same dimension. So subsets indexed in $\{t+1,\ldots,n\}$ span a space of dimension at least equal to their cardinality. In addition, none of the $F_i, i>t+r$ is contained in H. So every subset indexed in $\{t,\ldots,n\}$ containing $\{t\}\cup J$, for $J\subset\{t+r+1,\ldots,n\}$, will be of cardinality $\leq r+|J|$ and span a space of dimension $r+|J|$. Hence there are no other essential subsets. □

For $n=3$, all admissible secondary cells have d_{F_v} pieces, since there is no extra artificial polytope in the input of Alg. A. We distinguish cases on the dimension $k-1$ of the space generated by the essential set $\{F_1,\ldots,F_k\}$, $1\leq k\leq 3$, on which the recursion of Alg. A occurs:

1. If $k-1$ is 0 or 1, the recursion is either trivial (occurs on a vertex), or corresponds to the Sylvester case.

2. If $k-1=2$ and $\dim F_i=1, i=1,2,3$, the two algorithms behave similarly, since Definition 3.1.2 defines points c_{2js} in the edges of Q_2 and Lemma 3.3.9 applies. Notice that $\dim Q_2\geq 1$; otherwise the Q_i's would not form an essential set.

3. If $k-1=2$, then $\dim F_i\in\{1,2\}$ for $i=1,2,3$ and at least one face is two-dimensional. If $\dim F_1=2$, then Lemma 3.3.9 applies. Otherwise, $\dim F_1=1$ and $\dim F_2\geq 1$. Irrespective of $\dim F_2$, the c_{2js}'s play the role of distinguished points and Lemma 3.3.9 applies again.

Chapter 4

The Newton polygon of the implicit equation of rational parametric curves

Implicitization is the problem of switching from a parametric representation of a hypersurface to an algebraic one. It is a fundamental question with several applications. Here we consider the implicitization problem for a planar curve, where the polynomials in its parameterization have fixed Newton polytopes. We determine the vertices of the Newton polygon of the implicit equation, or *implicit polygon*, without computing the equation, under the assumption of *generic* coefficients relative to the given supports, i.e. our results hold for all coefficient vectors in some open dense subset of the coefficient space. The support of the implicit equation, or *implicit support*, is taken to be all interior points inside the implicit polygon.

This problem was posed in [40] but has received much attention lately. According to [41], "apriori knowledge of the Newton polytope would greatly facilitate the subsequent computation of recovering the coefficients of the implicit equation [...] This is a problem of numerical linear algebra ...". Reducing implicitization to linear algebra is also the premise of [13, 42]. Of course, this can be nontrivial if coefficients are not generic. Another potential application of knowing the implicit polygon is to approximate implicitization, see [43].

Our approach considers the symbolic resultant which eliminates the parameters and, then, is specialized to yield an equation in the implicit variables. This method applies, more generally, to applications, including the computation of the u-resultant or the offset of a parametric curve or surface, where the resultant coefficients are polynomials in a few variables, and we wish to study the resultant as a polynomial in these variables.

Previous work includes [42, 44], where an algorithm constructs the Newton polytope of any implicit equation. That method had to compute all mixed subdivisions, then applies cor. 1.1.11. In [4, chapter 12], the authors study the resultant of two univariate polynomials and describe the facets of its Newton polytope. In [45], the extreme monomials of the Sylvester resultant are described. The approaches in [42, 4] cannot exploit the fact that the denominators in a rational parameterization may be identical.

By employing tropical geometry, [41, 46] compute the implicit polytope for any hypersurface parameterized by Laurent polynomials. In particular, in [46] the implicit polytope

is characterized as the *mixed fiber polytope* of the input polytopes and software *TrIm* offers implementations of tropical implicitization to compute it. Their theory extends to arbitrary implicit ideals. They give a generically optimal implicit support; for curves, the support is described in [41, example 1.1]. Their approach also handles rational parameterizations with the same denominator by homogenizing the parameter as well as the implicit space. The implicit equation is homogeneous, hence its Newton polytope lies in a hyperplane.

More recently, in [47] the problem was solved in an abstract way by means of composite bodies and mixed fiber polytopes. In [48] the normal fan of the implicit polygon is determined. This is computed by the multiplicities of any parameterization of the rational plane curve. The authors reduce the problem to studying the support function of the implicit polytope and counting the number of solutions of a certain system of equations. The latter is solved by applying a refinement of the Kushnirenko-Bernstein formula for the computation of the isolated roots of a polynomial system in the torus, given in [49]. As a corollary, they obtain the optimal implicit polygon in the case of generic coefficients. They also address the inverse question, namely when can a given polygon be the Newton polygon of an implicit curve. They show that the variety of rational curves with given Newton polytope is unirational.

In [50], we computed the Newton polytope of specialized resultants while avoiding to compute the entire secondary polytope; our approach was to examine the silhouette of the latter with respect to an orthogonal projection. This method is revisited in [51] by studying output-sensitive methods to compute the resultant polytope. We also presented a method to compute the vertices of the implicit polygon of polynomial or rational parametric curves, when denominators differ. In [52] we give the final result. We also introduced a method and gave partial results for the case when denominators are equal; the latter method is described in final form in the present article. Our main contribution is to determine the vertex structure of the implicit polygon of a rational parameterized planar curve, or implicit vertices, under the assumption of *generic* coefficients. If the coefficients are not sufficiently generic, then the computed polygon contains the implicit polygon. In the case of rationally parameterized curves with different denominators (which includes the case of Laurent polynomial parameterizations), the Cayley trick reduces the problem to computing regular triangulations of point sets in the plane. If the denominators are identical, two-dimensional mixed subdivisions are examined; we show that only subdivisions obtained by *linear* liftings are relevant. These results also apply if the two parametric expressions share the same numerator, or the numerator of one equals the denominator of the other. We prove that, in these cases, only extremal terms matter in determining the implicit polygon as well as in ensuring the genericity hypothesis on the coefficients.

The following proposition collects our main corollaries regarding the shape of the implicit polygon in terms of corner cuts on an initial polygon. A corner cut on a polygon P is a line that intersects the polygon, excluding one vertex while leaving the rest intact. ϕ is the implicit equation and $N(\phi)$ is the implicit polygon.

Proposition 4.0.2. *$N(\phi)$ is a polygon with one vertex at the origin and two edges lying on the axes. In particular, for polynomial parameterizations, $N(\phi)$ is a right triangle with at most one corner cut, which excludes the origin. For rational parameterizations with equal*

denominators, $N(\phi)$ is a right triangle with at most two cuts, on the same or different corners. For rational parameterizations with different denominators, $N(\phi)$ is a quadrilateral with at most two cuts, on the same or different corners.

Example 4.0.3. Consider the plane curve parameterized by:

$$x = \frac{t^6 + 2t^2}{t^7 + 1}, y = \frac{t^4 - t^3}{t^7 + 1},$$

Theorem 4.2.11 yields vertices $(7,0),(0,7),(0,3),(3,1),(6,0)$, which define the actual implicit polygon (see Figure 4.1, left) because the implicit equation is

$$\begin{aligned}\phi = &-32y^4 - 30x^3y^2 - x^4y - 12x^2y^2 - 3x^3y - 7x^6y - 2x^7 + 20xy^3 + 280x^2y^5 \\ &-7^3y^4x - 70x^4y^3 - 22x^3y^3 - 49x^5y^2 - 21x^4y^2 + 11x^5y + 216y^5 + 129y^7 \\ &-248y^6 + 70xy^6 + 185xy^5 + 24y^3 + 100xy^4 + 43x^2y^3 + 72x^2y^4 + 3x^6.\end{aligned} \tag{4.1}$$

Changing the coefficient of t^2 to -1, leads to an implicit polygon with four cuts which is contained in the polygon predicted by Theorem 4.2.11. This shows the importance of the genericity condition on the coefficients of the parametric polynomials. See Example 4.2.21 for details.

An instance where the implicit polygon has 6 vertices is:

$$x = \frac{t^3 + 2t^2 + t}{t^2 + 3t - 2},\ y = \frac{t^3 - t^2}{t - 2}.$$

Our results in Section 4.1 yield implicit vertices $(0,1),(0,3),(3,0),(1,3),(2,0),\ (3,2)$ which define the actual implicit polygon (see Figure 4.1, right). See Example 4.1.10 for details.

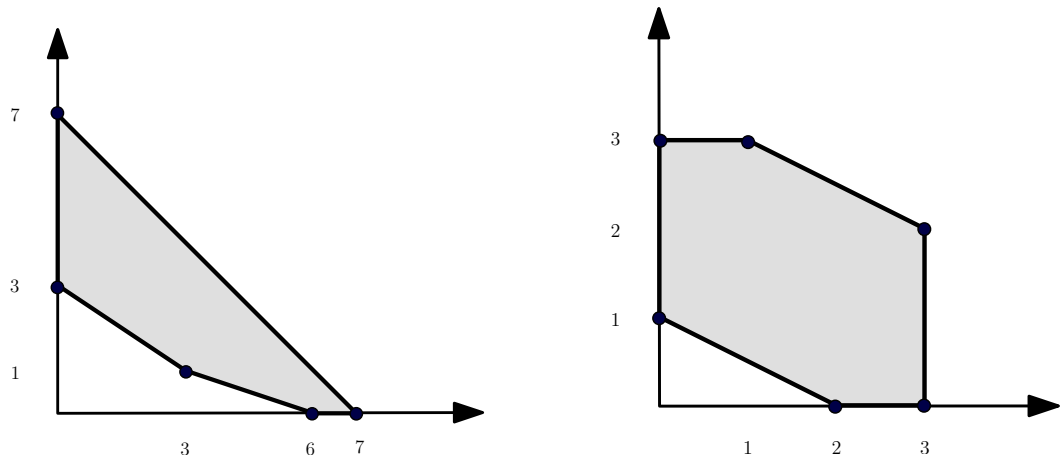

Figure 4.1: The implicit polygons of the curves of Example 4.0.3

Let $h_0,\ldots,h_n \in \mathbb{C}[t_1,\ldots,t_r]$ be polynomials in parameters t_i. The implicitization problem is to compute the prime ideal I of all polynomials $\phi \in \mathbb{C}[x_0,\ldots,x_n]$ which satisfy $\phi(h_0,\ldots,h_n) \equiv 0$ in $\mathbb{C}[t_1,\ldots,t_r]$. We are interested in parametric curves where $r = n = 1$, and generalize h_i to be rational expressions in $\mathbb{C}(t)$. Then $I = \langle\phi\rangle$ is a principal ideal. Note that $\phi \in \mathbb{C}[x_0,x_1]$ is uniquely defined up to sign. The x_i are called implicit variables, $A(\phi)$ is

the *implicit support* and $N(\phi)$ is the implicit polygon. Usually a rational parameterization of a plane curve may be defined by

$$x_i = \frac{P_i(t)}{Q_i(t)},\ i = 0, 1, \quad \gcd(P_i(t), Q_i(t)) = 1, \tag{4.2}$$

where the denominators may be equal. All polynomials have fixed supports. We assume that the parameterization is *proper* i.e. the *degree* of the induced rational map equals 1. This avoids, e.g., having all terms in t^a for some $a > 1$. This assumption is justified by the fact that every rational plane curve has a proper parameterization and there are algorithms for computing it (see [53]).

Define $f_0 = x_0 Q_0(t) - P_0(t), f_1 = x_1 Q_1(t) - P_1(t) \in \mathbb{C}[t]$. Then the following proposition gives an explicit formula for the implicit equation of the parametric curve in terms of a Sylvester resultant.

Proposition 4.0.4. [54] *Let $f_0, f_1 \in \mathbb{C}[t]$ be non-zero univariate polynomials as above. Then*

$$Res_t(f_0(t), f_1(t)) = c \cdot \phi(x_0, x_1)^q, \quad c \in \mathbb{C},$$

where q is the degree of the parameterization.

Since $\mathrm{Res}_t(f_0(t), f_1(t))$ is not identically zero, we can compute $N(\phi)$ as the Newton polytope of a specialized resultant. Furthermore, since the parameterization is proper, then (cf. [55])

$$deg_{x_i}(\phi(x_0, x_1)) = \max\{deg_t(P_j(t)), deg_t(Q_j(t))\},\ \{i, j\} = \{0, 1\}.$$

The implicit supports predicted solely by degree bounds are typically larger than optimal.

4.1 Rational parameterizations with different denominators

We now turn to the case of rationally parameterized curves, with different denominators. We have

$$f_0(t) = xQ_0(t) - P_0(t),\ f_1(t) = yQ_1(t) - P_1(t)\ \in (\mathbb{C}[x, y])[t], \gcd(P_i, Q_i) = 1,$$

where all polynomials have fixed supports and generic coefficients with respect to these supports. Let $c_{ij}\ (0 \le j \le m_i)$, $q_{ij}\ (0 \le j \le k_i)$ denote the coefficients of polynomials $P_i(\mathrm{t})$ and $Q_i(t)$, and $N_i = \mathcal{A}(P_i)$, $D_i = \mathcal{A}(Q_i)$ their supports respectively; note that for $i = 1, 2$, $N_i \neq \emptyset$ and $D_i \neq \emptyset$. Then, the supports of f_0, f_1 are

$$A_0 = N_0 \cup D_0 = \{0, a_{01}, \ldots, a_{0n}\} \quad \text{and} \quad A_1 = N_1 \cup D_1 = \{0, a_{11}, \ldots, a_{1m}\},$$

where the a_{0i} and a_{1j} are sorted in ascending order; it holds that $a_{00} = a_{10} = 0$ because $\gcd(P_i, Q_i) = 1$. Elements of A_0, A_1 are embedded by the Cayley embedding κ in $\mathbb{R}^2$. The embedded points are denoted by $(a_{0i}, 0), (a_{1i}, 1)$; by abusing notation, we shall omit the second coordinate.

