A Subdivision-Based Algorithm for the Sparse Resultant

John F. Canny*   Ioannis Z. Emiris†

April 20, 1999

Abstract

Multivariate resultants generalize the Sylvester resultant of two polynomials and characterize the solvability of a polynomial system. They also reduce the computation of all common roots to a problem in linear algebra. We propose a determinantal formula for the sparse resultant of an arbitrary system of $n+1$ polynomials in n variables. This resultant generalizes the classical one and has significantly lower degree for polynomials that are sparse in the sense that their mixed volume is lower than their Bézout number. Our algorithm uses a mixed polyhedral subdivision of the Minkowski sum of the Newton polytopes in order to construct a Newton matrix. Its determinant is a nonzero multiple of the sparse resultant and the latter equals the GCD of at most $n+1$ such determinants. This construction implies a restricted version of an effective sparse Nullstellensatz. For an arbitrary specialization of the coefficients there are two methods which use one extra variable and yield the sparse resultant. This is the first algorithm to handle the general case with complexity polynomial in the resultant degree and simply exponential in n. We conjecture its extension to producing an exact rational expression for the sparse resultant.

Categories and Subject Descriptors: I.1.2 Algorithms (Algebraic algorithms, Analysis of algorithms). F.2.1 Numerical Algorithms and Problems (Computations on matrices, Computations on polynomials). F.2.2 Non-numerical Algorithms and Problems (Computations on discrete structures, Geometrical problems and computations).

General Terms: Algorithms, Theory.

Additional Key Words and Phrases: Sparse elimination theory, multivariate resultant, Newton polytope, mixed volume, polyhedral subdivision, effective Nullstellensatz, asymptotic complexity.

1   Introduction

The *resultant* of a system of $n+1$ arbitrary polynomial equations in $n+k$ variables is a polynomial in k variables, which characterizes the solvability of the system. In other words, for a particular specialization of the k remaining variables, the resultant vanishes if and only if the given polynomial system has a nontrivial solution. As it allows the elimination of n variables, the resultant is also called *eliminant*. The resultant of two univariate polynomials is named after Sylvester, while for an arbitrary number of linear polynomials the resultant coincides with the determinant of the coefficient matrix.

Classical elimination theory and the classical multivariate resultant have a long and rich history, briefly sketched in section 2. The classical resultant characterizes the existence of common roots in projective space and its degree depends on the Bézout bound on the number of common projective roots [vdW50, Zip93].

This article considers the *sparse resultant,* which generalizes the classical resultant and exploits the monomial structure of the given polynomials. We shall formalize the notion of sparseness in section 3. In general, the sparse resultant has smaller degree than its classical counterpart because its degree depends on the Bernstein bound on the number of affine roots [Ber75]. Bernstein's bound is at most equal to Bézout's and, for sparse systems, it is substantially smaller and often exact.

Our main contribution is to present historically the first general and efficient algorithm to compute the sparse resultant, by completing and expanding on the construction of [CE93]. The algorithm defines a matrix with entries equal to the input coefficients or zero, whose determinant is a nontrivial multiple of the sparse resultant,

---

*Computer Science Division, University of California at Berkeley, Berkeley, CA 94720, USA. E-mail: jfc@cs.Berkeley.edu.

†INRIA, B.P. 93, Sophia-Antipolis 06902 France. E-mail: emiris@sophia.inria.fr.

and from which the resultant can be recovered. The construction relies on a mixed polyhedral subdivision, and yields a bound on matrix size in terms of Newton polytopes. This leads to a bound on the Newton polytopes of the polynomials in the ideal membership formula, in other words an effective sparse Nullstellensatz. This is historically the first algorithm with total complexity bounded by a polynomial in the resultant degree and a simple exponential in n.

In general, matrices with the above properties are called *resultant matrices*. We introduce the terminology *Newton matrix* to distinguish our matrix from other matrix formulae of the same resultant. Moreover, we wish to emphasize the fact that a different matrix is constructed for every distinct set of Newton polytopes. The algorithm generalizes Sylvester's algorithm for two univariate polynomials, since it produces Sylvester's resultant matrix in this case. For an arbitrary number of dense polynomials, the algorithm produces the classical Macaulay matrix, discussed in the next section.

The rest of this section motivates resultant-based methods and sparse elimination, and concludes with an outline of the article. Several variable elimination and system solving problems are most efficiently solved by resultants in general, and U-resultants in particular. Application areas include complexity theory, quantifier elimination, algebraic number arithmetic, and integration [Loo82, Ren92, Zip93, LM95], as well as robotics, vision, geometric modeling and computational biology [Can88, BGW88, MC93, Emi97, RR95, EM99].

A specific example is given by the implicitization problem, of central importance in geometric and solid modeling. Given a parametrized surface

$$(x, y, z, w) = (X(s, t), Y(s, t), Z(s, t), W(s, t)),$$

where X, Y, Z and W are polynomials in the parameters s, t, the question is to find an implicit description of this surface as the zero set of a single polynomial in x, y, z, w. This is achieved by eliminating the parameters s, t from the system

$$wX(s, t) - xW(s, t) = wY(s, t) - yW(s, t) = wZ(s, t) - zW(s, t) = 0,$$

which is equivalent to computing the system's resultant. For a bicubic surface, methods based on customized resultants exploiting sparseness have achieved a speedup of at least 10^3 in the running time over approaches relying on Gröbner bases and the Ritt-Wu method [MC93].

Sparseness can lead to an important improvement over classical elimination methods in practice. To illustrate the disparity between the classical Bézout bound and Bernstein's sparse bound, consider the problem of computing all eigenvalues and eigenvectors of a generic complex $n \times n$ matrix A. This reduces to solving a system of n equations of the form $\sum_j A_{ij} v_j = \lambda v_i$, $1 \le i \le n$, and $\sum_i v_i^2 = 1$, for unknowns $v_1, \ldots, v_n$ and λ. The Bézout bound is 2^{n+1}, though the number of solutions is only $2n$, two opposite eigenvectors per eigenvalue. Bernstein's bound is exact for this system.

Methods for the construction of resultants which exploit monomial structure had been *ad hoc,* for they relied on the specific problem. Hence the need of a general algorithm, which is precisely the topic of this article. One problem from computer vision is computing the structure of the environment from motion. Ignoring the complexity of the initial off-line phase, the average on-line running time is 0.2 seconds on an 80 MHz DEC Alpha 3000, and results for most systems are accurate to 6 decimal digits. The running time and the accuracy compare favorably to sparse homotopies exploiting the monomial structure; furthermore, the accuracy is higher than that of least-square techniques, which require more information [Emi97].

The remainder of this article is organized as follows. The next section points to previous work and compares it with ours. Section 3 introduces the basic notions of sparse elimination theory, and presents the mathematical background necessary for our algorithm. Section 4 specifies a mixed subdivision of the Minkowski sum of the input Newton polytopes, and section 5 describes the construction of Newton matrix M, thus establishing an a priori bound on the matrix size. The main properties of M, namely that $\det(M)$ is a multiple of the sparse resultant and is not identically zero, are established in the following section. Some important properties on the degree of the determinant in the coefficients of the given polynomials are established in section 7, thus implying that the sparse resultant equals the Greatest Common Divisor (GCD) of at most $n + 1$ determinants. Section 8 demonstrates a restricted version of a sparse effective Nullstellensatz and states a conjecture for the general case. Section 9 discusses two ways to compute the sparse resultant itself for arbitrary specializations. We illustrate the algorithm in section 10. Sections 11 and 12 analyze the worst-case asymptotic bit complexity and randomization complexity of constructing the Newton matrix and computing the sparse resultant, respectively. The article concludes with a conjecture on generalizing Macaulay's exact rational formula to Newton matrices.

The basic algorithm and the main results of sections 4 to 7 and of section 9 first appeared in preliminary form in [CE93].

2 Related Work

Classical elimination theory considers systems of n *homogeneous* polynomials in n variables and k parameters or coefficients. The classical multivariate resultant is a single polynomial in the k coefficients that vanishes for a specialization of the coefficients if and only if the specialized system has a common root in the projective space over the coefficient field, denoted $\mathbb{P}^n$. The resultant degree in the coefficients of polynomial f_i is

$$\prod_{i=1, j\neq i}^{n} \deg f_j, \qquad \text{where } \deg f_j \text{ is the total degree of } f_j.$$

This is Bézout's bound on the number of common projective solutions of the system $f_j = 0$, $j \neq i$ [vdW50].

One approach for the resultant of two homogeneous polynomials is named after Bézout and is based on discrete differentials. This yields small matrices whose entries are *polynomials* in the input coefficients. Its generalization, the Bezoutian matrix, works in arbitrary dimension and does not require any genericity assumption on the inputs [Mou97]. Another generalization is Dixon's matrix; see, for instance, [KS95].

A different approach that also obtains determinantal expressions for the resultant stems from Sylvester's formulation for $n = 2$. This is the determinant of a matrix of minimum possible size, where the entries are constrained to be either zero or some polynomial coefficient. For higher n, matrices whose determinant equals the resultant do not exist in general, but Macaulay expressed the classical resultant as the quotient of a matrix determinant divided by one of its minors [vdW50, Can88, Ren92]. Our approach generalizes this kind of matrices. Alternative algorithms for computing the classical resultant, solving polynomial systems, and eliminating quantifiers have been proposed in [Laz81, CG84, Chi86, Gri86, GH91].

Sparse elimination theory exploits the fact that certain coefficients are known to be zero a priori. The foundations were laid in the late 1980's in the work of Gelfand, Kapranov and Zelevinsky [GKZ94]. The sparse resultant was called the $(\mathcal{A}_1, \ldots, \mathcal{A}_{n+1})$-resultant, where $\mathcal{A}_i \subset \mathbb{Z}^n$ is the support of the i-th polynomial. Pedersen and Sturmfels [PS93] gave a product formula of Poisson type for the sparse resultant, namely $R' \prod_{\xi \in V(f_1, \ldots, f_n)} f_{n+1}(\xi)$, where the extraneous factor R' is a rational function in the coefficients of $f_1, \ldots, f_n$ and $V(f_1, \ldots, f_n)$ is the zero-dimensional variety (or zero set) of $f_1, \ldots, f_n$. This construction is too costly to have any practical significance. The first constructive methods for computing and evaluating the sparse resultant were proposed by Sturmfels in [Stu93], the most efficient having complexity super-polynomial in the total degree of the sparse resultant and exponential in n with a quadratic exponent.

A greedy variant of our algorithm has been proposed by Canny and Pedersen [CP93] which, based on a mixed subdivision, typically constructs smaller matrices. This algorithm also removes a rather technical requirement on the input supports, formalized in section 3. A second generalization has been proposed by Sturmfels [Stu94, sect. 2, 3] for weakening the genericity requirement on the lifting functions used in our construction. An incremental randomized algorithm has been proposed by Emiris and Canny in order to construct Newton matrices of smaller size, which are optimal for all classes of polynomial systems where such matrices provably exist [EC95]. More recent work focuses on the structure of these matrices, which has been shown to generalize Toeplitz structure [EP97].

For solving systems of n polynomial equations in n unknowns, certain properties of the Newton matrix must be established. One approach is that of [PS96], whereas a simpler proof, based on the present algorithm, which reduces root-finding to an eigenproblem is found in [Emi96]. This result extends older work in [AS88, MC93]. Observe that the exact sparse resultant is not necessary, since a Newton matrix suffices. The computation of solution sets with positive dimension has been undertaken in [KM95]. In practice, questions of degeneracy may have to be addressed, as in [Man94, Mou98, Roj99].

A related problem of independent significance is the computation of mixed volumes. Different algorithms and implementations have been suggested [HS95, EC95, VGC96]. *Sparse homotopies* have been proposed in order to reduce the number of paths by relating their cardinality to Bernstein's bound rather than Bézout's [HS95, VGC96]. The mixed polyhedral subdivision constructed by our algorithm allows computation of the mixed volume and specifies a start system for these homotopies.
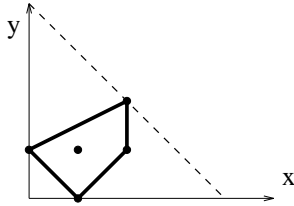
Figure 1: The Newton polytope of polynomial $c_1 y + c_2 x^2 y^2 + c_3 x^2 y + c_4 x + c_5 xy$. The dotted triangle is the Newton polytope of the dense polynomial of the same total degree.

Different notions of sparseness include straight-line programs [AHU74, GHMP95] and Khovanskii's fewnomials [Kho91].

3   Sparse Elimination Theory

This section introduces the theory of sparse elimination and some necessary definitions for the study of polynomial systems. For background on polynomial systems see [vdW50, Zip93], and for background on combinatorial geometry and polytope theory [Sch93].

Sparse elimination theory generalizes several results of classical elimination theory on multivariate polynomial systems by considering the structure of the given polynomials, namely their Newton polytopes. This leads to stronger algebraic and combinatorial results. Assume the input polynomial coefficients lie in complex space $\mathbb{C}$. By considering common roots in $\mathbb{P}^n$, the classical theory accounts for several projective solutions that are useless in physical applications and whose cardinality often dominates that of the affine roots. Being interested in affine roots only, sparse elimination focuses on $(\mathbb{C}^*)^n$ where $\mathbb{C}^* = \mathbb{C} \setminus \{0\} \subset \mathbb{C} \subset \mathbb{P}$.

The main problem is, given $n+1$ arbitrary polynomials $f_1, \ldots, f_{n+1}$ in n variables, to find a condition on the coefficients of the f_i that characterizes the solvability of the system. For now, we regard the coefficients as indeterminates and concentrate on solutions $\xi \in (\mathbb{C}^*)^n$. Under this assumption, we can deal with the more general case where f_i is a *Laurent polynomial*, i.e.,

$$f_1, \ldots, f_{n+1} \in \mathbb{C}[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}].$$

We use x^a to denote the monomial $x_1^{a_1} \cdots x_n^{a_n}$, where $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ is an exponent vector.

