On the Bézout Construction of the Resultant

PIET BIKKER[†] and ALEXEI YU. UTESHEV[‡]

[†] Research Institute for Symbolic Computation A-4040, Linz, AUSTRIA, e-mail: pbikker@risc.uni-linz.ac.at

[‡] Faculty of Applied Mathematics, St.-Petersburg State University, Bibliotechnaja pl.2, Petrodvoretc, 198904, St.-Petersburg, RUSSIA, e-mail: irina@utesh.spb.su

Abstract This paper deals with some ideas of Bézout and his successors Poisson, Netto and Laurent for solving polynomial systems. We treat them from the determinantal and from the Gröbner basis point of view. This results in effective algorithms for constructing the multivariate resultant. Other problems of Elimination Theory are discussed: how to find an eliminant for a polynomial system, how to represent its zeros as the rational functions of the roots of this eliminant and how to separate zeros.

1 Introduction

Among the different methods for constructing the multivariate resultant for a polynomial system the one introduced by Bézout in 1779 [7] was the first in history. Although it is contained in some old textbooks in Algebra such as [20], [23], [28], recent studies have preferred to focus on the development of later approaches — such as Sylvester's, Cayley's, Macaulay's or Dixon's. Perhaps this is due to the fact that Bézout's investigation is not in the spirit of determinantal formalism — an ideology dominant since the middle of the nineteenth century. Hence the name of Étienne Bézout (1730–1783) is now mentioned only either with respect to the Bézoutiants [19] or to his famous theorem on the number of zeros of a polynomial system. However, nobody now knows how it was originally proved. Such a neglect of Classical Algebra heritage is not a sin of our times solely.[1] Even Macaulay declared in 1902 ([21], see footnote on page 6) that he had not read Bézout's book; at the same time he pointed out several fatal errors in Laurent's treatise [20] of the method (*ibid.*, see footnote on page 4).

To restore historical justice is not the aim of the present paper. A special investigation is needed to clarify the significance of Bézout's book. This paper aims to interpret some of the original ideas of Bézout and his successors into the language of today's mathematics; after that, they will appear to be not only compatible with some recent investigations in the theory but also promising from the computational point of view. The interpretation mentioned will be carried out in the two "official languages": the determinantal and the Gröbner basis.

[1] "The men of old are not remembered, and those who follow him will not be remembered by those who follow them" (Bible, Eccl. 1.11)

The paper is structured as follows. Section 2 is devoted to the Poisson recursive definition of the resultant for $L-$variate polynomials

$$f_1(X),\ldots,f_L(X) \text{ and } g(X) \quad (\deg\ f_j=n_j,\deg\ g=m), X=(x_1,\ldots,x_L).$$

Let us first expand $f_j(X)$ in decreasing powers of indeterminates:

$$f_j(X)\equiv f_{j,n_j}(X)+f_{j,n_j-1}(X)+\ldots+f_{j,0}.$$

Here $f_{j,k}(X)$ stands for the form of degree k. Provided that the $(L-1)$-variate resultant of the leading forms

$$\mathcal{A}_0:=\mathcal{R}_{x_1,\ldots,x_{L-1}}\left(f_{1,n_1}(x_1,\ldots,x_{L-1},1),\ldots,f_{L,n_L}(x_1,\ldots,x_{L-1},1)\right) \tag{1.1}$$

differs from zero, the number N^* of zeros Λ_j for the system

$$f_1(X)=0,\ldots,f_L(X)=0 \tag{1.2}$$

equals the Bézout bound $N:=n_1\ldots n_L$. Then the L-variate resultant is defined as

$$\mathcal{R}_X(f_1,\ldots,f_L,g):=\mathcal{A}_0^m\mathcal{R}_X^g(f_1,\ldots,f_L),\ \text{where}\ \mathcal{R}_X^g(f_1,\ldots,f_L):=g(\Lambda_1)\ldots g(\Lambda_{N^*}).$$

For the non-generic case, it may turn out that $N^*<N$. The first aim of the paper is a constructive computation of the expression $\mathcal{R}_X^g(f_1,\ldots,f_L)$.