Recall that each $p \in A_0$ corresponds to a monomial of f_0. The corresponding coefficient either lies in $\mathbb{C}$, or is a monomial $q_{0i}x$, or a binomial $q_{0i}x + c_{0j}$, where $q_{0i}, c_{0j} \in \mathbb{C}$. The resultant $\mathrm{Res}(f_0, f_1)$ is a polynomial in x, y, c_{ij}, q_{ij}. We consider the specialization of coefficients c_{ij}, q_{ij} in order to study ϕ; this specialization yields the implicit equation. The relevant terms are products of one polynomial in x and one in y. The former is the product of powers of terms of the form $q_{0i}x$ or $q_{0i}x+c_{0j}$; the y-polynomial is obtained analogously. The exponents in A_0 and A_1 relevant to the implicit polygon are the ones corresponding to coefficients which are non-constant polynomials in x. These exponents fall into two different categories: the exponents in D_0 and those in $D_0 \setminus N_0$; the latter contains the exponents corresponding to coefficients which are monomials in x. An analogous description holds for the second polynomial.

We need consider only i-mixed cells associated with a vertex coming from D_i or $D_i \setminus N_i$. For any triangulation, these mixed cells correspond either to triangles with vertices $\{a_{0i}, a_{1\ell}, a_{1r}\}$, where $\ell, r \in \{0, \ldots, m\}$, or to $\{a_{0\ell}, a_{0r}, a_{1j}\}$, where $\ell, r \in \{0, \ldots, n\}$. Given a triangulation, we set

$$e_0 = \sum_{i,\ell,r} \mathrm{Vol}(a_{0i}, a_{1\ell}, a_{1r}), \qquad e_1 = \sum_{\ell,r,j} \mathrm{Vol}(a_{0\ell}, a_{0r}, a_{1j}), \tag{4.3}$$

where i, j range over all elements of D_0 or $D_0 \setminus N_0$ and D_1 or $D_1 \setminus N_1$, respectively, and we sum up the normalized volumes of mixed triangles.

In the following, we use the upper (lower, resp.) hull of a convex polygon in $\mathbb{R}^2$ w.r.t. some direction $v \in \mathbb{R}^2$. Let us consider the unbounded convex polygons defined by the computed upper and lower hulls. The union of these two unbounded polygons is the implicit Newton polygon.

Lemma 4.1.1. *Consider all points (e_0, e_1), defined by expressions (4.3), over all possible triangulations. The polygon defined by the upper hull of points (e_0, e_1) w.r.t. to vector $(0, 1)$, where the corresponding vertex comes from D_i, $i = 0, 1$, and the lower hull of points (e_0, e_1) w.r.t. to vector $(0, 1)$, where the corresponding vertex comes from $D_i \setminus N_i$, $i = 0, 1$, equals the implicit polygon $N(\phi)$.*

Proof. Consider the extreme terms of the resultant, given by Proposition 1.1.10. After the specialization of the coefficients, those associated with i-mixed cells having a vertex $p \in N_i \setminus D_i$ contribute only a coefficient in $\mathbb{C}$ to the corresponding term of ϕ. This is why they are not taken into account in (4.3).

Now consider triangles with vertices from D_i. By maximizing e_0 or e_1, as defined in (4.3), it is clear that we shall obtain the maximum possible exponents in the terms which are polynomials in x and y respectively, hence the largest degrees in x, y in ϕ. Under certain genericity assumptions, we shall obtain all vertices in the implicit polygon, which appear in its upper hull with respect to vector $(0, 1)$.

Triangles with vertices from $D_i \setminus N_i$ minimize the powers of coefficients corresponding to monomials in the implicit variables. All other coefficients are in $\mathbb{C}$ or are binomials in x (or y), so they contain a constant term, hence their product will contain a constant, assuming generic coefficients in the parametric equations. Therefore these are vertices on the lower hull with respect to $(0, 1)$. □

4.1.1 The implicit vertices

For any $p \in A_i,\ i = 0, 1$, let $\mathcal{X}_{D_i}(p)$ and $\mathcal{X}_{D_i \setminus N_i}(p)$ be the characteristic functions of the sets D_i and $D_i \setminus N_i$: $\mathcal{X}_{D_i}(p) = 1$ if $p \in D_i$, and $\mathcal{X}_{D_i}(p) = 0$ otherwise; similarly, $\mathcal{X}_{D_i \setminus N_i}(p) = 1$ if $p \in D_i \setminus N_i$, and $\mathcal{X}_{D_i \setminus N_i}(p) = 0$ otherwise.

Now we give formulas for the coordinates of the vertices of $N(\phi)$. The vertices computed are not necessarily distinct; they lie on the lines $e_0 = 0,\ e_0 = a_{1m},\ e_1 = 0$ and $e_1 = a_{0n}$.

Theorem 4.1.2.
(i) The maximum exponent of x in the implicit equation is $e_0^{max} = a_{1m}$. When this is attained, the maximum exponent of y is

$$e_1^{max}|_{e_0^{max}} = \max(D_0) - \min(D_0) + \mathcal{X}_{D_1}(0) \cdot \min(D_0) + \mathcal{X}_{D_1}(a_{1m}) \cdot (a_{0n} - \max(D_0)),$$

and the minimum exponent of y is

$$e_1^{min}|_{e_0^{max}} = \mathcal{X}_{D_1 \setminus N_1}(0) \cdot \min(D_0 \setminus N_0) + \mathcal{X}_{D_1 \setminus N_1}(a_{1m}) \cdot (a_{0n} - \max(D_0 \setminus N_0)).$$

(ii) The maximum exponent of y in the implicit equation is $e_1^{max} = a_{0n}$. When this is attained, the maximum exponent of x is

$$e_0^{max}|_{e_1^{max}} = \max(D_1) - \min(D_1) + \mathcal{X}_{D_0}(0) \cdot \min(D_1) + \mathcal{X}_{D_0}(a_{0n}) \cdot (a_{1m} - \max(D_1)),$$

and the minimum exponent of x is

$$e_0^{min}|_{e_1^{max}} = \mathcal{X}_{D_0}(0) \cdot \min(D_1) + \mathcal{X}_{D_0}(a_{0n}) \cdot (a_{1m} - \max(D_1)) + \prod_{j \geq 0} \mathcal{X}_{D_0}(a_{0j}) \cdot (\max(D_1) - \min(D_1)).$$

(iii) The minimum exponent of x in the implicit equation is $e_0^{min} = 0$. When this is attained, the maximum exponent of y is

$$e_1^{max}|_{e_0^{min}} = \max(N_0 \setminus D_0) - \min(N_0 \setminus D_0) + \mathcal{X}_{D_1}(0) \cdot \min(N_0 \setminus D_0) + \mathcal{X}_{D_1}(a_{1m}) \cdot (a_{0n} - \max(N_0 \setminus D_0)),$$

and the minimum exponent of y is

$$e_1^{min}|_{e_0^{min}} = \mathcal{X}_{D_1 \setminus N_1}(0) \cdot \min(N_0) + \mathcal{X}_{D_1 \setminus N_1}(a_{1m}) \cdot (a_{0n} - \max(N_0)).$$

(iv) The minimum exponent of y in the implicit equation is $e_1^{min} = 0$. When this is attained, the maximum exponent of x is

$$e_0^{max}|_{e_1^{min}} = \max(N_1) - \min(N_1) + \mathcal{X}_{D_0 \setminus N_0}(0) \cdot \min(N_1) + \mathcal{X}_{D_0 \setminus N_0}(a_{0n}) \cdot (a_{1m} - \max(N_1)),$$

and the minimum exponent of x is

$$e_0^{min}|_{e_1^{min}} = \mathcal{X}_{D_0 \setminus N_0}(0) \cdot \min(N_1) + \mathcal{X}_{D_0 \setminus N_0}(a_{0n}) \cdot (a_{1m} - \max(N_1)).$$

Proof. We shall prove only case (i), the rest are either symmetric, or similar.

Since the vertex corresponding to the maximum exponent of y when the maximum exponent of x is attained belongs to the upper hull of the implicit polygon, the exponents are obtained by mixed triangles in eq. (4.3) where i, j range over all elements of D_0, D_1, respectively. The maximum possible exponent of x is a_{1m}, and this is attained by a triangulation in which the entire segment $[0, a_{1m}]$ is visible by any element of D_0; recall $D_0 \neq \emptyset$. Then, the maximum exponent of y is attained from any triangulation such that a maximum part of segment $[0, a_{0n}]$ is visible from some points in D_1. A triangulation achieving the maximum exponent of y given in the theorem is shown in Figure 4.2, left subfigure (note that a_{1i} may coincide with 0 or a_{1m}); recall $D_1 \neq \emptyset$.

We will show that this exponent of y is the maximum that can be achieved. Since all points to the left of $\min(D_0)$ do not contribute to the exponent of x in eq. (4.3), any triangulation obtaining the maximum exponent of x (i.e., a_{1m}) cannot contain edges connecting these points to points in A_1. Then, since we have triangles, $0 \in A_1$ is connected to a point in A_0 which should in fact belong to D_0; if $0 \notin D_1$, 0 should be adjacent to $\min(D_0)$, in order that the part of segment $[0, a_{0n}]$ visible by 0 is minimized. A similar argument holds for a_{1m}; note that all the points to the right of $\max(D_0)$ do not contribute to the exponent of x in eq. (4.3).

The vertex corresponding to the minimum exponent of y when the maximum exponent of x is attained belongs to the lower hull of the implicit polygon, hence the exponents are obtained by mixed triangles in eq. (4.3) where i, j range over all elements of $D_0 \setminus N_0$, $D_1 \setminus N_1$, respectively. Then, the minimum exponent of y stated in the theorem can be achieved by the triangulations shown in Figure 4.2; the center figure corresponds to the case that $a_{1m} \in N_1$, the right to the case that $a_{1m} \in D_1 \setminus N_1$. As above, in order to attain the maximum exponent of x, $0 \in A_1$ is connected to a point in A_0 which should in fact belong to $D_0 \setminus N_0$; if $0 \in D_1 \setminus N_1$, the minimum is obtained if 0 is connected to $\min D_0 \setminus N_0$; this leads to the first term of the expression of the exponent in the theorem. The second term is obtained by a similar argument for a_{1m}. □

Remark 4.1.3. The product $\prod_{j\geq 0} \mathcal{X}_{D_0}(a_{0j})$ is equal to 1 if $D_0 = A_0$ and is equal to 0 otherwise. Note that similar products do not exist in the expressions of $e_1^{min}|_{e_0^{max}}$, $e_1^{min}|_{e_0^{min}}$, and $e_0^{min}|_{e_1^{min}}$, since in these cases the products would be $\prod_{j\geq 0} \mathcal{X}_{D_1\setminus N_1}(a_{1j})$ in the first and second case, and $\prod_{j\geq 0} \mathcal{X}_{D_0\setminus N_0}(a_{0j})$ in the third case; in either case, the product is equal to 0 since $D_i \setminus N_i \neq A_i$.

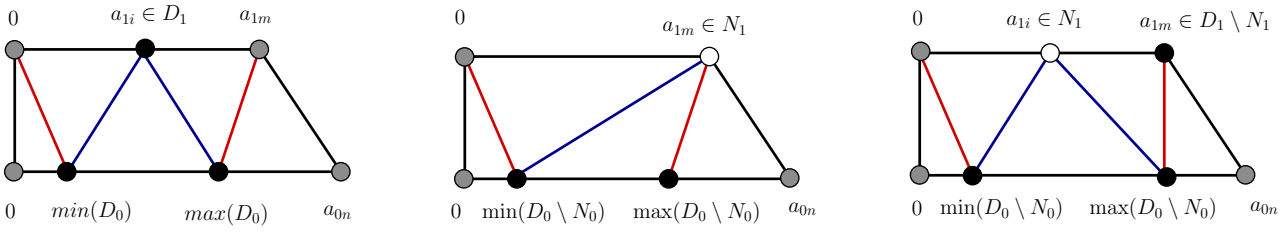

Figure 4.2: The triangulations of C in Thm. 4.1.2 giving vertices $e_1^{max}|_{e_0^{max}}$ and $e_1^{min}|_{e_0^{max}}$; the color of the disks (black, grey, white) indicates membership (belongs, does not belong, may belong, respectively) to D_i or $D_i \setminus N_i$

Theorem 4.1.2 yields a set of eight (not necessarily distinct) possible vertices for $N(\phi)$. Consider the rectangle $ABCD$, with vertices defined by the intersections of lines $e_0 = 0$, $e_0 = a_{1m}$, $e_1 = 0$, and $e_1 = a_{0n}$; in particular, $A = (0,0)$, $B = (0, a_{0n})$, $C = (a_{1m}, a_{0n})$, and $D = (a_{1m}, 0)$. $N(\phi)$ is defined from this rectangle after an appropriate number of corner cuts.

