An Efficient Algorithm for the Sparse Mixed Resultant

John Canny * and Ioannis Emiris*

Computer Science Division, 571 Evans Hall,
University of California at Berkeley, Berkeley CA 94720.
E-mail: jfc@cs.berkeley.edu and emiris@cs.berkeley.edu.

Abstract. We propose a compact formula for the mixed resultant of a system of $n+1$ sparse Laurent polynomials in n variables. Our approach is conceptually simple and geometric, in that it applies a mixed subdivision to the Minkowski Sum of the input Newton polytopes. It constructs a matrix whose determinant is a non-zero multiple of the resultant so that the latter can be defined as the GCD of $n+1$ such determinants. For any specialization of the coefficients there are two methods which use one extra perturbation variable and return the resultant. Our algorithm is the first to present a determinantal formula for arbitrary systems; moreover, its complexity for unmixed systems is polynomial in the resultant degree. Further empirical results suggest that this is the most efficient method to date for sparse elimination.

1 Introduction

We are given $n+1$ polynomials $f_1, \ldots, f_{n+1} \in \mathbb{C}[x_1, \ldots, x_n]$ and we seek a condition on the coefficients of the f_i that indicates when the system has a solution. Sparsity implies that only certain monomials have non-zero coefficients in the f_i. Such systems may have trivial solutions with some $x_i = 0$ for all coefficient specializations, so we concentrate on solutions $x = \xi$ with $\xi \in (\mathbb{C}^*)^n$, where $\mathbb{C}^* = \mathbb{C} - \{0\}$. Under this assumption, we can deal with the more general case of f_i's which are *Laurent* polynomials in $\mathbb{C}[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$.

We use x^e to denote the monomial $x_1^{e_1} \cdots x_n^{e_n}$, where $e = (e_1, \ldots, e_n) \in \mathbb{Z}^n$ is a multi-exponent. Let $\mathcal{A}_i = \{a_{i1}, \ldots, a_{im_i}\} \subseteq \mathbb{Z}^n$ denote the set of exponents occurring in f_i, then

$$f_i = \sum_{j=1}^{m_i} c_{ij} x^{a_{ij}} \ , \qquad \text{for } i = 1, \ldots, n+1 \ , \tag{1}$$

and we suppose $c_{ij} \neq 0$ so that $\mathcal{A}_i$ is uniquely defined given f_i.

Definition 1. The finite set $\mathcal{A}_i \subset \mathbb{Z}^n$ of all monomial exponents appearing in f_i is the *support* of f_i. The *Newton Polytope* of f_i is $Q_i = \mathrm{Conv}(\mathcal{A}_i) \subset \mathbb{R}^n$, the convex hull of $\mathcal{A}_i$.

* Supported by a David and Lucile Packard Foundation Fellowship and by NSF Presidential Young Investigator Grant IRI-8958577.

A polynomial system is *unmixed* if all supports $\mathcal{A}_i$ are the same for $i = 1, \ldots, n+1$, otherwise it is *mixed*.

Definition 2. The *Minkowski Sum* $A + B$ of convex polytopes A and B in $\mathbb{R}^n$ is the set

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

$A + B$ is a convex polytope. Let $\mathrm{Vol}(A)$ denote the usual n-dimensional volume of A.

Definition 3. Given convex polytopes $A_1, \ldots, A_n \subseteq \mathbb{R}^n$, there is a unique real-valued function $MV(A_1, \ldots, A_n)$ called the *Mixed Volume* which is multilinear with respect to Minkowski sum, such that $MV(A_1, \ldots, A_1) = n!\mathrm{Vol}(A_1)$. Equivalently, if $\lambda_1, \ldots, \lambda_n$ are scalars, then $MV(A_1, \ldots, A_n)$ is precisely the coefficient of $\lambda_1 \lambda_2 \cdots \lambda_n$ in $\mathrm{Vol}(\lambda_1 A_1 + \cdots + \lambda_n A_n)$ expanded as a polynomial in $\lambda_1, \ldots, \lambda_n$.

The Newton polytopes offer a convenient model for the sparsity of a polynomial system, in light of the following upper bound on the number of common roots, see [1], [11], [9].

Theorem 4. *[1] Let $f_1, \ldots, f_n \in \mathbb{C}[x_1, x^{-1}, \ldots, x_n, x_n^{-1}]$. 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 specialization of the coefficients c_{ij} the number of solutions is exactly $MV(Q_1, \ldots, Q_n)$.*

For systems of $n + 1$ polynomials in n unknowns, there are generically no solutions, and the resultant delimits those systems that do have a solution. We adopt the following definition for the *sparse* resultant from [15]; it is identical to the $(\mathcal{A}_1, \ldots, \mathcal{A}_{n+1})$-*resultant* of [4]. Regard a polynomial f_i as a generic point $(c_{i1}, \ldots, c_{im_i}) \in \mathbb{P}^{m_i}$ in the space of all possible polynomials with the given set of exponents $\mathcal{A}_i$, after identifying scalar multiples. Then the input system is a point $c = (c_{11}, \ldots, c_{1m_1}, \ldots, c_{(n+1)1}, \ldots, c_{(n+1)m_{n+1}})$ in $\mathbb{P}^{m_1 - 1} \times \cdots \times \mathbb{P}^{m_{n+1} - 1}$. Let $Z_0 = Z_0(\mathcal{A}_1, \ldots, \mathcal{A}_{n+1})$ be the set of all points c such that the 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.

Definition 5. The *sparse resultant* $R(\mathcal{A}_1, \ldots, \mathcal{A}_{n+1})$ of the system (1) is an irreducible polynomial in $\mathbb{Z}[c]$. If $\mathrm{codim}(Z) = 1$ then $R(\mathcal{A}_1, \ldots, \mathcal{A}_{n+1})$ is the defining polynomial of the hypersurface Z. If $\mathrm{codim}(Z) > 1$ then $R(\mathcal{A}_1, \ldots, \mathcal{A}_{n+1}) = 1$.