To take advantage of sparseness we take into account the fact that certain coefficients are known a priori to be zero. Let μ_i be the number of nonzero coefficients, then every polynomial is written as follows:

$$f_i = \sum_{j=1}^{\mu_i} c_{ij} x^{a_{ij}}, \qquad c_{ij} \neq 0, \ i = 1, \ldots, n+1. \tag{1}$$

Definition 3.1 *The finite set $\mathcal{A}_i = \{a_{i1}, \ldots, a_{i\mu_i}\} \subset \mathbb{Z}^n$ of all monomial exponents appearing in f_i is the* support *of f_i, denoted* $\mathrm{supp}(f_i)$. *Its cardinality is $\mu_i = |\mathcal{A}_i|$. The* Newton polytope *$Q_i \subset \mathbb{R}^n$ of f_i is the convex hull of $\mathcal{A}_i$. We shall assume that $\{a_{i1}, \ldots, a_{im_i}\}$ is the vertex set of Q_i for $m_i \leq \mu_i$.*

A polynomial system is *unmixed* if all supports $\mathcal{A}_i$ are identical, otherwise it is *mixed*. The example of section 10 shows a mixed system. Figure 1 depicts the Newton polytope for a bivariate polynomial and compares it with the Newton polytope of the *dense* polynomial with the same total degree, i.e., a polynomial in which *every* coefficient is nonzero. Clearly, Newton polytopes provide a more precise description than the total degree does, and thus express the sparse structure of a given polynomial. Dealing with Laurent polynomials implies that multiplying a polynomial by a monomial gives an equivalent polynomial. In other words, translates of a Newton polytope are identified.

Newton polytopes cast the problem in geometric terms, which calls for some definitions from polytope theory. For arbitrary sets in $\mathbb{R}^n$ there is a natural associative and commutative addition operation which generalizes vector addition and is called Minkowski addition.

4

Definition 3.2 *The* Minkowski sum $A + B$ *of convex polytopes A and B in $\mathbb{R}^n$ is the set*

$$A + B = \{a + b \mid a \in A, b \in B\}.$$

It is easy to prove that $A + B$ is convex if A, B are convex [Sch93].

Definition 3.3 *Given convex polytopes $A_1, \ldots, A_n \subset \mathbb{R}^n$, there is a unique, up to multiplication by a scalar, real-valued function $MV(A_1, \ldots, A_n)$, called the* mixed volume *of the given polytopes, which is multilinear with respect to Minkowski addition and scalar multiplication, i.e., for $\lambda, \rho \in \mathbb{R}_{\geq 0}$ and convex polytope $A'_k \subset \mathbb{R}^n$,*

$$MV(A_1, \ldots, \lambda A_k + \rho A'_k, \ldots, A_n) =$$
$$\lambda MV(A_1, \ldots, A_k, \ldots, A_n) + \rho MV(A_1, \ldots, A'_k, \ldots, A_n).$$

To define mixed volume exactly we require that

$$MV(A_1, \ldots, A_1) = n! \operatorname{Vol}(A_1),$$

where $\operatorname{Vol}(\cdot)$ denotes n-dimensional Euclidean volume, such that it assigns unit volume to the the unit cube.

An equivalent definition [Sch93] is the following.

Definition 3.4 *For $\lambda_1, \ldots, \lambda_n \in \mathbb{R}_{\geq 0}$ and convex polytopes $A_1, \ldots, A_n \subset \mathbb{R}^n$, the* mixed volume $MV(A_1, \ldots, A_n)$ *is precisely the coefficient of $\lambda_1 \lambda_2 \cdots \lambda_n$ in $\operatorname{Vol}(\lambda_1 A_1 + \cdots + \lambda_n A_n)$ expanded as a polynomial in $\lambda_1, \ldots, \lambda_n$.*

The Newton polytopes offer a model of the sparseness of a polynomial system, in light of Bernstein's upper bound on the number of common roots. This bound is also called the BKK bound to underline the contributions of Kushnirenko and Khovanskii in its development and proof [Kus76, Kho78].

Theorem 3.5 [Ber75] *Let $f_1, \ldots, f_n \in \mathbb{C}[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$. The number of common zeros in $(\mathbb{C}^*)^n$ is either infinite, or does not exceed $MV(Q_1, \ldots, Q_n)$. For almost all specializations of the coefficients c_{ij}, the number of solutions is exactly $MV(Q_1, \ldots, Q_n)$.*

The mixed volume is typically significantly lower than Bézout's bound. Recall, for instance, the eigenproblem presented in section 1, or see the system of section 10. The two bounds coincide for dense polynomials, because then each Newton polytope is an n-dimensional unit simplex scaled by $\deg f_i$, thus, by definition, the mixed volume of the dense system is

$$\prod_{i=1}^{n} \deg f_i \; MV(S, \ldots, S) = \prod_{i=1}^{n} \deg f_i,$$

where S is the unit simplex in $\mathbb{R}^n$.

The main object for the study and solution of polynomial systems will be the *sparse resultant*, which is a necessary and sufficient condition for the given Laurent polynomials to have a common root. We use a simpler definition than the one in [GKZ94], relying on an additional assumption on the genericity of the coefficients [PS93]. We regard a polynomial f_i as the following generic point:

$$(c_{i1}, \ldots, c_{i\mu_i}) \in \mathbb{P}^{\mu_i - 1}, \qquad i = 1, \ldots, n + 1,$$

in the space of all possible polynomials with the given support $\mathcal{A}_i$, after identifying scalar multiples. Then the input system is the following point:

$$c = (c_{11}, \ldots, c_{1\mu_1}, \ldots, c_{(n+1)1}, \ldots, c_{(n+1)\mu_{n+1}}),$$
$$\text{such that } c \in \mathbb{P}^{\mu_1 - 1} \times \cdots \times \mathbb{P}^{\mu_{n+1} - 1}.$$

Let $Z_0 = Z_0(\mathcal{A}_1, \ldots, \mathcal{A}_{n+1})$ be the set of all points c such that the corresponding polynomial system has a solution in $(\mathbb{C}^*)^n$, and let $Z = Z(\mathcal{A}_1, \ldots, \mathcal{A}_{n+1})$ denote the Zariski closure of Z_0 in the product of projective spaces. Z is an irreducible algebraic set [PS93].

Definition 3.6 [PS93] *With the above notation, the* sparse resultant $R(\mathcal{A}_1, \ldots, \mathcal{A}_{n+1})$ *of system (1) is a polynomial in* $\mathbb{Z}[c]$. *If* $codim(Z) = 1$, *then* $R(\mathcal{A}_1, \ldots, \mathcal{A}_{n+1})$ *is the defining irreducible polynomial of hypersurface* Z. *If* $codim(Z) > 1$, *then* $R(\mathcal{A}_1, \ldots, \mathcal{A}_{n+1}) = 1$.

Observe that this defines R within a nonzero scalar factor.

It is assumed without loss of generality that the affine lattice generated by $\sum_{i=1}^{n+1} \mathcal{A}_i$ is n-dimensional. This technical hypothesis is removed in [CP93]. This lattice is identified with $\mathbb{Z}^n$ possibly after a change of variables, which can be implemented by applying Smith's normal form [Stu94]. Under this hypothesis the resultant's degree can be specified.

Proposition 3.7 [PS93] *The sparse resultant is separately homogeneous in the coefficients* $(c_{i1}, \ldots, c_{i\mu_i})$ *of each* f_i *and its degree in these coefficients equals the mixed volume of the other n Newton polytopes, denoted* MV_{-i}, *i.e.*,

$$\deg_{f_i} R = MV(Q_1, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_{n+1}) = MV_{-i}, \qquad i = 1, 2, \ldots, n+1.$$

Consequently, the total degree of the sparse resultant is $\deg R = \sum_{i=1}^{n+1} MV_{-i}$.

A crucial question in the complexity analysis of sparse elimination algorithms is the relation between mixed volume and the volume of the Minkowski sum $Q = Q_1, \ldots, Q_{n+1} \subset \mathbb{R}^n$. We denote by $e < 2.718$ the exponential base. A weaker version of the following result first appeared in [CE93].

Lemma 3.8 [Emi96] *For unmixed systems with Newton polytopes* $Q_1 = \cdots = Q_{n+1}$,

$$\mathrm{Vol}(Q_1 + \cdots + Q_{n+1}) = \Theta\left(\frac{e^n \deg R}{n^{3/2}}\right),$$

where $\deg R$ *is the total degree of the sparse resultant in the input coefficients.*

To model mixed systems we have to express their difference in shape and volume.

Definition 3.9 [Emi96] *Let the polytope of minimum volume be* Q_ρ, $1 \le \rho \le n+1$, *such that*

$$\mathrm{Vol}(Q_\rho) = \min\{\mathrm{Vol}(Q_i) \mid i = 1, \ldots, n+1\},$$

and the system's scaling factor s *be the minimum value such that*

$$\exists\, \lambda_i \in \mathbb{R}^n \quad : \quad \lambda_i + Q_i \subset s\, Q_\rho, \qquad i = 1, \ldots, n+1.$$

Clearly, $s \ge 1$ and s is finite precisely when the n-dimensional volume of every Newton polytope is positive.

Theorem 3.10 [Emi96] *Given are polynomials with Newton polytopes* $Q_1, \ldots, Q_{n+1} \subset \mathbb{R}^n$, *such that* $\mathrm{Vol}(Q_i) > 0$ *for all i, and let s be the system's scaling factor. If* $\deg R$ *denotes the total degree of the sparse resultant in the input coefficients, then*

$$\mathrm{Vol}(Q_1 + \cdots + Q_{n+1}) = O\left(\frac{s^n e^{n+1}}{n^{3/2}} \deg R\right).$$

4   Mixed Polyhedral Subdivisions

This section introduces some notation and defines a mixed polyhedral subdivision of the Minkowski sum of the Newton polytopes; for geometric definitions and details refer to [BS92, Sch93].

Let Q denote the Minkowski sum of all input Newton polytopes

$$Q = Q_1 + Q_2 + \cdots + Q_{n+1} \subset \mathbb{R}^n.$$

Consider the following function expressing Minkowski addition.

$$\alpha : (\mathbb{R}^n)^{n+1} \to \mathbb{R}^n : Q_1 \times \cdots \times Q_{n+1} \to Q : (p_1, \ldots, p_{n+1}) \mapsto p_1 + \cdots + p_{n+1}. \tag{2}$$

This is clearly a many-to-one mapping. We wish, for each $q \in Q$, to define a unique inverse $(p_1, \ldots, p_{n+1})$ in $Q_1 \times \cdots \times Q_{n+1}$.

To this end the following method is employed from [Stu94]. Choose $n+1$ sufficiently generic linear *lifting* homogeneous forms $l_1, \ldots, l_{n+1} \in \mathbb{Z}[x_1, \ldots, x_n]$. In other words, every l_i is of the form $L_1 x_1 + \cdots + L_n x_n$, for generic $L_1, \ldots, L_n \in \mathbb{Z}$. We shall formalize below the genericity requirements on l_i; see [Stu94] for an approach that weakens these requirements. Define the *lifted* Newton polytopes

$$\widehat{Q}_i = \{\widehat{p}_i = (p_i, l_i(p_i)) : p_i \in Q_i\} \subset \mathbb{R}^{n+1} \qquad i = 1, 2, \ldots, n+1.$$

The "hat" notation implies lifting; note, however, that the lifted point is well-defined only when the corresponding point in $\mathbb{R}^n$ is expressed as a sum of points in the Q_i. The linearity of every l_i implies that the dimension of $\widehat{Q}_i$ is the same as the dimension of Q_i, even if the former lies in $(n+1)$-dimensional space. Similarly, the dimension of every face of Q_i does not change by lifting. Let the Minkowski sum of the lifted Newton polytopes be

$$\widehat{Q} = \widehat{Q}_1 + \cdots + \widehat{Q}_{n+1} \subset \mathbb{R}^{n+1}.$$

Definition 4.1 *Given is a convex polytope in $\mathbb{R}^{n+1}$ of positive $(n+1)$-dimensional volume. Its* lower envelope *(with respect to vector $(0, \ldots, 0, 1) \in \mathbb{R}^{n+1}$) is the union of all n-dimensional faces, or* facets, *whose inner normal vector has positive last component.*

Recall, from section 3, the hypothesis on the full-dimensionality of the lattice generated by the supports. It implies that Q has dimension n, $\widehat{Q}$ has dimension $n+1$ (for a sufficiently generic lifting), and therefore its lower envelope has dimension n. Let $\pi : \mathbb{R}^{n+1} \to \mathbb{R}^n : (p_1, \ldots, p_{n+1}) \mapsto (p_1, \ldots, p_n)$ denote projection on the first n coordinates. Both $\widehat{Q}$ and its lower envelope project, under π, to Q, but the first mapping is many-to-one while the second is one-to-one. Let $h : \mathbb{R}^{n+1} \to \mathbb{R} : (p_1, \ldots, p_{n+1}) \mapsto p_{n+1}$ denote projection on the $(n+1)$-st coordinate, thus expressing the "height" of a lifted point. The following function is now well-defined.

$$s : Q \to \widehat{Q} : q \mapsto \widehat{q} \in \pi^{-1}(q) \cap \widehat{Q}, \qquad \text{such that } h(\widehat{q}) \text{ is minimized.}$$

The lower envelope of $\widehat{Q}$ is then $s(Q)$. The genericity requirement on l_i is that every point $\widehat{q}$ on the lower envelope can be *uniquely* expressed as a sum of points $\widehat{q}_1 + \cdots + \widehat{q}_{n+1}$ with $\widehat{q}_i \in \widehat{Q}_i$; this is quantified in lemma 11.1. Hence, we define a *unique inverse* for function α over Q as follows.

$$\alpha^{-1}|_Q : Q \to Q_1 \times \cdots \times Q_{n+1} : q \mapsto (q_1, \ldots, q_{n+1}), \quad \text{where } s(q) = \widehat{q}_1 + \cdots + \widehat{q}_{n+1} \in \mathbb{R}^{n+1}. \tag{3}$$

By construction, the sum of the projections under π of these points is $q = q_1 + \cdots + q_{n+1} \in \mathbb{R}^n$.

Definition 4.2 *Let $\widehat{q}_1 + \cdots + \widehat{q}_{n+1}$, with $\widehat{q}_i \in \widehat{Q}_i$, be the unique Minkowski sum that sums up to $s(q)$. Then, $q_1 + \cdots + q_{n+1}$, which sums up to $q \in Q$, is the* optimal (Minkowski) sum *of $q \in Q$. The optimal summands are equivalently specified by $\alpha^{-1}|_Q(q)$.*

This definition is extended below to optimal sums expressing point sets of positive dimension. In the rest of this article we sometimes refer to an optimal sum as the unique sum expressing a point (or point set) in Q.

The genericity condition is met in practice by picking, for every i, a random integer vector of coefficients for l_i. Each entry is independently and uniformly distributed. The probability of failure of this scheme is analyzed in section 11. It is straightforward to check deterministically whether a particular choice of lifting functions satisfies the genericity requirement when $s(Q)$ is constructed.