In order to have a cut, a term $\mathcal{X}_A(t) \cdot r$ in the expression of $e_i^{min}|_\epsilon$ yields the condition "$t \in A$ and $r \neq 0$," whereas the same term in the expression of $e_i^{max}|_\epsilon$ yields the condition "$t \notin A$ and $r \neq 0$." Then, the following follows from Theorem 4.1.2:

Corollary 4.1.4. *The conditions for a cut in each of the four corners of $ABCD$ are:*

- cut at A: $(0 \in D_0 \setminus N_0$ *and* $0 \in D_1 \setminus N_1)$ *or* $(a_{0n} \in D_0 \setminus N_0$ *and* $a_{1m} \in D_1 \setminus N_1)$;
- cut at B: $(0 \in D_0$ *and* $0 \in N_1 \setminus D_1)$ *or* $(a_{0n} \in D_0$ *and* $a_{1m} \in N_1 \setminus D_1)$;
- cut at C: $(0 \in N_0 \setminus D_0$ *and* $0 \in N_1 \setminus D_1)$ *or* $(a_{0n} \in N_0 \setminus D_0$ *and* $a_{1m} \in N_1 \setminus D_1)$;
- cut at D: $(0 \in N_0$ *and* $0 \in D_1 \setminus N_1)$ *or* $(a_{0n} \in N_0$ *and* $a_{1m} \in D_1 \setminus N_1)$.

From this corollary and from the fact that if $D_0 = A_0$, then $e_0^{max}|_{e_1^{max}} = e_0^{max}|_{e_1^{max}} = a_{1m}$, we have:

Corollary 4.1.5. *There can be at most two corner cuts in different corners of rectangle $ABCD$, defined by the vertices of Theorem 4.1.2 which do not coincide.*

Now, suppose that there is only one corner cut in rectangle $ABCD$. Then, there may exist an additional vertex of $N(\phi)$ which does not follow from Theorem 4.1.2. We define:

$$\delta_A = \det \begin{bmatrix} a_{0n} - \max(N_0) & a_{1m} - \max(N_1) \\ \min(N_0) & \min(N_1) \end{bmatrix}, \tag{4.4}$$

$$\delta_B = \det \begin{bmatrix} a_{0n} - \max(N_0 \setminus D_0) & a_{1m} - \max(D_1) \\ \min(N_0 \setminus D_0) & \min(D_1) \end{bmatrix}. \tag{4.5}$$

Moreover, δ_C is defined by replacing the sets N_i by the sets D_i in Equation (4.4) and δ_D is defined by replacing the set $N_0 \setminus D_0$ by the set $D_0 \setminus N_0$, and the set D_1 by the set N_1 in Equation (4.5).

Theorem 4.1.6. *Suppose that the vertices of Theorem 4.1.2 yield only one corner cut in rectangle $ABCD$. Then, the implicit polygon is equal to the cut rectangle $ABCD$ unless:*

(i) cut at A: $0, a_{0n} \in D_0 \setminus N_0$ and $0, a_{1m} \in D_1 \setminus N_1$ and $\delta_A \neq 0$, in which case there exists a vertex p s.t.

$$p = (\min(N_1), a_{0n} - \max(N_0)) \text{ if } \delta_A < 0, \text{ and}$$
$$p = (a_{1m} - \max(N_1), \min(N_0)) \text{ if } \delta_A > 0.$$

(ii) cut at B: $0, a_{0n} \in D_0$ and $0, a_{1m} \in N_1 \setminus D_1$ and $\delta_B \neq 0$, in which case there exists a vertex p s.t.

$$p = (\min(D_1), \max(N_0 \setminus D_0)) \text{ if } \delta_B < 0, \text{ and}$$
$$p = (a_{1m} - \max(D_1), a_{0n} - \min(N_0 \setminus D_0)) \text{ if } \delta_B > 0.$$

(iii) cut at C: $0, a_{0n} \in N_0 \setminus D_0$ *and* $0, a_{1m} \in N_1 \setminus D_1$ *and* $\delta_C \neq 0$*, in which case there exists a vertex* p *s.t.*

$$p = (a_{1m} - \min(D_1), \max(D_0)) \text{ if } \delta_C < 0, \quad \text{and}$$
$$p = (\max(D_1), a_{0n} - \min(D_0)) \text{ if } \delta_C > 0.$$

(iv) cut at D: $0, a_{0n} \in N_0$ *and* $0, a_{1m} \in D_1 \setminus N_1$ *and* $\delta_D \neq 0$*, in which case there exists a vertex* p *s.t.*

$$p = (\min(D_0 \setminus N_0), \max(N_1)) \text{ if } \delta_D < 0, \quad \text{and}$$
$$p = (a_{0n} - \max(D_0 \setminus N_0), a_{1m} - \min(N_1)) \text{ if } \delta_D > 0.$$

Proof. We prove only case (ii). The other cases are either similar or symmetric.

Suppose that Theorem 4.1.2 yields a cut in the rectangle $ABCD$, excluding vertex B. Then, Corollary 4.1.4 implies that $0 \in D_0$ and $0 \in N_1 \setminus D_1$, or $a_{0n} \in D_0$ and $a_{1m} \in N_1 \setminus D_1$.

Let us consider the case in which $0 \in D_0$, $0 \in N_1 \setminus D_1$, and ($a_{0n} \notin D_0$ or $a_{1m} \notin N_1 \setminus D_1$ or both). Then, $e_1^{max}|_{e_0^{min}} = a_{0n} - \min(N_0 \setminus D_0)$ and $e_0^{min}|_{e_1^{max}} = \min(D_1)$ yielding the vertices $(0, a_{0n} - \min(N_0 \setminus D_0))$ and $(\min(D_1), a_{0n})$. Suppose, for contradiction, that there exists a triangulation T corresponding to a point $p_T = (x_T, y_T)$ with $x_T < \min(D_1)$ and $y_T > a_{0n} - \min(N_0 \setminus D_0)$. Consider the edges a_{0i}-a_{1j} of T; as these edges do not cross, they can be ordered from left to right. The leftmost edge is 0-0 with $0 \in D_0$ and $0 \in N_1 \setminus D_1$. Let a_{0i}-a_{1j} be the leftmost edge such that either $a_{0i} \notin D_0$ or $a_{1j} \notin N_1 \setminus D_1$; exactly one of these two conditions will hold, since any two consecutive such edges share an endpoint. If $a_{0i} \notin D_0$, then all the points $0, \ldots, a_{1j} \in N_1 \setminus D_1$, and thus no portion of the segment $[0, a_{0i}]$ contributes to the y-coordinate y_t of p_T, i.e., $y_T \leq a_{0n} - a_{0i} \leq a_{0n} - \min(N_0 \setminus D_0)$, a contradiction. Similarly, if $a_{1j} \notin N_1 \setminus D_1$, that is, $a_{1j} \in D_1$, then all the points $0, \ldots, a_{0i} \in D_0$, and thus the entire segment $[0, a_{1j}]$ contributes to the x-coordinate x_t, i.e., $x_T \geq a_{1j} \geq \min(D_1)$, a contradiction again. Therefore, the cut in the rectangle $ABCD$ that excludes vertex B is the only possible one and the implicit polygon equals the polygon defined by the rectangle and the corner cut. The case in which $a_{0n} \in D_0$, $a_{1m} \in N_1 \setminus D_1$, and ($0 \notin D_0$ or $0 \notin N_1 \setminus D_1$ or both) is right-to-left symmetric yielding a similar result.

Finally, we consider the case in which $0, a_{0n} \in D_0$ and $0, a_{1m} \in N_1 \setminus D_1$. Then, $e_1^{max}|_{e_0^{min}} = \max(N_0 \setminus D_0) - \min(N_0 \setminus D_0)$ and $e_0^{min}|_{e_1^{max}} = \min(D_1) + a_{1m} - \max(D_1)$ leading to points $q_1 = (0, \max(N_0 \setminus D_0) - \min(N_0 \setminus D_0))$ and $q_2 = (\min(D_1) + a_{1m} - \max(D_1), a_{0n})$. Consider the points $p_1 = (\min(D_1), \max(N_0 \setminus D_0))$ and $p_2 = (a_{1m} - \max(D_1), a_{0n} - \min(N_0 \setminus D_0))$. It is not difficult to see that one can obtain triangulations corresponding to these points. Points q_1, q_2, p_1, p_2 form a parallelogram which degenerates to a line segment if $\delta_B = 0$; otherwise, p_1 (p_2, resp.) is above the line through q_1, q_2 if $\delta_B < 0$ ($\delta_B > 0$, resp.).

Without loss of generality, assume $\delta_B < 0$. We will show that q_1p_1 is an edge of $N(\phi)$; suppose, for contradiction, that there exists a triangulation T corresponding to a point $p_T = (x_T, y_T)$ which has $x_T < \min(D_1)$, $y_T > \max(N_0 \setminus D_0) - \min(N_0 \setminus D_0)$ and lies above the line through q_1, p_1. Since $0 \in D_0$ and $0 \in N_1 \setminus D_1$, we consider the ordered edges a_{0i}-a_{1j} of T (from left to right) and as above we show that either the entire segment $[0, \min(D_1)]$ contributes to the x-coordinate of p_T or no part of the segment $[0, \min(N_0 \setminus D_0)]$ contributes to its y-coordinate; the former is in contradiction with the fact that $x_T < \min(D_1)$, and thus

the latter case holds. Moreover, by considering the edges a_{0i}-a_{1j} of T from right to left, we can show that either the entire segment $[\max(D_1), a_{1m}]$ contributes to the x-coordinate of p_T or no part of the segment $[\max(N_0 \setminus D_0), a_{0n}]$ contributes to its y-coordinate; the latter case, in conjunction with the latter case of the previous observation, is in contradiction with $y_T > \max(N_0 \setminus D_0) - \min(N_0 \setminus D_0)$, and hence the former case holds. Thus, $x_T \geq a_{1m} - \max(D_1)$ and $y_T \leq a_{0n} - \min(N_0 \setminus D_0)$. For p_T to be above the line through q_1 and p_1, it should hold that

$$\frac{y_T - (\max(N_0 \setminus D_0) - \min(N_0 \setminus D_0))}{x_T} > \frac{\min(N_0 \setminus D_0)}{\min(D_1)};$$

this is not possible because

$$\frac{y_T - (\max(N_0 \setminus D_0) - \min(N_0 \setminus D_0))}{x_T} \leq \frac{a_{0n} - \max(N_0 \setminus D_0)}{a_{1m} - \max(D_1)}$$

$$\text{and} \quad \delta_B < 0 \quad \Rightarrow \quad \frac{a_{0n} - \max(N_0 \setminus D_0)}{a_{1m} - \max(D_1)} < \frac{\min(N_0 \setminus D_0)}{\min(D_1)}.$$

Therefore, the segment q_1p_1 is an edge of $N(\phi)$. For $\delta_B < 0$, in a similar fashion we can show that the segment q_2p_1 is also an edge of $N(\phi)$. The cases for $\delta_B > 0$ are symmetric involving point p_2. □

Example 4.1.7.

$$x = \frac{a + t^2}{ct},\ y = \frac{b}{dt}, \quad a, b, c, d \neq 0.$$

With generic coefficients, the denominators are different. The input supports are $N_0 = \{0, 2\},\ N_1 = \{0\},\ D_0 = D_1 = \{1\}$. Theorem 4.1.2 yields points $(1, 1)$, $(1, 1)$, $(0, 2)$, $(0, 2)$, $(0, 2)$, $(0, 0)$, $(0, 0)$, $(0, 0)$, in the order stated by the theorem, which define the actual implicit polygon since $\phi = ad^2y^2 - bcdxy + b^2$.

Example 4.1.8.

$$x = \frac{t^7 + t^4 + t^3 + t^2}{t^3 + 1},\ y = \frac{t^5 + t^4 + t}{t^5 + t^2 + 1}.$$

The input supports are $N_0 = \{2, 3, 4, 7\},\ N_1 = \{1, 4, 5\},\ D_0 = \{0, 3\}$ and $D_1 = \{0, 2, 5\}$. Theorem 4.1.2 yields points $(5, 7), (5, 0), (5, 7), (0, 7), (0, 7), (0, 2),\ (5, 0), (1, 0)$ in the order stated by the theorem. These points define the actual implicit polygon.

Example 4.1.9. For the unit circle, $x = 2t/(t^2+1),\ y = (1-t^2)/(t^2+1)$, the supports are $N_0 = \{1\},\ D_0 = \{0, 2\}$, and $N_1 = D_1 = \{0, 2\}$. The set $C = \kappa(A_0, A_1)$ has 5 triangulations shown in Figure 4.3 which, after applying Proposition 1.1.10, give the terms $y^2 - 1,\ x^2y^2 - 2x^2y + x^2$ and $x^2y^2+2x^2y+x^2$. This method yields points $(2, 2), (2, 0), (0, 2), (0, 0)$. By degree bounds, we end up with vertices $(2, 0), (0, 2), (0, 0)$. Interestingly, to see the cancellation of term x^2y^2 it does not suffice to consider only terms coming from extremal monomials in the resultant. See Example 4.2.18 for a treatment taking into account the identical denominators.