In Section 3 we consider the univariate case. Briefly, the resultant of polynomials $f(x)$ and $g(x)$ equals the determinant of the matrix formed from the coefficients of the remainders obtained on dividing $x^jg(x)$, $(j=0,\ldots,\deg f-1)$ by $f(x)$. Although this case was elaborated in papers by Euler, Bézout, Cauchy and Cayley, we present a new proof for the representation of the $\gcd(f,g)$ which is based on the relationship between the minors of the matrix with the subresultants. Although these results are close to those presented in [3], [15], they are treated in a different way.

For the multivariate case considered in Sections 4 and 7, the division process is replaced by that of finding the normal form (or, in Bézout's version, the *reduction*) modulo the ideal $\mathcal{I}(f_1,\ldots,f_L)$. One has first to choose a set of power products $M=\{\mu_j(X)\}_{j=1}^{N^*}$ as a basis for the vector space $\mathbf{K}[X]/\mathcal{I}(f_1,\ldots,f_L)$, and then to find the normal form for $\mu_j(X)g(X)$:

$$\mu_j(X)g(X)+\mathcal{I}(f_1,\ldots,f_L)=b_{j1}\mu_1(X)+\ldots+b_{jN^*}\mu_{N^*}(X),\ \{b_{jk}\}_{j,k=1}^{N^*}\subset\mathbf{K}.$$

The basis M can be predicted via consideration of the leading forms $f_{jn_j}(X)$. For the generic case $N^*=N$, one may choose Bézout's set

$$M=\{x_1^{p_1}\cdots x_L^{p_L}\mid 0\le p_1<n_1,\ldots,0\le p_L<n_L\}.$$

The matrix formed from the coefficients b_{jk} will be referred to as the **Bézout matrix**. One has

$$\mathcal{R}_X^g(f_1,\ldots,f_L)=\det\left[b_{jk}\right]_{j,k=1}^{N^*}.$$

In Section 5, we present a constructive reduction algorithm. It consists of resolving a succession of linear systems with respect to the power products. We formulate some determinantal conditions for its performability.

It turns out that the key condition is that the number (1.1) does not vanish. In Section 6 we compare this approach with the method of Macaulay.

As mentioned above, Bézout did not use the determinantal formalism. [2] His approach was closer to that of using Gröbner bases. In Section 7 we investigate the Bézout method with the aid of the Gröbner basis construction for the ideal $\mathcal{I}(f_1, \ldots, f_L)$, and explore its links to some recent investigations [2], [12], [34]. Selection of the set M can be organized via analysis of the leading power products of the polynomials from a Gröbner basis. A problem appears if the structure of the Gröbner basis depends on the parameters involved. The concept of *suspicious factors* is introduced, i.e. polynomial expressions in the parameters, whose vanishing might influence the number of zeros for the system or the Gröbner basis construction.

Simultaneously, in Sections 5 and 7, we address some other problems of Elimination Theory. One of them is how to find an eliminant for the system (1.2), say in x_L:

$$\mathcal{X}_L(x_L) := \mathcal{R}^{f_L}_{x_1,\ldots,x_{L-1}}(f_1, \ldots, f_{L-1}).$$

Another problem is how to represent Λ_j as rational functions of the roots of $\mathcal{X}_L(x_L)$ (an analogue of the Shape Lemma from Gröbner basis theory). Of particular interest to Control Theory is the problem of how to find a linear representation of the resultant, i.e. polynomials $P_1, \ldots, P_L, Q$ providing the so-called identity of Bézout [5], [6]:

$$P_1(X)f_1(X) + \ldots + P_L(X)f_L(X) + Q(X)g(X) \equiv \mathcal{R}(f_1, \ldots, f_L, g).$$

These problems are illustrated with several examples. In Section 8 some well-known polynomial systems are analysed and computing times are given.