Throughout this article, it is assumed without loss of generality that the affine lattice generated by $\sum_{i=1}^{n+1} \mathcal{A}_i$ is n-dimensional. Moreover, this lattice is identified with $\mathbb{Z}^n$ after a change of variables, if necessary [21]. Then,

Proposition 6. *[15] The sparse resultant is separately homogeneous in the coefficients $(c_{i1}, \ldots, c_{im_i})$ of each f_i and its degree in these coefficients equals the mixed volume of the other n Newton polytopes $MV(Q_1, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_{n+1})$.*

This implies that the total degree $\deg R$ of the resultant equals the sum of all $n+1$ n-fold Mixed Volumes.

The practical significance of this approach relies on the fact that polynomial systems are frequently sparse in several applications such as computer vision, robot kinematics, graphics and geometric modeling. More precise examples include the cyclic n-roots problem, computing the motion from point matches and inverse kinematics. For the later problem, the homogeneous approach leads to an intractable problem, while the custom approach of [14] requires time in the order of milliseconds.

The following section points to previous works on which our approach is based and briefly states our results. Section 3 describes the construction of a matrix M of the correct degree in the coefficients of f_1. Section 4 proves that $\det(M)$ is a multiple of the sparse resultant and is not identically zero. Section 5 shows that the resultant is the Greatest Common Divisor (GCD) of $n+1$ such determinants and sketches two ways to compute it for various specializations. We illustrate the algorithm with an example in Sect. 6 and analyze its complexity in Sect. 7. The article concludes with some open questions.

2 Background and the Present Approach

Our approach consists of regarding the coefficients c_{ij} as indeterminates and expressing the sparse resultant through various determinants in these coefficients. We shall define the resultant as the GCD of $n+1$ such determinants, each of which is a multiple of the resultant and may be thought of as a generalized *inertia form* [23]; Hurwitz showed for the general homogeneous case that the resultant is the GCD of all inertia forms [6]. Alternatively, we may compute the resultant via a series of n divisions of determinants, similarly to Cayley's method [16]. Lastly, our construction is closely related to that of Macauley's [13].

More recently, the sparse unmixed resultant was defined as the Chow form of a projective toric variety in [10], see also [4]. Algorithms for its computation and evaluation were proposed in [20], the most efficient one having complexity higher than polynomial in the degree of the resultant and exponential in n with a quadratic exponent.

For *multigraded* systems, an optimal determinantal formula, called of *Sylvester type*, is given in [22], These systems are unmixed and include polynomials that are homogeneous of degree d_j in each group of variables $\mathbf{x}_j$, where $\mathbf{x}_j$ has l_j+1 variables. The main theorem defines a matrix whose determinant is the resultant for such a system, provided that for each j, $l_j = 1$ or $d_j = 1$.

An explicit formula for the sparse resultant was given in [15] as a *Poisson product* $R' \prod_{\xi \in V(f_1,\ldots,f_n)} f_{n+1}(\xi)$ where R' is a rational function in the coefficients of $f_1, \ldots, f_n$.

Our algorithm requires two randomized steps, the success of which has arbitrarily high probability and can be verified deterministically. The running time for unmixed systems is given in the following restatement of Theorem 24, which makes the algorithm the most efficient to date for this case.

Theorem 7. *Assume that our algorithm executes on an arbitrary unmixed system. Then its asymptotic bit complexity, if we omit logarithmic factors, is polynomial in* $\max_i\{m_i\}$ *and the total degree of the resultant and exponential in* n *with a linear exponent.*

Furthermore, this is the first algorithm that produces a determinantal formula for mixed systems. Although a similar complexity bound as above is not possible in this case, empirical results and a heuristic analysis imply that, for most mixed systems in practice, the algorithm's complexity is given by the above theorem.

3 Matrix Construction

We define and analyze the properties of matrix M associated with the polynomial f_1. Let Q denote the Minkowski Sum of all input Newton polytopes

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

If we define an $(n+1)$-argument vector sum

$$\oplus : (\mathbb{R}^n)^{(n+1)} \rightarrow \mathbb{R}^n : (p_1, \ldots, p_{n+1}) \mapsto p_1 + \cdots + p_{n+1} \quad ,$$

then Q may be thought of as the image of $Q_1 \times \cdots \times Q_{n+1}$ under $\oplus$. This is clearly a many-to-one mapping; to define a unique inverse $(p_1, \ldots, p_{n+1})$ in $\oplus^{-1}(q) \cap Q_1 \times \cdots \times Q_{n+1}$, for each $q \in Q$, a method from [21] and [2] is employed. Choose $n+1$ sufficiently generic linear forms $l_1, \ldots, l_{n+1} \in \mathbb{Z}[x_1, \ldots, x_n]$ and define, for $1 \leq i \leq n+1$, *lifted* Newton polytopes

$$\hat{Q}_i \stackrel{\triangle}{=} \{(p_i, l_i(p_i)) : p_i \in Q_i\} \subset \mathbb{R}^{n+1} \quad .$$

Let the Minkowski Sum of the lifted Newton polytopes be

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

We make use of

Definition 8. Given a convex polytope in $\mathbb{R}^{n+1}$, its *lower envelope* with respect to vector $v \in \mathbb{R}^{n+1}$ is the closure of the subset of all points r on its surface such that, given a point z at infinity in the direction of v, the segment (r, z) intersects the polytope at a point other than r.