Example 4.1.10. Consider the parameterization

$$x = \frac{t^3 + 2t^2 + t}{t^2 + 3t - 2},\ y = \frac{t^3 - t^2}{t - 2}.$$

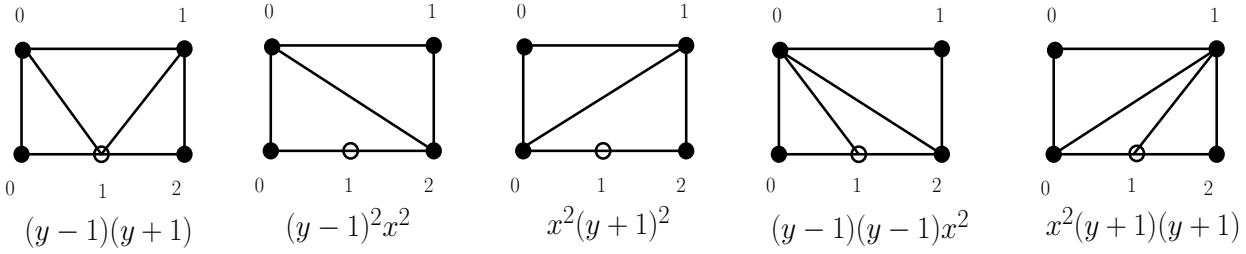

Figure 4.3: The triangulations of C in Example 4.1.9, and the corresponding terms

The supports are $N_0 = \{1, 2, 3\}$, $D_0 = \{0, 1, 2\}$, and $N_1 = \{2, 3\}, D_1 = \{0, 1\}$. Theorem 4.1.2 yields points $(3, 2), (3, 0), (1, 3), (0, 3), (0, 3), (0, 1), (3, 0), (2, 0)$, in the order stated by the theorem, which define the actual implicit polygon. The implicit polygon is shown in Figure 4.1, right.

4.2 Rational parameterizations with equal denominators

We study rationally parameterized planar curves, when both denominators are the same.

$$x = \frac{P_0(t)}{Q(t)},\ y = \frac{P_1(t)}{Q(t)},\quad \gcd(P_i(t), Q(t)) = 1,\ P_i, Q \in \mathbb{C}[t],\ i = 0, 1, \tag{4.6}$$

where the P_i, Q have fixed supports and generic coefficients. If some $P_i(t), Q(t)$ have a nontrivial GCD, then common terms are divided out and the problem reduces to the case of different denominators. In general, the P_i, Q are Laurent polynomials, but this case can be reduced to the case of polynomials by shifting the supports.

The results of this section are useful if the two parametric expressions have the same numerator and different denominators. Then, we consider implicit variables x^{-1}, y^{-1}, compute the implicit polygon, and transform it so as to yield the implicit polygon of the original problem. Similarly, if the numerator of one parametric expression equals the denominator of the other, then we can again apply the tools of this section.

Considering the more general case of different denominators does not lead to optimal implicit support, because this does not exploit the fact that the coefficients of $Q(t)$ are the same in the polynomials $xQ - P_0, yQ - P_1$. Therefore, we introduce a new variable r and consider the following system

$$f_0 = xr - P_0(t),\ f_1 = yr - P_1(t),\ f_2 = r - Q(t) \in \mathbb{C}[t, r]. \tag{4.7}$$

By eliminating t, r the resultant gives, for generic coefficients, the implicit equation in x, y. Consider the parameterization

$$\tau : \mathbb{P} \to \mathbb{P}^2 : (t : t_0) \mapsto (x_0 : x_1 : x_2) = (P_0^h : P_1^h : Q^h), \tag{4.8}$$

where P_0^h, P_1^h, Q^h are the homogenizations of P_0, P_1, Q. The resultant of polynomials defined by equations (4.8) is homogeneous in x_0, x_1, x_2 and generically equals the implicit

equation $\Phi \in \mathbb{C}[x_0, x_1, x_2]$ of parameterization τ. The resultant of polynomials (4.7) is the de-homogenization of Φ. Let the input supports be

$$B_i = \mathcal{A}(P_i), i = 0, 1,\ B_2 = \mathcal{A}(Q),\ \text{where } B_i = \{b_{iL}, \ldots, b_{iR}\}, i = 0, 1, 2,$$

where indices L, R denote the leftmost and rightmost points respectively, i.e., $b_{iL},\ b_{iR}$ are the minimum and maximum points respectively in B_i. The supports of the f_i are

$$A_0 = \{a_{00}, a_{0L}, \ldots, a_{0R}\}, A_1 = \{a_{10}, a_{1L}, \ldots, a_{1R}\}, A_2 = \{a_{20}, a_{2L}, \ldots, a_{2R}\} \in \mathbb{N}^2,$$

where

- each point $a_{i0} = (0, 1)$, for $i = 0, 1, 2$, corresponds to the unique term in f_i which depends on r,
- each other point a_{it}, for $t \neq 0$, is of the form $(b_{it}, 0)$, for one $b_{it} \in B_i$.

One could think that index $L = 1$ whereas each R equals the cardinality of the respective B_i. By the above hypotheses A_2 or both A_0, A_1 contain $(0, 0)$.

Lemma 4.2.1. *$MV_{\mathbb{R}}(B_i \cup B_j) = MV_{\mathbb{R}^2}(A_i, A_j),\ i, j \in \{0, 1, 2\}$, where $MV_{\mathbb{R}^d}$ denotes mixed volume in $\mathbb{R}^d$.*

Proof. Let $\mathrm{CH}(B_i) = [m_i, l_i]$, $\mathrm{CH}(B_j) = [m_j, l_j]$ be intervals in $\mathbb{N}$. If $m_i \leq m_j$ and $l_i \leq l_j$, then $\mathrm{MV}_{\mathbb{R}}(B_i \cup B_j) = l_j - m_i$. Consider a mixed subdivision of $A_i + A_j$, with unique mixed cell $((0, 1), (m_i, 0)) + ((0, 1), (l_j, 0))$, hence $\mathrm{MV}_{\mathbb{R}^2}(A_i, A_j) = l_j - m_i$. If $m_i \leq m_j \leq l_j \leq l_i$, then $\mathrm{MV}_{\mathbb{R}}(B_i \cup B_j) = l_i - m_i$, and a similar subdivision as above yields a unique mixed cell with this volume. The rest of the cases are symmetric. □

In what follows, we shall make use of integer $u = \max\{b_{0R}, b_{1R}, b_{2R}\}$.

Let $C_i = \mathrm{CH}(A_i)$ and consider the mixed subdivisions of $C = C_0 + C_1 + C_2$. The following points lie on the boundary of C: $(u, 2), (0, 3), (0, 2), (b_{0L} + b_{1L} + b_{2L}, 0)$ and $(b_{0R} + b_{1R} + b_{2R}, 0)$.

The vertices e_0, e_1, e_2 of implicit Newton polytope $N(\Phi)$ correspond to monomials in x_0, x_1, x_2; the power of each x_i is determined by the volumes of a_{i0}-mixed (or simply i-mixed) cells, for $i = 0, 1, 2$. This leads us to computing mixed subdivisions of three polygons in the plane.

Lemma 4.2.2. [Cell types] *In any mixed subdivision of C, the i-mixed cells, with vertex summand a_{i0}, for some $i \in \{0, 1, 2\}$, have an edge summand $(a_{j0}, a_{jh}),\ i \neq j,\ h > 0$. Their second edge summand is from B_l, where $\{i, j, l\} = \{0, 1, 2\}$ and classifies the i-mixed cells in two types:*
(I) If it is (a_{l0}, a_{lm}), where $a_{lm} = (b_{lm}, 0)$, then the cell vertices are $(0, 3)$, $(b_{jh}, 2)$, $(b_{lm}, 2)$, $(b_{jh} + b_{lm}, 1)$, provided $b_{jh} \neq b_{lm}$.
(II) If it is (a_{lt}, a_{lm}), where $a_{lt} = (b_{lt}, 0), a_{lm} = (b_{lm}, 0)$, then the cell vertices are $(b_{lt}, 2)$, $(b_{lm}, 2)$, $(b_{jh} + b_{lt}, 1), (b_{jh} + b_{lm}, 1)$.

Proof. Any mixed cell has two non-parallel edge summands, hence one of the edges is (a_{j0}, a_{jh}) for some $i \neq j,\ h > 0$. The rest of the statements follow from the definition of a mixed subdivision. □

Observe that for every type-II cell, there is a non-mixed cell with vertices $(0,3), (b_{lt},2), (b_{lm},2)$.

Example 4.2.3. We consider the folium of Descartes:

$$x = \frac{3t^2}{1+t^3}, y = \frac{3t}{1+t^3} \Rightarrow \phi = x^3 + y^3 - 3xy = 0.$$

Now $f_0 = xr - 3t^2, f_1 = yr - 3t, f_2 = r - (t^3+1)$. Figure 4.4 shows the Newton polygons, C and two mixed subdivisions. The shaded triangle is the only unmixed cell with nonzero area; it is a copy of C_2. The first subdivision shows two cells of type I, of area 1 and 2, which yield factors x and y^2 respectively, to give term xy^2. The second subdivision has one cell of type II and area 3, which yields term x^3. We shall obtain an optimal support in example 4.2.19. Now, $u = 3$ which equals the total degree of ϕ.

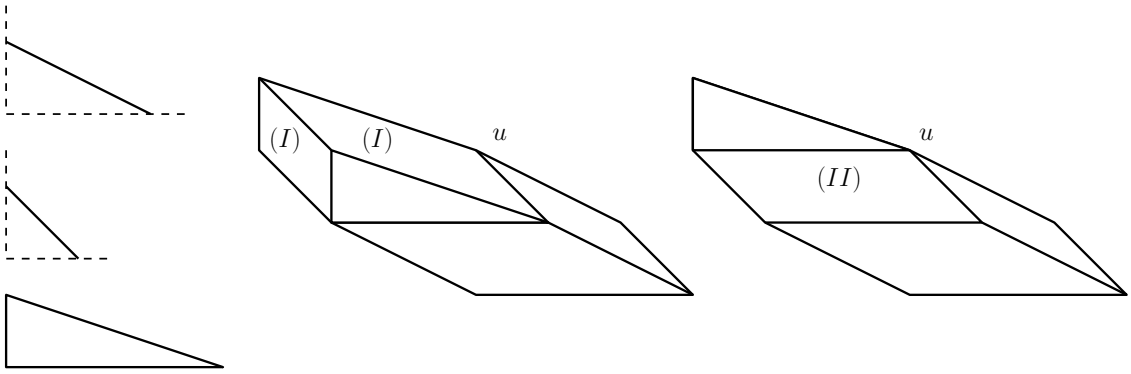

Figure 4.4: Example 4.2.3: polygons C_i, and two mixed subdivisions of C

Consider segment E defined by vertices $(0,2), (u,2)$ in C.

Lemma 4.2.4. *The resultant of the f_i's $\in \mathbb{C}[t,r]$ defined by equations (4.7) is homogeneous, of degree u, w.r.t. the coefficients of the a_{i0}, for $i = 0,1,2$.*

Proof. Consider any mixed subdivision of C and the cells of type I and II. Consider these cells as closed polygons: We claim that their union contains segment E. Then, it is easy to see that the total volume of these cells equals u.

Consider the closed cells that intersect E. If the intersection lies in the cell interior, then it is a parallelogram, hence it is mixed and its vertex summand is $(0,1)$, thus it is of type I. If the intersection is a cell edge, say (a_{kl}, a_{km}), for $k \in \{0,1,2\}$ and $1 \leq l < m$, then the cell above E is unmixed, namely a triangle with basis (a_{kl}, a_{km}) and apex at $(0,3)$. In this case, the cell below E is mixed of type II. □

Generically, u equals the total degree of every term in the implicit equation $\phi(x,y)$ w.r.t. x, y and the coefficient of r in f_2. The degree of $\Phi(x_0,x_1,x_2)$ is u.

In the following, we focus on segment E and subsegments defined by points $(b_{it},2) \in L, i \in \{0,1,2\}$. Usually, we shall omit the ordinate, so the corresponding segments will be denoted by $[b_{jt}, b_{kl}]$. We say that such a segment contributes to some coordinate e_i when a i-mixed cell of the mixed subdivision contains this segment. Moreover,

- a type-I, i-mixed cell $a_{i0} + (a_{j0}, a_{jt}) + (a_{k0}, a_{kl})$ is identified with segment $[b_{jt}, b_{kl}]$.

- a type-II, i-mixed cell $a_{i0} + (a_{jt}, a_{js}) + (a_{k0}, a_{kl})$ is identified with segment $[b_{jt}, b_{js}]$ and the coordinate e_i to which it contributes.

We show that one needs to examine only subsegments defined by endpoints $b_{iL}, b_{iR} \in B_i$. This is equivalent to saying that it suffices to consider mixed subdivisions induced by linear liftings.

