RISC-Linz Report Series 1995

On Bézout's Method for Computing the Resultant

P. Bikker[†]

Research Institute for Symbolic Computation
Johannes Kepler University
A-4040 Linz, Austria

pbikker@risc.uni-linz.ac.at

21 September 1995

Bézout's method for computing the resultant of a set of multivariate polynomials is discussed. We modified the method so that it can also be applied to polynomials not in generic form. In this modification a Gröbner basis of one polynomial fewer is used. The constructed Bézout matrix is the smallest among all matrices appearing in resultant formulations. Bézout's method provides a sufficient condition for any factor of the final result to be non-extraneous.

Acknowledgement Thanks to A.Y. Uteshev, who told me about the method of Bézout.

1. Introduction

Let $X = \{x_1, \ldots, x_n\}$ be a set of variables and let x be a variable not in X. In this paper we consider polynomials $f_1, \ldots, f_n, g \in K[x, x_1, \ldots, x_n]$, where K is a field, $n \geq 1$. We are interested in the common zeroes of these polynomials over $\overline{K}$. The variable x can be viewed as the parameter, and, for convenience, we consider having just one parameter.

We aim to determine a necessary and sufficient condition on $x \in \overline{K}$ for the existence of a common zero for $f_1, \ldots, f_n$ and g over $\overline{K}$. For this we use the formulation of the resultant by means of the so-called Poisson product. We give this definition because the method of Bézout is directly connected with it.

Definition. The *g-resultant from eliminating* $x_1, \ldots, x_n$, denoted by $\mathcal{R}_X^g$, is defined to be

$$\mathcal{R}_X^g = \prod_i g(x, \Lambda_i), \tag{1.1}$$

where the Λ_i's are the common zeroes of $f_1, \ldots, f_n$ over $\overline{K[x]}$, i.e., $\Lambda_i \in \overline{K[x]}^n$ such that $f_1(x, \Lambda_i) = \ldots = f_n(x, \Lambda_i) = 0$.

† Supported by the ÖAD, grant 553.102/7-IV/A/5a/94

Note that the term g-resultant is not found in the literature. It is a matter of convenience to use it throughout this paper.

$\mathcal{R}_X^g$ is symmetric in the roots Λ_i, and, therefore, is a rational function in x, i.e. $\mathcal{R}_X^g \in K(x)$. It was proven that, if $f_1, \ldots, f_n, g$ are in *generic* form[1], i.e., homogeneous, complete in all their terms and independent (parametric) coefficients, vanishing of the *numerator* of $\mathcal{R}_X^g$ is a necessary and sufficient condition for $f_1, \ldots, f_n, g$ to have a common zero over $\overline{K}$ (see [4]). In order to handle non-generic cases, we define the resultant more carefully.

DEFINITION. The *resultant from eliminating* $x_1, \ldots, x_n$, also called the *eliminant in* x, denoted by $\mathcal{R}_X$, is defined to be

$$\mathcal{R}_X = \mathcal{D}_X^g \mathcal{R}_X^g,$$

where $\mathcal{D}_X^g$ is a polynomial in $K[x]$ such that $\mathcal{R}_X \in K[x]$ and the vanishing of $\mathcal{R}_X$ is a necessary and sufficient condition on x for $f_1, \ldots, f_n$ and g to have a common zero over $\overline{K}$.

As already said, in the generic case, we can choose, $\mathcal{D}_X^g$ to be the denominator of $\mathcal{R}_X^g$. Note that $\mathcal{R}_X$ is not unique, but is defined up to a multiplicative non-zero constant in K. Also we did not say anything about the squarefreeness of $\mathcal{R}_X$. In the generic case we have squarefreeness guarenteed, choosing $\mathcal{R}_X$ to be the numerator of $\mathcal{R}_X^g$. We could define the resultant more strictly, by saying that it should have the correct multiplicities of the factors, meaning that if $\bar{x} \in \overline{K}$ is a root of multiplicity m of $\mathcal{R}_X$, then there are common zeroes of $f_1, \ldots, f_n, g$ at $\bar{x}$, with total multiplicity m.

Remark: if there are infinitely many common zeroes of $f_1, \ldots, f_n$ over $\overline{K[x]}$ then it still can happen that the g-resultant is defined correctly, namely in case there exists a polynomial in $K[x]$ such that vanishing of this polynomial is a necessary and sufficient condition for $f_1, \ldots, f_n$ and g to have a common zero. If such a polynomial does not exist, then the eliminant in x is defined to be 0.

Methods for computing the resultant are due to Bézout ([1]), Sylvester ([2]), Cayley ([3]), Macaulay ([4]) and Dixon ([5]). Also Gröbner bases ([6]) can be used to compute the so-called *elimination ideal*, defined as $\langle f_1, \ldots, f_n, g \rangle \cap K[x]$. The generator of this elimination ideal and the eliminant in x have the same squarefree factors over $K[x]$. We refer to [7] for an introduction to the different methods. In this paper also the Characteristic Set (or Ritt-Wu's) method is discussed. We refer to [12] for a comparison of the methods of Dixon and Macaulay.

We will concentrate on the method of Bézout. In Section 2 that method is described. In Section 3, we will present a modification of the method, so that it also works in non-generic cases. Section 4 is devoted to proving of the correctness of the modified Bézout method. In Section 5, we will discuss the phenomenon of extraneous factors, on which the modified Bézout's method gives more insight. After giving a few additional examples in Section 6, we will discuss, in Section 7, some efficiency and applicability considerations.

[1] Macaulay calls this *general* form.

In [11] a method, very close to our modification of Bézout's method, was already briefly mentioned. As far as we know, our modification of Bézout's method is new.

2. Resultant computation: Bézout's method

More than 200 years ago, Bézout presented a method for computing the resultant. The method was almost forgotten, maybe due to Sylvester's method, which was introduced about 50 years later and is still the most popular till now.

Bézout considered $f_1, \ldots, f_n, g$ to be in generic form. He used the set of monomials

$$M = \{x_1^{p_1} \cdots x_n^{p_n} \mid p_1 < d_1, \ldots, p_n < d_n\},$$

where $d_i = \deg(f_i)$. The set M contains $d = \prod_{i=1}^{n} d_i$ monomials [2]. Let $m_1, \ldots, m_d$ be the elements of M.

For any $m_i \in M$, determine $a_{i1}, \ldots, a_{in} \in K(x)[x_1, \ldots, x_n]$, such that

$$m_i g = \sum_{j=1}^{n} a_{ij} f_i + R_i,$$

where R_i is in $K(x)[x_1, \ldots, x_n]$ with monomials in M, i.e., $R_i = \sum_{j=1}^{d} r_{ij} m_j$ for some $r_{ij} \in K(x)$. The R_i can be determined by means of linear algebra. The *Bézout matrix* is defined to be the matrix, in which the ith column contains the coefficients of the monomials $m_1, \ldots, m_d$ in R_i. This matrix is obviously a square matrix. The determinant of the Bézout matrix is the g-resultant and its numerator is the resultant (in the generic case).

For the two-polynomial case ($n = 1$) we will work out the method in more detail. So let f and g be polynomials in x_1 of degree respectively d_f and d_g. We have that $M = \{1, x_1, \ldots, x_1^{d_f - 1}\}$. Determining the R_i's is straighforward: it is the remainder of division of $x_1^i g$ by f. If $f = a_{d_f} x_1^{d_f} + \ldots + a_1 x_1 + a_0$, then we have

$$R_{i+1} = x_1 R_i - r_i / a_{d_f} f,$$

where r_i is the coefficient of $x_1^{d_f - 1}$ in R_i. R_1 is the remainder of division of g by f.