Let $\pi : \mathbb{R}^{n+1} \rightarrow \mathbb{R}^n$ denote projection on the first n coordinates, and $h : \mathbb{R}^{n+1} \rightarrow \mathbb{R}$ denote projection on the $(n+1)$-st. Now consider the lower envelope of $\hat{Q}$ with respect to $(0, \ldots, 0, 1)$ and let $s : \mathbb{R}^n \rightarrow \mathbb{R}^{n+1}$ map each point in Q to the point on this envelope that lies in $\pi^{-1}(q)$. Equivalently

$$s(q) \;=\; \hat{q} \in \pi^{-1}(q) \cap \hat{Q} \quad , \qquad \text{such that } h(\hat{q}) \text{ is minimized} \quad .$$

The lower envelope of $\hat{Q}$ is then $s(Q)$. By construction the l_i's are generic enough so that every point $\hat{q}$ on the lower envelope can be *uniquely* expressed as a sum of points $\hat{q}_1 + \cdots + \hat{q}_{n+1}$ with $\hat{q}_i \in \hat{Q}_i$. This is implemented by picking, for each i, a random integer vector with independent entries whose bit size is $\log c$, for some constant $c > 1$. Then the probability that the genericity condition fails is bounded by $1/c$ [17, Lemma 1].

Let $\hat{\Delta}$ denote the natural (coarsest) polyhedral subdivision of the lower envelope of $\hat{Q}$. Each facet (n-dimensional face) of $\hat{\Delta}$ is a Minkowski sum $\hat{F}_1 + \cdots + \hat{F}_{n+1}$ with $\hat{F}_i$ a face of $\hat{Q}_i$, and since lower envelope points have unique expressions as sums,

$$\sum_{i=1}^{n+1} \dim(\hat{F}_i) = n \quad .$$

The image of $\hat{\Delta}$ under π induces a polyhedral subdivision Δ of Q whose cells are of the form $F_1 + \cdots + F_{n+1}$ with the same dimension property, a consequence of which is the following

Remark. For every cell $F_1 + \cdots + F_{n+1}$ in Δ, F_i a face of Q_i, at least one of the F_i is zero-dimensional, i.e. a vertex.

Definition 9. A *mixed cell* of the induced subdivision is a cell which is 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.

For selecting the matrix entries in a well-defined manner, we must perturb the Minkowski sum slightly so that each integer lattice point lies in the *interior* of a cell of Δ. Thus we choose a sufficiently small generic vector $\delta \in \mathbb{Q}^n$, and the set of exponents that indexes the rows and columns of M is

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

If Δ_δ denotes the subdivision obtained by shifting all faces of Δ by δ, the choice of δ is satisfactory if every $p \in \mathcal{E}$ lies in the interior of a cell of Δ_δ. We can now define our selection rule for elements of M based on a function $RC : \mathcal{E} \to \mathbb{Z}^2$, for row content.

Definition 10. (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. Let i be the largest integer such that F_i is a vertex, so $F_i = a_{ij}$ for some j. Then $RC(p) = (i, j)$.

The row of M indexed by $p \in \mathcal{E}$ contains the coefficients of f_i, and represents a multiple of f_i which is

$$x^{(p - a_{ij})} f_i \tag{2}$$

where $(i, j) = RC(p)$. Let $|\mathcal{E}|$ denote the cardinality of set $\mathcal{E}$; then,

Definition 11. M is an $|\mathcal{E}| \times |\mathcal{E}|$ matrix whose rows and columns are indexed by elements of $\mathcal{E}$, and whose element at row p and column q is as below, for arbitrary $p, q \in \mathcal{E}$ with $RC(p) = (i, j)$:

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

Therefore $M_{pp} = c_{ij}$ where $(i, j) = RC(p)$. The matrix is well-defined since it is easily seen that all exponent vectors $p - a_{ij} + a_{ik}$ for $a_{ik} \in \mathcal{A}_i$ lie within $\mathcal{E}$; this is also implied by the discussion in the next section.

4 A Nonzero Multiple of the Resultant

First we prove that the determinant of M is a multiple of the resultant. M represents a linear map $\mathbb{C}^{|\mathcal{E}|} \to \mathbb{C}^{|\mathcal{E}|}$ which we can interpret as the map taking the vector of coefficients of $(g_1, \ldots, g_{n+1})$ to the vector of coefficients of g, where

$$g = g_1 f_1 + \cdots + g_{n+1} f_{n+1} \tag{3}$$

and the support of g is $\mathcal{E}$; in addition, the support of g_i is $\{p - a_{ij} \,|\, p \in \mathcal{E},\ RC(p) = (i, j)\}$. Thus $|\mathcal{E}|$ is the total number of non-zero coefficients in the g_i's.

Lemma 12. *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 non-singular. Then the linear map defined by M is surjective and we can choose polynomials $g_1, \ldots, g_{n+1}$ such that g in (3) is a monomial. This monomial must be zero at every solution ξ, which is infeasible for $\xi \in (\mathbb{C}^*)^n$. Hence there can be no solution in $(\mathbb{C}^*)^n$, which is a contradiction. □

Proposition 13. *The sparse resultant divides the determinant of M.*

Proof. The lemma implies that $\det(M) = 0$ on the set Z_0 of specializations of c_{ij} such that the system has a solution in $(\mathbb{C}^*)^n$. Thus it is zero on the closure Z of Z_0, which is exactly the zero set of the resultant $R(\mathcal{A}_1, \ldots, \mathcal{A}_{n+1})$. Since the resultant is irreducible it must divide $\det(M)$. □

To alleviate the possibility that $\det(M)$ is identically zero, we show that under the following specialization of the coefficients c_{ij}, $\det(M) \neq 0$:

$$c_{ij} \mapsto t^{l_i(a_{ij})}$$

so that each c_{ij} becomes an integral power of t where t is a new indeterminate. Observe that the Newton polytope of the specialized f_i as a polynomial in $\mathbb{C}[x_1, \ldots, x_n, t]$ is precisely $\hat{Q}_i$. 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.