Definition 4.3 *A polyhedral* subdivision *of a point set S is a collection of polyhedra whose union equals S, such that each intersection of two polyhedra of the same dimension is another polyhedron in the subdivision of lower dimension. The polyhedra of maximal dimension are called* maximal cells *or* facets. *We sometimes abuse terminology and refer to maximal cells simply as cells; moreover, we refer to the collection of maximal cells as the subdivision.*

Consider the natural polyhedral subdivision of the lower envelope $s(Q)$ of $\widehat{Q}$ into its faces. Let $\widehat{\Delta}$ denote the collection of lower envelope facets. It is easy to see that, in the same way that $\widehat{Q}$ is defined as the Minkowski sum of the lifted polytopes, every one of its faces can be expressed as the Minkowski sum of $n+1$ faces from the
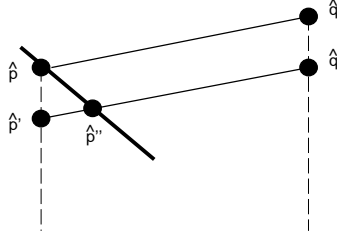
Figure 2: Proof of geometric lemma 4.5.

corresponding lifted polytopes, namely $\widehat{F}_1 + \cdots + \widehat{F}_{n+1}$, where $\widehat{F}_i$ a face of $\widehat{Q}_i$. The sum of dimensions of all $\widehat{F}_i$, for $1 \le i \le n+1$, is larger or equal to the face dimension, which lies in $\{0, 1, \ldots, n\}$. The genericity requirement on l_i implies the following property; the proof is found in [BS92].

$$\dim \widehat{F}_1 + \cdots + \dim \widehat{F}_{n+1} = \dim \sum_{i=1}^{n+1} \widehat{F}_i.$$

Moreover, given a face in $\widehat{\Delta}$, the collection $\widehat{F}_1, \ldots, \widehat{F}_{n+1}$ is uniquely defined by $\alpha^{-1}|_Q$.

The image of $\widehat{\Delta}$ under π *induces* a polyhedral subdivision Δ of Q whose maximal cells have a unique expression $F_1 + \cdots + F_{n+1}$, where F_i is the face of Q_i corresponding to $\widehat{F}_i$. When the lifting is generic, it is called a *mixed* subdivision. By inducing a subdivision we extend definition 4.2 to the cells of Δ.

Definition 4.2 (Continued) If a facet of $\widehat{\Delta}$ is the Minkowski sum $\widehat{F}_1 + \cdots + \widehat{F}_{n+1}$, where $\widehat{F}_i$ is a face of $\widehat{Q}_i$, then the Minkowski sum $F_1 + \cdots + F_{n+1}$, which expresses the corresponding cell of Δ, is called the *optimal* Minkowski sum of this cell.

For any q lying in a cell $F_1 + \cdots + F_{n+1}$, its optimal summand points q_i lie in F_i. Similarly, for $\widehat{q}$ lying on a lower envelope facet $\widehat{F}_1 + \cdots + \widehat{F}_{n+1}$, every summand in the point's unique sum is in $\widehat{F}_i$.

Lemma 4.4 *Consider any cell in Δ, of arbitrary dimension. If its optimal sum is $F_1 + \cdots + F_{n+1}$, F_i a face of Q_i, then at least one of the F_i is zero-dimensional, i.e., a vertex. In particular, this holds for maximal cells as well as points.*

Proof Since the lifting is linear, it does not affect the face dimension. Therefore, for the optimal summands F_i of a cell in Δ, $\sum_i \dim F_i = \sum_i \dim \widehat{F}_i \le n$. Since dimension is a non-negative quantity, we have established the lemma. $\square$

Lemma 4.5 (Geometric) *Let $\widehat{p}$ be a point in the interior of some facet of the subdivision $\widehat{\Delta}$ of the lower envelope $s(Q)$. By construction, $\widehat{p}$ has a unique optimal expression as a sum of points from $\widehat{Q}_1, \ldots, \widehat{Q}_{n+1}$, and at least one of these is vertex $\widehat{a}_{ij} = (a_{ij}, l_i(a_{ij}))$. Then $(\widehat{p} - \widehat{a}_{ij} + \widehat{Q}_i) \cap s(Q) = \widehat{p}$.*

Proof It suffices to show that every other point $\widehat{q} \in \widehat{p} - \widehat{a}_{ij} + \widehat{Q}_i$ lies above the lower envelope. It is easy to see that $\widehat{q}$ is contained in $\widehat{Q}$, because it is the sum of $n+1$ points, one from each lifted polytope. So $\widehat{q}$ is either on or above the lower envelope.

Now displace both $\widehat{p}$ and $\widehat{q}$ by decreasing their $(n+1)$-st coordinate by the same amount, thus defining points $\widehat{p}', \widehat{q}' \in \mathbb{R}^{n+1}$, see figure 2. The displacement should be small enough so that the line through $\widehat{p}', \widehat{q}'$ intersects the lower envelope in the facet that contains $\widehat{p}$. This is always possible because $\widehat{p}$ lies in the interior of a facet. If $\widehat{p}''$ is this intersection point, it is clear that $\widehat{Q}$ also contains $\widehat{p}'' - \widehat{a}_{ij} + \widehat{Q}_i$ by the previous argument.

Consider $\widehat{q} - \widehat{p}$ and $\widehat{q}' - \widehat{p}''$ as vectors rooted at the origin. By convexity, vector $\widehat{q}' - \widehat{p}''$ is smaller than $\widehat{q} - \widehat{p}$ and is also in the same direction, see figure 2. Now $\widehat{q} - \widehat{p}$ is contained in the convex set $\widehat{Q}_i - \widehat{a}_{ij}$, which contains the origin. It follows that $\widehat{q}' - \widehat{p}''$ is also contained in $\widehat{Q}_i - \widehat{a}_{ij}$, so $\widehat{q}' \in \widehat{p}'' - \widehat{a}_{ij} + \widehat{Q}_i \subset \widehat{Q}$. We have found point $\widehat{q}'$ such that $\pi(\widehat{q}) = \pi(\widehat{q}')$ but $h(\widehat{q}') < h(\widehat{q})$. Thus $\widehat{q}$ is not on the lower envelope. $\square$

8

Definition 4.6 *A* mixed cell *of mixed subdivision Δ is a (maximal) cell which is optimally expressed as a sum $F_1 + \cdots + F_{n+1}$ where exactly one F_i is a vertex. Thus the remaining F_j, for $j \neq i$, are edges. All (maximal) cells that are not mixed are called* non-mixed.

Lemma 4.7 [Stu94] *Let Δ be a mixed subdivision of Q. From the multilinearity of mixed volume it can be shown that the mixed volume of any n Newton polytopes is the sum of cell volumes, over all mixed cells with a vertex from the $(n+1)$-st support in their optimal sum. In other words,*

$$MV_{-i} = \sum_{\sigma = F_1 + \cdots + F_{i-1} + a_{ij} + F_{i+1} + \cdots + F_{n+1}} \mathrm{Vol}(\sigma), \qquad i = 1, \ldots, n+1,$$

where each F_k is an edge of Q_k, and $a_{ij} \in \mathcal{A}_i$.

5 Newton Matrix Construction

Relying on the properties of mixed subdivisions, we shall define a square Newton matrix M whose determinant is a nontrivial multiple of the sparse resultant. Relevant background material can be found in [GLS93, Sch93].

Matrix M is constructed by assigning a special role to polynomial f_1; any polynomial can assume this special role and an analogous construction will define the respective matrix. We say that f_1 is *distinguished* or that M is *associated* to f_1.

We shall index the rows and columns of M by a subset of the integer lattice points in Q. In order to associate a unique maximal cell to each point we perturb Q slightly so that each integer lattice point lies in the relative *interior* of a maximal cell of Δ. Let $\delta \in \mathbb{Q}^n$ be a sufficiently small vector in sufficiently generic position; the probability that a random δ is valid is analyzed in section 11.

Definition 5.1 *Let $\mathcal{E}$ be the following set of integer lattice points or, equivalently, n-dimensional exponent vectors:*

$$\mathcal{E} = \mathbb{Z}^n \cap (Q + \delta), \qquad \delta \in \mathbb{Q}^n.$$

This set is in bijective correspondence with a set of Laurent monomials in n variables. Let Δ_δ denote the subdivision obtained by shifting all cells of Δ by δ, which means

$$\Delta_\delta = \{\sigma + \delta : \sigma \in \Delta\}.$$

$\mathcal{E}$ will be the set that indexes the rows and columns of M. We shall denote by $\widehat{\Delta}_\delta$ the perturbed subdivision of the lower envelope $s(Q)$. We now define our selection rule for the elements of M; recall that m_i denotes the vertex cardinality of Q_i.

Definition 5.2 (Row content function) *Let $p \in \mathcal{E}$ lie in the interior of a cell $\delta + F_1 + \cdots + F_{n+1}$ of Δ_δ. The row content function RC is defined as follows.*

$$RC : \mathcal{E} \to \{1, \ldots, n+1\} \times \mathbb{N} : p \mapsto (i, j), \qquad j \in \{1, \ldots, m_i\},$$

where $i \in \{1, \ldots, n+1\}$ is the largest integer such that F_i is a vertex, and $F_i = a_{ij} \in \mathcal{A}_i$ for some $j \in \{1, \ldots, m_i\}$. In other words, $RC(p) = (i, j)$ implies that $\dim F_k > 0$, for all $k > i$.

It is clear that j lies in $\{1, \ldots, m_i\}$, since the corresponding summand a_{ij} is a vertex. Given the input supports, function RC can be computed as follows.

Algorithm 5.3 (RC Computation)
Input: Supports $\mathcal{A}_1, \ldots, \mathcal{A}_{n+1} \subset \mathbb{Z}^n$, lifting functions $l_1, \ldots, l_{n+1} \in \mathbb{Z}[x_1, \ldots, x_n]$, and perturbation vector $\delta \in \mathbb{Q}^n$.
Output: Vertex sets of Newton polytopes $Q_1, \ldots, Q_{n+1}$ and the pair $RC(p) \in \{1, 2, \ldots, n+1\} \times \mathbb{N}$ at every $p \in \mathcal{E}$.

9

Description The first stage constructs the vertex sets of Q_i by repeated application of linear programming, as discussed in [GLS93]. For a point a_{ik} in $\mathcal{A}_i = \{a_{i1}, \ldots, a_{i\mu_i}\}$, we test whether there is a feasible solution to the following system.

$$a_{ik} = \sum_{j=1, j \neq k}^{\mu_j} \lambda_j a_{ij}, \qquad \sum_{j=1, j \neq k}^{\mu_j} \lambda_j = 1, \qquad \lambda_j \geq 0, \; j = 1, \ldots, \mu_i.$$

Feasibility implies a_{ik} is not a vertex and can be dropped from the first sum above, for subsequent tests. Infeasibility implies a_{ik} is a vertex of Q_i.

Now assume Q_i has vertex set $\{a_{i1}, \ldots, a_{im_i}\}$ for $m_i \leq \mu_i$. For a point $p \in \mathcal{E}$, $p \in \sigma + \delta$ is equivalent to $p - \delta \in \sigma$, for some (maximal) cell σ of Δ_δ. We wish to find the optimal sum expressing $p - \delta$ in terms of points $p_i \in Q_i$. If $p - \delta$ lies in a mixed cell, exactly one p_i will be a vertex, otherwise at least two of them are vertices. To reduce to linear programming we introduce constraints

$$p - \delta = \sum_{i=1}^{n+1} p_i = \sum_{i=1}^{n+1} \sum_{j=1}^{m_i} \lambda_{ij} a_{ij},$$

where

$$\lambda_{ij} \geq 0, \text{ for } 1 \leq j \leq m_i, \qquad \text{and} \sum_{j=1}^{m_i} \lambda_{ij} = 1, \qquad i = 1, 2, \ldots, n+1.$$

The objective function must force the lifted point $s(p - \delta)$ to lie on the lower envelope of $\widehat{Q}$ by requiring that

$$\sum_{i=1}^{n+1} \sum_{j=1}^{m_i} \lambda_{ij} l_i(a_{ij}) \text{ be minimized,}$$

where the l_i are the generic lifting linear forms. For every i, the λ_{ij} that are positive in the optimal solution correspond to vertices a_{ij} summing up to $p_i \in Q_i$ in the optimal Minkowski sum of $p - \delta$. For points in the same cell $\sigma = F_1 + \cdots + F_{n+1}$, every summand face F_i in the optimal sum of σ is defined by all distinct vertices of Q_i appearing as summands in optimal sums of points in σ. The maximum i such that F_i is a vertex a_{ij}, defines $(i, j) = RC(p)$ for all $p \in \sigma$. $\square$

Finding all optimal sums offers a deterministic test for the genericity of δ by the following argument. If there exists a (non-maximal) cell $\sigma = \sum_i F_i$, where the F_i are computed by algorithm 5.3 and $\sum_i \dim F_i < n$, then for all $p \in \sigma$, $p - \delta$ does not lie in the interior of any maximal cell. In this case, the chosen δ is not sufficiently generic and a new one must be chosen.

Lemma 5.4 $p \in \mathcal{E}$ and $RC(p) = (i, j)$ implies $p - a_{ij} + a_{ik} \in \mathcal{E}$, for all $a_{ik} \in \mathcal{A}_i$.

Proof Since $p \in \mathcal{E}$, we have $p \in \sigma + \delta$, for some cell σ which can be expressed as a Minkowski sum $F_1 + \cdots + F_{i-1} + a_{ij} + F_{i+1} + \cdots + F_{n+1}$, where F_k is a face of Q_k. This implies that $p - a_{ij} + a_{ik}$ lies in

$$\sigma - a_{ij} + a_{ik} + \delta = F_1 + \cdots + F_{i-1} + a_{ik} + F_{i+1} + \cdots + F_{n+1} + \delta,$$

which is a subset of $Q + \delta$, for any $a_{ik} \in \mathcal{A}_i$. $\square$

This lemma implies that a square matrix can be defined as follows.

Definition 5.5 (Newton matrix) *Assume the notation used so far for polynomial system (1). The Newton matrix M is a matrix whose rows and columns are indexed by elements of $\mathcal{E}$. The element of M at row p and column q, for arbitrary $p, q \in \mathcal{E}$ with $RC(p) = (i, j)$, $i \in \{1, \ldots, n+1\}$, $j \in \{1, \ldots, m_i\}$, is*

$$M_{pq} = \begin{cases} c_{ik}, & \text{if } q - p + a_{ij} = a_{ik} \in \mathcal{A}_i, \text{ for some } k \in \{1, \ldots, \mu_i\}, \\ 0, & \text{if } q - p + a_{ij} \notin \mathcal{A}_i. \end{cases}$$

Therefore $M_{pp} = c_{ij}$, where $(i, j) = RC(p)$, for every $p \in \mathcal{E}$. The row of M indexed by $p \in \mathcal{E}$ is filled in à la Sylvester, or Macaulay, and represents the following monomial multiple of f_i :

$$x^{p-a_{ij}} f_i, \qquad \text{where } (i, j) = RC(p).$$

This discussion leads to the following theorem.