Example 1 *Two polynomials*

$$\begin{aligned} f &= y^3 - xy^2 + x^2 y - x^3 + 1 \\ g &= y^4 + x^2 y^2 + x^4 + 1 \end{aligned}$$

We want to eliminate y. The degree in y of f is 3, so $M = \{1, y, y^2\}$. We have that $R_1 = x^2 y^2 - y + 2x^4 - x + 1$. R_2 and R_3 can be determined with the recurrence relation:

$$\begin{aligned} R_2 = yR_1 - x^2 f &= (x^3 - 1)y^2 + (x^4 - x + 1) + x^5 - x^2 \\ R_3 = yR_2 - (x^3 - 1)f &= (2x^4 - 2x + 1)y^2 + x^6 - 2x^3 + 1 \end{aligned}$$

[2] d equals Bézout's upper bound on the number of common zeroes of $f_1, \ldots, f_n$ over $\overline{K[x]}$.

The Bézout matrix is the coefficient matrix of R_1, R_2 and R_3:

$$\begin{pmatrix} 2x^4 - x + 1 & -1 & x^2 \\ x^5 - x^2 & x^4 - x + 1 & x^3 - 1 \\ x^6 - 2x^3 + 1 & 0 & 2x^4 - 2x + 1 \end{pmatrix}.$$

Its determinant is $3x^{12} - 6x^9 + 7x^8 + 4x^6 - 10x^5 + 5x^4 - 2x^3 + 3x^2 - 4x + 2$. Interchanging f and g gives a 4×4 matrix. Note that the Sylvester matrix is a 7×7 matrix.

We will now give two examples with three polynomials. In the second one we see how Bézout's method can fail.

Example 2 *The cyclic 3-roots system*

$$\begin{aligned} f_1 &= x + y + z \\ f_2 &= xy + yz + zx \\ g &= xyz - 1 \end{aligned}$$

We want to eliminate y and z. We have $M = \{1, y\}$, because $d_1 = 1$ and $d_2 = 2$, and

$$\begin{aligned} 1 \cdot g &= xf_2 - x^2 f_1 + x^3 - 1 \\ y \cdot g &= yxf_2 - yx^2 f_1 + y(x^3 - 1) \end{aligned}$$

Hence the Bézout matrix equals

$$\begin{pmatrix} x^3 - 1 & 0 \\ 0 & x^3 - 1 \end{pmatrix}.$$

The determinant of this matrix equals the eliminant in x:

$$\mathcal{R}_{y,z} = (x^3 - 1)^2 = (x - 1)^2 (x^2 + x + 1)^2$$

Example 3

$$\begin{aligned} f_1 &= x^2 + xy + y^2 - 2xz - 4yz + 3z^2 + x + 2y - z - 2 \\ f_2 &= 2x^2 - xy + y^2 - xz - yz - 6z^2 + 2x - y + z + 2 \\ g &= x^3 + y^3 - x^2 z + xyz - 5y^2 z - 5xz^2 \\ &\quad +7yz^2 - 3z^3 + x^2 - 3xy + 2y^2 - xz - z^2 + 9 \end{aligned}$$

We want to eliminate x and y. $d_1 = d_2 = 2$, so $M = \{1, x, y, xy\}$. For determining the R_1, R_x, R_y and R_{xy} we can use that, for instance, $x^2 = f_2 - f_1 + 2xy - xz - 3yz + 9z^2 - x + 3y - 2z - 4$, etc.

We have, for instance,

$$\begin{aligned} R_1 &= \frac{1}{7}\left((-36z^2 + 145z - 62)y + (38z - 52)xy + \right. \\ &\quad \left. (-30z^2 + 29z - 22)x + 108z^3 - 186z^2 - 34z + 135\right). \end{aligned}$$

The determinant of the Bézout matrix equals the eliminant:

$$\begin{array}{c}\frac{1}{343}(z-1)(268272z^{10}+7248096z^9+4009656z^8\\ -4822376z^7+10090424z^6+14239382z^5+3419036z^4\\ -15245405z^3-16554200z^2+908208z-1987677)\end{array}$$

Applying Bézout's method to the same polynomials, eliminating y and z, it fails. Let's see what happens. We have $M=\{1,y,z,yz\}$. The power products y^2,z^2,y^3,z^3 etc. have to be expressed in terms of f_1, f_2 and a term with monomials in M, which we will denote with $o(M)$. For the power products y^2 and z^2 there are no difficulties:

$$\begin{aligned}3y^2 &= 2f_1+f_2+o(M)\\ 9z^2 &= f_1-f_2+o(M)\end{aligned}$$

In order to derive such expressions for the degree 3 monomials, y^3,z^3,yz^2 and y^2z, we multiply the expressions for y^2 and z^2 by y and z:

$$\begin{aligned}3y^3-9y^2z &= y(2f_1+f_2)+o(M)\\ 3y^2z-9yz^2 &= z(2f_1+f_2)+o(M)\\ 9yz^2-3y^2z &= y(f_1-f_2)+o(M)\\ 9z^3-3yz^2 &= z(f_1-f_2)+o(M)\end{aligned}$$

The second term in the left-hand side comes from the $o(M)$ term in the expression for y^2 and z^2. From the second and the third equation we should be able to extract equations for y^2z and yz^2. This is not possible because the coefficient matrix of the left-hand sides of these two equations is singular.

3. Bézout's method modified

In this section we will present a modification of Bézout's method, that works also in the non-generic case. The idea is to use a different set of monomials M.

Let I be the ideal generated by $f_1,\ldots,f_n$ over $K(x)[x_1,\ldots,x_n]$. Fix some monomial ordering on the monomials in $x_1,\ldots,x_n$. Compute with respect to this ordering the reduced Gröbner basis[3] of the ideal I. Let's call this Gröbner basis G, containing polynomials from $K(x)[x_1,\ldots,x_n]$. From G, a set of so-called independent monomials over $K(x)$ can be derived. We call this set M, which is basis for $K(x)[x_1,\ldots,x_n]/I$.

From now on, we consider the case where $f_1,\ldots,f_n$ have at least one and not infinitely many common zeroes over $\overline{K[x]}$. This is equivalent with the condition that M is a non-empty and finite set. The condition on M can be easily checked by inspecting G. At the end of this section we will come back to the case where M is not finite.

Hence let $M=\{m_1,\ldots,m_d\}$, $d\geq 1$. We can choose $m_1=1$. Recall that we can compute the normal form of any $h\in K(x)[x_1,\ldots,x_n]$ w.r.t. I using G, i.e., we can compute an h' with monomials in M for which $h\equiv_I h'$ (or $h-h'\in I$).

[3] For anything concerning Gröbner bases, we refer to [6] and [9].

Let R_i be the normal form of $m_i \cdot g$, $i = 1, \ldots, d$. We will call the matrix, containing in its ith column the coefficients of the monomials from M in R_i, the *(generalized) Bézout matrix*. In the sequel, we will denote this matrix by B. B is a $d \times d$ matrix with entries in $K(x)$. We have:

$$\left(\begin{array}{c} \cdot \\ \cdot \\ B : \text{elements in } K(x) \\ \cdot \\ \cdot \end{array} \right) \left(\begin{array}{c} m_1 \\ \cdot \\ \cdot \\ \cdot \\ m_d \end{array} \right) = \left(\begin{array}{c} m_1 g - a_{11} f_1 - \ldots - a_{1n} f_n \\ \cdot \\ \cdot \\ \cdot \\ m_d g - a_{d1} f_1 - \ldots - a_{dn} f_n \end{array} \right) \tag{3.1}$$

Note that the a_{ij}'s are from $K(x)[x_1, \ldots, x_n]$.

Remark Using this method for over-determined systems is no problem. We define I to be the ideal generated by all polynomials in the system, except one of them (which becomes the g).