Theorem 14. *The lowest degree term of* $\det(M)(t)$ *is the product of leading diagonal elements of* $M(t)$*. That is, it has coefficient 1 and (integer) exponent*

$$\sum_{p \in \mathcal{E}} l_i(a_{ij})$$

where for each p, $(i,j) = RC(p)$*. Therefore this determinant is non-vanishing.*

This theorem follows from the following series of lemmas.

Lemma 15 (Geometric). *Let* $\hat{p}$ *be a point in the interior of some facet of the subdivision* $\hat{\Delta}$ *of the lower envelope* $s(Q)$*. By construction,* $\hat{p}$ *has a unique expression as a sum of points from* $\hat{Q}_1, \ldots, \hat{Q}_{n+1}$*, and one of these is a vertex* $\hat{a}_{ij} = (a_{ij}, l_i(a_{ij}))$*. Then* $(\hat{p} - \hat{a}_{ij} + \hat{Q}_i) \cap s(Q) = \hat{p}$*.*

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

Now displace both $\hat{p}$ and $\hat{q}$ by decreasing their $(n+1)$-st coordinate by the same amount, thus defining points $\hat{p}', \hat{q}' \in \mathbb{R}^{n+1}$. The displacement should be small enough so that the line $(\hat{p}', \hat{q}')$ intersects the lower envelope in the face that contains $\hat{p}$. Let $\hat{p}''$ be this intersection point. $\hat{Q}$ also contains $\hat{p}'' - \hat{a}_{ij} + \hat{Q}_i$.

Clearly (Fig. 1) the vector $\hat{q}' - \hat{p}''$ is smaller than $\hat{q} - \hat{p}$ and in the same direction. Now $\hat{q} - \hat{p}$ is contained in the convex set $\hat{Q}_i - \hat{a}_{ij}$, and it follows that $\hat{q}' - \hat{p}''$ is also contained in $\hat{Q}_i - \hat{a}_{ij}$ (which contains the origin). Thus $\hat{q}' \in \hat{p}'' - \hat{a}_{ij} + \hat{Q}_i \subset \hat{Q}$. So we have demonstrated a point $\hat{q}'$ such that $\pi(\hat{q}) = \pi(\hat{q}')$ but $h(\hat{q}') < h(\hat{q})$. Thus $\hat{q}$ is not on the lower envelope. □

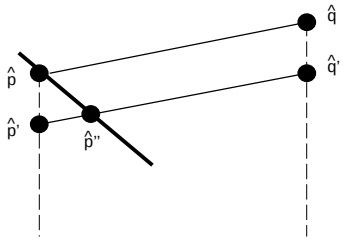

Fig. 1. Proof of the geometric lemma

Define a matrix $M'(t)$ by scaling the rows of $M(t)$:

$$M'_{pq} \stackrel{\triangle}{=} t^{(h(\hat{p}) - l_i(a_{ij}))} M_{pq}$$

for every $q \in \mathcal{E}$, where $(i,j) = RC(p)$ and $\hat{p} = s(p)$. Then the previous lemma leads to an inequality on the degree in t of the M' entries.

Lemma 16. *For all non-zero elements M'_{pq} with $p \neq q$, $\deg(M'_{pq}) > \deg(M'_{qq})$.*

Proof. Let $\hat{p}$ and $\hat{q}_0$ be the points on the lower envelope $s(Q) + \delta$ such that $\pi(\hat{p}) = p$ and $\pi(\hat{q}_0) = q$. Let $(\iota, \gamma) = RC(q)$ and, since $\deg(M_{qq}(t)) = l_\iota(a_{\iota\gamma})$, we have

$$\deg(M'_{qq}(t)) = (h(\hat{q}_0) - l_i(a_{ij})) + l_i(a_{ij}) = h(\hat{q}_0) \ .$$

Note that $\hat{p}$ will lie in the interior of a facet of $\hat{\Delta}_\delta$. Let $\hat{q}$ be the intersection $\pi^{-1}(q) \cap (\hat{p} - \hat{a}_{ij} + \hat{Q}_i)$. The intersection is non-empty because if M_{pq} contains a non-zero coefficient c_{ik}, then $q = p - a_{ij} + a_{ik}$. In fact $\hat{q} = \hat{p} - \hat{a}_{ij} + \hat{a}_{ik}$, hence

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

From the previous lemma $\hat{q}$ does not lie on the lower envelope and since $\hat{q}_0$ does lie on the lower envelope, we have $h(\hat{q}) > h(\hat{q}_0)$. □

The previous lemmas are more easily understood by recalling that the $\hat{Q}_i$'s are the Newton polytopes of the specialized system, where t is the $(n+1)$-st variable. More precisely, the Newton polytope of the polynomial in row p is $\hat{Q}_i$ shifted so that its vertex $\hat{a}_{ij}$ lies over p. The row-scaling of M by powers of t corresponds to lifting the Newton polytopes of the rows so that the optimal vertex touches the lower envelope. The rest of the polytope will lie above the lower envelope. Looking down column q of M' corresponds to looking at points in the various Newton polytopes that lie over the lattice point q. There will be a unique point of minimum $(n+1)$-st coordinate on the lower envelope over q corresponding to the leading diagonal element M'_{qq}. All other points will have larger $(n+1)$-st coordinate, therefore the corresponding entries have higher degree in t than that of M'_{qq}.