Theorem 5.6 *Newton matrix M is well-defined by definition 5.5 and can be constructed by algorithm 5.3, given the input supports $\mathcal{A}_i$, lifting functions l_i and perturbation δ. M is square and has dimension $|\mathcal{E}|$.*

6 A Nonzero Multiple of the Resultant

First we prove that the determinant of M is a multiple of the sparse resultant and then, using properties of the subdivision, that this multiple is not zero for almost all specializations of the coefficients.

Regarding polynomial rings as vector spaces over the coordinate field, with respect to some fixed monomial basis, has been a fruitful viewpoint in the study of resultants. An $(n+1)$-tuple of polynomials can be written as the concatenation of the $n+1$ respective polynomial coefficient vectors. Let M denote the endomorphism represented by matrix M.

$$M : \mathbb{C}^{|\mathcal{E}|} \to \mathbb{C}^{|\mathcal{E}|} : (g_1, \ldots, g_{n+1}) \mapsto g = g_1 f_1 + \cdots + g_{n+1} f_{n+1}, \tag{4}$$

where $g_1, \ldots, g_{n+1}, g$ lie in $\mathbb{C}[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$, and the support of every g_i is defined to be $\text{supp}(g_i) = \{p - a_{ij} | \, p \in \mathcal{E}, \, RC(p) = (i, j)\}$. The support of g_i coincides with the set of monomials that multiply f_i in defining the rows of M. This means there is a bijective correspondence, defined by function RC, between $\mathcal{E}$ and the union of the supports $\text{supp}(g_i)$. Since these supports are disjoint, they partition $\mathcal{E}$. Moreover, the support of g corresponds exactly to the monomials indexing the columns of M and equals $\mathcal{E}$. Endomorphism (4) is expressed as premultiplication of M by a row vector indexed by $\mathcal{E}$.

Lemma 6.1 *If there exists $\xi \in (\mathbb{C}^*)^n$ such that $f_1(\xi) = \cdots = f_{n+1}(\xi) = 0$, then $\det(M) = 0$.*

Proof   Assume that M is nonsingular. Then endomorphism M is surjective and we can choose polynomials $g_1, \ldots, g_{n+1}$ such that g in expression (4) is a monomial. This monomial is the sum of all products $g_i f_i$ so it must be zero at every solution ξ. This is impossible since ξ has no zero component. $\square$

Theorem 6.2 (Divisibility) *The sparse resultant R divides the determinant of Newton matrix M.*

Proof   For definitions and facts from algebraic geometry see [vdW50, Zip93]. The above lemma implies that $\det(M) = 0$ on the set Z_0 of specializations of c_{ij} such that the system has a solution in $(\mathbb{C}^*)^n$. Hence the variety of $\det(M)$ in the space of all coefficients contains Z_0 so it must also contain its closure Z; recall that a (algebraic) variety is the set of common zeros of a set of polynomials. By Hilbert's Nullstellensatz, $\det(M)$ is in the radical of the ideal generated by the resultant $R(\mathcal{A}_1, \ldots, \mathcal{A}_{n+1})$. Since the resultant is irreducible [PS93] its ideal coincides with the ideal's radical; such an ideal is called radical or self-radical. Therefore the ideal contains $\det(M)$, which is equivalent to saying that $\det(M)$ is the product of R with some polynomial over the coefficients c_{ij}. $\square$

To exclude the possibility that $\det(M)$ is identically zero, we show that it does not vanish under some family of specializations of the coefficients. We choose a parametrized specialization:

$$c_{ij} \mapsto t^{l_i(a_{ij})}, \qquad i = 1, \ldots, n+1, \; j = 1, \ldots, \mu_i, \tag{5}$$

where l_i are the lifting functions of the previous section, $\mu_i = |\mathcal{A}_i|$ and t is a new real indeterminate. Observe that the Newton polytope of the specialized f_i as a polynomial in $\mathbb{C}[x_1, x_1^{-1} \ldots, x_n, x_n^{-1}, t, t^{-1}]$ is precisely $\widehat{Q}_i$. Let $M(t)$ denote the matrix M under this specialization, and $\det(M)(t)$ denote its determinant, which is a polynomial in t with integer coefficients. We wish to show that this determinant does not vanish.

The Newton polytope of the polynomial in row p is $\widehat{Q}_i$ shifted so that its vertex $\widehat{a}_{ij}$ lies on the lower envelope, over p. Geometric lemma 4.5 essentially states that the rest of the polytope lies strictly above the lower envelope.

Now define a matrix $M'(t)$ by scaling the rows of $M(t)$; recall that $h(\widehat{p})$ is defined to express the $(n+1)$-st coordinate of any $\widehat{p} \in \widehat{Q}$.

$$M'_{pq}(t) = t^{h(\widehat{p})-l_i(a_{ij})} M_{pq}(t), \qquad p, q \in \mathcal{E}, \text{ where } (i, j) = RC(p), \ \widehat{p} = s(p - \delta).$$

In the language of lifted Newton polytopes, the row-scaling of $M(t)$ by powers of t corresponds to translating the Newton polytope of row p so that vertex $\widehat{a}_{ij}$ touches the lower envelope at $\widehat{p}$. With the current notation, the new determinant is expressed as follows.

$$\det(M')(t) = \det(M)(t) \prod_{p \in \mathcal{E}} t^{h(\widehat{p})-l_i(a_{ij})}. \tag{6}$$

Lemma 6.3 *For all nonzero elements $M'_{pq}(t)$ with $p \neq q$, $\deg(M'_{pq})(t) > \deg(M'_{qq})(t)$ holds for the degrees in t.*

Proof   Let $\widehat{p}$ and $\widehat{q}$ be the points on the lower envelope $s(Q)$ such that $\pi(\widehat{p}) = p - \delta$ and $\pi(\widehat{q}) = q - \delta$. Let $(\iota, \gamma) = RC(q)$, then $\deg M_{qq}(t) = l_\iota(a_{\iota\gamma})$ is the diagonal entry's degree in t.

$$\deg M'_{qq}(t) = h(\widehat{q}) - l_\iota(a_{\iota\gamma}) + \deg M_{qq}(t) = h(\widehat{q}).$$

Let $M_{pq} = c_{ik} \neq 0$, where $(i, j) = RC(p)$, then $q = p - a_{ij} + a_{ik}$, for some $a_{ik} \in \mathcal{A}_i$. Let $\widehat{q}' = \widehat{p} - \widehat{a}_{ij} + \widehat{a}_{ik}$.

$$\pi(\widehat{q}') = \pi(\widehat{p}) - a_{ij} + a_{ik} = p - \delta - a_{ij} + a_{ik} = q - \delta = \pi(\widehat{q}),$$

and

$$\deg M'_{pq}(t) = h(\widehat{p}) - l_i(a_{ij}) + l_i(a_{ik}) = h(\widehat{q}').$$

By geometric lemma 4.5, there is a unique point of minimum $(n+1)$-st coordinate on the lower envelope over $q - \delta$, namely $\widehat{q}$, so $\widehat{q}'$ cannot lie on the lower envelope, hence $h(\widehat{q}') > h(\widehat{q})$.   □

Theorem 6.4 *The lowest degree term in t of $\det(M)(t)$ is the product of the leading diagonal elements of $M(t)$. This term has unit coefficient and integer exponent $\sum_{p \in \mathcal{E}} l_i(a_{ij})$, where $(i, j) = RC(p)$. Therefore $\det(M)(t)$ does not vanish.*

Proof   The determinant of $M'(t)$ is

$$\det(M')(t) = \sum_{\sigma \in S(\mathcal{E})} (-1)^{\text{sign}(\sigma)} \prod_{q \in \mathcal{E}} M'_{\sigma(q)q}(t)$$

where $S(\mathcal{E})$ is the symmetric group on $\mathcal{E}$. For every σ not equal to the identity, we have $\sigma(q) \neq q$ for some q, so $\deg(M'_{\sigma(q)q})(t) > \deg(M'_{qq})(t)$ by the previous lemma. Thus

$$\deg \left(\prod_{q \in \mathcal{E}} M'_{qq}(t) \right) < \deg \left(\prod_{q \in \mathcal{E}} M'_{\sigma(q)q}(t) \right)$$

for every permutation σ other than the identity. This implies that the product of leading diagonal entries is a unique lowest power of t.   □

In particular, expression (6) implies that the trailing terms in $\det(M')(t)$ and $\det(M)(t)$ are, respectively,

$$\prod_{p \in \mathcal{E}} t^{h(\widehat{p})} : \widehat{p} = s(p - \delta) \qquad \text{and} \qquad \prod_{p \in \mathcal{E}} t^{l_i(a_{ij})} : \ RC(p) = (i, j). \tag{7}$$

Therefore there exists some sufficiently small value $t_0 > 0$ such that for every $t \in (0, t_0)$, the leading diagonal product is not canceled.

Corollary 6.5 *Matrix M is not singular for almost all coefficient specializations.*

Proof   There exists specialization (5) and an open interval for t between zero and a sufficiently small positive value t_0 so that $\det(M)(t)$ is nonzero by theorem 6.4. Hence $\det(M)$ is not identically zero. Consider the variety, in the space of complex coefficients, defined by $\det(M) = 0$, where the latter is considered as a polynomial in the coefficients. We have proven that this variety is not full-dimensional, hence it has zero volume [vdW50, Zip93]. □

It has been shown that the Newton matrix determinant gives a nontrivial multiple of the sparse resultant. The next question is how close this multiple is to the actual resultant.

7   The Determinant Degree

This section examines the degree of $\det(M)$ in the coefficients of each input polynomial f_i and compares it to the respective degrees of the sparse resultant.

Given fixed integer vectors $e_1, \ldots, e_n \in \mathbb{Z}^n$, define an n-dimensional *half-open integral parallelotope HO* :

$$HO = \{r_1 e_1 + r_2 e_2 + \cdots + r_n e_n \mid r_1, \ldots, r_n \in [0, 1)\}.$$

The point subset where $r_i = 0$ constitutes a facet of HO, while for $r_i = 1$ the opposite facet is defined, where HO is open. The two facets are related by a displacement vector $v = e_i$.

Lemma 7.1 *The number of integer lattice points in a half-open integral parallelotope equals its volume* $\mathrm{Vol}(HO)$.

Proof   It follows from [Sta80, Remark, p.335] that the number of lattice points is $n! \,\mathrm{Vol}(S)$ where S is the simplex with vertex set the origin and the endpoints of $e_1, \ldots, e_n$. The volume of the parallelotope HO is known to be $n! \,\mathrm{Vol}(S)$.   □

Proposition 7.2 *For any $\delta \in \mathbb{R}^n$, the number of integer lattice points in $HO + \delta$ equals* $\mathrm{Vol}(HO)$.

Proof   Imagine that HO is displaced by $t\delta$ as t varies from 0 to 1. Observe that for each facet of HO that is open or closed, the opposite facet is closed or open respectively, and that opposite facets are displaced from each other by an integral vector v. Thus as HO moves, whenever a lattice point p enters HO, a corresponding point at $p + v$ exits, and vice versa. Thus the number of lattice points inside HO remains constant. By lemma 7.1 this number is the parallelotope's volume.   □

A mixed cell in Δ_δ is the Minkowski sum of n edges and a vertex, hence a parallelotope in $\mathbb{R}^n$.

Lemma 7.3 *The number of rows indexed by all integer points in a mixed cell equals the cell's volume.*

Proof   The perturbation by δ guarantees that all integer points in $\mathcal{E}$ lie in the relative interior of a mixed cell, hence the number of these points equals the number of integer points in the half-open parallelotope defined by the n edges in the optimal sum of the cell. Since each point corresponds to exactly one row, proposition 7.2 implies the lemma.   □

The degree of $\det(M)$ in the coefficients of some f_i equals the number of rows expressing multiples of f_i.

Theorem 7.4 *Suppose that Newton matrix M is constructed having assigned a special role to f_1, i.e., with the row content function of definition 5.2. The degree of $\det(M)$ in the coefficients of f_1 equals $MV(Q_2, \ldots, Q_{n+1})$, which equals the degree of $R(\mathcal{A}_1, \ldots, \mathcal{A}_{n+1})$ in the same coefficients. Moreover, the degree of $\det(M)$ in the coefficients of f_j, for $j > 1$, is at least as large as MV_{-j}, which equals the respective degree of $R(\mathcal{A}_1, \ldots, \mathcal{A}_{n+1})$.*

Proof   The row content function RC chooses f_1 precisely at the mixed cells to which Q_1 contributes a vertex. By lemma 4.7, the total volume of these cells equals $MV(Q_2, \ldots, Q_{n+1})$. So the number of rows containing coefficients of f_1 is precisely $MV(Q_2, \ldots, Q_{n+1})$.

For every f_j, $j > 1$, the number of rows containing a multiple of f_j is at least as large as the number of points in the mixed cells to which Q_j contributes a vertex, because for these cells RC has no choice but to pick a vertex

in $\mathcal{A}_j$. These cells have point cardinality MV_{-j}. The correlation of MV_{-j} and the respective resultant degree is given by proposition 3.7. $\quad\square$

In other words, the determinant degree is tight with respect to the distinguished polynomial, so the GCD of $n + 1$ such determinants would give R. Before studying the computation of R in section 9, we examine certain ramifications.

8 Sparse Effective Nullstellensatz

The Newton matrix construction directly implies a sparse version of the effective Nullstellensatz, albeit only for ideals generated by at least $n + 1$ sufficiently generic polynomials. In other words, it is possible to bound the Newton polytopes of the polynomial coefficients in the ideal membership formula in terms of the Newton polytopes of the ideal generators. Recall that Newton polytopes provide a more precise characterization of a polynomial than total degree. For definitions and notation see [vdW50, Zip93].

Hilbert's Nullstellensatz is a fundamental result in algebraic geometry, and its effective version is crucial in computational algebraic geometry. For the classical Nullstellensatz, the problem was settled by Brownawell and Kollár.