Example 3 continued The reduced Gröbner basis of f_1 and f_2 over $\mathbb{Q}(x)[y, z]$ w.r.t. the lexicographic ordering $y > z$, contains the following two polynomials:

$$(-14x^3 - 36x^2 - 42x - 34) + (16x^2 + 7x - 23)z + (39x + 87)z^2 + (7x^2 + 26x + 9)y,$$

$$\begin{array}{c} (7x^4 + 27x^3 + 43x^2 + 27x + 22) + (-27x^3 - 70x^2 - 54x - 17)z \\ +(11x^2 - 12x - 83)z^2 + (39x + 87)z^3 \end{array}$$

So $M = \{1, z, z^2\}$ is a set of independent monomials. The 3×3 matrix B has rational polynomials in x as entries. We have

$$\begin{aligned} |B| \quad = \quad & \frac{-1}{9\,(13x + 29)^2}\,(x - 1)\,(432x^{10} - 8704x^9 \\ & -48504x^8 + 1072x^7 - 31028x^6 - 1214942x^5 \\ & -1640780x^4 + 920303x^3 - 226067x^2 - 2527401x + 3622467) \end{aligned}$$

which equals the g-resultant $\mathcal{R}^g_{y,z}$. Its numerator equals the resultant $\mathcal{R}_{y,z}$. Note the relation between the the denominator of $\mathcal{R}_{y,z}$ and the leading coefficients of the polynomials in the Gröbner basis. However the denominator of $\mathcal{R}_{y,z}$ is not due to the use of a Gröbner basis!

Remark The modified method may lead to more complicated computations. In example 3, eliminating x and y, we will never get the independent monomials $M = \{1, x, y, xy\}$, like the original method uses. For any monomial ordering we have that either M is $\{1, x, y, y^2\}$ or $\{1, y, x, x^2\}$.

On finding $\mathcal{D}^g_X$

We know that $|B|$ is, in general, a rational polynomial in x. In the generic case, we know that we can omit the denominator (or $\mathcal{D}^g_X$ equals the denominator of $|B|$): the numerator of $|B|$ equals the resultant. This happens also in the previous example (although it is not in generic form). We will now define a matrix B', whose determinant is a polynomial in x and a multiple of $|B|$.

Rationality of $|B|$, may occur in case a leading coefficient of a polynomial g' in the Gröbner basis G is not in K. Important is that we normalize every $g' \in G$ such that $g' \in K[x, x_1, \ldots, x_n]$. Then the normal form of $m_i g$ may contain rational polynomials in x as coefficients, with denominators that are products of factors of the leading coefficients of polynomials in G.

We will use the pseudo-normal form for computing the normal forms of each $m_i g$ (in fact, we also have to use the pseudo-normal form in the Gröbner basis computation, but we will not go into the details of this complication now). Then we find a polynomial p_i in x, a product of factors of the leading coefficients of polynomials in G, such that the normal form of $p_i m_i g$ can be written as

$$p_i m_i g = \sum_{j=1}^{n} a_{ij} f_j,$$

where the a_{ij}'s are from $K[x, x_1, \ldots, x_n]$.

We will denote the matrix, containing in its ith column the coefficients of the monomials from M in the normal form of $p_i m_i g$, by B'. This matrix is of the same size as B and has its entries in $K[x]$.

$$\begin{pmatrix} \cdot \\ \cdot \\ B' : \text{elements in } K[x] \\ \cdot \\ \cdot \end{pmatrix} \begin{pmatrix} m_1 \\ \cdot \\ \cdot \\ \cdot \\ m_d \end{pmatrix} = \begin{pmatrix} p_1 m_1 g - a_{11} f_1 - \ldots - a_{1n} f_n \\ \cdot \\ \cdot \\ \cdot \\ p_d m_d g - a_{d1} f_1 - \ldots - a_{dn} f_n \end{pmatrix} \tag{3.2}$$

Obviously,

$$|B'| = |B| \prod_{i=1}^{d} p_i.$$

Note that with the previous procedure we do more than remove just the denominator in $|B|$. We force to have the a_{ij} in $K[x, x_1, \ldots, x_n]$. This is stronger, because $|B|$ might be a polynomial in x, even when some a_{ij} are rational (example III in Section 6).

Example 3 continued $|B'|$ equals $(13x + 29)^2\ |B|$, the correct eliminant in x.

The case where M is not a finite set

When M is not finite, i.e., I is not zero-dimensional, we have infinitely many common zeroes of $f_1, \ldots, f_n$ and the Poisson product (equation 1.1), defining the g-resultant, seems not to be defined properly. However if $f_1, \ldots, f_n$ and g have finitely many common zeroes, then we have to consider only finitely many Λ_i's in the Poisson product, because only these contribute to the product.

We propose a procedure to find a finite M, when I is not zero-dimensional. It is the following. We start out with an M containing only the element 1. We compute the normal form of $1 \cdot g$, collect all its power products and put them into M (if it is already in M we do not put it into). Then we take another monomial m from M, compute the normal form of $m \cdot g$ and follow the same procedure until all monomials from M are considered (after M stabilizes).

This procedure was succesfully applied to example X and XI (Section 6). In the next section we will prove that if this procedure terminates it gives the same results as when I is zero-dimensional.

An example with three polynomials is the following:

$$\begin{aligned} f_1 &= (y-z)(y-z-1) \\ f_2 &= (y-z)(z+1) \\ g &= (y-z)x-1 \end{aligned}$$

We want to eliminate y and z. The ideal generated by f_1 and f_2 over $K(x)[y,z]$ is not zero-dimensional, while the ideal generated by f_1, f_2 and g over $K[x,y,z]$ is zero-dimensional. There is one solution: $(x,y,z) = (1,0,-1)$. Applying Bézout's method, we found $M = \{1, y, z\}$ and the 3×3 Bézout matrix has determinantn $x - 1$.

4. Correctness of the modified Bézout method

In this section we prove that $|B|$ equals the g-resultant, in case $K(x)$ is a perfect field and I is a radical ideal. We also give a result for $|B'|$ in the general case, namely that vanishing of $|B'|$ is a necessary and sufficient (under some condition) condition on x for $f_1, \ldots, f_n, g$ to have a common zero.

If not otherwise indicated, I is the ideal generated by $f_1, \ldots, f_n$ in $K(x)[x_1, \ldots, x_n]$. G is the reduced Gröbner basis of I w.r.t. some monomial ordering. Every $g' \in G$ is normed such that $g' \in K[x, x_1, \ldots, x_n]$. I is zero-dimensional, so we can construct the Bézout matrices B and B' as described in the previous section. At the end of this section we will pay attention to the case where I is not zero-dimensional.

Let's start out with an easy, but important, result, which says that the resultant is 0 in case the Bézout matrix has zero determinant. In other multivariate resultant methods this is not the case and many techniques were developed for handling singular matrices, in order to get the non-zero resultant.

THEOREM 4.1. *Let J be the ideal generated by $f_1, \ldots, f_n, g$ over $K[x, x_1, \ldots, x_n]$. J is positive dimensional if and only if $|B|$ vanishes identically.*

PROOF. If J is positive dimensional, then for infinitely many values of $x \in \overline{K}$ the right-hand side of equation (3.1) vanishes. Because $m_1 = 1$, $|B|$ must vanish for infinitely many values of $x \in \overline{K}$. $|B| \in K(x)$, therefore $|B| = 0$.

On the other hand, if B has determinant 0, there is a linear dependency between the columns of B, i.e., there exist $r_1, \ldots, r_d \in K(x)$, not all zero, such that

$$g\ (r_1 + r_2 m_2 + \ldots + r_d m_d) \in I.$$

Let $h = r_1 + r_2 m_2 + \ldots + r_d m_d$. First we will prove that $f_1, \ldots, f_n$ and g have a common zero over $\overline{K[x]}$.

Let J be the ideal generated by $f_1, \ldots, f_n, g$ over $K(x)[x_1, \ldots, x_n]$, i.e., $J = I + \langle g \rangle$. If $f_1, \ldots, f_n$ and g do not have a common zero over $\overline{K[x]}$, then $1 \in J$ (from Hilbert's Nullstellensatz). This implies $h \in hJ = hI + h\langle g \rangle$. Hence $h \in I$ because $hg \in I$. This contradicts the fact that $1, m_2, \ldots, m_d$ are independent monomials modulo I.

So, let $\Lambda(x) \in \overline{K[x]}^n$ be a common zero of $f_1, \ldots, f_n$ and g. But then $f_1, \ldots, f_n, g$ have infinitely many common zeroes over $\overline{K}$, namely $(x, \Lambda(x))$ for almost all $x \in \overline{K}$ (except finitely many for which $\Lambda(x)$ is not defined). Therefore J is not zero-dimensional. $\square$

For our main theorem we will need the following three lemmas.