Theorem 4.2.5. *Let S be a mixed subdivision of $C_0 + C_1 + C_2$, where an internal point $b_i \in B_i$ defines a 0-dimensional face $(b_i, 2) = (b_i, 0) + (0, 1) + (0, 1) \in L$. Then, the point of $N(\phi)$ obtained by S cannot be a vertex because it is a convex combination of points obtained by other mixed subdivisions defined by points of B_0, B_1, B_2 which are either endpoints, or are used in defining S except from $(b_i, 2)$.*

The theorem is established by Lemmas 4.2.6, 4.2.7 and 4.2.8. We shall construct mixed subdivisions that yield points in the $e_k e_j$-plane whose convex hull contains the initial point. All cells of the original subdivision which are not mentioned are taken to be fixed, therefore we can ignore their contribution to e_k, e_j. All convex combinations in these lemmas are decided by the 3×3 orientation determinant (cf. Expression (4.10)).

Lemma 4.2.6. [II-II] *Consider the setting of Theorem 4.2.5 and suppose that $(b_i, 2)$ is a vertex of two adjacent type II cells. Then, the theorem follows.*

Proof. If both cells are j-mixed, then the same point in $e_k e_j$-plane is obtained by one j-mixed cell equal to their union, $\{i, j, k\} = \{0, 1, 2\}$. If the cells are j- and k-mixed, then there are two mixed subdivisions yielding points in the $e_k e_j$-plane, which define a segment that contains the initial point. The subdivisions have one j-mixed or one k-mixed cell respectively, intersecting the entire subsegment. □

Lemma 4.2.7. [I-I] *Consider the setting of Theorem 4.2.5 and suppose that $(b_i, 2)$ is a vertex of two adjacent type I cells. Without loss of generality, these are k- and j-mixed cells, $\{i, j, k\} = \{0, 1, 2\}$. Then, the theorem follows.*

Proof. Let $[b_{jl}, b_i], [b_i, b_{kt}]$ be the subsegments defined on E by the two mixed cells, and let α, β be their respective lengths. Since b_i is internal, b_{iR} lies to its right-hand side and b_{iL} lies to its left-hand side.

Case $b_{iR} < b_{kt}$ and $b_{iL} > b_{jl}$. Let $\gamma = b_i - b_{iL}$ and $\delta = b_{iR} - b_i$. The initial point (α, β) shall be enclosed by two points. The mixed subdivision with type-I cells corresponding to $[b_{jl}, b_{iR}]$ and $[b_{iR}, b_{kt}]$ yields point $(\alpha + \delta, \beta - \delta)$. The subdivision with type-I cells corresponding to $[b_{jl}, b_{iL}], [b_{iL}, b_{kt}]$ yields point $(\alpha - \gamma, \beta + \gamma)$.

Case $b_{iR} < b_{kt}$ and $b_{iL} < b_{jl}$. Let $\gamma = b_{jl} - b_{iL}$ and $\delta = b_{iR} - b_i < \beta$. The initial point is $(\alpha + v_k, \beta + v_j)$, where $v_k, v_j \geq 0$ is the contribution to e_k, e_j respectively from subsegment $[b_{iL}, b_{jl}]$, and $v_k + v_j \leq \gamma$. Now consider 3 mixed subdivisions on $[b_{iL}, b_{kt}]$: The first containing the type-II k-mixed cell $[b_{iL}, b_{iR}]$ and the type-I j-mixed cell $[b_{iR}, b_{kt}]$ gives point $(\alpha + \gamma + \delta, \beta - \delta)$. The second containing the type-I j-mixed cell $[b_{iL}, b_{kt}]$ gives point $(0, \alpha + \beta + \gamma)$. The third containing the type-I i-mixed cell $[b_{jl}, b_{kt}]$ and the initial cells in $[b_{iL}, b_{jl}]$, gives (v_k, v_j).

Case $b_{iR} > b_{kt}$ and $b_{iL} > b_{jl}$. Let $\gamma = b_i - b_{iL} < \alpha$ and $\delta = b_{iR} - b_{kt}$. The initial point is $(\alpha + v_k, \beta + v_j)$, where $v_k, v_j \geq 0$ is the contribution to e_k, e_j respectively from $[b_{kt}, b_{iR}]$,

and $v_k + v_j \leq \delta$. Now consider 3 mixed subdivisions on $[b_{jl}, b_{iR}]$: The first containing the type-I i-mixed cell $[b_{jl}, b_{kt}]$ and the initial cells in $[b_{kt}, b_{iR}]$, gives point (v_k, v_j). The second containing the type-I k-mixed cell $[b_{jl}, b_{iR}]$, gives point $(\alpha + \beta + \delta, 0)$. The third containing the type-I k-mixed cell $[b_{jl}, b_{iL}]$ and the type-II j-mixed cell $[b_{iL}, b_{iR}]$, gives $(\alpha - \gamma, \beta + \gamma + \delta)$.

Case $b_{iR} > b_{kt}$ and $b_{iL} < b_{jl}$. Let $\gamma = b_{jl} - b_{iL}$ and $\delta = b_{iR} - b_{kt}$. The initial point is $(\alpha+v_k+u_k, \beta+v_j+u_j)$, where $v_k, v_j \geq 0$ is the contribution to e_k, e_j respectively from $[b_{kt}, b_{iR}]$, and $v_k + v_j \leq \delta$. Similarly, $u_k, u_j \geq 0$ is the contribution to e_k, e_j respectively from $[b_{iL}, b_{jl}]$, and $u_k + u_j \leq \gamma$. Now consider 3 mixed subdivisions on $[b_{iL}, b_{iR}]$: The first containing the type-II k-mixed cell $[b_{iL}, b_{iR}]$, gives point $(\alpha+\beta+\gamma+\delta, 0)$. The second containing the type-II j-mixed cell $[b_{iL}, b_{iR}]$, gives point $(0, \alpha + \beta + \gamma + \delta)$. The third containing the type-I i-mixed cell $[b_{jl}, b_{kt}]$ and the initial cells in $[b_{iL}, b_{jl}]$ and $[b_{kt}, b_{iR}]$, gives point $(v_k + u_k, v_j + u_j)$.

□

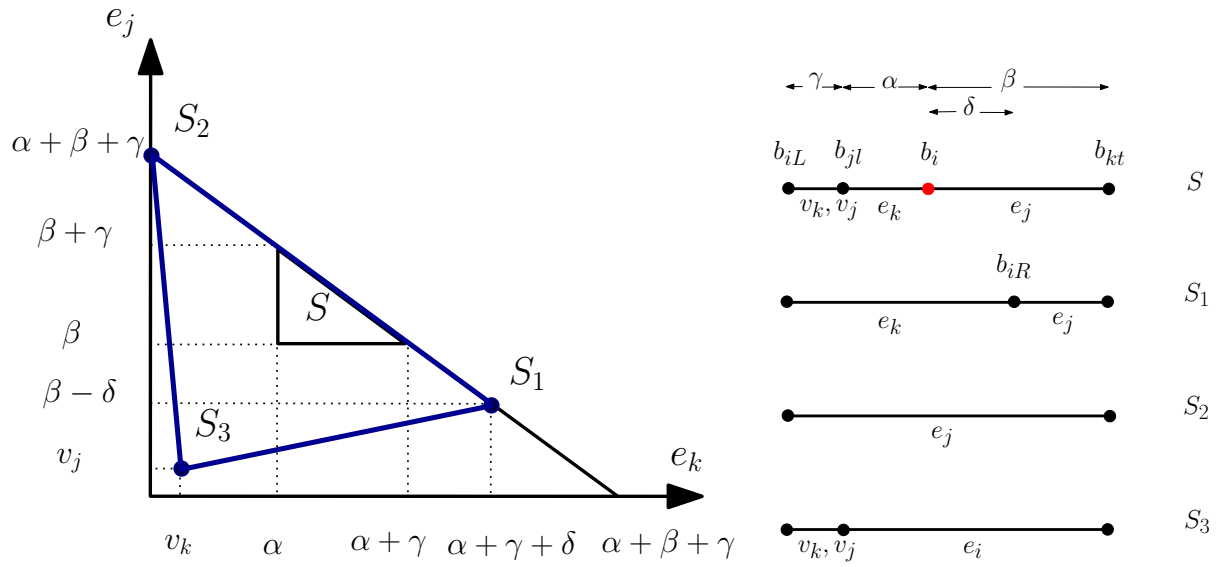

Figure 4.5: The three points that enclose the point given by S and the corresponding mixed subdivisions for the second case of Lem. 4.2.7

Lemma 4.2.8. [I-II] *Consider the setting of Theorem 4.2.5 and suppose that* $(b_i, 2)$ *is a vertex of two adjacent type II and I cells. Without loss of generality, these are* k- *and* j-*mixed cells,* $\{i, j, k\} = \{0, 1, 2\}$. *Then, the theorem follows.*

Proof. Let $[b_{il}, b_i], [b_i, b_{kt}]$ be the subsegments defined on E by the two mixed cells, and let α, β be their respective lengths. Since b_i is internal, b_{iR} lies to its right-hand side. Moreover, the initial k-mixed cell implies the existence of 1-dimensional face $(b_i, 2) + a_{k0} + E_{jl}$, for some edge $E_{jl} = (a_{j0}, a_{jl}) \subset B_j$. The initial j-mixed cell implies the existence of 1-face $(b_i, 2) + a_{j0} + E_{kt}$, for edge $E_{kt} = (a_{k0}, a_{kt}) \subset B_k$. The second 1-face cannot be to the left of the first one, hence $b_{jl} \leq b_{kt}$. Hence, $b_{jL} \leq b_{kt}$.

Case $b_{iR} \leq b_{kt}$. The initial point (α, β) shall be enclosed by two points. The mixed subdivision with type-I cell $[b_{il}, b_{kt}]$ yields point $(0, \alpha + \beta)$. The subdivision with type-II and type-I cells corresponding to $[b_{il}, b_{iR}], [b_{iR}, b_{kt}]$ sets $e_k > \alpha, e_j < \beta$, where $e_k + e_j = \alpha + \beta$.

Case $b_{iR} > b_{kt}$ and $b_{jL} > b_{il}$. Consider subsegment $[b_{il}, b_{iR}]$: the initial point is $(\alpha+v_k, \beta+v_j)$, where $v_k, v_j \geq 0$ is the contribution to e_k, e_j respectively from subsegment $[b_{kt}, b_{iR}]$, and $v_k + v_j \leq \gamma = b_{iR} - b_{kt}$. Now consider 3 mixed subdivisions on $[b_{il}, b_{iR}]$: One k-mixed cell $[b_{il}, b_{iR}]$ gives point $(\alpha+\beta+\gamma, 0)$. One j-mixed cell $[b_{il}, b_{kt}]$ and the initial cells in $[b_{kt}, b_{iR}]$ give $(v_k, \alpha+\beta+v_j)$. One k-mixed cell $[b_{il}, b_{jL}]$, one i-mixed cell $[b_{jL}, b_{kt}]$ and the initial cells in $[b_{kt}, b_{iR}]$ give (e_k+v_k, v_j), for some $e_k \leq \alpha+\beta$.

Case $b_{iR} > b_{kt}$ and $b_{jL} \leq b_{il}$ is established analogously to the previous ones. □

In the next lemma and corollary, we shall determine certain points in $N(\Phi)$. We shall later see that among these points lie the vertices of $N(\Phi)$ and, therefore, from these points we can recover the vertices of $N(\phi)$. Recall that $\mathrm{MV}_i = \mathrm{MV}_{\mathbb{R}^2}(A_j, A_k)$, where $\{i,j,k\} = \{0,1,2\}$.

Lemma 4.2.9. *Given supports B_0, B_1, B_2, let $b_{tL} = \min\{b_{iL}, b_{jL}\}$, $b_{mR} = \max\{b_{iR}, b_{jR}\}$ and $\Delta = [b_{tL}, b_{mR}]$, for $i \neq j \in \{0,1,2\}$ and $t, m \in \{i,j\}$ not necessarily distinct. Set $e_\lambda = |\Delta|$, where $\lambda \in \{0,1,2\} \setminus \{i,j\}$, and $e_i = e_j = 0$. Then, add b_{tL} to e_τ, where $\tau \in \{i,j\} \setminus \{t\}$, and add $u - b_{mR}$ to e_μ, where $\mu \in \{i,j\} \setminus \{m\}$. Then, (e_0, e_1, e_2) is a vertex of $N(\Phi)$.*

Proof. Clearly $\Delta = \mathrm{CH}(B_i \cup B_j) \subseteq [0,u]$, so $\mathrm{MV}_\lambda = |\Delta|$. It is possible to construct a mixed subdivision that yields the implicit vertex. If $t \neq m$, then the mixed subdivision contains a type-I mixed cell $(a_{t0}, a_{tL}) + (a_{m0}, a_{mR_m}) + a_{\lambda 0}$ which intersects segment E at subsegment $[b_{tL}, b_{mR}]$. This contributes $\mathrm{MV}_\lambda = b_{mR} - b_{tL}$ to e_λ. There is a type-I cell $(a_{\lambda 0}, a_{\lambda L}) + (a_{t0}, a_{tL}) + a_{\tau 0}$ which intersects E at subsegment $[0, b_{tL}]$. This contributes b_{tL} to e_τ. Similarly, we assign the area $u - b_{mR}$ of the type-I cell $(a_{\lambda 0}, a_{\lambda R}) + (a_{m0}, a_{mR_m}) + a_{\mu 0}$ to e_μ.