Theorem 8.1 (Classical effective Nullstellensatz) [Bro87, Kol88] *Suppose $I = (f_1, \ldots, f_r)$ is an ideal in polynomial ring $K[x_1, \ldots, x_n]$, where K is an arbitrary field and $\deg f_i \le d$, for $i = 1, \ldots, r$. Let $h \in K[x_1, \ldots, x_n]$ have total degree $\deg h$. Polynomial h vanishes at the common zeros of I, i.e., $h \in \sqrt{I}$, if and only if there exist polynomials $g_1, \ldots, g_r \in K[x_1, \ldots, x_n]$ such that $\exists q \le 2(d + 1)^n$: $h^q = \sum_{i=1}^{r} g_i f_i$, where $\deg(g_i f_i) \le 2(\deg h + 1)(d + 1)^n$, $i = 1, \ldots, r$. If $I = (1)$ then*

$$1 = \sum_{i=1}^{r} g_i f_i, \qquad where \ \deg g_i f_i \le 2(d + 1)^n, \ i = 1, \ldots, r.$$

For the special case of sets of $n + 1$ *generic* polynomials over $\mathbb{C}$, matrix M is nonsingular by corollary 6.5 and function (4) is surjective. In addition, ideal I equals the entire ring and the associated variety is empty. This implies a restricted version of a sparse, or Newton, effective Nullstellensatz.

Theorem 8.2 *Suppose $f_1, \ldots, f_{n+1}$ are generic Laurent polynomials in $L = \mathbb{C}[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$ with Newton polytopes Q_i, and the generated ideal is $I = L$. Then there exist Laurent polynomials $g_1, \ldots, g_{n+1} \in L$, with Newton polytopes Q_i', such that*

$$1 = \sum_{i=1}^{n+1} g_i f_i \ : \quad Q_i' \subset Q_1 + \cdots + Q_{i-1} + Q_{i+1} + \cdots + Q_{n+1}, \quad i = 1, 2, \ldots, n + 1.$$

Proof   The surjectivity of M implies the existence of polynomials g_i such that their image under M is 1, possibly after translating some Newton polytopes Q_i. By definition, the support of g_i contains vector differences of the form $p - p_i$, where $p \in \mathcal{E}$ and p_i is a summand of p and a vertex of Q_i. Therefore,

$$\operatorname{supp}(g_i) \subset Q_1 + \cdots + Q_{i-1} + Q_{i+1} + \cdots + Q_{n+1}.$$

This proves the result. $\quad\square$

This result can easily be extended to arbitrary fields K and to an arbitrary number of polynomials. A harder step is considering the case where the Newton matrix construction does not apply, most importantly when the common roots form a set of positive dimension.

Conjecture 8.3 (Sparse effective Nullstellensatz) *Suppose $f_1, \ldots, f_r$, $r \ge 1$, are arbitrary Laurent polynomials in $L = K[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$ with Newton polytopes Q_i, where K is an arbitrary field and $I = L$ is the generated ideal. Then there exist Laurent polynomials $g_1, \ldots, g_r \in L$, with Newton polytopes Q_i', such that*

$$1 = \sum_{i=1}^{r} g_i f_i : \qquad Q_i' \subset Q_1 + \cdots + Q_{i-1} + Q_{i+1} + \cdots + Q_r.$$

9 Sparse Resultant Computation

This section discusses efficient ways for computing the sparse resultant from a set of Newton matrices. We wish to compute the resultant of a specialized system, as opposed to the resultant of a generic system which has been considered so far.

We first construct $n+1$ matrices $M_1, \ldots, M_{n+1}$, where each M_i has the minimum number of rows containing coefficients of f_i. These are obtained by modifying the row content function so that it returns (k, j), for $k \neq i$ and any j, whenever possible; equivalently, it returns (i, j), for some j, only at the corresponding mixed cells. Let $D_1, \ldots, D_{n+1}$ be the respective determinants, which are all multiples of the resultant. The GCD of $D_1, \ldots, D_{n+1}$ has the correct degree in the coefficients of every f_i and, since the GCD is divisible by the resultant R, it must be equal to R.

Unfortunately, this method does not always work because, although specialization commutes with addition and multiplication, it does not commute with the GCD operation. This is a fundamental problem in computing resultants for specialized systems, given a resultant matrix defined generically. The naive GCD approach can be used after a suitable perturbation of the specialized system, but here we propose two economical methods based on the approach of [Can88].

9.1 Division Method

Let $g_1, \ldots, g_{n+1}$ be the specializations of the given polynomials with coefficients in an arbitrary coefficient field. The idea is to introduce some indeterminates that will guarantee that, in dividing out the extraneous factors, denominators do not vanish. Then we compute with this smaller set of indeterminates and eliminate them at the end.

First, we choose polynomials $h_1, \ldots, h_{n+1}$ with *random* integer coefficients, such that h_i has support $\mathcal{A}_i$. Then, the input to the matrix construction algorithm is $f_1, \ldots, f_{n+1}$ specialized to the following system:

$$g_1 + u_1 h_1, \ldots, g_{n+1} + u_{n+1} h_{n+1},$$

where each u_i is a new indeterminate. $D_i(u_1, \ldots, u_n)$ is the determinant of matrix M_i constructed so that the number of rows corresponding to $g_i + u_i h_i$ is minimal. Let $b_i(u_1, \ldots, u_n)$ be the extraneous factor D_i/R, $i = 1, 2, \ldots, n+1$.

Lemma 9.1 *The extraneous factor $b_i(u_1, \ldots, u_n)$ in $D_i(u_1, \ldots, u_n)$, with respect to the sparse resultant $R(u_1, \ldots, u_n)$, does not depend on the coefficients of the i-th polynomial, hence it is independent of u_i, for any $i \in \{1, \ldots, n+1\}$. Therefore we can write*

$$D_i(u_1, \ldots, u_n) = b_i(u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n) R(u_1, \ldots, u_n).$$

Let $R^{(j)}(u_1, \ldots, u_j)$ be the coefficient of the highest-degree term, when R is regarded as a polynomial in indeterminates $u_{j+1}, \ldots, u_{n+1}$, for $j = 1, 2, \ldots, n+1$; lemma 9.3 elaborates on this notion. We define $D_i^{(j)}(u_1, \ldots, u_j)$ and $b_i^{(j)}(u_1, \ldots, u_j)$ analogously, for $i = 1, 2, \ldots, n+1$. Each $D_i^{(j)}$ is the determinant of Newton matrix M_i for the following specialized system:

$$g_1 + u_1 h_1, \ldots, g_j + u_j h_j, h_{j+1}, \ldots, h_{n+1}.$$

Observe that $R^{(n+1)} = R$, $D_i^{(n+1)} = D_i$, and $b_i^{(n+1)} = b_i$. Moreover, since b_i is independent of u_i, we must have $b_i^{(i)} = b_i^{(i-1)}$.

Definition 9.2 *Suppose that a polynomial $P(u_1, \ldots, u_{n+1})$ has maximum degree d_i in u_i. Then P is said to be* rectangular *if its support contains exponent vector $(d_1, d_2, \ldots d_{n+1})$.*

Lemma 9.3 *$R^{(j)}, D_i^{(j)}$, and $b_i^{(j)}$ are all rectangular polynomials, for $i, j = 1, 2, \ldots, n+1$.*

Proof   The degree of R in u_i is MV_{-i} by proposition 3.7. The coefficient of $\prod_i u_i^{(MV_{-i})}$ in R is the sparse resultant of system $h_1, \ldots, h_{n+1}$. To see this, consider what happens when the u_i take arbitrarily large values.

The resultant of the h_i is nonzero for sufficiently generic h_i because, in this case, the h_i have no common roots, and they have no zero coefficients by construction. Hence R and $R^{(j)}$ are rectangular, for $j = 1, 2, \ldots, n+1$.

Similarly, each determinant D_i is rectangular, because the coefficient of the monomial with highest degree in every u_i is the determinant of the same Newton matrix for system $h_1, \ldots, h_{n+1}$. This implies b_i is rectangular, and the same argument extends to $D_i^{(j)}, b_i^{(j)}$, for $j = 1, 2, \ldots, n+1$. $\qquad \square$

It follows that $D_i^{(j)} = b_i^{(j)} R^{(j)}$ for all i and j, and, since $b_i^{(i)} = b_i^{(i-1)}$, we can eliminate $b_i^{(i)}$:

$$R^{(i)} = \frac{D_i^{(i)}}{D_i^{(i-1)}} R^{(i-1)}, \qquad i = 1, \ldots, n+1. \tag{8}$$

$R^{(0)}$ is some nonzero scalar, which does not affect the computation of R. $R = R^{(n+1)}$, so setting $u_1 = \cdots = u_{n+1} = 0$ in $R^{(n+1)}$ will give the resultant of system $g_1, \ldots, g_{n+1}$. This computation requires $2n + 1$ divisions, because for $i = 1, 2, \ldots, n+1$, we must compute $b_i^{(i-1)} = D_i^{(i-1)}/R^{(i-1)}$ and then $R^{(i)} = D_i^{(i)}/b_i^{(i-1)}$, except for $i = 1$, where $R^{(1)} = D_1^{(1)}/D_1^{(0)}$. However, the computation involves polynomials in $u_1, \ldots, u_{n+1}$ and would be practical only for small n. In what follows we reduce the number of indeterminates to one.

Observe that identity (8) is valid for any specialization of the u_i indeterminates, as long as no denominator vanishes. So we take $u_1 = u_2 = \cdots = u_{n+1} = u$. Lemma 9.3 still holds by an analogous proof, provided the h_i have no common roots. Hence, recurrence (8) establishes the following theorem.

Theorem 9.4 *Suppose that the choice of $h_1, \ldots, h_{n+1}$ is sufficiently generic as specified above. Then this method constructs the sparse resultant from the Newton matrices associated to the $n+1$ polynomials after a sequence of $2n + 1$ exact divisions on univariate polynomials.*

It is possible to detect failure of the condition on the h_i deterministically, in which case new randomized variables are chosen as the h_i coefficients. A bound on the probability of failure and the asymptotic bit complexity are analyzed in section 12.1.

In the more favorable case that the g_i polynomials are sufficiently generic, which means that no $D_i^{(j)}$ vanishes, we may compute $D_i^{(j)}$ for $u = 0$, i.e., for specialized system $g_1, \ldots, g_j, h_{j+1}, \ldots, h_{n+1}$.

9.2   GCD Method

We present a simpler method that strongly exploits the subdivision-based construction and applies to the case that the specialized coefficients are nonzero and chosen from some polynomial ring over $\mathbb{Q}$. It is illustrated in the example of section 10.

Again we choose polynomials h_i with random integer coefficients and supports $\mathcal{A}_i$. Then, the specialized system is as follows.

$$g_1 + uh_1, \ldots, g_{n+1} + uh_{n+1}.$$

By Hilbert's irreducibility theorem [Zip93, sect. 19.3], the resultant R will remain irreducible over $\mathbb{Q}[u]$ for sufficiently generic h_i. This is a Las Vegas step in the sense that failure of the choices is detected deterministically; the error probability is calculated in section 12.2. Let $D_1(u)$ be the determinant of M_1 under this specialization, and let $b(u)$ be the extraneous factor defined by $D_1(u) = b(u)R(u)$.

Suppose, without loss of generality, that M_1 was defined using a linear form l_1 which is so much larger than the others that whenever a vertex a_{1j} of Q_1 appears in the optimal Minkowski sum of a point in $\mathcal{E}$, this vertex must be the one which minimizes l_1. In other words, in every row containing coefficients of f_1, the leading diagonal element will be c_{1j}, with j such that

$$l_1(a_{1j}) = \min \{l_1(a_{1k}) \; : \; a_{1k} \in \mathcal{A}_1\}.$$

Now consider the following system:

$$x^{a_{1j}} + uh_1, g_2 + uh_2, \ldots, g_{n+1} + uh_{n+1},$$

and construct Newton matrix M_1' associated to the first polynomial. Let $D_1'(u)$ be the determinant of M_1', with $D_1'(u) = b'(u)R'(u)$, where $R'(u)$ is the sparse resultant of the new system and $b'(u)$ is the extraneous factor. $R'(u)$ is irreducible for sufficiently generic h_i.
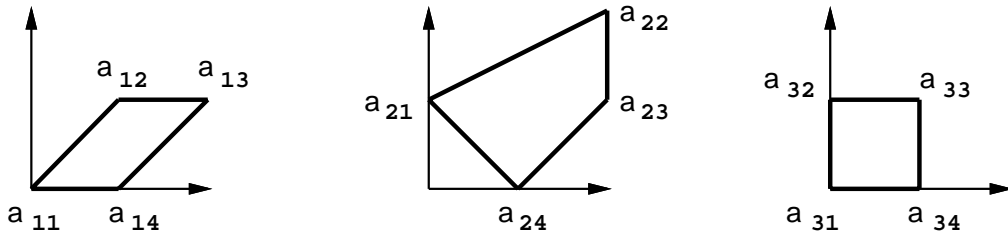
Figure 3: The Newton polytopes and the exponent vectors a_{ij}, each corresponding to the term with coefficient c_{ij}.

$b'(u)$ does not depend on the first polynomial by lemma 9.1. The two systems have the same supports and the last n polynomials are identical, hence the extraneous factors are equal to each other, i.e., $b'(u) = b(u)$. Since $R(u)$ and $R'(u)$ are irreducible, $b(u) = \mathrm{GCD}(D_1(u), D'_1(u))$. Therefore

$$R(u) = \frac{D_1(u)}{\mathrm{GCD}(D_1(u), D'_1(u))},$$

and specializing $u = 0$ gives the resultant of $g_1, \ldots, g_{n+1}$.

Theorem 9.5 *If the choice of $h_1, \ldots, h_{n+1}$ is sufficiently generic as specified above, then the sparse resultant can be computed by a GCD operation on univariate Newton matrix determinants, followed by an exact division on univariate polynomials.*

It is worth noting that the degree of $b(u)$ is known in advance, namely it is the difference of the size of M_1 minus the total degree of the sparse resultant. Thus the GCD computation is branch-free and reduces to calculation of the appropriate minors of the Sylvester matrix, or subresultants, of $D_1(u)$ and $D'_1(u)$ [Loo82]. The complexity of the method is analyzed in section 12.2.

Once again, there is a more favorable case that simplifies the situation. Namely, if the given polynomials g_i are generic enough, meaning that their sparse resultant is irreducible and the determinants $D_1(0)$ and $D'_1(0)$ are both nonzero, then R can be computed directly as $D_1(0)/\mathrm{GCD}(D_1(0), D'_1(0))$.