In Section 9 we put forward the possibility of using the Bézout method for the zero separation problem (for $\mathbf{K} = \mathbf{R}$). It turns out that by analysing the sign of minors of the appropriate Bézout matrices one can obtain the number of the real zeros for the system (1.2), and those satisfying the inequality $g(X) > 0$.

In Appendix I we outline Bézout's original reasoning, while in Appendix II we give a proof for an auxiliary result.

2 Poisson's definition of the resultant

Let $\mathbf{K}$ be an integral domain. Denote the quotient field of $\mathbf{K}$ by $Qt(\mathbf{K})$ and the algebraic closure of $\mathbf{K}$ by $\overline{\mathbf{K}}$. In order to establish a necessary and sufficient condition for the existence of a common zero for $f_1(X), \ldots, f_L(X)$ and $g(X)$ over $\overline{\mathbf{K}}$, we first recall the inductive definition of the resultant due to Poisson [23], [27].

For $L = 1$, if a polynomial $f(x) = a_0x^n + \ldots + a_n$ $(a_0 \neq 0)$ has the zeros $\lambda_1, \ldots, \lambda_n$, then $\mathcal{R}(f, g)$ is defined formally as a symmetric polynomial of these zeros, namely:

$$\mathcal{R}(f, g) = a_0^m g(\lambda_1) \ldots g(\lambda_n). \tag{2.1}$$

Its value is a polynomial in the coefficients of f and g, and practically can be found by any of the well-known methods, e.g., as the Sylvester determinant [1], [23].

[2] Although he invented his own method for computing the determinant.

Assuming that the resultant is already defined for any L polynomials in $L-1$ indeterminates, let us first define it for polynomials $f_1(X), \dots, f_L(X), g(X)$ in generic form, i.e., complete in all their terms and independent (parametric) coefficients. Here one should accept an important assumption. Expand $f_j(X)$ in decreasing powers of the indeterminates:

$$f_j(X) = f_{jn_j}(X) + f_{jn_j-1}(X) + \ldots + f_{j0} \quad (j = 1, \dots, L). \tag{2.2}$$

Here $f_{jk}(X)$ stands for the homogeneous polynomial (form) of degree k. Consider the leading forms $f_{jn_j}(X)$ in (2.2) and assume, for definiteness, that they do not have a common non-trivial zero with $x_L = 0$. Based on the inductive hypothesis, we may introduce the resultant

$$\mathcal{A}_0 := \mathcal{R}(f_{1n_1}(x_1, \dots, x_{L-1}, 1), \dots, f_{Ln_L}(x_1, \dots, x_{L-1}, 1)). \tag{2.3}$$

For generic polynomials, it can be proved that $\mathcal{A}_0 \neq 0$, and under this condition the system of equations

$$f_1(X) = 0, \dots, f_L(X) = 0 \tag{2.4}$$

has exactly

$$N := n_1 \dots n_L \tag{2.5}$$

zeros $X = \Lambda_j := (\lambda_{j1}, \dots, \lambda_{jL}) \in \overline{\mathbf{K}}^L$ counted with their multiplicities (celebrated Bézout's theorem). The proof of this fact is carried out by constructing the **eliminant** for the system (2.4) with respect to x_L, i.e. the resultant of the polynomials $f_1, \dots, f_L$ considered as polynomials in $x_1, \dots, x_{L-1}$. (Because of the inductive hypothesis, this construction is allowed). The eliminant turns out to be a polynomial in a single indeterminate:

$$\mathcal{X}_L(x_L) := \mathcal{A}_0 x_L^N + \ \textit{lower order terms} \tag{2.6}$$

with the coefficients polynomially dependent on those of $f_1, \dots, f_L$. The roots λ_{jL} of $\mathcal{X}_L$ give the L-th components of the zeros Λ_j of the system (2.4). Furthermore, there exist polynomials $P_1(X), \dots, P_L(X) \in \mathbf{K}[X]$, $\deg P_j \le N - n_j$, satisfying the following equality

$$P_1(X) f_1(X) + \ldots + P_L(X) f_L(X) \equiv \mathcal{X}_L(x_L) \tag{2.7}$$

(known also as the **Bézout identity**).