If $t = m$, then Δ is an edge of one of the initial Newton segments, say B_t, and $\Delta = [b_{tL}, b_{tR}]$. The mixed subdivision contains the type-II mixed cell $(a_{\tau 0}, a_{\tau L}) + (a_{tL}, a_{tR}) + a_{\lambda 0}$ which contributes $\mathrm{MV}_\lambda = |\Delta| = b_{tR} - b_{tL}$ to e_λ. There are also two type-I cells intersecting E at its leftmost and rightmost subsegments, as in the previous case. Since $t = m$, we have $\mu = \tau$, hence $e_t = 0$.

The type-I mixed cells in any of the above mixed subdivisions vanish when $b_{tL} = 0$ or $b_{mR} = u$. Notice that $e_i + e_j + e_\lambda = u$ and since e_λ is maximized, (e_0, e_1, e_2) defines a vertex of $N(\Phi) \subset \mathbb{R}^3$. □

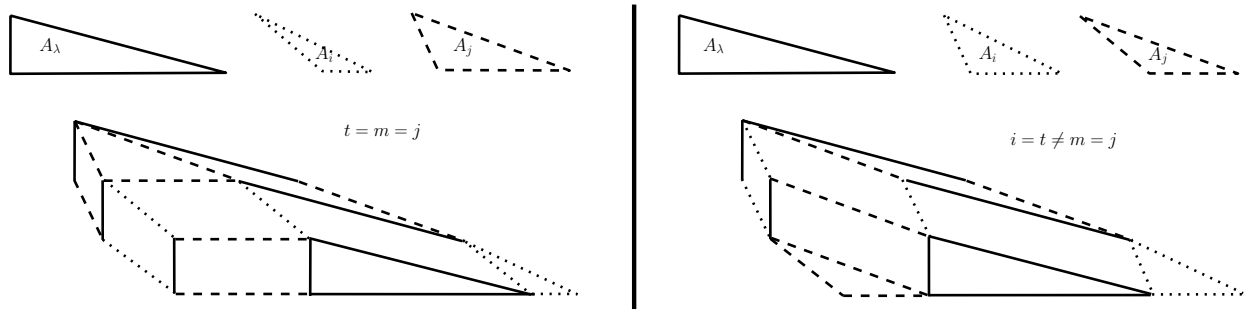

Figure 4.6: Lemma 4.2.9: the mixed subdivisions for a certain choice of B_i's and cases $t = m$ and $t \neq m$

The following corollary is proven similarly.

Corollary 4.2.10. *Under the notation of Lemma 4.2.9 consider the following definition:*

1. $b_{tL} = \min\{b_{iL}, b_{jL}\},\ b_{mR} = \min\{b_{iR}, b_{jR}\}$, *provided that* $b_{\lambda R} = u$.
2. $b_{tL} = \max\{b_{iL}, b_{jL}\},\ b_{mR} = \max\{b_{iR}, b_{jR}\}$, *provided that* $b_{\lambda L} = 0$.
3. $b_{tL} = \max\{b_{iL}, b_{jL}\},\ b_{mR} = \min\{b_{iR}, b_{jR}\}$, *provided that* $b_{tL} \leq b_{mR}$, $b_{\lambda R} = u$ *and* $b_{\lambda L} = 0$.

Let $\Delta = [\delta_{tL}, \delta_{mR}]$ *and in each case, define integers* e_0, e_1, e_2 *as in Lemma 4.2.9. Then,* (e_0, e_1, e_2) *is a vertex of* $N(\Phi)$.

4.2.1 The implicit vertices

Overall, there are three cases for the relative positions of the B_i:

1. $\mathrm{CH}(B_i \cup B_j) = [0, u]$ for all pairs i, j.
2. $\mathrm{CH}(B_j \cup B_l) = \mathrm{CH}(B_i \cup B_l) = [0, u] \neq \mathrm{CH}(B_i \cup B_j)$.
3. $\mathrm{CH}(B_i \cup B_j) = [0, u] \neq \mathrm{CH}(B_l \cup B_t)$ for $t = i, j$.

Orthogonally, we can distinguish the following two cases:
(A) there exists at least one $\mathrm{CH}(B_i) = [0, u]$,
(B) none of the B_i's satisfies $\mathrm{CH}(B_i) = [0, u]$.

In case (B), every union $B_i \cup B_j$ contains either 0 or u. Cases (1B) and (3A) cannot exist, which leaves four cases overall. In the sequel, we let E_{it} denote a segment $(a_{i0}, a_{it}) \subset B_i$.

Theorem 4.2.11. [case (A)] *Recall that* $u = \max\{b_{0R}, b_{1R}, b_{2R}\}$. *If all unions* $CH(B_i \cup B_j) = [0, u], i \neq j$, *then the implicit polygon* $N(\phi)$ *is a triangle with vertices* $(0, 0)$, $(0, u)$, $(u, 0)$. *Otherwise, if exactly one support, say* B_k, $k \in \{0, 1, 2\}$, *equals* $[0, u]$, *then* $N(\phi)$ *has up to five vertices* (e_0, e_1) *which can be read of from the following set of* (e_i, e_j, e_k) *vectors:*

$$\{((u, 0, 0), (0, u, 0), (0, u - b_{iR} + b_{iL}, b_{iR} - b_{iL}), (b_{jL}, u - b_{iR}, 0),\\ (u - b_{jR} + b_{jL}, 0, b_{jR} - b_{jL})\},$$

where $\{i, j, k\} = \{0, 1, 2\}$, *assuming* i, j *are chosen so that*

$$b_{iL}(u - b_{jR}) \geq b_{jL}(u - b_{iR}). \tag{4.9}$$

Proof. First is the case (1A), established by Lemma 4.2.9. The second statement concerns case (2A): By switching i and j, assumption (4.9) can always be satisfied. Unless $B_i \subset B_j$ or $B_j \subset B_i$, this assumption holds simply by choosing i, j so that $b_{jL} \leq b_{iL}$.

The vertices $(u, 0, 0), (0, u, 0)$ are obtained by Lemma 4.2.9, applied to $\mathrm{CH}(B_j \cup B_k)$ and $\mathrm{CH}(B_i \cup B_k)$ respectively. The third point is obtained by a mixed subdivision with two type-I cells $E_{iL} + a_{j0} + E_{kL}, E_{iR} + a_{j0} + E_{kR}$, which contribute the lengths of $[b_{kL}, b_{iL}], [b_{iR}, b_{kR}]$ to e_j, and one type-II cell $E_{i0} + E_{jt} + a_{k0}$, contributing the length of $[b_{iL}, b_{iR}]$ to e_k, where E_{i0} is the horizontal edge of A_i and $t \in \{L, R\}$; see Figure 4.7. By switching i and j we define a subdivision that yields the fifth point.

The fourth point is obtained by a subdivision with 3 type-I cells: $a_{i0} + E_{jL} + E_{kL}, E_{iR} + a_{j0} + E_{kR}$ and $E_{iR} + E_{jL} + a_{k0}$, which contribute to e_i, e_j and e_k respectively, see Figure 4.7.

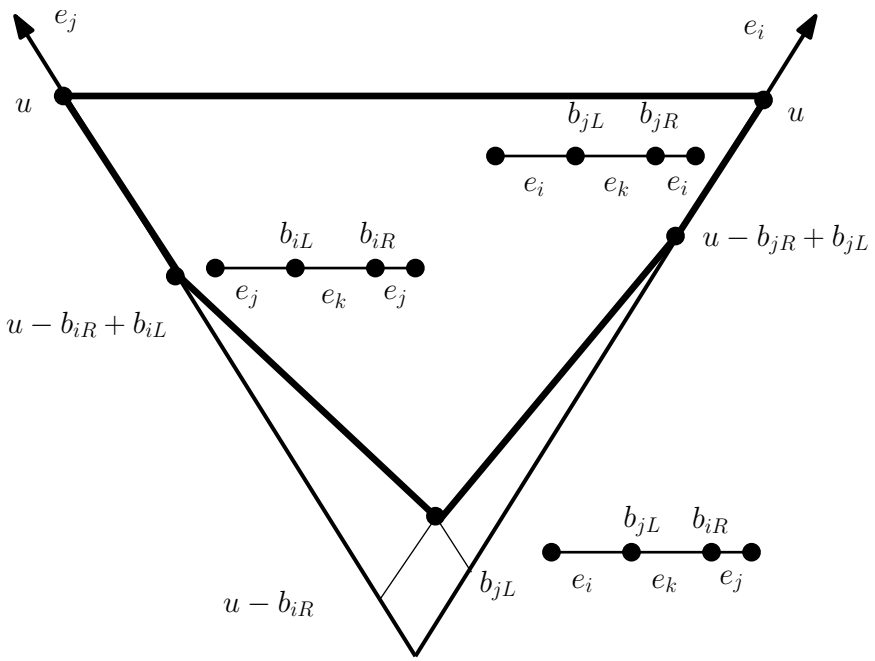

Figure 4.7: The implicit polygon in case (2A), in the $e_i e_j$-plane, and the subdivisions of the proof of Thm. 4.2.11

It suffices to show that the line defined by this and the third point supports the implicit polygon. An analogous proof then shows that the line defined by this and the fifth point also supports the polygon, and the theorem follows. Our claim is equivalent to showing

$$\det \begin{bmatrix} b_{jR} & u - b_{iR} & 1 \\ 0 & u - b_{iR} + b_{iL} & 1 \\ e_i & e_j & 1 \end{bmatrix} \leq 0 \Leftrightarrow b_{iL}(e_i - b_{jL}) \geq b_{jL}(u - b_{iR} - e_j). \tag{4.10}$$

We consider the rightmost subsegment on E, where one endpoint is $b_{kR} = u$. This contributes to either e_i or e_j an amount equal to the length of a subsegment extending at least as far left as b_{jR} or b_{iR}, respectively. Symmetrically, the leftmost subsegment has endpoint $b_{kL} = 0$ and contributes to e_i or e_j the length of a subsegment extending at least as far right as b_{jL} or b_{iL}, respectively. In general, there are four cases, depending on the contribution of the rightmost and leftmost subsegments. The last case is infeasible if B_i, B_j have no overlap.

If the rightmost subsegment contributes to e_j then $e_j \geq u - b_{iR}$. If the leftmost subsegment contributes to e_j then this contribution is at least b_{iL}, hence $e_j \geq u - b_{iR} + b_{iL}$, where $e_i \geq 0$. Otherwise, the leftmost subsegment contributes to e_i, thus $e_i \geq b_{jL}$. In both cases, inequality (4.10) follows.

If the rightmost subsegment contributes to e_i then $e_i \geq u - b_{jR}$. If the leftmost subsegment also contributes to e_i, then $e_i \geq u - b_{jR} + b_{jL}$. Using also $e_j \geq 0$, it suffices to prove $b_{iL}(u - b_{jR}) \geq b_{jL}(u - b_{iR})$. Otherwise, the leftmost subsegment contributes to e_j, so $e_j \geq b_{iL}$, and it suffices to prove $b_{iL}(u - b_{jR} - b_{jL}) \geq b_{jL}(u - b_{iR} - b_{iL})$. Both sufficient conditions are equivalent to assumption (4.9). □

Theorem 4.2.12. [case (B)] *Recall that* $u = \max\{b_{0R}, b_{1R}, b_{2R}\}$. *If none of the* B_t*'s is equal to* $[0, u]$, *then we may choose* $\{i, j, k\} = \{0, 1, 2\}$ *such that:*

$$0 < b_{iL} \leq b_{iR} = u,\ 0 = b_{jL} \leq b_{jR} < u,\ 0 \leq b_{kL} \leq b_{kR} \leq u,\ B_k \neq [0, u].$$

Then, $N(\phi)$ *has at most 5 or 4 vertices, depending on whether* b_{kL} *is positive or 0. In the former case, the vertices* (e_0, e_1) *can be read of from the following set of* (e_i, e_j, e_k) *vectors:*

$$\{(b_{jR}, 0, u - b_{jR}), (b_{kR}, u - b_{kR}, 0), (b_{kL}, u - b_{kL}, 0), (0, u - b_{iL}, b_{iL}), (0, 0, u), \}$$

and, in the latter case, the third and fourth vertices are replaced by $(0, u, 0)$.

By Lemma 4.2.4, at every point $e_k = u - e_i - e_j$. The theorem is established by the following two lemmas.