10 A Bivariate Example

The Newton matrix construction is illustrated for a system of 3 polynomials in 2 unknowns:

$$
\begin{aligned}
f_1 &= c_{11} + c_{12}xy + c_{13}x^2y + c_{14}x, \\
f_2 &= c_{21}y + c_{22}x^2y^2 + c_{23}x^2y + c_{24}x, \\
f_3 &= c_{31} + c_{32}y + c_{33}xy + c_{34}x.
\end{aligned}
$$

The Newton polytopes are shown in figure 3. The mixed volumes are $MV(Q_1, Q_2) = 4$, $MV(Q_2, Q_3) = 4$, $MV(Q_3, Q_1) = 3$, so the sparse resultant degree is 11. Compare this with the Bézout numbers of these subsystems: $8, 6, 12$; hence the classical resultant degree is 26. Assume, without loss of generality, that the lifting functions are $l_1(x, y) = Lx + L^2y, l_2(x, y) = -L^2x - y, l_3(x, y) = x - Ly$, where L is a sufficiently large positive integer. The three lifted Newton polytopes lie in three-dimensional space, the third coordinate being defined by the lifting functions. The linearity of l_i implies that the lifted polytopes lie in a two-dimensional plane, as shown in figure 4 from a perspective view. The figure also depicts the lower envelope $s(Q)$ of their Minkowski sum $\widehat{Q}$ constructed by the convex hull program of [Emi98]. The program automatically triangulates all output facets; this triangulation is immaterial in inducing a mixed subdivision of Q. This figure, as well as figure 5, are drawn by GEOMVIEW.

Figure 5 depicts the projection of the lower envelope, which lies in three-dimensional space, to the two-dimensional Euclidean plane, thus yielding the Minkowski sum Q of the original Newton polytopes. The perspective view shows the bijective correspondence between facets of $s(Q)$ and maximal cells of Q. Again, all cells are triangulated as a side-effect of the convex hull code. Having computed the mixed subdivision of Q for the
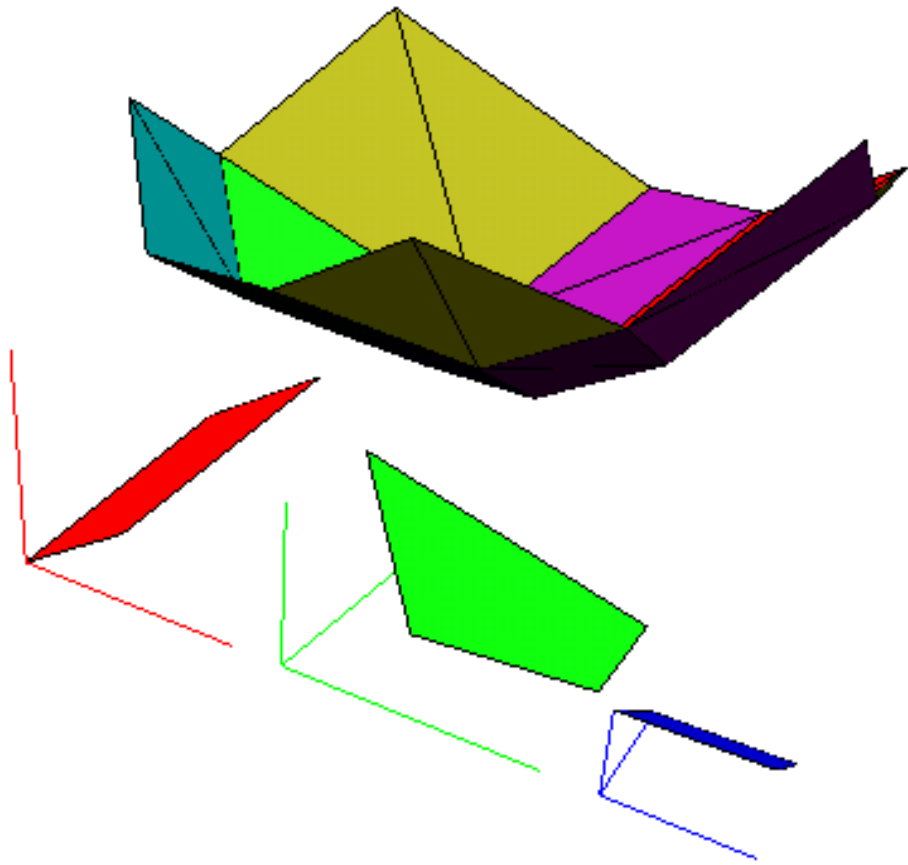
Figure 4: The lifted Newton polytopes and a triangulation of the lower envelope of their Minkowski sum.
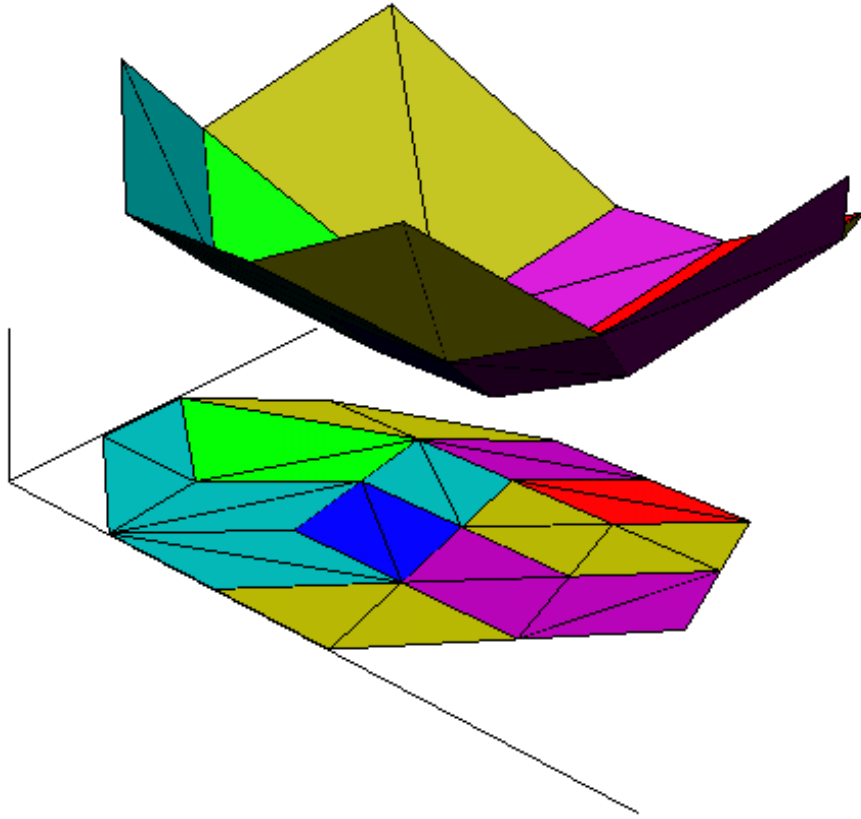
Figure 5: The lower envelope of the Minkowski sum of all lifted Newton polytopes and its planar projection.
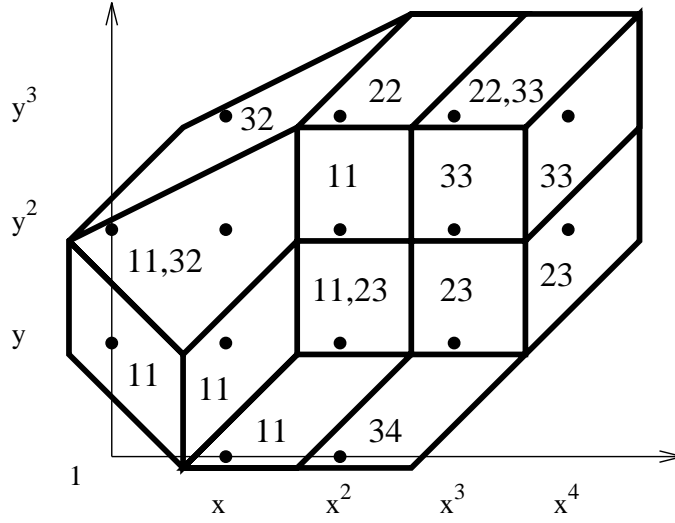
Figure 6: The mixed subdivision Δ_δ of $Q + \delta$, where $\delta = (-3/8, -1/8)$. Each cell is labeled with the indices of the Newton polytope vertices that appear in its optimal sum: ij denotes vertex a_{ij}.

given lifting, we apply a small perturbation in order to associate a unique sum of Newton polytope faces to each maximal cell. The subdivision Δ_δ of $Q + \delta$ into maximal cells and the indices of the Newton polytope vertices in the optimal sums are shown in figure 6, for $\delta = (-3/8, -1/8)$. Only mixed cells have a unique vertex associated; for the other three, we pick the vertex maximizing the first index.

Matrix M, the Newton matrix associated to f_1, appears below with rows and columns indexed by the integer points in $\mathcal{E}$, and has dimension 15. For instance, the first row corresponds to point $(1, 0)$ which lies in a maximal mixed cell expressed uniquely as $a_{11} + [a_{24}, a_{23}] + [a_{31}, a_{34}]$, where $[a, a']$ stands for a Newton polytope edge. Since $a_{11} = (0, 0)$, the polynomial filling in the row is $x f_1 = c_{11} x + c_{12} x^2 y + c_{13} x^3 y + c_{14} x^2$. M contains, by construction, the minimum number of f_1 rows, namely 4. The total number of rows is $4 + 4 + 7 = 15$, i.e. the determinant degree is higher than optimal by 1 and 3, respectively, in the coefficients of f_2 and f_3.

	1,0	2,0	0,1	1,1	2,1	3,1	0,2	1,2	2,2	3,2	4,2	1,3	2,3	3,3	4,3
1,0	c_{11}	c_{14}	0	0	c_{12}	c_{13}	0	0	0	0	0	0	0	0	0
2,0	c_{31}	c_{34}	0	c_{32}	c_{33}	0	0	0	0	0	0	0	0	0	0
0,1	0	0	c_{11}	c_{14}	0	0	0	c_{12}	c_{13}	0	0	0	0	0	0
1,1	0	0	0	c_{11}	c_{14}	0	0	0	c_{12}	c_{13}	0	0	0	0	0
2,1	c_{24}	0	c_{21}	0	c_{23}	0	0	0	c_{22}	0	0	0	0	0	0
3,1	0	c_{24}	0	c_{21}	0	c_{23}	0	0	0	c_{22}	0	0	0	0	0
0,2	0	0	c_{31}	c_{34}	0	0	c_{32}	c_{33}	0	0	0	0	0	0	0
1,2	0	0	0	c_{31}	c_{34}	0	0	c_{32}	c_{33}	0	0	0	0	0	0
2,2	0	0	0	0	0	0	0	0	c_{11}	c_{14}	0	0	0	c_{12}	c_{13}
3,2	0	0	0	0	c_{31}	c_{34}	0	0	c_{32}	c_{33}	0	0	0	0	0
4,2	0	0	0	0	0	c_{24}	0	0	c_{21}	0	c_{23}	0	0	0	c_{22}
1,3	0	0	0	0	0	0	0	c_{31}	c_{34}	0	0	c_{32}	c_{33}	0	0
2,3	0	0	0	c_{24}	0	0	c_{21}	0	c_{23}	0	0	0	c_{22}	0	0
3,3	0	0	0	0	0	0	0	0	c_{31}	c_{34}	0	0	c_{32}	c_{33}	0
4,3	0	0	0	0	0	0	0	0	0	c_{31}	c_{34}	0	0	c_{32}	c_{33}

To illustrate the computation of the sparse resultant we consider a specialization of the system to

$$
\begin{aligned}
g_1 &= -1 + 2xy - 3x^2 y - 5x, \\
g_2 &= 7y - 11x^2 y^2 + 13x^2 y - 17x, \\
g_3 &= -19 - 23y - xy + 3x.
\end{aligned}
$$

In order to apply the GCD method of section 9.2, we choose random integer polynomials, with coefficients

uniformly and independently distributed in $[0, 1000]$:

$$
\begin{aligned}
h_1 &= 82 + 271xy + 698x^2y + 564x, \\
h_2 &= 977y + 539x^2y^2 + 86x^2y + 769x, \\
h_3 &= 922 + 410y + 656xy + 164x.
\end{aligned}
$$

Then $D_1(u)$ and $D_1(u)'$ are both of degree 15 in u. Their GCD is

$$
b(u) = 9483529600u^4 + 355094440u^3 - 131557356u^2 + 4710998u - 6877,
$$

which gives $R(u)$ as a u-polynomial of degree 11 and

$$
R(0) = 541503745717.
$$

This proves that there are no common solutions in $(\mathbb{C}^*)^2$ for g_1, g_2, g_3.

Section 13 states conjecture 13.1 on the existence of a submatrix $M^{(nm)}$ of M, defined by the points in non-mixed cells, such that the quotient $\det M / \det M^{(nm)}$ equals the sparse resultant. In this example,

$$
M^{(nm)} = \begin{bmatrix}
c_{23} & 0 & 0 & 0 \\
0 & c_{32} & c_{33} & 0 \\
c_{34} & 0 & c_{32} & 0 \\
0 & 0 & 0 & c_{33}
\end{bmatrix},
$$

and $\det M / \det M^{(nm)}$ produces $R(u)$ as above, for the specialized system $g_i + uh_i, i = 1, 2, \ldots, n + 1$, and the correct sparse resultant, by setting $u = 0$. Hence the conjecture is verified for this example.

11 Complexity of the Matrix Construction

This section analyzes the randomization and time complexity of constructing the Newton matrix, and combines the two in estimating the overall complexity. The viewpoint is that of worst-case asymptotic bit complexity, in the computational model of the *bit-cost*, or logarithmic-cost, RAM [AHU74, Ch. 1]. In complexity bounds we sometimes ignore polylogarithmic factors in the parameters appearing in polynomial factors; this is denoted by $O^*(\cdot)$.

The first step is to bound the error probabilities in the two randomized steps, namely choosing l_i and δ. Recall that both steps are of the Las Vegas type.

Lemma 11.1 *Let m be the maximum vertex cardinality of any Q_i over all $i \in \{1, \ldots, n + 1\}$. If all $n(n + 1)$ coefficients of $l_i \in \mathbb{Z}[x_1, \ldots, x_n]$ are chosen independently and uniformly from an interval of size 2^{L_l}, where $L_l \in \mathbb{Z}_{>0}$, then the probability $\epsilon_l \in (0, 1)$ that the lifting is not sufficiently generic is bounded as follows.*

$$
\epsilon_l \leq \frac{1}{2^{L_l}} \frac{1}{2} m^{n+1}(m^n - 1), \quad \text{which implies} \quad L_l = O\left(n \log m + \log \frac{1}{\epsilon_l}\right),
$$

Proof The l_i are not sufficiently generic if there exist two distinct sequences $(p_1, \ldots, p_{n+1})$ and $(q_1, \ldots, q_{n+1})$, with p_i, q_i vertices of Q_i, such that $\sum_i p_i = \sum_i q_i$ and the sums of their lifted images are equal. We bound the probability ϵ_l that $\sum_i l_i(p_i) = \sum_i l_i(q_i)$.