LEMMA 4.1. *Let I be a zero-dimensional ideal in the ring $K[x_1, \ldots, x_n]$, where K is a perfect field*[4]*. Then I is radical if and only if I contains a univariate squarefree polynomial in each variable.*

PROOF. We refer to [9].

LEMMA 4.2. *Let I be a zero-dimensional ideal in the ring $K[x_1, \ldots, x_n]$, where K is a perfect field. Let $d = dim(K[x_1, \ldots, x_n]/I)$. Then the polynomials in I have d distinct common zeroes if and only if I is radical.*

PROOF. There are multiple zeroes if and only if there is a non squarefree univariate polynomial in I. According to Lemma 4.1, I is radical if and only if I contains a univariate squarefree polynomial in each variable. $\square$

LEMMA 4.3. (GENERALIZED VANDERMONDE MATRIX PROPERTY) *Let I be a radical zero-dimensional polynomial ideal in the ring $K[x_1, \ldots, x_n]$, where K is a perfect field. Let $1, m_2, \ldots, m_d$ be a set of independent monomials modulo I, i.e., a basis of $K[x_1, \ldots, x_n]/I$. Let $\Lambda_1, \ldots, \Lambda_d \in \overline{K}$ be the d distinct common zeroes of the polynomials in I. Then the generalized Vandermonde matrix*

$$V = \begin{pmatrix} 1 & \cdot\ \cdot & 1 \\ m_2(\Lambda_1) & \cdot\ \cdot & m_2(\Lambda_d) \\ \cdot & & \cdot \\ \cdot & & \cdot \\ m_d(\Lambda_1) & \cdot\ \cdot & m_d(\Lambda_d) \end{pmatrix},$$

consisting of the columns $(1, m_2(\Lambda_i), \ldots, m_d(\Lambda_i))$, $1 \le i \le d$, has non-zero determinant.

PROOF. Note that Lemma 4.2 justifies that there are d distinct common zeroes. If the determinant of V is zero, we have a linear dependency between the columns of V, giving a non-zero polynomial $h \in K[x_1, \ldots, x_n]$, with monomials among $1, m_2, \ldots, m_d$, which has

[4] See [9]. K is a perfect field if every non-constant polynomial $f \in K[x]$ is squarefree if and only if $\gcd(f, f') = 1$. For instance fields of characteristic zero: $\mathbb{Q}$ and $\mathbb{Q}(x)$. $\mathbb{F}_p$ is perfect, but $\mathbb{F}_p(x)$ is not.

zeroes $\Lambda_1, \ldots, \Lambda_d$. Hence $h \in \sqrt{I}$. But I is radical and therefore $h \in I$. This contradicts the fact that $1, m_2, \ldots, m_d$ are independent monomials modulo I. □

THEOREM 4.2. (MAIN THEOREM I) *Let $K(x)$ be a perfect field and let I be radical. Then $|B|$ is equal to the g-resultant $\mathcal{R}_X^g$.*

PROOF. Let $\Lambda_1, \ldots, \Lambda_d \in \overline{K(x)}^n$ be such that $f_1(x, \Lambda_i) = \ldots = f_n(x, \Lambda_i) = 0$, $1 \leq i \leq d$. We have the following equation:

$$B\ V = V \begin{pmatrix} g(x,\Lambda_1) & & & \\ & \cdot & & \\ & & \cdot & \\ & & & g(x,\Lambda_d) \end{pmatrix}$$

where V is the generalized Vandermonde matrix. Taking the determinant on both sides, we find that

$$|B|\ |V| = |V| \prod_{i=1}^{d} g(x, \Lambda_i).$$

Since I is radical and $K(x)$ is a perfect field, Lemma 4.3 gives $|V| \neq 0$. So we can divide out $|V|$, leaving

$$|B| = \mathcal{R}_X^g.$$

□

THEOREM 4.3. (MAIN THEOREM II) *Let $|B'|$ be a non-zero polynomial in $K[x]$. For every $\bar{x} \in \overline{K}$ which is a root of $|B'|$, $\bar{x}$ can be extended to a common zero of $f_1, \ldots, f_n$ and g over $\overline{K}$, or else the leading coefficient of some $g' \in G$ vanishes at $\bar{x}$.*

PROOF. Let $\bar{x} \in \overline{K}$ be a root of $|B'|$, and $\beta(x)$ the factor of $|B'|$ equal to the minimal polynomial of $\bar{x}$ over K. We define J to be the ideal generated by $f_1, \ldots, f_n$ over $K[x]/\beta(x)[x_1, \ldots, x_n]$. If no leading coefficient of the polynomials in G vanishes at $\bar{x}$, we have that M is also an independent set of monomials modulo J. Note that if one of them vanishes, it may happen that M is still an independent set of monomials modulo J.

$|B'|$ vanishes, so there exist polynomials $p_1, \ldots, p_d \in K[x]/\beta(x)$, not all zero, such that

$$g\ (p_1 + p_2 m_2 + \ldots + p_d m_d) \in J.$$

Let $h = p_1 + p_2 m_2 + \ldots + p_d m_d$. If g has no common zero with $f_1, \ldots, f_n$ modulo $\beta(x)$, we have $1 \in J + \langle g \rangle$ (from Hilbert's Nullstellensatz), implying $h \in hJ + h\langle g \rangle \subset J$. Hence $h \in J$ because $hg \in J$. This contradicts the fact that M is an independent set of monomials modulo J. □

THEOREM 4.4. (MAIN THEOREM III) *Let $|B'|$ be a non-zero polynomial in $K[x]$. Then vanishing of $|B'|$ is a necessary condition on x for $f_1, \ldots, f_n, g$ to have a common zero over $\overline{K}$.*

PROOF. Let $\Lambda \in \overline{K}^{n+1}$ be a common zero of $f_1, \ldots, f_n$ and g. Let $\bar{x}$ be the x-component of Λ. The right-hand side of equation (3.2) vanishes at Λ. Because $m_1 = 1$, $|B'|$ must vanish at $\bar{x}$. □

Remark This theorem does not hold for $|B|$. For instance, $f_1 = xx_1$ and $g = x_1 + 1$, gives $|B| = 1$. So $|B|$ does not vanish, although f_1 and g have a common zero. Note that the reduced Gröbner basis of f_1 over $K(x)[x_1]$ equals $\{x_1\}$, so the leading coefficient is 1. Hence we should be alert on how to compute the reduced Gröbner basis: also using pseudo-normal forms during the Gröbner basis computation.

THEOREM 4.5. *Let I be radical and $K(x)$ be a perfect field. If all leading coefficients of the polynomials in G are in K then $|B|$ equals the resultant $\mathcal{R}_X$.*

PROOF. A corollary of theorem 4.2 and 4.3. □

THEOREM 4.6. *If all leading coefficients of the polynomials in G are in K then $|B'|$ and $\mathcal{R}_X$ have the same squarefree factors.*

PROOF. A corollary of theorem 4.3 and 4.4. □

Remark It is straightforward how to generalize the previous statements to the case where there are more parameters than only x. For the previous two theorems the change is that the leading coefficients of the polynomials in G do not depend on the parameters.

Special case: I is not zero-dimensional

We still did not pay attention to the case where I is not zero-dimensional. In the previous section we gave a procedure to find a finite set M of independent monomials. There is to prove that this procedure works, i.e., terminates and gives a useful result.

So let I be the ideal generated by $f_1, \ldots, f_n$ over $K(x)[x_1, \ldots, x_n]$, I is positive non-zero dimensional. Let J be the ideal generated by $f_1, \ldots, f_n, g$ over $K[x, x_1, \ldots, x_n]$.

The proofs of theorem 4.1, 4.3 and 4.4 can be copied for the case M is obtained with the different procedure. It then remains to prove that this procedure terminates. The conjecture is that it terminates in case J is zero-dimensional. In the proof we may use that I is positive non-zero dimensional, but that $I + \langle g \rangle$ equals $\langle 1 \rangle$ over $K(x)[x_1, \ldots, x_n]$, so the dimension of I drops at least 2, if we add g. It is not difficult to construct examples for which the procedure does not terminate and J is not zero-dimensional. It would be interesting to be able to detect if this procedure is not terminating.