Definition. The function $\Phi(X_1, X_2, \dots, X_\ell) : \overline{\mathbf{K}}^{\ell L} \to \overline{\mathbf{K}}$ with $X_1, X_2, \dots, X_\ell \in \overline{\mathbf{K}}^L$ is called a *symmetric function* of the ℓ vectors of indeterminates if its value does not change under any permutation of these vectors:

$$\Phi(X_1, X_2, \dots, X_\ell) \equiv \Phi(X_{j_1}, X_{j_2}, \dots, X_{j_\ell})$$

for distinct $j_1, \dots, j_\ell$.

Theorem 2.1 (Schläfli [27]) [3] *If $\mathcal{A}_0 \neq 0$, then the value of any symmetric polynomial of the N vectors of indeterminates on the zeros $\Lambda_1, \dots, \Lambda_N$ of the system* (2.4) *is a rational function in the coefficients of $f_1, \dots, f_L$.*

[3] An idea of Schläfli's proof can also be found in [32].

Now the resultant of the polynomials $f_1, \dots, f_L, g$ is defined by

$$\mathcal{R}(f_1(X), \dots, f_L(X), g(X)) := \mathcal{A}_0^m \, g(\Lambda_1) \dots g(\Lambda_N). \tag{2.8}$$

Thus, under assumption $\mathcal{A}_0 \neq 0$, the condition

$$\mathcal{R}(f_1, \dots, f_L, g) = 0$$

is necessary and sufficient for $f_1, \dots, f_L$ and g to have a common zero.

Since the right-hand side of (2.8) is a symmetric polynomial in the zeros Λ_j, it follows that, by Theorem 2.1, $\mathcal{R}(f_1, \dots, f_L, g)$ can be represented as a rational function in the coefficients of $f_1, \dots, f_L, g$. Moreover, by the choice of a factor $\mathcal{A}_0^m$, it becomes a polynomial in these coefficients. Therefore $\mathcal{R}(f_1, \dots, f_L, g) \in \mathbf{K}$. In the generic case this polynomial over $\mathbf{K}$ is irreducible over $\mathbf{K}$. Some other properties of the resultant can be established, in particular that $\mathcal{R}(f_1, \dots, f_L, g)$ is independent (up to its sign) of the order of its arguments, and that there exist polynomials $P_1(X), \dots, P_L(X), Q(X)$ from $\mathbf{K}[X]$ providing the following equality

$$P_1(X) f_1(X) + \dots + P_L(X) f_L(X) + Q(X) g(X) \equiv \mathcal{R}(f_1, \dots, f_L, g). \tag{2.9}$$

This completes the inductive definition of the resultant. In order to handle the non-generic case (where the resultant (2.3) might vanish), let us modify the definition above assuming that system (2.4) has a finite number $N^* \leq N$ of zeros $\Lambda_1, \dots, \Lambda_{N^*}$ (counted with their multiplicities). We take

$$\mathcal{R}_X^g(f_1, \dots, f_L) := g(\Lambda_1) \dots g(\Lambda_{N^*}) \tag{2.10}$$

and will refer to it as the **Poisson product**. So, in the generic case this object differs from the canonical resultant (2.8) by the factor $\mathcal{A}_0^m$, and expression (2.10) is a rational function in the coefficients of $f_1, \dots, f_L, g$. Thus $\mathcal{R}_X^g \in Qt(\mathbf{K})$ (the quotient field of $\mathbf{K}$). In the non-generic case, we can no longer use Theorem 2.1, since $\mathcal{A}_0 = 0$. It can be proved, however, (see Section 7) that the statement $\mathcal{R}_X^g \in Qt(\mathbf{K})$ remains valid, and thus, expression (2.10) can be considered as a generalization of (2.8).

