

# Matrix-based methods for solving polynomial systems

*Ioannis Emiris*

Projet SAFIR, Inria Sophia-Antipolis

11 mars, 1996

[summary by Frédéric Chyzak]

## Abstract

We present a uniform approach to the elimination of variables between polynomials and the construction of matrices that express resultants. Building a matrix whose determinant is a multiple of the resultant reduces the solving of a polynomial system to a generalized eigenvalues/eigenvectors problem for a square matrix. Several such matrices are of interest, in particular the Newton and Bézout/Dixon matrices, which lead to efficient calculations.

## 1. Classical resultants versus sparse resultants

Classically, the resultant is a single polynomial which characterizes the solvability of a system of dense polynomials [7]. We introduce another concept of resultant which takes the structure of the coefficients into account.

Let  $f_1(\mathbf{c}, x), \dots, f_{n+1}(\mathbf{c}, x)$  be  $n + 1$  polynomials in the  $n$  indeterminates  $x_1, \dots, x_n$  and with coefficients that are polynomial in  $c_1, \dots, c_N$  over a field  $\mathbb{K}$ . A *sparse resultant*  $R(\mathbf{c})$  with respect to a subfield  $\mathbb{L}$  of the algebraic closure  $\overline{\mathbb{K}}$  is an irreducible polynomial of  $\mathbb{K}[c_1, \dots, c_N]$  that vanishes at a specialization  $\gamma$  of the  $c_i$ 's if and only if the corresponding specializations of the  $f_i$ 's have a common zero. In other words, the resultant satisfies

$$\forall \gamma \in \mathbb{L}^N \quad (R(\gamma) = 0 \iff \exists \xi \in \mathbb{L}^n \quad \forall i = 1, \dots, n \quad f_i(\gamma, \xi) = 0).$$

For some applications, one requires that the coefficients of the  $f_i$ 's be generic, i.e., that one  $c_i$  be introduced for each coefficient. Special cases are of particular interest. In the case of dense homogenized polynomials

$$f_i(x_0, x_1, \dots, x_n) = \sum_{a_0 + \dots + a_n = d_i} c_{a_0, \dots, a_n} x_0^{a_0} \dots x_n^{a_n},$$

we recover the classical *homogeneous resultant* [7]. In the case of two (dense) univariate polynomials, we recover Sylvester's classical notion of the *univariate resultant* [6], whose expression as a determinant is recalled in the next section. In the case of (possibly sparse) polynomials with generic coefficients, i.e., when

$$f_i(x_1, \dots, x_n) = \sum_{j=1}^{r_i} c_{i,j} x_1^{a_{i,j,1}} \dots x_n^{a_{i,j,n}}$$

for non-zero undetermined coefficients  $c_{i,j}$  that are transcendental over the field  $\mathbb{K}$ , the resultant  $R(\mathbf{c})$  is called the *sparse resultant* of the  $f_i$ 's.

A major difference between the classical and the sparse resultants is that the former express simultaneous solvability in a *projective* space  $\mathbb{P}^n(\overline{\mathbb{K}})$  whereas the latter express simultaneous solvability in the *torus*  $(\overline{\mathbb{K}}^*)^n$  which is a proper subset of  $\mathbb{P}^n(\overline{\mathbb{K}})$ .

## 2. Expression of the resultant as a determinant

Two important examples of classical resultants are given as the determinant of a matrix. First, in the case of dense linear polynomials  $f_i = c_{i,0} + c_{i,1}x_1 + \dots + c_{i,n}x_n$ , the corresponding homogeneous resultant [7] is

$$R(\mathbf{c}) = \det \begin{bmatrix} c_{1,0} & \dots & c_{1,n} \\ \vdots & & \vdots \\ c_{n+1,0} & \dots & c_{n+1,n} \end{bmatrix}.$$

Second, in the case of dense univariate polynomials  $f(a, x) = a_n x^n + \dots + a_0$  and  $g(b, x) = b_m x^m + \dots + b_0$ , the univariate resultant [6] is the following determinant

$$R(a, b) = \det \begin{bmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_2 & a_1 & a_0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & a_{n-2} & \dots & a_2 & a_1 & a_0 & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & & & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & a_n & a_{n-1} & a_{n-2} & \dots & a_2 & a_1 & a_0 \\ b_m & b_{m-1} & b_{m-2} & \dots & b_2 & b_1 & b_0 & 0 & \dots & 0 \\ 0 & b_m & b_{m-1} & b_{m-2} & \dots & b_2 & b_1 & b_0 & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & & & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & b_m & b_{m-1} & b_{m-2} & \dots & b_2 & b_1 & b_0 \end{bmatrix},$$

where the matrix has constant values on diagonals and each row corresponds to the product of either polynomial times a power of  $x$ , written in the basis  $(x^{\max(n,m)}, \dots, x, 1)$ . Sparse resultants can be expressed as the determinant of a matrix. More precisely, we proceed to give an expression of a multiple of the resultant in the case of sparse polynomials with generic undetermined coefficients.