5. Extraneous factors

We are not aware of any existing method to determine for factors in the final result of a multi-polynomial resultant method whether they are extraneous or not. The modified method of Bézout says something about it. Theorem 4.3 gives a sufficient condition on factors in the final result $|B'|$ to be non-extraneous. Those factors are non-extraneous who do not appear as a factor in any of the leading coefficients of polynomials in G. In fact, it is reasonable that we gain something, using a powerful tool like Gröbner bases.

Example 4 *Due to D. Kapur and T. Saxena*

$$\begin{aligned} f_1 &= ax^2 + bxy + (b+c-a)x + ay + 3(c-1) \\ f_2 &= 2a^2x^2 + 2abxy + aby + b^3 \\ g &= 4(a-b)x + c(a+b)y + 4ab \end{aligned}$$

We want to eliminate x and y. Using total degree ordering $x > y$ we get as leading terms in the reduced Gröbner basis G of f_1 and f_2 over $K(z)[x, y]$:

$$a(a-b-c)x, a(2a-b)(2a^2+ab-2b^2-2bc)y^2$$

Hence $M = \{1, y\}$. $|B'|$ turned out to be a factor $a^2(2a-b)(2a^2+ab-2b^2-2bc)(a-b-c)^2$ times $|B|$ and is equal to $(a-b-c)^2 \cdot R$ (R turns out to be the resultant. R can be found in [12]). The extraneous factors showing up in the sparse, perturbation and rank submatrix method, discussed in [12], are $a-b-c$, a, b, c, $a+b$ and $a^2c + abc - 4ab + 4b^2$.

With Bézout's method, we know which factor in the final result $|B'|$ is certainly not extraneous, namely the factors of $|B'|$, not appearing as factor in any of the leading coefficients of polynomials in G. In this case all, except $a-b-c$, are certainly not extraneous. Checking whether $a-b-c$ is extraneous or not is left. It turns out out that this is an extraneous factor indeed.

In case I is radical or all the factors in the numerator of $|B|$ are simple, and the degree of the numerator of $|B|$ equals the maximum number of zeroes, we can conclude immedeately that the numerator of $|B|$ is the eliminant. This principle could be applied to example VII (Section 6).

6. Examples

In this section we will present some more examples. We made an implementation for ASIR[5] ([8]), which has a C-like programming language. All computations were done on a SUN Sparc10 with 32 Mb and timings are given excluding the time for garbage collection. Finally we make up a table of the timings for computing the Gröbner bases, constructing the Bézout matrix and evaluation of the determinant.

Note that ASIR uses fraction-free Gaussian elimination for computing determinants. For computing the Gröbner basis, the total degree reverse lexicographic ordering is used, and we only will specify the ordering between the variables.

Example I (C5) *The cyclic 5-roots system*

$$\begin{aligned} f_1 &= a+b+c+d+e \\ f_2 &= ab+bc+cd+de+ea \\ f_3 &= abc+bcd+cde+dea+eab \\ f_4 &= abcd+bcde+cdea+deab+eabc \\ g &= abcde-1 \end{aligned}$$

[5] ASIR is pretty good for computing Gröbner bases. For various examples we measured that Maple was a factor 50 or more slower.

We are going to eliminate a, b, c and d. We computed G, the reduced Gröbner basis w.r.t. the ordering $a > b > c > d$. All leading coefficients of the polynomials in G are 1. Indeed $|B|$ equals the eliminant in e:

$$\begin{aligned} |B| &= (e^2+3e+1)^2(e^4-4e^3+6e^2+e+1)^2 \\ &\quad (e^4+e^3+6e^2-4e+1)^2(e-1)^{10}(e^4+e^3+e^2+e+1)^{10} \end{aligned}$$

We used the monomial basis (the set of independent monomials following from G):

$$M = \{1, b, c, c^2, c^3, d, d^2, d^3, d^4, bc, bd, bd^2, bd^3, cd, cd^2, cd^3, c^2d, bcd\}.$$

The computation (including the computation of G) took about 4 seconds. We also computed the resultant with Dixon's method and got an answer in the same amount of time. There were some problems though: the matrix was singular (a 22×22 matrix with rank 20) and two extraneous factors appeared.

Example II (MC5) *Modified cyclic 5-roots system*

$$\begin{aligned} f_1 &= a+b+c+d+e \\ f_2 &= ab+bc+cd+de+ea \\ f_3 &= abc+bcd+cde+dea+eab \\ f_4 &= bcd+bcde+cdea+deab+eabc \\ g &= abcde-1 \end{aligned}$$

This system is used as a benchmark for Gröbner basis computations, and it is considered as much more difficult than the normal cyclic 5-roots system from the previous example. The computation took longer indeed: about 80 seconds. The matrix B is smaller (15×15), but with more complicated entries.

G, the reduced Gröbner basis w.r.t. the ordering $a > b > c > d$, gives us a different independent set of monomials:

$$M = \{1, b, c, c^2, c^3, d, d^2, d^3, d^4, bc, bd, bd^2, cd, cd^2, c^2d\}.$$

The leading coefficients of the polynomials in G are not all 1 anymore. The leading terms in G are the following:

$$\begin{gathered} a, (2e-1)c^3d, (2e-1)bc^2, e^2(2e-1)bd^3, (2e-1)c^2d^2, \\ b^2, e^4(2e-1)d^5, e(2e-1)cd^3, e^2(2e-1)c^4, (2e-1)bcd \end{gathered}$$

Hence, we expect rational polynomials in e as entries in B. This happens indeed and $|B'| = (2e-1)^{15}e^{35}|B|$. $|B|$ is a degree 64 polynomial in e. It turns out that $e = 0$ and $e = \frac{1}{2}$ cannot be extended to a common zero of $f_1, \ldots, f_4$ and g. So $(2e-1)^{15}e^{30}$ is an extraneous factor. In fact, $|B|$ was closer to the correct eliminant than $|B'|$ was: $|B|$ just contained e^5 in its denominator and the correct eliminant equals $e^5|B|$, or the numerator of $|B|$.

Example III (CAP) *Caprassa's system (not radical)*

$$\begin{aligned} f_1 &= y^2z+2xyt-2x-z \\ f_2 &= -x^3z+4xy^2z+4x^2yt+2y^3t+4x^2-10y^2+4xz-10yt+2 \\ f_3 &= 2yzt+xt^2-x-2z \\ g &= -xz^3+4yz^2t+4xzt^2+2yt^3+4xz+4z^2-10yt-10t^2+2 \end{aligned}$$

We used monomial ordering $x > y > z$ for computing the reduced Gröbner basis G. G gave the following set of 11 independent monomials:

$$M = \{1, x, y, y^2, y^3, z, z^2, z^3, z^4, xz, xz^2\}.$$

The leading terms of the polynomials in G are:

$$t^2(3t^2+1)y^4, (t^2-1)xz^3, t(3t^2+1)xy, tyz, z^5, (3t^2+1)x^2$$

The 11×11 matrix B contains rational polynomials in t, but the determinant of B equals the generator of the elimination ideal (not the eliminant in t because the multiplicity of the factors is different), suprisingly:

$$|B| = 322486272(t-1)(t+1)(t^2+1)(t^4-10t^2+1)(3t^2+1)^4(t^2+3)^8.$$

The computation took 1 second. We have $|B'| = |B|\ t^2(t^2-1)^7(3t^2+1)^9$, with t^2 an extraneous factor.

Remark w.r.t. multiplicities: $t+1$ and $t-1$ have both multiplicity 9, t^2+1 has 1, $3t^2+1$ and t^2+3 both 4, and t^4-10t^2+1 just 1. So the total number of zeroes, counting multiplicity, is 40. The multiplicities do not coincide with the multiplicities in $|B'|$. Moreover $K[x,y,z,t]/\langle f_1, f_2, f_3, g\rangle$ has dimension 56. The difference is caused by the fact that the ideal $I = \langle f_1, f_2, f_3\rangle$ over $K(t)[x,y,z]$ is not radical.