Since the sequences are distinct, we can assume, without loss of generality, that p_1 and q_1 differ in their first coordinate. Fix all coefficients in the $n + 1$ lifting functions, except for the the first coefficient of l_1. Then there is at most one integer value of this coefficient for which the two sums of lifted points are equal. The probability of picking the single undesired integer is $1/2^{L_l}$.

This probability must be multiplied by the number of distinct pairs $((p_i), (q_i))$ whose respective sums are equal in $\mathbb{R}^n$. To obtain an upper bound suppose that all points in (p_i) are chosen at will, in any of m^{n+1} ways. Once $q_1, q_2, \ldots, q_n$ are chosen, q_{n+1} shall be determined. If the subsequences of n elements are identical, then $q_{n+1} = p_{n+1}$, which makes the complete sequences identical. Hence the two subsequences must differ. There are at most $m^n - 1$ valid choices for $(q_1, q_2, \ldots, q_n)$, given (p_i). Since the two sequences are interchangeable, the total number of possible pairs is at most $m^{n+1}(m^n - 1)/2$. $\square$

The following result, also known as Schwartz's lemma, shall be applied repeatedly.

Lemma 11.2 [Sch80, lem. 1], [Zip93, prop. 98] *Given is nonzero polynomial P in any number of variables, with total degree $\deg P$. Consider a specialization of the variables, distributed independently and uniformly in a set of S values. Then, the probability that the specialized polynomial vanishes is bounded by $\deg P / S$.*

Let $e < 2.718$ denote the exponential base and s the scaling factor of the system as defined in definition 3.9.

Lemma 11.3 *Assume that the entries of $\delta \in \mathbb{Q}^n$ have the numerators distributed uniformly and independently in a set of 2^{L_δ} integer values and the denominators are all equal to some sufficiently large integer. The total probability of failure for the random choice of δ, denoted $\epsilon_\delta \in (0,1)$, is bounded as follows.*

$$\epsilon_\delta \leq \frac{(|\mathcal{E}|\, n!)^2}{2^{L_\delta}}, \quad \text{which implies} \quad L_\delta = O\left(\log|\mathcal{E}| + n\log n + \log\frac{1}{\epsilon_\delta}\right).$$

Proof Every maximal cell boundary is comprised of cells in Δ of dimension $n-1$, each being part of a hyperplane in $\mathbb{R}^n$. Therefore, every $(n-1)$-dimensional cell is expressed as a subset of the roots of a linear polynomial. The random choice for δ is not generic if δ lies in some $(n-1)$-dimensional cell, which happens with probability at most $1/2^{L_\delta}$, by lemma 11.2.

Now we have to bound the number of $(n-1)$-dimensional cells in Δ. We know that each maximal cell has volume at least $1/n!$ because it is defined by integer points. The volume of a convex polytope is asymptotically equal to the number of integer lattice points in its interior, by Ehrart's theorem [Ehr67]. The number of maximal cells is then $O(|\mathcal{E}|\, n!)$. Since every $(n-1)$-dimensional cell can be defined as the intersection of two maximal cells, the number of the former is at most $O((|\mathcal{E}|\, n!)^2)$. We use Stirling's approximation [AHU74, Zip93] to bound $n! = O(n\log n)$ in estimating L_δ. $\quad\square$

Instead of applying Ehrart's theorem, we can bound the volume of Q by theorem 3.10 under the additional hypothesis that all Q_i have positive volume.

We now examine the complexity of constructing M. The change of variables that may be required to ensure that $\sum_{i=1}^{n+1} \mathcal{A}_i$ generates $\mathbb{Z}^n$ involves the computation of a Smith normal form [HM91]. Its asymptotic complexity is dominated so we ignore it in the sequel.

Identifying the vertices of all Newton polytopes may be reduced to linear programming. We can apply any polynomial-time algorithm such as Khachiyan's ellipsoid method or Karmarkar's algorithm. In the case of Karmarkar's algorithm [Kar84] the bit complexity for a linear program of V variables, C constraints and B bits per coefficient is

$$O^*(C^2 V^{5.5} B^2).$$

Let d be the highest degree of any input polynomial in a single variable and $\mu = \max_i\{\mu_i\}$ be the maximum number of support points per polynomial. Recall that the vertex set of Q_i has cardinality m_i, $m_i \leq \mu_i$, and that $m = \max_i\{m_i\}$.

Lemma 11.4 *The bit complexity for computing all Newton polytope vertices is $O(n^3\mu^{6.5}\log^2 d)$.*

Proof To compute the vertices of each Q_i algorithm 5.3 applies linear programming with $C = O(n)$ constraints and $V = O(\mu_i)$ variables, where the maximum size of any coefficient is $\log d$. The bit complexity to decide whether a support point is a vertex is $O^*(n^2\mu_i^{5.5}\log^2 d)$. There are at most μ tests for each of the $n+1$ polytopes. $\quad\square$

The rest of algorithm 5.3 associates a unique optimal sum of points $p_i \in Q_i$ to every $p \in \mathcal{E}$.

Lemma 11.5 *With the current notation, the total bit complexity for computing the optimal sum expression of every $p \in \mathcal{E}$ is*

$$O^*\left(|\mathcal{E}|n^{9.5}m^{5.5}\log^2 d\,\log^2\frac{1}{\epsilon_l\epsilon_\delta}\right).$$

Proof Optimal sum expressions are computed in the second phase of algorithm 5.3 by linear programming. Each linear program has $C = O(n)$ constraints in $V = O(nm)$ variables. The bit size of the coefficients depends on the bit size of δ, of the points in Q_i and of $l_i(a_{ij})$. By lemma 11.3 the first two give a total of $O^*(\log|\mathcal{E}| + n + \log(1/\epsilon_\delta) + \log d)$. A lifted coordinate is a sum of $n+1$ products, each of a l_i coefficient multiplied by an input

point coordinate, hence of size $O(\log n + \log d + L_l)$. By lemma 11.1, this is $O^*(\log d + n \log m + \log(1/\epsilon_l))$. Hence the coefficient bit size is

$$B = O^* \left(\log |\mathcal{E}| + n \log m + \log d + \log \frac{1}{\epsilon_\delta \epsilon_l} \right).$$

For simplicity, we use $B = O^*(\log |\mathcal{E}| + n \log m \log d \, \log(1/\epsilon_\delta \epsilon_l))$, and the claim follows. □

Given the optimal sum of every point in $\mathcal{E}$, Newton matrix M is completely specified and can be represented implicitly by the polynomials and the monomials which index its rows and columns. The overall complexity is established in the next theorem, by combining the two previous lemmas. If an explicit dense representation is required, then an additional cost of $O(|\mathcal{E}|^2)$ must be included. For different matrix representations, see [AHU74].

Theorem 11.6 *Given polynomials $f_1, \ldots, f_{n+1}$, the algorithm computes an implicit representation of Newton matrix M with worst-case bit complexity*

$$O^* \left(|\mathcal{E}| n^{9.5} \mu^{6.5} \log^2 d \, \log^2 \frac{1}{\epsilon_l \epsilon_\delta} \right),$$

where μ is the maximum point cardinality of the $n+1$ supports, d is the maximum degree of any polynomial in any variable, and $\epsilon_l, \epsilon_\delta \in (0,1)$ are the error probabilities for the lifting scheme and the perturbation, respectively.

Corollary 11.7 *Assume the notation of the previous theorem. Let the system's scaling factor be s and the total degree of the sparse resultant be $\deg R$. If all Newton polytopes have positive volume then the bit complexity is*

$$O^* \left((se)^n \deg R \, \mu^{6.5} \log^2 \frac{1}{\epsilon_l \epsilon_\delta} \right).$$

Proof The bound follows by applying Ehrart's theorem [Ehr67], which bounds $|\mathcal{E}|$ asymptotically by the volume of Q. Then $|\mathcal{E}| = O(s^n e^{n+1} \deg R / n^{3/2})$ by theorem 3.10. Moreover, since all Newton polytopes are full-dimensional, $|\mathcal{E}| \geq d$, so the logarithmic factor in d can be dropped. Similarly, the polynomial factor in n is dropped because of $(se)^n$. □

This bound demonstrates the polynomial dependence of the complexity on the sparse resultant's total degree and the simply exponential dependence on n. Note that s is typically a small constant.

12 Complexity of the Resultant Computation

This section analyzes the worst-case asymptotic bit complexity and randomization complexity of computing the actual sparse resultant from a set of Newton matrices. First, the error probabilities are bounded for the randomized steps and then the total bit complexity is asserted.

The computational model is again the bit-cost RAM. $O^*(\cdot)$ indicates that we have ignored polylogarithmic factors, and e denotes the exponential base. This section applies the current record asymptotic complexity for matrix multiplication, namely $O(N^{2.376})$ for $N \times N$ matrices [CW90].

In manipulating univariate polynomials, we shall use asymptotic bounds based on the Fast Fourier Transform (FFT). The running time for the interpolation of a univariate polynomial of degree D from its values at D points is $O^*(DB)$, where B stands for the bit size of the polynomial's coefficients [AHU74, sect. 7]. Given two univariate polynomials of degree at most D and with coefficient size bounded by B, where one polynomial divides the other, the computation of their quotient and product has bit complexity $O^*(DB)$ [AHU74, sect. 8].

12.1 Division Method

We consider the division method of section 9.1. First, we have to bound the probability that a particular choice of a set of h_i polynomials makes their sparse resultant vanish or causes $D_i^{(j)}(u_1, \ldots, u_j)$ to drop degree, for some $i, j \in \{1, \ldots, n+1\}$. Both events reduce to the vanishing, under a specialization, of a nonzero polynomial in the coefficients of h_i.

Lemma 12.1 *When the h_i are specialized with each coefficient having L_h bits, the probability $\epsilon_h \in (0,1)$ that this choice is not sufficiently generic for our algorithm is*

$$\epsilon_h \leq \left((n+1)^2 + 1\right) \frac{\deg R}{2^{L_h}}, \quad \text{which implies} \quad L_h = O\left(\log n + \log(\deg R) + \log \frac{1}{\epsilon_h}\right),$$

where $\deg R$ is the total degree of the sparse resultant.

Proof The resultant of the h_i has the same degree as the resultant of f_i, since the two polynomial systems have identical supports. Moreover, the degree is at least as high as that of any $D_i^{(j)}$, so the highest error probability occurs for the resultant of the h_i. This probability is bounded by $\deg R / 2^{L_h}$, by lemma 11.2. The number of distinct polynomials that may vanish is at most $(n+1)^2 + 1$. □

Theorem 12.2 *Let b and L_h be the maximum bit length of the g_i and the h_i coefficients respectively. Given the $2(n+1)$ required Newton matrices, the computation of the sparse resultant of the g_i by the division method has bit complexity*

$$O^*\left(|\mathcal{E}|^{3.376} \deg R \left(b + L_h\right)\right),$$

where $\deg R$ is the total degree of the sparse resultant.

Proof A straightforward approach is to evaluate the $2(n+1)$ determinants at certain points, then multiply and divide, as specified by recurrence (8), the respective values pointwise. This produces the values of $R(u)$ at these points. Given $\deg R$ values, we can interpolate $R(u)$ in $O((\deg R)^2(b + L_h))$ bit operations. As for the complexity of the evaluation phase, there are $O(n \deg R)$ determinant evaluations, each with bit complexity $O^*(|\mathcal{E}|^{3.376}(b + L_h))$. The overall bound follows by applying $\deg R \leq |\mathcal{E}|$. □

Corollary 12.3 *Consider the context of the previous theorem and assume that all $n+1$ input Newton polytopes have positive volume. Let the system's scaling factor be s and let μ be the maximum support cardinality. Then the total bit complexity of constructing the required Newton matrices and computing the sparse resultant R for an arbitrary specialization is*

$$O^*\left((s^n e^n)^{3.376} (\deg R)^{4.376}\, \mu^{6.5} \left(\log^2 \frac{1}{\epsilon_l \epsilon_\delta} + b + \log \frac{1}{\epsilon_h}\right)\right).$$

Proof Theorem 3.10 bounds $|\mathcal{E}|$ via Ehrart's theorem, Lemma 12.1 bounds L_h and corollary 11.7 bounds the complexity of constructing each of the $2(n+1)$ Newton matrices. □

12.2 GCD Method

In the GCD method of section 9.2, we pick the coefficients of each h_i uniformly and independently with L_h bits each. To estimate the error probability we adapt a quantified version of Hilbert's irreducibility theorem to our case.

Proposition 12.4 [Zip93, prop. 133] *Given polynomial $R(c_h, u)$, where c_h is the vector of all h_i coefficients and u a variable, such that R is irreducible over $\mathbb{Q}$, we specialize c_h to random integer values of absolute value bounded by $S > 0$. Then the number of c_h specializations for which $R(u)$ is reducible, is bounded by $D\, S^{|c_h|-1/2} \log S$, where D is a function of the total degree $\deg R$.*

For independently and uniformly chosen coefficients, the probability of a choice that makes $R(c_h, u)$ reducible is at most $D \log S/(2^{|c_h|} S^{1/2})$. We make use of the following conjecture.

Conjecture 12.5 [Zip93, sect. 19.3] *In the context of the last proposition, there exist absolute constants c, ρ, such that $D < c(\deg R)^\rho$.*

Lemma 12.6 *Assume the validity of the previous conjecture and suppose that the coefficients of every h_i are independently and uniformly distributed, each with L_h bits. Then the probability $\epsilon_h \in (0,1)$ that they are not sufficiently generic with respect to the GCD method is*

$$\epsilon_h \le \frac{c(\deg R)^\rho L_h}{2^n(2^{L_h/2}-1)}, \quad which \ implies \quad L_h = O\left(\log(\deg R) + \log\frac{1}{\epsilon_h}\right),$$

where c, ρ are the constants of the previous conjecture.

Proof The h_i are sufficiently generic if the resultant of the system perturbed by these h_i is irreducible. It suffices to guarantee that the resultant of the h_i is irreducible. If we set $S = 2^{L_h} - 1$ and $|c_h| \ge n$ in proposition 12.4, the bound on ϵ_h follows. $\square$

Using the GCD approach reduces to computing the determinants of two Newton matrices by evaluation and interpolation, then finding their GCD by a subresultant polynomial sequence and, finally, performing an exact polynomial division.