Proposition 17. *The lowest-degree term of* $\det(M')(t)$ *equals the product of the leading diagonal elements of $M'(t)$, therefore this determinant is non-vanishing.*

Proof. The determinant can be written

$$\det(M') = \sum_{\sigma \in S(\mathcal{E})} (-1)^{\mathrm{sign}(\sigma)} \prod_{q \in \mathcal{E}} M'_{\sigma(q)q}$$

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 $\deg(M'_{\sigma(q)q}) > \deg(M'_{qq})$ by the previous lemma. Thus

$$\deg(\prod_{q \in \mathcal{E}} M'_{qq}) < \deg(\prod_{q \in \mathcal{E}} M'_{\sigma(q)q})$$

for every permutation σ other than the identity. This implies that the product of leading diagonal entries is a unique lowest power of t and therefore there exists some value $t_0 \neq 0$ of t for which this product is not canceled and $\det(M')(t_0) \neq 0$. □

The main result (Theorem 14) of this section is a straightforward consequence of this proposition by observing that

$$\det(M')(t) = t^\alpha \det(M)(t)$$

where t^α is the product of the scale factors.

5 Computing the Resultant

We show that the degree of $\det(M)$ in the coefficients of the polynomial f_1 equals that of the resultant R. The row content function chooses f_1 if there is no other possibility, which happens precisely at the mixed cells to which Q_1 contributes a vertex. The total volume of these cells equals the mixed volume of the other n Newton polytopes $MV(Q_2, \ldots, Q_{n+1})$. We define an n-dimensional *half-open integral parallelotope* HO:

$$HO = \{\sum_{i=1}^{n} r_i \mathbf{e}_i \mid r_i \in [0,1),\ \mathbf{e}_i \in \mathbb{Z}^n\} \ .$$

Lemma 18. *The number of integer lattice points in a half-open integral parallelotope equals its volume.*

Proof. It follows from [18, Remark, p.335] that the number of these lattice points is $n!\mathrm{Vol}(S)$ where S is the simplex $\mathrm{Conv}(0, \mathbf{e}_1, \ldots, \mathbf{e}_n)$. The volume of the parallelotope HO is also $n!\mathrm{Vol}(S)$. □

Corollary 19. *For any $\delta \in \mathbb{R}^n$, the number of integer lattice points in $HO + \delta$ is* $\mathrm{Vol}(HO)$.

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 (open), and that the opposite facet is displaced from the first 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. □

A mixed facet of the subdivision $\hat{\Delta}_\delta$ is the Minkowski sum of n edges, hence a parallelotope in $\mathbb{R}^n$. The perturbation by δ guarantees that all lattice points lie in the interior of a facet. So the number of rows containing coefficients of f_1 is precisely $MV(Q_2, \ldots, Q_{n+1})$.

Proposition 20. *The degree of the determinant of M in the coefficients of f_1 equals $MV(Q_2, \ldots, Q_{n+1})$, which equals that of $R(\mathcal{A}_1, \ldots, \mathcal{A}_{n+1})$. Moreover, the degree of* $\det(M)$ *in the coefficients of every other f_j for $j \neq 1$ is at least as large as the respective degree of $R(\mathcal{A}_1, \ldots, \mathcal{A}_{n+1})$.*

For computing R we could use Hurwitz's idea [6] and 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. For example, we could modify the row contents function so that it never returns i when there is another choice. Let $D_1, \ldots, D_{n+1}$ be the determinants formed in this way. The GCD of $D_1, \ldots, D_{n+1}$ has the correct degree in all f_i's and, since the GCD is divisible by R, it equals R. Unfortunately, this method does not work when the coefficients of the f_i are specialized. It can be used after a suitable perturbation of the specialized system, but there is a more economical method, essentially the one in [3], with a straightforward adaptation; two variants follow.

5.1 Division Method

Let $g_1, \ldots, g_{n+1}$ be the specialized polynomials. 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 perturbed system is

$$(f_1, \ldots, f_{n+1}) \mapsto (g_1 + u_1 h_1, \ldots, g_{n+1} + u_{n+1} h_{n+1})$$

where each u_i is a new indeterminate. Define the extraneous factor b_i of each D_i via

$$D_i = b_i R$$

and notice that b_i will be independent of u_i.

Definition 21. Suppose a polynomial $A(u_1, \ldots, u_{n+1})$ has maximum degree d_i in u_i. Then A is said to be *rectangular* if it contains a monomial of the form $u_1^{d_1} u_2^{d_2} \cdots u_{n+1}^{d_{n+1}}$.

Under the specialization above, note that R as well as $D_1, \ldots, D_{n+1}$ will be rectangular, because the coefficient of $u_1^{d_1} u_2^{d_2} \cdots u_{n+1}^{d_{n+1}}$ will be the resultant (or one of the determinants) when each f_i is specialized to h_i.

Define $R^{(j)}(u_1, \ldots, u_j)$ to be the leading coefficient, with respect to total degree, of R considered as a polynomial in $u_{j+1}, \ldots, u_{n+1}$. Define $D_i^{(j)}(u_1, \ldots, u_j)$ and $b_i^{(j)}(u_1, \ldots, u_j)$ analogously and notice that all these polynomials are rectangular. Then $D_i^{(j)} = b_i^{(j)} R^{(j)}$ for all i and j. But notice that since b_i is independent of u_i, $b_i^{(i)} = b_i^{(i-1)}$, which we can use to eliminate b_i:

$$R^{(i)} = \frac{D_i^{(i)}}{D_i^{(i-1)}} R^{(i-1)} \quad . \tag{4}$$

Now notice that $R^{(n+1)}$ is exactly the resultant of the f_i, so setting $u_1 = \cdots = u_{n+1} = 0$ in $R^{(n+1)}$ will give the resultant of the g_i.

The recurrence (4) has initial term $R^{(0)}$ which is some integer that we may set to 1, thus obtaining $R^{(n+1)}$ equal to a scalar multiple of the resultant.