To give this expression, define the *support* of a polynomial  $f = \sum_{a_1, \dots, a_n} c_{a_1, \dots, a_n} x_1^{a_1} \dots x_n^{a_n}$  as the set  $\text{Supp}(f) \subset \mathbb{N}^n$  of those  $(a_1, \dots, a_n)$  such that  $c_{a_1, \dots, a_n} \neq 0$ . Note that

$$\text{Supp}(fg) \subset \text{Supp}(f) + \text{Supp}(g) \quad \text{and} \quad \text{Supp}(f + g) \subset \text{Supp}(f) \cup \text{Supp}(g).$$

With this definition, we now construct matrices that represent the specialization application of polynomials  $f_i(\mathbf{c}, x)$  on a point  $\xi \in \mathbb{K}^n$ . For  $i = 1, \dots, n$ , let  $S_i$  be a subset of  $\mathbb{N}^n$ . Next define  $S_0$  to be  $\bigcup_{i=1}^n (S_i + \text{Supp}(f_i))$ . For  $i = 0, \dots, n$ , call  $P_i$  the set of polynomials  $f \in \mathbb{K}[\mathbf{c}, x]$  such that  $\text{Supp}(f) \subset S_i$ . Then, the application  $\mathcal{M}$  from  $P_1 \times \dots \times P_n$  to  $P_0$  given by  $\mathcal{M}(l_1, \dots, l_n) = \sum_{i=1}^n l_i f_i$  is a well-defined linear application. For  $i = 0, \dots, n$ , write  $S_i = \{s_{i,1}, \dots, s_{i,N_i}\} \subset \mathbb{N}^n$ . Then  $\mathcal{M}$  has a matrix representation,  $M = [m_{(i,i'),j}(\mathbf{c})]$ , where, for convenience, we number the rows of  $M$  by  $(i, i')$  and the columns by  $j$ . This matrix is given by

$$x^{s_{i,i'}} f_i(\mathbf{c}, x) = \sum_{j=1}^{N_0} m_{(i,i'),j}(\mathbf{c}) x^{s_{0,j}}, \quad \text{for } i = 1, \dots, n \text{ and } i' = 1, \dots, N_i.$$

Under this representation, the evaluation of  $\mathcal{M}$  at the tuple  $(\sum_{j=1}^{N_1} l_{1,j}(\mathbf{c}) x^{s_{1,j}}, \dots, \sum_{j=1}^{N_n} l_{n,j}(\mathbf{c}) x^{s_{n,j}})$  of  $P_1 \times \dots \times P_n$  is given by the product:

$$\begin{bmatrix} l_{(1,1)}(\mathbf{c}) & \dots & l_{(n,N_n)}(\mathbf{c}) \end{bmatrix} \begin{bmatrix} m_{(1,1),1}(\mathbf{c}) & \dots & m_{(1,1),N_0}(\mathbf{c}) \\ \vdots & \ddots & \vdots \\ m_{(n,N_n),1}(\mathbf{c}) & \dots & m_{(n,N_n),N_0}(\mathbf{c}) \end{bmatrix} \begin{bmatrix} x^{s_{1,1}} \\ \vdots \\ x^{s_{n,N_n}} \end{bmatrix}.$$

On the other hand, the product of  $M$  by a column vector yields the simultaneous specialization of multiples of the  $f_i$ 's at a point  $\xi \in \mathbb{K}^n$ :

$$\begin{bmatrix} m_{(1,1),1}(\mathbf{c}) & \cdots & m_{(1,1),N_0}(\mathbf{c}) \\ \vdots & \ddots & \vdots \\ m_{(n,N_n),1}(\mathbf{c}) & \cdots & m_{(n,N_n),N_0}(\mathbf{c}) \end{bmatrix} \begin{bmatrix} \xi^{s_{0,1}} \\ \vdots \\ \xi^{s_{0,N_0}} \end{bmatrix} = \begin{bmatrix} \xi^{s_{1,1}} f_1(\mathbf{c}, \xi) \\ \vdots \\ \xi^{s_{n,N_n}} f_n(\mathbf{c}, \xi) \end{bmatrix}.$$