Lemma 4.2.13. [case (2B)] *Suppose* $b_{kL} = 0$ *in Theorem 4.2.12 and w.l.o.g. assume* $b_{jR} \leq b_{kR}$. *Then,* $N(\phi)$ *has up to 4 vertices* (e_0, e_1) *which can be read of from the following set of* (e_i, e_j, e_k) *vectors:*

$$\{(b_{jR}, 0, u - b_{jR}), (b_{kR}, u - b_{kR}, 0), (0, u, 0), (0, 0, u)\}.$$

Proof. The last two vertices follow from Lemma 4.2.9, applied to B_i, B_k and B_i, B_j, respectively. The same lemma, applied to B_j, B_k, yields the second vertex and Corollary 4.2.10 applied to B_j, B_k, yields the first vertex. It suffices to show that any point $(e_i, e_j) \in N(\phi)$ defines a counter-clockwise turn in the $e_i e_j$-plane, when appended to $(b_{jR}, 0)$ and $(b_{kR}, u - b_{kR})$. This is equivalent to proving

$$\det \begin{bmatrix} b_{jR} & 0 & 1 \\ b_{kR} & u - b_{kR} & 1 \\ e_i & e_j & 1 \end{bmatrix} \geq 0 \Leftrightarrow e_j(b_{kR} - b_{jR}) \geq (u - b_{kR})(e_i - b_{jR}). \tag{4.11}$$

Rightmost segment $[b_{kR}, b_{iR} = u]$ cannot contribute to e_i, since each corresponding mixed cell has an edge summand from A_i. If the segment lies in a j-mixed cell, then $e_j \geq u - b_{kR}$ and $e_i \leq b_{kR}$, and inequality (4.11) is proven. Otherwise, at least a subsegment contributes to a k-mixed cell.

If this subsegment contains b_{kR}, then it must extend at least to the next endpoint lying left of b_{kR}, hence to b_{jR} or b_{iL}. In the latter case, the subsegment to the left of b_{iL} cannot contribute to e_i. Thus, in any case, $e_i \leq b_{jR}$, so (4.11) is proven.

If none of the above happens, then the subsegment contributing to e_k does not contain b_{kR}, so the only way for the k-mixed cell to be defined is to have b_{iL} lie in (b_{kR}, b_{iR}) and k-mixed cell intersecting E at $[b_{iL}, b_{iR}]$. Then, $[b_{kR}, b_{iL}]$ contributes to e_j, so the j-mixed cell intersects E at $[b_{kt}, b_{iL}]$, where $t \in \{L, R\}$. If $b_{kt} = b_{kL}$, then $e_i = 0$ and (4.11) is proven.

Otherwise, $b_{kt} = b_{kR}$. The j-mixed cell is of type I and implies that the 1-dimensional face $(b_{iL}, 2) + E_{kR}$ belongs to the subdivision, see Lemma 4.2.2. The k-mixed cell is of type II, with some edge summand $E_{jt} \subset A_j$, which implies that the 1-face $(b_{iL}, 2) + E_{jt}$ is in the subdivision and cannot lie to the left of the previous 1-face. Since $b_{jR} \leq b_{kR}$, we have $b_{kR} = b_{jR}$, hence $e_i \leq b_{jR}$. □

Lemma 4.2.14. [case (3B)] *Suppose $b_{kL} > 0$ in Theorem 4.2.12. Then, $N(\phi)$ has up to 5 vertices (e_0, e_1) which can be read of from the following set of (e_i, e_j, e_k) vectors:*

$$\{(b_{jR}, 0, u - b_{jR}), (b_{kR}, u - b_{kR}, 0), (b_{kL}, u - b_{kL}, 0), (0, u - b_{iL}, b_{iL}), (0, 0, u)\}.$$

Proof. The last vertex follows from Lemma 4.2.9, applied to B_i, B_j. We shall prove that the first two points are vertices. When $b_{jR} \geq b_{kR}$, the first point is obtained by Lemma 4.2.9 applied to B_j, B_k, and the second one by Corollary 4.2.10 applied to B_j, B_k, and vice versa when $b_{jR} < b_{kR}$. The third and fourth vertices are established analogously, by considering B_i, B_k.

Our proof shall establish inequality (4.11). If $b_{jR} \leq b_{kR}$, this is similar to the proof of Lemma 4.2.13. Otherwise, $b_{kR} < b_{jR}$, and the rightmost segment $[b_{jR}, b_{iR} = u]$ cannot contribute to e_i. If it contributes to e_k only, then $e_k \geq u - b_{jR}$ so $e_i + e_j \leq b_{jR}$ and (4.11) follows.

If it contributes to e_j only, the union of the corresponding j-mixed cells intersect E at a segment with an endpoint to the left of b_{jR}, namely b_{kt}, $t \in \{L, R\}$, or b_{iL}. In the former case, $e_i \leq b_{kR}$ and $e_j \geq u - b_{kR}$. In the latter case, $[0, b_{iL}]$ contributes to e_k only, so $e_i = 0, e_j = u - b_{iL}$. In both cases, (4.11) follows readily.

Lastly, $[b_{jR}, b_{iR}]$ might be split into subsegments $[b_{jR}, b_{iL}], [b_{iL}, b_{iR}]$, contributing to e_k, e_j respectively. The corresponding cells are of type I and type II, the latter having an edge summand from A_k. This requires the subdivision to have j-faces $(b_{iL}, k) + E_{jR}$ and $(b_{iL}, 2) + E_{kt}, t \in \{L, R\}$, where the first lies to the left of the second, see Lemma 4.2.2. This cannot happen because $b_{kR} < b_{jR}$. □

Now we consider the case of polynomial parameterizations $x = P_0(t)$, $y = P_1(t)$. Let $B_i = \{b_{iR}, \ldots, b_{iR}\}$, $i = 0, 1$, be the supports of polynomials P_0, P_1. The following is an immediate corollary of Theorems 4.2.11 and 4.2.12 when $B_2 = \{0\}$.

Corollary 4.2.15. *If P_0 or P_1 (or both) contain a constant term, then the implicit polygon is the triangle with vertices $(0, 0)$, $(b_{1R}, 0)$, $(0, b_{0R})$. Otherwise, P_0, P_1 contain no constant terms, and the implicit polygon is the quadrilateral with vertices $(b_{1L}, 0)$, $(b_{1R}, 0)$, $(0, b_{0R})$, $(0, b_{0L})$.*

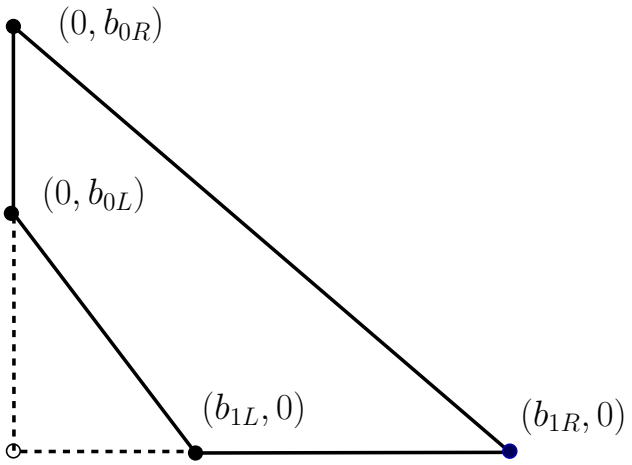

Figure 4.8: The implicit polygon of a polynomially parameterized curve

We use [45, prop. 15] to arrive at the following; recall that the implicit equation is defined up to a sign. Let $c \in \{-1, 1\}$; the coefficient of $x^{a_{1m}}$ is $c(-1)^{(1+a_{0n})a_{1m}}c_{1m}^{a_{0n}}$ and that of $y^{a_{0n}}$ is $c(-1)^{a_{0n}(1+a_{1m})}c_{0n}^{a_{1m}}$.

Corollary 4.2.16. *There exists $c \in \{-1, 1\}$ s.t. the coefficient of $x^{a_{1m}}$ is $c(-c_{1m})^{a_{0n}}$ and that of $y^{a_{0n}}$ is $c(-c_{0n})^{a_{1m}}$.*

We give certain examples of polynomial parameterizations, all leading to optimal implicit supports.

Example 4.2.17. Parameterization $x = y = t$ yields implicit equation $\phi = x - y$. Our method yields vertices $(1, 0)$ and $(0, 1)$ which are optimal.

Parameterization $x = 2t^3 - t + 1, y = t^4 - 2t^2 + 3$ yields implicit equation $\phi = 608 - 136x + 569y + 168y^2 - 72x^2 - 32xy - 4x^3 - 16x^2y - x^4 + 16y^3$. Our method yields the vertices $(0, 0), (4, 0), (0, 3)$ which are optimal. The degree bounds describe a larger quadrilateral with vertices $(0, 0), (4, 0), (1, 3), (0, 3)$. Corollary 4.2.16 predicts, for x^4, coefficient $(-1)^{16} = 1$, and for y^3, coefficient $(-1)^{15}2^4 = -16$, up to a fixed sign which equals -1 in $\phi(x, y)$.

For the Fröberg-Dickenstein example [44, Exam.3.3],

$$x = t^{48} - t^{56} - t^{60} - t^{62} - t^{63}, y = t^{32},$$

our method yields vertices $(32, 0), (0, 48), (0, 63)$, which define the optimal polygon. Here the degree bounds describe the larger quadrilateral with vertices $(0, 0), (32, 0), (32, 31), (0, 63)$.

Parameterization $x = t+t^2, y = 2t-t^2$ yields implicit equation $\phi = 6x-3y+x^2+2xy+y^2$. Corollary 4.2.15 yields vertices $(1, 0), (2, 0), (0, 2), (0, 1)$, which define the actual implicit polygon. Here the degree bounds imply a larger triangle, with vertices $(0, 0), (2, 0), (0, 2)$. Corollary 4.2.16 predicts, for x^2 and y^2, coefficients $(-1)^6(-1)^2 = 1$ and $(-1)^6(1)^2 = 1$ respectively.

Example 4.2.18. [Cont'd from Example 4.1.9] For the unit circle, $x = 2t/(t^2 + 1)$, $y = (1 - t^2)/(t^2 + 1)$, we have $f_0 = xt^2 - 2t + x$, $f_1 = (y + 1)t^2 + (y - 1)$. In Lemma 4.2.9, the sets $B_0 = \{1\}, B_1 = \{0, 2\}, B_2 = \{0, 2\}$ yield implicit vertices $(2, 0), (0, 2), (0, 0)$, corresponding to terms $x^2, y^2, 1$ in ϕ and, hence, an optimal support. See Example 4.1.9 for a treatment assuming different denominators.

Example 4.2.19. [Cont'd from Example 4.2.3] For the folium of Descartes

$$x = \frac{3t^2}{t^3 + 1}, y = \frac{3t}{t^3 + 1} \Rightarrow \phi = x^3 + y^3 - 3xy = 0;$$

see Figure 4.4. Now, $B_0 = \{2\}, B_1 = \{1\}, B_2 = \{0, 3\}$, hence this is case (A). In Theorem 4.2.11, we set $i = 0, j = 1, k = 2$ and obtain, implicit vertices in the order stated by the theorem: $(3, 0)$, $(0, 3)$, $(1, 1)$, $(0, 3)$ corresponding to terms x^3, y^3, y^3, xy, x^3, hence an optimal support.

If we do not account for the same denominators, use degree bounds alone, or project the Sylvester resultant, we obtain the additional vertex $(0, 0)$ which leads to a support with 5 extra points.

Example 4.2.20.

$$x = \frac{2t^3 + t + 1}{t^2 + 1}, y = \frac{t^4 + t^3 - 1}{t^2 + 1},$$

hence $B_0 = \{0, 1, 3\}, B_1 = \{0, 3, 4\}, B_2 = \{0, 2\}$, so this is case (2A) with $B_1 = [0, u]$. In Theorem 4.2.11, we set $i = 0, j = 2$ and obtain the vectors $(e_i, e_j) = (e_0, e_2) = (4, 0)$, $(0, 4)$, $(0, 1)$, $(0, 3)$, $(2, 0)$, in the order stated by the theorem. This yields the implicit points $(e_0, e_1) = (4, 0)$, $(0, 0)$, $(0, 3)$, $(0, 1)$, $(2, 2)$, hence vertices $(4, 0)$, $(0, 0)$, $(0, 3)$, $(2, 2)$. These define the optimal polygon because the implicit equation is

$$\phi = 59 - 21x + 110y + 52y^2 - 13x^2 - 48xy + 5x^3 - 5x^2y - x^4 + 8y^3 - 2x^2y^2 + 2x^3y - 12xy^2.$$

If we do not exploit the identical denominators and use the method for different denominators, we obtain points $(4, 2)$, $(2, 3)$, $(4, 0)$, $(0, 0)$ and $(0, 3)$ which define a polygon that contains the implicit polygon. Taking into account the degree bound (total degree=4), rules out points $(4, 2)$ and $(2, 3)$, and introduces point $(1, 3)$, yielding a smaller polygon that still contains the implicit polygon.

Example 4.2.21. [Cont'd from Example 4.0.3]

$$x = \frac{t^6 + 2t^2}{t^7 + 1}, y = \frac{t^4 - t^3}{t^7 + 1},$$

hence $B_0 = \{2, 6\}, B_1 = \{3, 4\}, B_2 = \{0, 7\}$, so this is case (2A) with $B_2 = [0, u]$. In Theorem 4.2.11, we set $i = 0, j = 1$ and obtain the implicit points $(e_0, e_1) = (7, 0), (0, 7), (0, 3), (3, 1), (6, 0)$, in the order stated by the theorem. The first 3 points follow from Lemma 4.2.9, while the last 2 follow from Corollary 4.2.10(2) and (3) respectively, applied to $B0, B1$. These are also the implicit vertices and define the actual polygon because the implicit equation is eq. (4.1). In Figure 4.1 is shown the implicit polygon. Changing the coefficient of t^2 to -1, leads to an implicit polygon with six vertices $(1, 3), (0, 4), (0, 6), (2, 5), (7, 0), (4, 1)$, is contained in the polygon predicted by Theorem 4.2.11. This shows the importance of the genericity condition on the coefficients of the parametric polynomials.