Next observe that the identity (4) is valid for specializations of u_i's so long as no denominator vanishes. So we take $u_1 = u_2 = \cdots = u_{n+1} = u$, so that all the $D_i^{(j)}$'s become univariate polynomials in u. Since they are all rectangular, they have a unique term of highest total degree in the u_i's which cannot cancel, so none of them will vanish under this specialization. Each $D_i^{(j)}(u)$ is easily seen to be the determinant of M under the specialization:

$$(f_1, \ldots, f_{n+1}) \mapsto (g_1 + uh_1, \ldots, g_j + uh_j, h_{j+1}, \ldots, h_{n+1})$$

and the leading coefficient of $D_i^{(j)}$ is once again non-zero for almost all choices of h_i's. Thus we have an almost guaranteed method of constructing the resultant at the cost of adding the single variable u. More precisely, to bound the probability of failure by $1/c$ for some arbitrary $c > 1$ it suffices, by Schwartz's lemma [17,

Lem. 1], to pick the coefficients of each h_i independently, each with $c \log |\mathcal{E}|$ bits. It is possible to detect failure deterministically, in which case new randomized variables must be chosen.

If the g_i's are sufficiently generic, which here means that no $D_i^{(j)}$ vanishes, we may compute $D_i^{(j)}$ as the determinant of M_i under the specialization

$$(f_1, \ldots, f_{n+1}) \mapsto (g_1, \ldots, g_j, h_{j+1}, \ldots, h_{n+1}) \ .$$

5.2 GCD Method

This method requires that the coefficients of the specialized system $g_1, \ldots, g_{n+1}$ be non-zero and chosen from some polynomial ring over $\mathbb{Q}$. Again we choose polynomials h_i with random coefficients, whose size is given by Schwartz's lemma, and specialize

$$(f_1, \ldots, f_{n+1}) \mapsto (g_1 + uh_1, \ldots, g_{n+1} + uh_{n+1}) \ .$$

By Hilbert's irreducibility theorem, R will remain irreducible over $\mathbb{Q}[u]$ after almost all such specializations. Let $D_1(u)$ be the determinant of M_1 with this specialization, and let $b(u)$ be the extraneous factor, $D_1(u) = b(u)R(u)$.

Suppose without loss of generality that M_1 was defined using a linear functional l_1 which is "much larger" than the others. The effect of this is that whenever a vertex a_{1j} of Q_1 contributes to an optimal sum, that vertex will be the one which minimizes l_1. Thus in every row containing coefficients of f_1, the leading diagonal element will be c_{1j}. Now let $D_2(u)$ be the determinant of M under the specialization

$$(f_1, f_2, \ldots, f_{n+1}) \mapsto (x^{a_{1j}}, g_2 + uh_2, \ldots, g_{n+1} + uh_{n+1})$$

with $D_2(u) = b(u)R'(u)$, where $R'(u)$ is the resultant under this new specialization. Therefore

$$R(u) = \frac{D_1(u)}{GCD(D_1(u), D_2(u))}$$

and specializing $u = 0$ gives the resultant of $g_1, \ldots, g_{n+1}$. It is worth remarking that the degree of $b(u)$ is known in advance, namely it is the number of elements of $\mathcal{E}$ that do not lie in mixed facets. Thus the GCD computation is branch-free and reduces to calculation of the appropriate minors of the Sylvester matrix of D_1 and D_2, [12].

Once again if the given g_i's are generic enough, in this case meaning that the specialized resultant under $f_i \mapsto g_i$ is irreducible, and the determinants $D_1(0)$ and $D_2(0)$ are both non-zero, then the resultant can be computed as simply $D_1(0)/GCD(D_1(0), D_2(0))$.

6 An Example

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

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

Pick generic functions

$$l_1(x,y) = L^5x + L^4y$$
$$l_2(x,y) = L^3x + L^2y$$
$$l_3(x,y) = Lx + y$$

where L is a sufficiently large integer. The input Newton polytopes are shown in Fig. 2 and a subdivision of $Q + \delta$ into 2-dimensional cells is shown in Fig. 3. Matrix M_1 appears at (5) with rows and columns indexed by exponent vectors

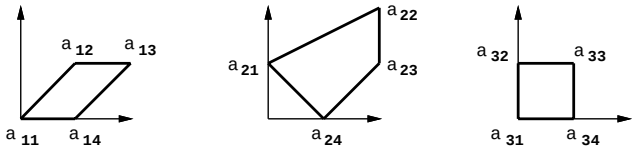

Fig. 2. The Newton polytopes and the exponents a_{ij}

from $\mathcal{E}$. Matrices corresponding to f_2 and f_3 are formed similarly.

$$\begin{array}{c} \\ 1,0 \\ 2,0 \\ 0,1 \\ 1,1 \\ 2,1 \\ 3,1 \\ 0,2 \\ 1,2 \\ 2,2 \\ 3,2 \\ 4,2 \\ 1,3 \\ 2,3 \\ 3,3 \\ 4,3 \end{array} \begin{array}{c} \begin{array}{ccccccccccccccc} 1,0 & 2,0 & 0,1 & 1,1 & 2,1 & 3,1 & 0,2 & 1,2 & 2,2 & 3,2 & 4,2 & 1,3 & 2,3 & 3,3 & 4,3 \end{array} \\ \left[\begin{array}{ccccccccccccccc} c_{11} & c_{14} & 0 & 0 & c_{12} & c_{13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ c_{31} & c_{34} & 0 & c_{32} & c_{33} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ c_{24} & 0 & c_{21} & 0 & c_{23} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & c_{11} & c_{14} & 0 & 0 & 0 & c_{12} & c_{13} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & c_{11} & c_{14} & 0 & 0 & 0 & c_{12} & c_{13} & 0 & 0 & 0 & 0 \\ 0 & c_{24} & 0 & c_{21} & 0 & c_{23} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & c_{11} & c_{14} & 0 & 0 & 0 & c_{12} & c_{13} & 0 & 0 \\ 0 & 0 & c_{31} & c_{34} & 0 & 0 & c_{32} & c_{33} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & c_{31} & c_{34} & 0 & 0 & c_{32} & c_{33} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & c_{31} & c_{34} & 0 & 0 & c_{32} & c_{33} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & c_{24} & 0 & 0 & c_{21} & 0 & c_{23} & 0 & 0 & 0 & c_{22} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & c_{31} & c_{34} & 0 & 0 & c_{32} & c_{33} & 0 & 0 \\ 0 & 0 & 0 & c_{24} & 0 & 0 & c_{21} & 0 & c_{23} & 0 & 0 & 0 & c_{22} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & c_{31} & c_{34} & 0 & 0 & c_{32} & c_{33} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & c_{31} & c_{34} & 0 & 0 & c_{32} & c_{33} \end{array}\right] \end{array} \tag{5}$$