From this second fact, it follows that if  $\xi \in (\overline{\mathbb{K}}^*)^n$  is a common zero of the specializations of the  $f_i(\mathbf{c}, x)$  at  $\mathbf{c} = \gamma$ , there exists  $v_\gamma = [\xi^{s_{1,1}}, \dots, \xi^{s_{n,N_n}}]^T \neq 0$  such that  $M(\gamma)v_\gamma = 0$ . Moreover, when  $M$  is a square matrix, we have that  $\det M(\gamma)$  is zero. More is true: in the case when such a  $v_\gamma$  exists,  $R(\mathbf{c})$  divides  $\det M(\mathbf{c})$ , and the matrix  $M$  is called a *matrix of the resultant*. One thus computes a multiple of the resultant as the determinant of the matrix  $M$  above. It only remains to determine suitable sets  $S_i$ , for which possible constructions are alluded to in Section 4.

### 3. Numerically solving polynomial systems

In this section, we assume that  $f_1, \dots, f_n \in \mathbb{K}[x_1, \dots, x_n]$  is a well-determined system of polynomials with *determined* coefficients, whose variety is zero-dimensional, i.e., the roots are isolated. We assume further that the ideal  $(f_1, \dots, f_n)$  is radical, i.e., that the roots are simple. Then, when the matrix  $M$  above is a matrix of the resultant, it can be used to numerically solve the system.

To do so, we look at an over-determined system in place of the well-determined system, so as to introduce genericness in the coefficients. Two such over-determined systems are available:

- (1) either we add  $f_{n+1} = r_1 x_1 + \cdots + r_n x_n + u$  for  $r_i$  in  $\mathbb{K}$ , and view the  $f_i$ 's as elements of  $\mathbb{K}[u][x_1, \dots, x_n]$ , and we look for their sparse resultant in  $\mathbb{K}[u]$ ;
- (2) or we conceal one variable, say  $x_n$ , and view the  $f_i$ 's as elements of  $\mathbb{K}[x_n][x_1, \dots, x_{n-1}]$ , and we look for their sparse resultant in  $\mathbb{K}[x_n]$ .

If the second system is chosen, we change  $n$  into  $n - 1$ , then  $x_{n+1}$  into  $u$ , so that in both cases, we look for the sparse resultant  $R(u) \in \mathbb{K}[u]$  of polynomials  $f_i(u, x) \in \mathbb{K}[u][x_1, \dots, x_n]$ . In either case, let us assume that the matrix  $M(u)$  is a matrix of the resultant.

Again, let  $\mathbb{L}$  be an algebraic field extension of  $\mathbb{K}$  in  $\overline{\mathbb{K}}$  and  $(\xi, \eta) \in \mathbb{L}^n \times \mathbb{L}$  be a solution in  $(x, u)$  of the over-determined system. Then  $\det M(\eta) = 0$  and  $M(\eta)v_\xi = 0$ . If case (1) above was chosen, we only need to determine  $\xi$ . If case (2) above was chosen, we need to determine both  $\xi$  and  $\eta$ . In both cases, we look for  $(\xi, \eta)$ , or equivalently for  $(v_\xi, \eta)$ . This reduces the initial problem of solving a polynomial system to a generalized eigenvalues/eigenvectors problem, for which optimized numerical algorithms are available. More specifically, this problem takes several possible forms, amongst which both following extreme cases:

- if the matrix  $M(u)$  is linear in  $u$ ,  $M(u) = M_1 u + M_0$ , with  $M_1$  invertible, the problem is a (simple) eigenvalues/eigenvectors problem:

$$M(\eta)v_\xi = 0 \iff (-M_1^{-1}M_0 - \eta \text{Id}) v_\xi = 0;$$

- if the matrix  $M(u)$  is non-linear in  $u$ ,  $M(u) = M_d u^d + \cdots + M_0$ , with  $M_d$  non-invertible, the problem is a generalized eigenvalues/eigenvectors problem:

$$M(\eta)v_\xi = 0 \iff \left( \begin{bmatrix} 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & 1 \\ -M_0 & -M_1 & \dots & M_{d-1} \end{bmatrix} - \eta \begin{bmatrix} 1 & 0 & 0 \\ & \ddots & \vdots \\ 0 & & 1 & 0 \\ 0 & \dots & 0 & M_d \end{bmatrix} \right) \begin{bmatrix} v_\xi \\ \eta v_\xi \\ \vdots \\ \eta^{d-1} v_\xi \end{bmatrix} = 0.$$