Example IV (FC7) *Obtained from the cyclic 7-roots system*

$$\begin{aligned}
f_1 &= a^2bc + ab^2c + abc^2 + abc + ab + ac + bc \\
f_2 &= a^2b^2c + ab^2c^2 + a^2bc + abc + bc + a + c \\
g &= a^2b^2c^2 + a^2b^2c + ab^2c + abc + ac + c + 1
\end{aligned}$$

We used the monomial ordering $a > b$. The reduced Gröbner basis gives the independent set of monomials $M = \{1, a, b, ab, b^2, b^3\}$. The leading terms of the polynomials in G are:

$$c(c-1)a^2, (2c+1)ab^2, c^2(c-1)(2c+1)b^4$$

We have

$$\begin{aligned}
|B| &= -\frac{1}{c^3(c-1)^2} \\
&\quad (c^2+5c+1)(c^{12}-12c^{11}+24c^{10}+4c^9-9c^8+27c^7 \\
&\quad -21c^6+27c^5-9c^4+4c^3+24c^2-12c+1)(c^6+c^5+c^4+c^3+c^2+c+1)
\end{aligned}$$

and $|B'| = c^5(2c+1)^6(c-1)^2|B|$. It turns out that the numerator of $|B|$ equals the eliminant in c. The factor $c^2(2c+1)^6$ is an extraneous factor. The total computation time was 1 second.

Example V (K4) *Katsura-4*

$$\begin{aligned}
f_1 &= 2x + 2y + 2z + 2t + u - 1 \\
f_2 &= xy + 2yz + 2zt + 2tu - t \\
f_3 &= 2xz + 2yt + t^2 + 2zu - z \\
f_4 &= 2xt + 2zt + 2yu - y \\
g &= 2x^2 + 2y^2 + 2z^2 + 2t^2 + u^2 - u
\end{aligned}$$

We used the monomial ordering $x > y > z > t$. The reduced Gröbner basis gives the independent set of monomials $M = \{1, y, z, z^2, t, t^2, t^3, zt\}$. The leading coefficients of the polynomials in G are all 1, so the matrices B and B' are equal.

$$\begin{aligned} |B| &= \frac{1}{512}(u-1)(2u-1)(3u-1)(7u^2-6u+1) \\ &\quad (897597140u^{10} - 4566250648u^9 + 10328439732u^8 \\ &\quad -13667431652u^7 + 11705231857u^6 - 6770873896u^5 \\ &\quad +2675055189u^4 - 711551700u^3 + 121717599u^2 - 12065320u + 525075) \end{aligned}$$

$|B|$ is equals the eliminant. Total computation time was less than 1 second.

Example VI (ES) *Due to E.R. Speer*

$$\begin{aligned} f_1 &= (4 - 6x_1 + 2x_2 + 2x_3 + 2x_4)(x_1^2 + x_2^2 + x_3^2 + x_4^2) - x_2x_3x_4 + x_2 + x_4 \\ f_2 &= (4 + 2x_1 - 6x_2 + 2x_3 + 2x_4)(x_1^2 + x_2^2 + x_3^2 + x_4^2) - x_1x_3x_4 + x_1 + x_3 \\ f_3 &= (4 + 2x_1 + 2x_2 - 6x_3 + 2x_4)(x_1^2 + x_2^2 + x_3^2 + x_4^2) - x_1x_2x_4 + x_2 + x_4 \\ g &= (4 + 2x_1 + 2x_2 + 2x_3 - 6x_4)(x_1^2 + x_2^2 + x_3^2 + x_4^2) - x_1x_2x_3 + x_1 + x_3 \end{aligned}$$

Our aim is to find the eliminant in x_4. We used the monomial ordering $x_1 > x_2 > x_3$. The reduced Gröbner basis G gives the independent set of monomials

$$M = \{1, x_1, x_1^2, x_2, x_2^2, x_3, x_3^2, x_3^3, x_3^4, x_1x_2x_3, x_2x_3, x_2x_3^2, x_1x_3, x_1x_3^2, x_1x_2\}.$$

The leading terms of the polynomials in G are:

$$\begin{gathered} x_4x_2^2x_3,\ x_4x_1^2x_2,\ x_4x_1^3,\ x_4x_1^2x_3,\ x_4^2x_1x_3^3, \\ x_4^3x_3^5,\ x_4^2x_2x_3^3,\ x_4^2x_1x_2x_3^2,\ x_4x_1x_2^2,\ x_4x_2^3 \end{gathered}$$

Remarkable is the fact that all the leading coefficients of the polynomials in G contain the factor x_4. So the matrix B contains rational polynomials in x_4 where the denominator is some power of x_4. It turns out that $|B'|$ is a factor x_4^{45} times $|B|$.

$$\begin{aligned} |B| &= \frac{-1}{227864434916783554 56\, x_4^{11}} \\ &\quad (x_4^2 - 2x_4 + 2)(x_4^2 + 2x_4 + 2)(11x_4^2 - 11x_4 + 6) \\ &\quad (184900x_4^8 + 104920x_4^7 - 121192x_4^6 + 777968x_4^5 \\ &\quad -4636676x_4^4 + 3575172x_4^3 + 5573487x_4^2 - 32261832x_4 + 36639441) \\ &\quad (x_4^2 - 16x_4 - 2)(215x_4^4 - 32x_4^3 + 96x_4^2 + 160x_4 + 128)^2 \\ &\quad (144x_4^4 - 96x_4^3 + 41x_4^2 + 96x_4 + 144)^2 \\ &\quad (264x_4^4 - 264x_4^3 + 95x_4^2 + 528x_4 + 1056)^2 \end{aligned}$$

Computation time was 56 seconds. $x_4 = 0$ can be extended to a solution of the system, so the numerator of $|B|$ did not contain all the factors of the resultant.

Example VII (AU) *Due to A.Y. Uteshev*

$$\begin{aligned} f_1 &= x^2 + xy + y^2 - 2xz - 4yz + 3z^2 + t(-3x + 2y + t) - 3x - 2y + 3z - 2t - 2 \\ f_2 &= 2x^2 - xy + y^2 - xz - yz - 6z^2 + t(-x + y - 5z - 3t) - 5x + y + 5z + 2t + 5 \\ f_3 &= xyz - x^2z - 3 - 2zt - 3xt - 5xz^2 + xt^2 + x^3 + y^3 - 3z^3 + 2t^3 - 3t^2 - 5z^2t \\ &\quad +7yz^2 + xyt - 5y^2z + 2z^2 - 2t + x^2 - x - y^2 + 11z - 3xy + y + 2xz \end{aligned}$$

$$
\begin{aligned}
g \;=\; & -4xyz - x^2z - 15 - zt + 5xz^2 + 11xt^2 - 7y^2t - 12xy^2 \\
& +2yt + 6x^2y - xzt - x^3 + 6y^3 + 15z^3 + 4t^3 + 5t^2 + 4yz^2 \\
& +6xyt + 6y^2z - z^2 - 10t + 3x^2 - 35x + 2y^2 + 4z + 2xy - 14y
\end{aligned}
$$

Using the ordering $x > y > z$ gives the independent set of monomials

$$M = \{1, x, y, y^2, z, z^2, z^3, xz, xz^2, yz, yz^2\}.$$

The leading terms in the Gröbner basis are:

$$(85t + 137)yz^3, (85t + 137)z^4, y^3, x^2, xy, y^2z, xz^3$$

We have

$$
\begin{aligned}
|B| &= \frac{1}{272097792\,(85t + 137)^3}\, t(t-1)(t-2)T(t) \\
|B'| &= \frac{1}{272097792}\,(85t + 137)^{14} t(t-1)(t-2)T(t)
\end{aligned}
$$

where $T(t)$ is an irreducible polynomial of degree 33 in t with coefficients that are around 55 digits long.