4.3 Conclusion and Further work

In conclusion, we have proven that in all cases only the extremal terms matter, both in determining the implicit polygon as well as in ensuring the genericity hypothesis on the coefficients.

It is possible to use our results in deciding which polygons can appear as Newton polygons of plane curves, and which parameterization is possible in the generic case. In particular, Corollary 4.2.15 and Corollary 4.2.16 imply that the Newton polygon of polynomial curves always has one vertex on each axis. These vertices define the edge that equals the polygon's upper hull in direction $(1, 1)$. The rest of the edges form the lower hull. If the implicit polygon is a segment, then the implicit polygon cannot contain interior points. Similar results hold for curves parameterized by Laurent polynomials.

We have shown that the case of common denominators reduces to a particular system of 3 bivariate polynomials, where only *linear* liftings matter. An interesting open question

is to examine to which systems of general dimension this observation holds, since it simplifies the enumeration of mixed subdivisions and, hence, of the extreme resultant monomials. In particular, we may ask whether this holds whenever the Newton polytopes are pyramids, or for systems with separated variables.

Another interesting question is whether we can extend our methods to the implicit polytope of a rational surface. Lastly, by approximating the given polygon by one of the polygons described above, one might formulate a question of approximate parameterization.

Index

Bernstein bound, 19
bistellar flip, 22

essential family of supports, 19
extreme monomial, 20

implicit polygon, 61
implicit support, 61
Implicitization, 61

Macaulay-type formula, 35
Minkowski cell, 20
Minkowski sum, 18
mixed cell configurations, 20
mixed subdivision, 20
mixed volume, 18

Newton polytope, 18

resultant polytope, 27
row content function, 24

secondary polytope, 22
simplicial complex, 31
sparse resultant, 19

Bibliography

[1] D. Cox, J. Little, and D. O'Shea, *Using Algebraic Geometry*. No. 185 in GTM, New York: Springer, 2nd ed., 2005.

[2] A. Dickenstein and I. Emiris, eds., *Solving Polynomial Equations: Foundations, Algorithms and Applications*, vol. 14 of *Algorithms and Computation in Mathematics*. Berlin: Springer-Verlag, May 2005.

[3] B. Sturmfels, *Solving Systems of Polynomial Equations*. No. 97 in CBMS Regional Conference Series in Math., Providence, RI: AMS, 2002.

[4] I. Gelfand, M. Kapranov, and A. Zelevinsky, *Discriminants, Resultants and Multidimensional Determinants*. Boston: Birkhäuser, 1994.

[5] F. Santos, "The Cayley trick and triangulations of products of simplices," in *Integer Points in Polyhedra: Geometry, Number Theory, Algebra, Optimization*, vol. 374 of *Contemporary Mathematics*, pp. 151–177, AMS, 2005.

[6] B. Sturmfels, "On the Newton polytope of the resultant," *J. Algebraic Combin.*, vol. 3, pp. 207–236, 1994.

[7] T. Michiels and J. Verschelde, "Enumerating regular mixed-cell configurations," *Discr. Comput. Geometry*, vol. 21, no. 4, pp. 569–579, 1999.

[8] F. Santos, "Geometric bistellar flips: The setting, the context and a construction," 2006. arXiv.org:math/0312069.

[9] L. Billera and B. Sturmfels, "Fiber polytopes," *Annals of Math.*, vol. 135, pp. 527–549, 1992.

[10] J. Canny and I. Emiris, "A subdivision-based algorithm for the sparse resultant," *J. ACM*, vol. 47, pp. 417–451, May 2000.

[11] I. Emiris, *Sparse Elimination and Applications in Kinematics*. PhD thesis, Computer Science Division, Univ. of California at Berkeley, Dec. 1994.

[12] J. Canny and P. Pedersen, "An algorithm for the Newton resultant," Tech. Rep. 1394, Comp. Science Dept., Cornell University, 1993.

[13] R. Corless, M. Giesbrecht, I. Kotsireas, and S. Watt, "Numerical implicitization of parametric hypersurfaces with linear algebra," in *Artificial intelligence and symbolic computation, (Madrid, 2000)*, pp. 174–183, Berlin: Springer, 2001.

[14] J. D. Loera, "PUNTOS," 1994. http://www.math.ucdavis.edu/~deloera/ RECENT_WORK/puntos2000.

[15] J. Rambau, "TOPCOM: Triangulations of point configurations and oriented matroids," in *Mathematical Software—ICMS 2002* (A. M. Cohen, X.-S. Gao, and N. Takayama, eds.), pp. 330–340, World Scientific, 2002.

[16] T. Masada, H. Imai, and K. Imai, "Enumeration of regular triangulations," in *SCG '96: Proceedings of the twelfth annual symposium on Computational geometry*, (New York, NY, USA), pp. 224–233, ACM Press, 1996.

[17] H. Imai, T. Masada, F. Takeuchi, and K. Imai, "Enumerating triangulations in general dimensions," *Intern. J. Comput. Geom. Appl.*, vol. 12, no. 6, pp. 455–480, 2002.

[18] D. Avis and K. Fukuda, "Reverse search for enumeration," *Discrete Appl. Math.*, vol. 65, no. 1-3, pp. 21–46, 1996.

[19] H. Edelsbrunner, *Algorithms in Combinatorial Geometry*. Heidelberg: Springer, 1987.

[20] C. D'Andrea and A. Dickenstein, "Explicit formulas for the multivariate resultant," *J. Pure Appl. Algebra*, vol. 164, no. 1-2, pp. 59–86, 2001.

[21] A. Dickenstein and I. Emiris, "Multihomogeneous resultant formulae by means of complexes," *J. Symbolic Computation*, vol. 36, no. 3-4, pp. 317–342, 2003. Special issue on ISSAC 2002.

[22] I. Emiris and A. Mantzaflaris, "Multihomogeneous resultant matrices for systems with scaled support," in *Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation*, pp. 143–150, ACM Press, 2009.

[23] A. Khetan, "The resultant of an unmixed bivariate system," *J. Symbolic Computation*, vol. 36, pp. 425–442, 2003.

[24] A. Khetan, N. Song, and R. Goldman, "Sylvester-resultants for bivariate polynomials with planar Newton polygons," in *Proc. ACM Intern. Symp. on Symbolic & Algebraic Comput.*, pp. 205–212, 2004.

[25] B. Sturmfels and A. Zelevinsky, "Multigraded resultants of Sylvester type," *J. Algebra*, vol. 163, no. 1, pp. 115–127, 1994.

[26] F. Macaulay, "Some formulae in elimination," *Proc. London Math. Soc.*, vol. 1, no. 33, pp. 3–27, 1902.

[27] E. Kaltofen and P. Koiran, "Expressing a fraction of two determinants as a determinant," in *ISSAC '08: Proceedings of the twenty-first international symposium on Symbolic and algebraic computation*, pp. 141–146, ACM Press, New York, 2008.

[28] J. Canny and I. Emiris, "An efficient algorithm for the sparse mixed resultant," in *Proc. Intern. Symp. on Applied Algebra, Algebraic Algor. and Error-Corr. Codes (Puerto Rico)* (G. Cohen, T. Mora, and O. Moreno, eds.), no. 263 in Lect. Notes in Comp. Science, (Berlin), pp. 89–104, Springer-Verlag, 1993.

[29] C. D'Andrea, "Macaulay-style formulas for the sparse resultant," *Trans. of the AMS*, vol. 354, pp. 2595–2629, 2002.

[30] H. Zhang, "Calculs de résidus toriques," *C.R. Acad. Sci. Paris*, pp. 639–634, 1998.

[31] C. D'Andrea, "Lifting functions and Macaulay-style formulas: The resultant of sparse reduced systems." Manuscript, 2001.

[32] C. D'Andrea and I. Emiris, "Lifting functions and Macaulay-Style formulas for computing sparse resultants." Manuscript, 2003.

[33] T. Gao, T. Li, and X. Wang, "Finding isolated zeros of polynomial systems in C^n with stable mixed volumes," *J. Symbolic Computation*, vol. 28, no. 1-2, pp. 187–211, 1999.

[34] D. Bernstein, "The number of roots of a system of equations," *Funct. Anal. and Appl.*, vol. 9, no. 2, pp. 183–185, 1975.

[35] B. Huber and B. Sturmfels, "A polyhedral method for solving sparse polynomial systems," *Math. Comp.*, vol. 64, no. 212, pp. 1542–1555, 1995.

[36] M. Minimair, "Sparse resultant under vanishing coefficients," *J. Algebraic Combin.*, vol. 18, no. 1, pp. 53–73, 2003.

[37] I. Emiris and C. Konaxis, "Single-lifting macaulay-type formulae of generalized unmixed sparse resultants," *J. Symbolic Computation,* Elsevier, 2010. Submitted.

[38] N. Karmarkar, "A new polynomial-time algorithm for linear programming," *Combinatorica*, vol. 4, pp. 373–395, 1984.

[39] I. Emiris, "Enumerating a subset of the integer points inside a Minkowski sum," *Comp. Geom.: Theory & Appl., Spec. Issue*, vol. 22, no. 1-3, pp. 143–166, 2002.

[40] B. Sturmfels and J. Yu, "Minimal polynomials and sparse resultants.," in *Proc. Zero-Dimensional Schemes (Ravello, June 1992)* (F. Orecchia and L. Chiantini, eds.), pp. 317–324, De Gruyter, 1994.

[41] B. Sturmfels, J. Tevelev, and J. Yu, "The Newton polytope of the implicit equation," *Moscow Math. J.*, vol. 7, no. 2, 2007.

[42] I. Emiris and I. Kotsireas, "Implicitization with polynomial support optimized for sparseness," in *Proc. Intern. Conf. Comput. Science & Appl. 2003, Montreal, Canada (Intern. Workshop Computer Graphics & Geom. Modeling)* (V. K. et al., ed.), vol. 2669 of *LNCS*, pp. 397–406, Springer, 2003.

[43] T. Dokken, "Approximate implicitization," in *Mathematical methods for curves and surfaces (Oslo 2000)*, Innov. Appl. Math., pp. 81–102, Nashville: Vanderbilt Univ. Press, 2001.

[44] I. Emiris and I. Kotsireas, "Implicitization exploiting sparseness," in *Geometric and Algorithmic Aspects of Computer-Aided Design and Manufacturing* (R. Janardan, M. Smid, and D. Dutta, eds.), vol. 67 of *DIMACS*, pp. 281–298, AMS/DIMACS, 2005.

[45] I. Gelfand, M. Kapranov, and A. Zelevinsky, "Discriminants of polynomials in several variables and triangulations of Newton polytopes," *Leningrad Math. J.*, vol. 2, no. 3, pp. 449–505, 1991. (Translated from *Algebra i Analiz* 2, 1990, pp. 1–62).

[46] B. Sturmfels and J. Yu, "Tropical implicitization and mixed fiber polytopes," in *Software for Algebraic Geometry*, vol. 148 of *IMA Volumes in Math. & its Applic.*, pp. 111–131, New York: Springer, 2008.

[47] A. Esterov and A. Khovanskii, "Elimination theory and Newton polytopes," 2007. arXiv.org:math/0611107v2.

[48] C. D'Andrea and M. Sombra, "The Newton polygon of a rational plane curve," *Mathematics in Computer Science - MCS Special Issue on Computational Geometry and Computer-Aided Design*, vol. 4, no. 1, pp. 3–24, 2010.

[49] P. Philippon and M. Sombra, "A refinement of the Bernstein-Kushnirenko estimate," *Advances in Mathematics*, vol. 218, pp. 1370–1418, 2008.

[50] I. Emiris, C. Konaxis, and L. Palios, "Computing the Newton polytope of specialized resultants," in *Proc. Intern. Conf. MEGA (Effective Methods in Algebraic Geometry)*, 2007. www.ricam.oeaw.ac.at/mega2007/electronic/45.pdf.

[51] I. Emiris, V. Fisikopoulos, and C. Konaxis, "Regular triangulations and resultant polytopes," in *Proc. 26th European Workshop on Computational Geometry*, (Dortmund, Germany), pp. 137–140, 2010.

[52] I. Emiris, C. Konaxis, and L. Palios, "Computing the Newton polygon of the implicit equation," *Mathematics in Computer Science - MCS Special Issue on Computational Geometry and Computer-Aided Design*, vol. 4, no. 1, p. 25, 2010.

[53] T. Sederberg, "Improperly parametrized rational curves," *Comp.-Aided Design*, vol. 3, pp. 67–75, 1986.

[54] D. A. Cox, T. W. Sederberg, and F. Chen, "The moving line ideal basis of planar rational curves," *Computer Aided Geometric Design*, vol. 15, no. 8, pp. 803–827, 1998.

[55] J. R. Sendra and F. Winkler, "Computation of the degree of rational maps between curves.," in *ISSAC '01: Proceedings of the 2001 international symposium on Symbolic and algebraic computation*, (New York, USA), pp. 317–322, 2001.