To reduce the size of the matrices and achieve more efficiency, we perform operations on rows and permutations on columns of  $M$  beforehand, rewriting  $M$  and  $v_\xi$  in the form

$$\tilde{M}(u) = \begin{bmatrix} \tilde{M}_{1,1} & \tilde{M}_{1,2}(u) \\ \tilde{M}_{2,1}(u) & \tilde{M}_{2,2}(u) \end{bmatrix} \quad \text{and} \quad \tilde{v}_\xi = \begin{bmatrix} w'_\xi \\ w''_\xi \end{bmatrix}, \quad \text{respectively.}$$

It follows that

$$M(\eta)v_\xi = 0 \iff \tilde{M}(\eta)\tilde{v}_\xi = 0 \iff \begin{bmatrix} \tilde{M}_{1,1} & \tilde{M}_{1,2}(u) \\ 0 & \tilde{M}_{2,2}(x) - \tilde{M}_{2,1}(u)\tilde{M}_{1,1}^{-1}\tilde{M}_{1,2}(u) \end{bmatrix} \begin{bmatrix} w'_\xi \\ w''_\xi \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix},$$

whence  $M'(x) = \tilde{M}_{2,2}(x) - \tilde{M}_{2,1}(u)\tilde{M}_{1,1}^{-1}\tilde{M}_{1,2}(u)$  satisfies  $M'(x)w'_\xi = 0$ . Solving this smaller problem yields possible roots of the initial problem.

#### 4. Mixed volume and various matrices of resultants

The *mixed volume* of convex polyhedra  $Q_1, \dots, Q_n \subset \mathbb{R}^n$  is classically defined by the single mapping VM to  $\mathbb{R}$  which is multilinear with respect to the addition of polyhedra and such that  $\text{VM}(Q, \dots, Q) = n! \text{Vol}(Q)$ , where Vol is the Euclidean volume. We next define the *Newton polytope* of a polynomial  $f$  as the convex hull of its support. A famous theorem by Bernstein [1] states the number of isolated roots of a polynomial system counted with multiplicity is bounded by the mixed volume of the Newton polytopes of the polynomials, a bound which is much better in case of sparse polynomials than the older Bézout's bound for dense polynomials. An efficient algorithm is given in [2, 5], where the construction of the Newton matrix of a resultant is derived.

Another matrix of a resultant is of interest, the Bézout-Dixon matrix [3], which is defined by introducing new indeterminates  $a_i$  as

$$\begin{bmatrix} f_1(x) & \dots & \frac{f_1(a_1, \dots, a_i, x_{i+1}, \dots, x_n) - f_1(a_1, \dots, a_{i-1}, x_i, \dots, x_n)}{a_i - x_i} & \dots & \frac{f_1(a) - f_1(a_1, \dots, a_{n-1}, x_n)}{a_n - x_n} \\ \vdots & & \vdots & & \vdots \\ f_{n+1}(x) & \dots & \frac{f_{n+1}(a_1, \dots, a_i, x_{i+1}, \dots, x_n) - f_{n+1}(a_1, \dots, a_{i-1}, x_i, \dots, x_n)}{a_i - x_i} & \dots & \frac{f_{n+1}(a) - f_{n+1}(a_1, \dots, a_{n-1}, x_n)}{a_n - x_n} \end{bmatrix}.$$

#### Bibliography

- [1] Bernstein (D. N.). – The number of roots of a system of equations. *Functional Analysis and Applications*, vol. 9, n° 2, 1975, pp. 183–185.
- [2] Canny (J.) and Emiris (I.). – An efficient algorithm for the sparse mixed resultant. In Cohen (G.), Mora (T.), and Moreno (O.) (editors), *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Lecture Notes in Computer Science*, pp. 89–104. – Springer Verlag, 1993. Proceedings AAEECC'93, May, Puerto Rico.
- [3] Dixon (A. L.). – The eliminant of three quantics in two independent variables. *Proceedings of the London Mathematical Society*, vol. 6, 1908, pp. 49–69 and 209–236.
- [4] Emiris (I. Z.). – *Sparse Elimination and Applications in Kinematics*. – PhD thesis, Computer Science Division, Dept. of Electrical Engineering and Computer Science, University of California, Berkeley, December 1994.
- [5] Emiris (I. Z.) and Canny (J.F.). – Efficient incremental algorithms for the sparse resultant and the mixed volume. *Journal of Symbolic Computation*, vol. 20, n° 2, August 1995, pp. 117–149.
- [6] Sylvester (J. J.). – On a theory of syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's functions, and that of the greatest algebraic common measure. *Philosophical Transactions*, vol. 143, 1853, pp. 407–548.
- [7] van der Waerden (B. L.). – *Modern Algebra*. – Frederick Ungar Publishing Co., New-York, 1950, third edition.