We can immediately conclude that the eliminant equals the numerator of $|B|$, because the numerator has degree 36, which is the maximal number of zeroes. Indeed $t = \frac{-137}{85}$ is not extendible to a common solution of f_1, f_2, f_3 and g. The total time needed for the computations was 27 seconds.

Example VIII (DW) *Due to D. Wang*

$$
\begin{aligned}
f_1 &= u^2 - 2xu + v^2 - 2yv + x^2 + y^2 - 1 \\
f_2 &= v^2 - u^3 \\
g &= -3u^2v + 3yu^2 - 2vu + 2xv
\end{aligned}
$$

We want to eliminate u and v. The degrees of f_1 and f_2 are respectively 2 and 3. We can choose M to be the set of monomials not divisible by v^2 or by u^3: $M = \{1, u, v, u^2, uv, u^2v\}$. Hence we have a 6×6 Bézout matrix. The determinant of the matrix equals

$$
\begin{gathered}
-(x^2 + y^2 - 1)^3 \\
(729y^6 - 1458y^4x^3 + 729y^4x^2 - 4158y^4x - 1685y^4 \\
+729y^2x^6 - 1458y^2x^5 - 2619y^2x^4 - 4892y^2x^3 \\
-297y^2x^2 + 5814y^2x + 427y^2 + 729x^8 + 216x^7 - 2900x^6 \\
-2376x^5 + 3870x^4 + 4072x^3 - 1188x^2 - 1656x + 529).
\end{gathered}
$$

It turned out that this is the eliminant and is exactly equal to the generator of $\langle f_1, f_2, g\rangle \cap \mathbb{Q}(x)[y]$. Computation time was 0.5 seconds.

Example IX (CH) *Implicitization problem due to C.M. Hoffmann*

$$
\begin{aligned}
f_1 \;=\; & t^3(-85s^3 - 55s^2 - 37s - 35) + t^2(97s^3 + 50s^2 + 79s + 56) \\
& +t(49s^3 + 63s^2 + 57s - 59) + 45s^3 - 8s^2 - 93s + 92 \\
& -x(t^3(-53s^3 + 85s^2 + 49s + 78) + t^2(17s^3 + 72s^2 - 99s - 85) \\
& +t(-86s^3 + 30s^2 + 80s + 72) + 66s^3 - 29s^2 - 91s - 53)
\end{aligned}
$$

$$\begin{aligned}
f_2 &= t^3(43s^3 - 62s^2 + 77s + 66) + t^2(54s^3 - 5s^2 + 99s - 61)\\
&\quad +t(-50s^3 - 12s^2 - 18s + 31) - 26s^3 - 62s^2 + s - 47\\
&\quad -y(t^3(-53s^3 + 85s^2 + 49s + 78) + t^2(17s^3 + 72s^2 - 99s - 85)\\
&\quad +t(-86s^3 + 30s^2 + 80s + 72) + 66s^3 - 29s^2 - 91s - 53)\\
g &= t^3(-91s^3 - 47s^2 - 61s + 41) + t^2(-58s^3 - 90s^2 + 53s - 1)\\
&\quad +t(94s^3 + 83s^2 - 86s + 23) - 84s^3 + 19s^2 - 50s + 88\\
&\quad -z(t^3(-53s^3 + 85s^2 + 49s + 78) + t^2(17s^3 + 72s^2 - 99s - 85)\\
&\quad +t(-86s^3 + 30s^2 + 80s + 72) + 66s^3 - 29s^2 - 91s - 53)
\end{aligned}$$

We want to eliminate s and t. We succeeded to construct the 18×18 Bézout matrix in about 15 minutes. It contains polynomials in x, y and z with up to 150-digit integer coefficients. We did not succeed computing the determinant. This could be possible with for instance a combination of modular and interpolation techniques.

Example X (C6) *The cyclic 6-roots system*

$$\begin{aligned}
f_1 &= x_1 + x_2 + x_3 + x_4 + x_5 + x_6\\
f_2 &= x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_6 + x_6x_1\\
f_3 &= x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_5 + x_4x_5x_6 + x_5x_6x_1 + x_6x_1x_2\\
f_4 &= x_1x_2x_3x_4 + x_2x_3x_4x_5 + x_3x_4x_5x_6 + x_4x_5x_6x_1 + x_5x_6x_1x_2\\
&\quad +x_6x_1x_2x_3\\
f_5 &= x_1x_2x_3x_4x_5 + x_2x_3x_4x_5x_6 + x_3x_4x_5x_6x_1 + x_4x_5x_6x_1x_2\\
&\quad +x_5x_6x_1x_2x_3 + x_6x_1x_2x_3x_4\\
g &= x_1x_2x_3x_4x_5x_6 - 1
\end{aligned}$$

We want to eliminate $x_1, \ldots, x_5$. We found that $I = \langle f_1, \ldots, f_5\rangle$ is not a zero-dimensional ideal in $K(x_6)[x_1, \ldots, x_5]$. The Poisson product (equation 1.1) is an infinte product. However, there is a way out. There are only finitely many zeroes who really contribute to the Poisson product. All solutions with $x_1x_2x_3x_4x_5 = 0$ do not contribute, because for these $g = 1$. It turns out that there are only finitely many solutions where $x_1x_2x_3x_4x_5 \neq 0$.

We constructed a Bézout matrix as follows. Initially, let M be $\{1\}$. First, we computed the normal form of g. The monomials appearing in this normal form, which are not in M, are added to M. Then another monomial m from M is taken and used to compute the normal form of mg. Monomials appearing in this normal form, which are not in M, are added to M etc. This procedure terminated with M containing 53 elements.

In about 26 minutes the whole computation was done and the correct eliminant in x_6 is found (all leading coefficients in the Gröbner basis are 1, so we do not have extraneous factors):

$$\begin{aligned}
|B| &= (x_6^2 + 4x_6 + 1)^2(x_6^2 - 4x_6 + 1)^2\\
&\quad (x_6^8 + 6x_6^7 + 16x_6^6 + 24x_6^5 + 27x_6^4 + 24x_6^3 + 16x_6^2 + 6x_6 + 1)^2\\
&\quad (x_6^4 - 4x_6^3 + 15x_6^2 - 4x_6 + 1)^2(x_6^4 + 4x_6^3 + 15x_6^2 + 4x_6 + 1)^2\\
&\quad (x_6^8 - 6x_6^7 + 16x_6^6 - 24x_6^5 + 27x_6^4 - 24x_6^3 + 16x_6^2 - 6x_6 + 1)^2\\
&\quad (x_6^8 + 4x_6^6 - 6x_6^4 + 4x_6^2 + 1)^2(x_6^2 + 1)^6(x_6^4 - x_6^2 + 1)^6
\end{aligned}$$

$$(x_6-1)^8(x_6+1)^8(x_6^2+x_6+1)^8(x_6^2-x_6+1)^8$$

If we interchange g with, for instance, f_5 we do not have problems with non-zero dimensionality of I. However, the Gröbner basis contains polynomials in x_6 in its leading coefficients and we get a more complicated Bézout matrix (although smaller, 36×36) together with extraneous factors. The computation time increased to more than 9 hours. We might be able to reduce the computation time drastically by using interpolation or modular techniques. However, the extraneous factor is really huge (degree 716 in x_6):

$$(2158660x_6^{18} - 2597367x_6^{12} + 83649x_6^6 + 36072)^{36}x_6^{68}.$$

Example XI (C7) *The cyclic 7-roots system*

We consider the cyclic 7-roots system in the indeterminants $x_1, \ldots, x_7$ and choose g to be $x_1x_2x_3x_4x_5x_6x_7 - 1$. As for the cyclic 6-roots system, the ideal I is not zero-dimensional. The alternative procedure to construct a finite M works however. We get a 272×272 Bézout matrix. The elements in the Gröbner basis all have 1 as leading coefficient, so we do not have extraneous factors in the final result.

Example XII (K6) *Katsura-6*

This is a system of 7 equations (in 7 variables), one of them is of degree 1, the others are of degree 2. We want to eliminate 6 variables.

We get a 32×32 Bézout matrix. The computation of the determinant took quite long: 35 minutes. The result is a polynomial of degree 64.