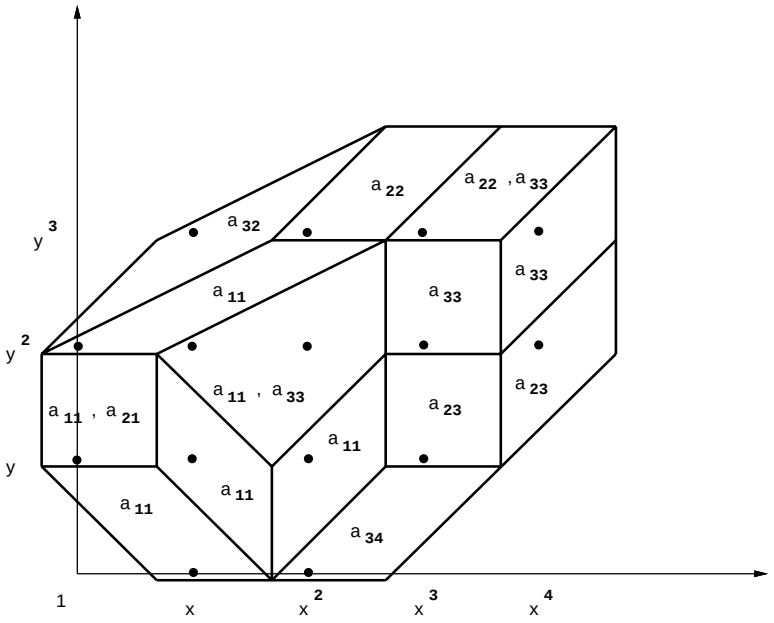

Fig. 3. The induced subdivision Δ_δ of $Q + \delta$; each facet is labeled with the vertices which contribute to optimal sums within that facet

7 Complexity

The change of variables that may be required to ensure that the supports generate the lattice $\mathbb{Z}^n$ involves linear algebra and has complexity which is dominated by that of the later steps.

Identifying the vertices of all Newton polytopes may be reduced to Linear Programming; then we can apply either Khachiyan's Ellipsoid or Karmarkar's algorithm. To bound the bit size of the input exponents a_{ij} we recall that the Newton polytopes have been translated to the origin, thus every exponent is bounded by $|\mathcal{E}|$.

In the case of Karmarkar's algorithm [8] the bit complexity, omitting the logarithmic factors, is $\mathcal{O}(m_i^{5.5} \log^2 |\mathcal{E}|)$ for each Q_i and the output is its vertex set, namely $\{a_{i1}, \ldots, a_{i\mu_i}\}$ with $\mu_i \leq m_i$, possibly after reindexing. The total complexity for all Newton polytopes is thus $\mathcal{O}(n(\max_i m_i)^{5.5} \log^2 |\mathcal{E}|)$.

The most expensive step of the algorithm is to associate an optimal sum of points $p_i \in Q_i$ with every $p \in \mathcal{E}$. To reduce this to Linear Programming we introduce constraints

$$p = \sum_{i=1}^{n+1} p_i = \sum_{i=1}^{n+1} \sum_{j=1}^{\mu_i} \lambda_{ij} a_{ij}$$

where

$$\lambda_{ij} \geq 0 \ , \qquad \text{for } 1 \leq j \leq \mu_i, \qquad \text{and } \sum_{j=1}^{\mu_i} \lambda_{ij} = 1$$

for each i in $\{1, \ldots, n+1\}$. The objective function forces the lifted point corresponding to p to lie on the lower envelope of $\hat{Q}$ by requiring that

$$\sum_{i=1}^{n+1} \sum_{j=1}^{\mu_i} \lambda_{ij} \, l_i(a_{ij})$$

is *minimized*, where the l_i's are the generic linear functionals.

Either polynomial-time algorithm may again be used; here we calculate the complexity of Karmarkar's. The bit size of $l_i(a_{ij})$ is constant, once the desired probability of success is fixed. As already seen, each $a_{ij} < |\mathcal{E}|$ so the bit complexity after omitting the logarithmic factors is $\mathcal{O}(n^{5.5}(\max_i \mu_i)^{5.5} \log^2 |\mathcal{E}|)$. Hence, finding the optimal sum for all lattice points $p \in \mathcal{E}$ takes time polynomial in n, $\max_i \mu_i$ and $\mathcal{E}$.

Lastly, we have to extract the resultant from matrix M by one of the described methods. This can be done with linear algebra and the arithmetic complexity is polynomial in the order of M. Since both the matrix order and the input exponents are bounded by $|\mathcal{E}|$, the overall complexity is polynomial in $|\mathcal{E}|$.