Theorem 12.7 *Assume the validity of conjecture 12.5. Let b and L_h be the maximum bit length of the g_i and the h_i coefficients respectively. Given Newton matrices M_1 and M_1', the computation of the sparse resultant by the GCD method has bit complexity*

$$O^*\left(|\mathcal{E}|^{4.376}(b + L_h)^2\right).$$

Proof Interpolating D_1, D_1' from the respective Newton matrices requires $|\mathcal{E}|$ evaluations, each reducing to the computation of a numeric determinant with bit complexity $O(|\mathcal{E}|^{3.376}(b + L_h))$. Interpolating D_1, D_1' from $|\mathcal{E}|$ values, as well as the division of two univariate polynomials of degree $|\mathcal{E}|$ specified by their coefficients, all take $O^*(|\mathcal{E}|^2(b + L_h))$ bit operations. Computing the GCD of two univariate polynomials of degree at most $|\mathcal{E}|$ can be accomplished, deterministically, in $O^*(|\mathcal{E}|^3(b + L_h)^2)$ bit operations [Loo82, sect. 5.7]. Combining the various costs establishes the overall complexity. $\square$

The computation of D_1 and D_1' explicitly, as coefficient vectors, is imposed by the fact that evaluation and the GCD operation do not commute in general (as seen at the beginning of section 9). Faster probabilistic interpolation techniques are surveyed in [Zip93, ch. 15].

Corollary 12.8 *Consider the context of the previous theorem and assume that all Newton polytopes have positive volume. Let the system's scaling factor be s and let μ be the maximum support cardinality of the $n + 1$ Newton polytopes. Then the total bit complexity of constructing the two required Newton matrices and of computing the sparse resultant R by the GCD method is*

$$O^*\left((s^n e^n \deg R)^{4.376}\mu^{6.5}\left(\log^2\frac{1}{\epsilon_l \epsilon_\delta} + b^2 + \log^2\frac{1}{\epsilon_h}\right)\right).$$

Proof We eliminate $|\mathcal{E}|$ from the previous theorem by applying theorem 3.10. Lemma 12.6 bounds L_h and corollary 11.7 bounds the complexity of constructing the two matrices M_1 and M_1'. $\square$

The GCD method for recovering the sparse resultant is more expensive than the division method due to the GCD computation, which forces us to compute the coefficients vectors of D_1, D_1'. It is also more prone to error; on the other hand, it is simpler to implement. It is also clear that manipulating the Newton matrices in order to compute the sparse resultant will typically dominate the complexity of constructing the matrices.

13 Research Directions

The main open question concerns the existence of an exact rational formula for the sparse resultant, in particular, an expression as the quotient of two Newton matrix determinants, in the fashion of Macaulay.

Let M be the Newton matrix, with rows and columns indexed by the integer points in $\mathcal{E}$. Define $\mathcal{E}^{(nm)} \subset \mathcal{E}$ to be the subset of these points that do not lie in mixed cells, and denote by $M^{(nm)}$ the square submatrix of M that includes all entries whose row and column indices lie in $\mathcal{E}^{(nm)}$. Then the diagonal elements of $M^{(nm)}$ constitute a subset of the diagonal elements of M, and the proof of theorem 6.4 implies that $M^{(nm)}$ is generically nonsingular.

Conjecture 13.1 *There exist perturbation vector δ and lifting functions $l_1, \ldots, l_{n+1}$ 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 $R = \det M / \det M^{(nm)}$.*

It is clear that the proposed rational expression has the same degree as R in the coefficients of every polynomial f_i, so it would suffice to prove divisibility. The conjecture clearly holds in the dense case: The choice of parameters that yield a Newton matrix identical to Macaulay's matrix can be adapted to yield a submatrix $M^{(nm)}$ identical to the submatrix defined by Macaulay [Can88].

For $n = 2, 3$ several empirical results confirm the conjecture; one of those is analyzed in section 10. We have experimented with different systems and found that, for most choices of the perturbation and the lifting, divisibility holds. For random δ and l_i, about 90% of the choices lead to positive results.

Interestingly, there exist values of δ and l_i that do not lead to a reducible rational expression. We conclude with a negative example, where $n = 2$ and $\delta = (\epsilon, \epsilon)$, for $1 \gg \epsilon > 0$. The polynomials are completely dense and have degrees $1, 2, 3$ respectively; the bad lifting is

$$l_1 = 10^4 x_1 + 10^3 x_2, \qquad l_2 = 10^5 x_1, \qquad l_3 = 10^2 x_1 + 10 x_2.$$

Acknowledgments

References

[AHU74] A.V. Aho, J.E. Hopcroft, and J.D. Ullman. *The Design and Analysis of Computer Algorithms.* Addison-Wesley, Reading, Mass., 1974.

[AS88] W. Auzinger and H.J. Stetter. An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations. In *Proc. Intern. Conf. on Numerical Math., Intern. Series of Numerical Math., 86,* pages 12–30. Birkhäuser, Basel, 1988.

[Ber75] D.N. Bernstein. The number of roots of a system of equations. *Funct. Anal. and Appl.,* 9(2):183–185, 1975.

[BGW88] C. Bajaj, T. Garrity, and J. Warren. On the applications of multi-equational resultants. Technical Report 826, Purdue Univ., 1988.

[Bro87] D. Brownawell. Bounds for the degree in the Nullstellensatz. *Annals of Math., Second Ser.,* 126(3):577–591, 1987.

[BS92] L.J. Billera and B. Sturmfels. Fiber polytopes. *Annals of Math.,* 135:527–549, 1992.

[Can88] J.F. Canny. *The Complexity of Robot Motion Planning.* M.I.T. Press, Cambridge, Mass., 1988.

[CE93] J. Canny and I. Emiris. An efficient algorithm for the sparse mixed resultant. In G. Cohen, T. Mora, and O. Moreno, editors, *Proc. Intern. Symp. on Applied Algebra, Algebraic Algor. and Error-Corr. Codes (Puerto Rico),* number 263 in Lect. Notes in Comp. Science, pages 89–104, Berlin, 1993. Springer-Verlag.

[CG84] A.L. Chistov and D.Y. Grigoryev. Complexity of quantifier elimination in the theory of algebraically closed fileds. In M.P. Chytil and V. Koubek, editors, *Proc. Symp. on Mathematical Foundations of Computer Science,* number 176 in Lect. Notes Comp. Sci., pages 17–31, New York, 1984. Springer-Verlag.

[Chi86] A. Chistov. Polynomial-time factoring algorithm for polynomials and finding components of varieties in subexponential time. *J. Soviet Math.,* 36:1838–1882, 1986.

[CP93] J. Canny and P. Pedersen. An algorithm for the Newton resultant. Technical Report 1394, Comp. Science Dept., Cornell University, 1993.

[CW90] D. Coppersmith and S. Winograd. Matrix multiplication via arithmetic progressions. *J. Symbolic Computation,* 9:251–280, 1990.

[EC95] I.Z. Emiris and J.F. Canny. Efficient incremental algorithms for the sparse resultant and the mixed volume. *J. Symbolic Computation,* 20(2):117–149, August 1995.

[Ehr67] E. Ehrart. Sur un problème de géométrie diophantienne, I. Polyèdres et réseaux. *J. Reine Angew. Math.,* 226:1–29, 1967.

[EM99]   I.Z. Emiris and B. Mourrain. Computer algebra methods for studying and computing molecular conformations. *Algorithmica, Special Issue on Algorithms for Computational Biology*, 1999. To appear. A preliminary version as Tech. Report 3075, INRIA, 1996.

[Emi96]   I.Z. Emiris. On the complexity of sparse elimination. *J. Complexity*, 12:134–166, 1996.

[Emi97]   I.Z. Emiris. A general solver based on sparse resultants: Numerical issues and kinematic applications. Technical Report 3110, INRIA Sophia-Antipolis, France, 1997.

[Emi98]   I.Z. Emiris. A complete implementation for computing general dimensional convex hulls. *Intern. J. Computational Geometry & Applications, Special Issue on Geometric Software*, 8(2):223–253, 1998.

[EP97]   I.Z. Emiris and V.Y. Pan. The structure of sparse resultant matrices. In *Proc. ACM Intern. Symp. on Symbolic and Algebraic Computation*, pages 189–196, Maui, Hawaii, July 1997.

[GH91]   M. Giusti and J. Heintz. Algorithmes - disons rapides - pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionelles. In Teo Mora and Carlo Traverso, editors, *Effective Methods in Algebraic Geometry*, volume 94 of *Progress in Mathematics*, pages 169–193, Boston, 1991. Birkhäuser. (Proc. MEGA '90, Livorno, Italy).

[GHMP95]   M. Giusti, J. Heintz, J.E. Morais, and L.M. Pardo. When polynomial equation systems can be "solved" fast ? In G. Cohen, M. Giusti, and T. Mora, editors, *Proc. Intern. Symp. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Lect. Notes in Comp. Science, pages 205–231, Berlin, 1995. Springer-Verlag.

[GKZ94]   I.M. Gelfand, M.M. Kapranov, and A.V. Zelevinsky. *Discriminants and Resultants*. Birkhäuser, Boston, 1994.

[GLS93]   M. Grötschel, L. Lovász, and A. Schrijver. *Geometric Algorithms and Combinatorial Optimization*. Springer-Verlag, Berlin, 2nd edition, 1993.

[Gri86]   D. Grigoryev. Polynomial factoring over a finite field and solving systems of algebraic equations. *J. Soviet Math.*, 34:1762–1803, 1986.

[HM91]   J.L. Hafner and K.S. McCurley. Asymptotically fast triangularization of matrices over rings. *SIAM J. Computing*, 20(6):1068–1083, 1991.

[HS95]   B. Huber and B. Sturmfels. A polyhedral method for solving sparse polynomial systems. *Math. Comp.*, 64(212):1542–1555, 1995.

[Kar84]   N. Karmarkar. A new polynomial-time algorithm for linear programming. *Combinatorica*, 4:373–395, 1984.

[Kho78]   A.G. Khovanskii. Newton polyhedra and the genus of complete intersections. *Funktsional'nyi Analiz i Ego Prilozheniya*, 12(1):51–61, Jan.–Mar. 1978.

[Kho91]   A.G. Khovanskii. *Fewnomials*. AMS Press, Providence, Rhode Island, 1991.

[KM95]   S. Krishnan and D. Manocha. Numeric-symbolic algorithms for evaluating one-dimensional algebraic sets. In *Proc. ACM Intern. Symp. on Symbolic and Algebraic Computation*, pages 59–67, 1995.

[Kol88]   J. Kollár. Sharp effective Nullstellensatz. *J. Amer. Math. Soc.*, 1:963–975, 1988.

[KS95]   D. Kapur and T. Saxena. Comparison of various multivariate resultant formulations. In *Proc. ACM Intern. Symp. on Symbolic and Algebraic Computation*, pages 187–194, 1995.

[Kus76]   A.G. Kushnirenko. Newton polytopes and the Bézout theorem. *Funktsional'nyi Analiz i Ego Prilozheniya*, 10(3), Jul.–Sep. 1976.

[Laz81]   D. Lazard. Résolution des systèmes d'Équations algébriques. *Theor. Comp. Science*, 15:77–110, 1981.

[LM95]   T. Lickteig and K. Meer. A note on testing the resultant. *J. of Complexity*, 11(3):344–351, 1995.

[Loo82]   R. Loos. Generalized polynomial remainder sequences. In B. Buchberger, G.E. Collins, and R. Loos, editors, *Computer Algebra: Symbolic and Algebraic Computation*, pages 115–137. Springer-Verlag, Wien, 2nd edition, 1982.

[Man94]   D. Manocha. Solving systems of polynomial equations. *IEEE Comp. Graphics and Appl., Special Issue on Solid Modeling*, pages 46–55, 1994.

[MC93]   D. Manocha and J. Canny. Multipolynomial resultant algorithms. *J. Symbolic Computation*, 15(2):99–122, 1993.

[Mou97]   B. Mourrain. Isolated points, duality and residues. *J. Pure Applied Algebra. Special Issue on Algorithms for Algebra*, 117 & 118:469–494, May 1997.

[Mou98]   B. Mourrain. Computing isolated roots by matrix methods. *J. Symbolic Computation*, 26:715–738, 1998.

[PS93]   P. Pedersen and B. Sturmfels. Product formulas for resultants and Chow forms. *Math. Zeitschrift*, 214:377–396, 1993.

[PS96]   P. Pedersen and B. Sturmfels. Mixed monomial bases. In L. Gonzalez-Vega and T. Recio, editors, *Effective Methods in Algebraic Geometry*, volume 143 of *Progress in Mathematics*, pages 307–316, Boston, 1996. Birkhäuser. (Proc. MEGA '94, Santander, Spain).

[Ren92]   J. Renegar. On the computational complexity of the first-order theory of the reals. *J. Symbolic Computation*, 13(3):255–352, 1992.

[Roj99]   J.M. Rojas. Solving degenerate sparse polynomial systems faster. *J. Symbolic Computation, Special Issue on Elimination*, 27, 1999.

[RR95]   M. Raghavan and B. Roth. Solving polynomial systems for the kinematics analysis and synthesis of mechanisms and robot manipulators. *Trans. ASME, Special 50th Annivers. Design Issue*, 117:71–79, June 1995.

[Sch80]   J.T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, 1980.

[Sch93]   R. Schneider. *Convex Bodies: The Brunn-Minkowski Theory*. Cambridge University Press, Cambridge, 1993.

[Sta80]   R.P. Stanley. Decompositions of Rational Convex Polyhedra. In J. Srivastava, editor, *Combinatorial Mathematics, Optimal Designs and Their Applications, Annals of Discrete Math. 6*, pages 333–342. North-Holland, Amsterdam, 1980.

[Stu93]   B. Sturmfels. Sparse elimination theory. In D. Eisenbud and L. Robbiano, editors, *Proc. Computat. Algebraic Geom. and Commut. Algebra 1991*, pages 264–298, Cortona, Italy, 1993. Cambridge Univ. Press.

[Stu94]   B. Sturmfels. On the Newton polytope of the resultant. *J. of Algebr. Combinatorics*, 3:207–236, 1994.

[vdW50]   B.L. van der Waerden. *Modern Algebra*. F. Ungar Publishing Co., New York, 3rd edition, 1950.

[VGC96]   J. Verschelde, K. Gatermann, and R. Cools. Mixed volume computation by dynamic lifting applied to polynomial system solving. *Discr. and Comput. Geometry*, 16(1):69–112, 1996.

[Zip93]   R. Zippel. *Effective Polynomial Computation*. Kluwer Academic Publishers, Boston, 1993.