Example XIII (K7) *Katsura-7*

This is a system of 8 equations (in 8 variables), one of them is of degree 1, the others are of degree 2. We want to eliminate 7 variables.

We get a 64×64 Bézout matrix with low degree polynomials (however with large integer coefficients) as entries. We tried to compute the determinant, but we gave up after computing 40 hours. We know that the result is a polynomial of degree 128 or less (the leading coefficients of polynomials in G are all 1). So for an interpolation algorithm we need at least 129 values. This will not be too easy too. We could evaluate the determinant, substituting for the indeterminant an integer, in about 5 minutes (the result for the integer 5 was an integer with 1200 digits)! So the interpolation algorithm will take at least about 11 hours. It might be that a combination with modular techniques helps.

Example XIV (K8) *Katsura-8*

This is a system of 9 equations (in 9 variables), one of them is of degree 1, the others are of degree 2. We want to eliminate 8 variables. We get a 128 Bézout matrix which construction took about half an hour. Computing the determinant modulo a prime took almost half an hour. The result is a degree 256 polynomial.

Example XV (K9) *Katsura-9*

This is a system of 10 equations (in 10 variables), one of them is of degree 1, the others are of degree 2. We want to eliminate 9 variables. We get a 256×256 Bézout matrix which construction took almost 5 hours. Computing the determinant modulo a prime took almost 7 hours. The result is a degree 512 polynomial.

Timings summarized

We summarize the computation times (in seconds) in the following table. The sign ∞ means that the computation took more than one day or the computation did not finish because of memory exhaustion.

	I (G)	III (B)	III ($\|B'\|$)	IV ($\|B'\|$)	$\#M$	V (GB)	VI (GB)
I (C5)	0.33	2.13	2.19	2.47(17.7)	18	1.59	2.05
II (MC5)	1.26	9.12	69.1	5.55(57.4)	15	9.67	554
III (CAP)	0.17	0.36	0.35	0.25(0.98)	11	0.94	4.76
IV (FC7)	0.12	0.83	0.34	0.13(0.30)	6	0.84	5.15
V (K4)	0.16	0.38	0.30	0.03(0.20)	8	0.69	4.27
VI (ES)	0.52	2.40	52.8	1.92(39.4)	15	7.06	623
VII (AU)	0.31	1.86	25.1	0.52(11.3)	11	10.6	720
VIII (DW)	0.03	0.14	0.37	0.40(1.03)	6	0.16	56.5
IX (CH)	49.6	705	∞	∞	18	∞(2644)	∞
X (C6)	5.67	45.8	1478	151(7540)	53	27.3	185
XI (C7)	573	7248	∞	∞	272	∞(1414)	∞
XII (K6)	5.04	21.0	2120	7.50(469)	32	27.5	18663
XIII (K7)	43.3	136	∞	113	64	231	∞
XIV (K8)	365	1417	∞	1610	128	2193	∞
XV (K9)	3180	13066	∞	24911	256	∞	∞

The columns I, II and III are the timings for computing G, constructing the Bézout matrix and computing the determinant, respectively.

Column IV contains the time needed for evaluating the determinant modulo a prime. The time in parenthesis is the time for evaluating the determinant, using modular computations and lifting. These computations were done by SACLIB (SACLIB uses a list of lists as representation of a matrix, which might be quite inefficient for determinant computation).

Column $\#M$ is the number of rows and columns of the Bézout matrix. In column V the time for computing the Gröbner basis for all polynomials w.r.t. the total degree reverse lexicographic ordering on all variables (including parameters) is given (in paranthesis the computation time for a computation modulo a prime). This basis can be used to compute the generator of the elimination ideal with the FGLM algorithm ([10]). Column VI contains the time needed for a computation of a Gröbner basis w.r.t. a lexicographic ordering.

We can see that the computation of Gröbner basis G and the construction of the Bézout matrix do not contribute much to the total computation time. This can increase in case we did not use efficient techniques for computing the determinant. Computing the determinant seems to be the bottleneck of the computation. In the examples II, VI, VII and XII computing the determinant using modular computations and lifting is faster.

7. Efficiency, applicability and further research

The Bézout matrix has size bounded by $\prod_{i=1}^{n} d_i$ where $d_i = \deg(f_i)$. This is bounded by d^n, where d is a bound for the d_i's. Note that the size of the matrix in Dixon's method is bounded by $\binom{nd}{d}$, which is of order $d^n e^n/\sqrt{n}$. So the Bézout matrix has order, a factor $e^n/\sqrt{n}$ smaller. However, the Bézout matrix is more complex to construct. Using a Gröbner basis, we face an additional complexity, polynomial in d^n. Note that we just need *a* Gröbner basis. As far as we know, not much research is done in finding Gröbner bases, without specifying the monomial ordering, minimizing the computation time.

Note that the efficiency might depend on the choice of g. The most efficient computation for the Gröbner basis would be choosing g as the polynomial of highest degree. However, the Bézout matrix will be more complicated to construct for higher degree g.

Bézout's method applied to computing the u-resultant becomes more similar to the FGLM method ([10]). Further investigations are needed.

It is something for further research to investigate the performance of Bézout's method in comparison with the other multivariate resultant methods. It is possible that other methods are more efficient if modular techniques with lifting are used to compute the determinant, because in Bézout's method we are doing a larger part of the computation non-modular. In case we use interpolation techniques, Bézout's method has the advantage to use a small matrix.

Further research can be done on the original method of Bézout. In the original method, no Gröbner basis is needed. It would also be interesting to study whether the Bézout matrix has special properties, which can be useful for some applications or can be used for speed-ups.

This method is very suitable in case the solutions have to be found for systems where $f_1, \ldots, f_n$ are fixed and only g varies. However, we are not aware of any application for this.

Note that the method will not give singular matrices, if the resultant is non-zero. This is a serious problem of other multivariate resultant methods.

8. Conclusions

We presented the method of Bézout for computing the resultant of a set of multivariate polynomials. A modification, using a Gröbner basis of one polynomial fewer, seems to be attractive. In fact, we will not get singular matrices, which often happens in other resultant methods. Besides this we gain information about extraneous factors, i.e., we have a sufficient condition for any factor of the final result to be non-extraneous. Applying the method on a few examples learns that the construction of the matrix usually takes much less time than the computation of the determinant of the matrix. The actual performance of the method, in relation to other methods, still needs more attention.

References

1 É. Bézout (1779), *Théorie générale des Equations Algébriques*, Paris.
2 J.J. Sylvester (1840), *On a general method of determining by mere inspection the derivations from two equations of any degree*, Philosophical Magazine 16, 132-135.
3 A. Cayley (1847) *On the Theory of Elimination.*
4 F.S. Macaulay (1903), *On some Formulae in Elimination*, Proceedings of The London Mathematical Society, Vol. XXXV, 3-27.
5 A.L. Dixon (1908), *The eliminant of three quantics in two independent variables*, Proceedings of The London Mathematical Society, 6, 468-478.
6 B. Buchberger (1985), *Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory*, Multidimensional Systems Theory, D. Reidel Publishing Company, 184-232.
7 D. Kapur, Y.N. Lakshman (1992), *Elimination Methods: an Introduction*, Symbolic and Numerical Computation for Artificial Intelligence, B. Donald et. al., Academic Press.
8 M. Noro, T. Takeshima (1992), *Risa/Asir - A Computer Algebra System*, Proceedings ISSAC '92, 387-396.
9 T. Becker, V. Weispfenning (1993), *Gröbner Bases - A Computational Approach to Commutative Algebra*, Springer-Verlag.
10 J.C. Faugère, P. Gianni, D. Lazard, T. Mora, *Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering*, Journal of Symbolic Computation 16/4, 329-344.
11 I.Z. Emiris, A. Rege (1994), *Monomial Bases and Polynomial System Solving*, Proceedings ISSAC '94, 114-122.
12 D. Kapur, T. Saxena (1995), *Comparison of Various Multivariate Resultant Formulations*, Proceedings ISSAC '95, 187-194.