This discussion proves

Proposition 22. *For any input system, the bit complexity of our algorithm is polynomial in in n, $\max_i\{m_i\}$ and $|\mathcal{E}|$.*

Now we estimate $|\mathcal{E}|$; unfortunately, only the unmixed case can be treated without requiring additional hypotheses. Consider the unmixed system

$$Q_1 = \cdots = Q_{n+1} \ .$$

Then the total degree of the resultant equals the sum of all $n+1$ n-fold Mixed Volumes, each being equal to $n!\mathrm{Vol}(Q_1)$. Hence

$$\deg R = (n+1)! \, \mathrm{Vol}(Q_1) \ .$$

The Minkowski Sum has volume $\mathrm{Vol}(Q) = n^n \mathrm{Vol}(Q_1)$ and the number of lattice points in it is asymptotically the same [7]. Then $|\mathcal{E}| = \mathcal{O}\left(\frac{n^n \deg R}{(n+1)!}\right)$. Using Sterling's approximation and letting e be the base of natural logarithms, we arrive at

Lemma 23. *For unmixed systems*

$$|\mathcal{E}| = \mathcal{O}(e^n \deg R) \ .$$

Therefore

Theorem 24. *Assume that our algorithm executes on an arbitrary unmixed system. Then its asymptotic bit complexity, if we omit logarithmic factors, is polynomial in* $\max_i\{m_i\}$ *and the total degree of the resultant and exponential in* n *with a linear exponent.*

We cannot obtain the same bounds in general because there exist cases like the following, in which the cardinality $|\mathcal{E}|$ is exponential over the sum of all n-fold mixed volumes. Suppose that all Newton polytopes are hypercubes, with edge length constant for the first n and proportional to n for the last polytope. Then $|\mathcal{E}| > n^n$, while the sum of mixed volumes is $\mathcal{O}(n^2)$, hence the algorithm's complexity is higher than polynomial in $\deg R$.

Nonetheless, our algorithm is roughly as efficient on mixed systems whose Newton polytopes do not differ so drastically as indicated in Theorem 24. Moreover, a greedy version of the algorithm has been implemented on *Maple V* by the first author and P. Pedersen, and preliminary empirical results imply that this approach is efficient for most systems encountered in practice.

8 Open Questions

We are currently looking into ways for decreasing the size of the determinantal formula, the final goal being to obtain Sylvester-type formulas for different systems. Characterizing these systems for which an optimal formula does not exist is another active area [24]. A more theoretical question is on the connection of our technique with Gröbner bases, in light of [19]. Lastly, this approach leads to improved methods for calculating the common roots of sparse polynomial systems [5].

Acknowledgment

We wish to thank the anonymous referee for his comments and Ashu Rege for several discussions.

References

1. Bernstein, D.N.: The number of roots of a system of equations. *Funktsional'nyi Analiz i Ego Prilozheniya*, 9(3):1–4, Jul-Sep 1975.
2. Betke, U.: Mixed volumes of polytopes. *Arch. der Math.*, 58:388–391, 1992.
3. Canny, J.F.: *The Complexity of Robot Motion Planning.* M.I.T. Press, Cambridge, 1988.
4. Gel'fand, I.M., Kapranov, M.M. and Zelevinsky, A.V.: Discriminants of polynomials in several variables and triangulations of Newton polytopes. *Algebra i Analiz*, 2:1–62, 1990.
5. Huber, B. and Sturmfels, B.: Homotopies preserving the Newton polytopes. Manuscript, presented at the "Workshop on Real Algebraic Geometry", August 1992.

6. Hurwitz, A.: Über die Trägheitsformen eines algebraischen Moduls. *Annali di Mat.*, Tomo XX(Ser. III):113–151, 1913.
7. Kantor, J.M.: Sur le polynôme associé à un polytope à sommets entiers. *Comptes rendues de l'Académie des Sciences, Série I*, 314:669–672, 1992.
8. Karmarkar, N.: A new polynomial-time algorithm for linear programming. *Combinatorica*, 4:373–395, 1984.
9. Khovanskii, A.G.: Newton polyhedra and the genus of complete intersections. *Funktsional'nyi Analiz i Ego Prilozheniya*, 12(1):51–61, Jan-Mar 1978.
10. Kushnirenko, A.G.: The Newton polyhedron and the number of solutions of a system of k equations in k unknowns. *Uspekhi Mat. Nauk.*, 30:266–267, 1975.
11. Kushnirenko, A.G.: Newton polytopes and the Bezout theorem. *Funktsional'nyi Analiz i Ego Prilozheniya*, 10(3), Jul-Sep 1976.
12. Loos, R.: 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.
13. Macaulay, F.S.: Some formulae in elimination. *Proc. London Math. Soc.*, 1(33):3–27, 1902.
14. Manocha, D. and Canny, J.: Real time inverse kinematics for general 6R manipulators. In *Proc. IEEE Intern. Conf. Robotics and Automation*, Nice, May 1992.
15. Pedersen, P. and Sturmfels, B.: Product formulas for sparse resultants. Manuscript, 1991.
16. Salmon, G.: *Modern Higher Algebra.* G.E. Stechert and Co., New York, 1885. reprinted 1924.
17. Schwartz, J.T.: Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, 1980.
18. Stanley, R.P.: 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.
19. Sturmfels, B.: Gröbner bases of toric varieties. *Tôhoku Math. J.*, 43:249–261, 1991.
20. Sturmfels, B.: Sparse elimination theory. In D. Eisenbud and L. Robbiano, editors, *Proc. Computat. Algebraic Geom. and Commut. Algebra*, Cortona, Italy, June 1991. Cambridge Univ. Press. To appear.
21. Sturmfels, B.: Combinatorics of the sparse resultant. Technical Report 020-93, MSRI, Berkeley, November 1992.
22. Sturmfels, B. and Zelevinsky, A.: Multigraded resultants of Sylvester type. *J. of Algebra.* To appear. Also, Manuscript, 1991.
23. van der Waerden, B.L.: *Modern Algebra.* Ungar Publishing Co., New York, 3rd edition, 1950.
24. Weyman, J. and Zelevinsky, A.: Determinantal formulas for multigraded resultants. Manuscript, 1992.

This article was processed using the LaTeX macro package with LLNCS style