An obstacle appears when we want to use (2.10) for the constructive computation of an eliminant. Imagine the following situation: one has to construct the eliminant in z for the polynomials $f_1(x, y, z)$, $f_2(x, y, z)$, $g(x, y, z)$. In case $\mathcal{A}_0 = \mathcal{R}(f_{1n_1}(z_1, 1, 0), f_{2n_2}(z_1, 1, 0)) \neq 0$, the number of zeros for the system $f_1 = 0$, $f_2 = 0$ considered with respect to indeterminates x, y equals to $N = n_1 n_2$ and, therefore, is independent of z. This is not the case if $\mathcal{A}_0 = 0$. It may happen that the number N^* of zeros depends on z. In terms of the definition above (2.10) this means: $\mathcal{R}_{x,y}^g(f_1, f_2)$ might be a rational function in z, so some particular (critical) values of z annihilate the denominator.

We leave aside some exceptional cases such as when the system (2.4) is inconsistent ($N^* = 0$), or has an infinite number of zeros (the eliminant in a particular indeterminate may still exist). Neither will we discuss the case when the forms $f_{jn_j}(X)$ have a common zero with, say, $x_L = 0$, and one has to find the eliminant in this indeterminate: if one wants to find the eliminant in y for the system $f_1(x, y) = xy - 1$, $f_2(x, y) = x^2 y + x - 2$ one has to take care of the case $y = 0$ when degrees of both polynomials decrease.

In Sections 4 and 5 we will deal mainly with the generic case $\mathcal{A}_0 \neq 0$, while the violation of this condition will be treated in Section 7.

3 The univariate case

For polynomials $f(x) = a_0x^n + \ldots + a_n, (a_0 \neq 0)$ and $g(x) = b_0x^m + \ldots + b_m, (b_0 \neq 0)$ let us find $g_k(x)$, i.e. the remainders of $x^k g(x)$ on division by $f(x)$ for $k = 0, 1, \ldots, n-1$:

$$g_k(x) = b_{k0}x^{n-1} + b_{k1}x^{n-2} + \ldots + b_{k,n-1}.$$

Coefficients of $g_k(x)$, for $k > 0$, can be obtained from those of $g_{k-1}(x)$ by the formulae

$$b_{kj} = b_{k-1,j+1} - b_{k-1,0}\frac{a_{j+1}}{a_0} \quad (j = 0, \ldots, n-1;\ b_{k-1,n} := 0). \tag{3.1}$$

Construct a matrix $\mathbf{B}$ from these coefficients:

$$\mathbf{B} = [b_{kj}]_{k,j=0}^{n-1} \tag{3.2}$$

and denote by $\mathbf{B}_j$ its j-th leading principal minor.

Theorem 3.1 *We have* **(1)**

$$\det \mathbf{B} = (-1)^{n(n-1)/2}\mathcal{R}(f,g)/a_0^m.$$

(2) *The degree of* $\gcd(f,g)$ *equals* D *iff* $\mathbf{B}_n = \mathbf{B}_{n-1} = \ldots = \mathbf{B}_{n-D+1} = 0,\ \mathbf{B}_{n-D} \neq 0$. *In this case,* $\gcd(f,g)$ *equals the determinant obtained from* $\mathbf{B}_{n-D}$ *on replacing its last column by*

$$\left[\sum_{j=n-D-1}^{n-1} b_{0j}x^{n-j-1}, \sum_{j=n-D-1}^{n-1} b_{1j}x^{n-j-1}, \ldots, \sum_{j=n-D-1}^{n-1} b_{n-D-1,j}x^{n-j-1}\right]^T$$

(here and elsewhere the superscript ^{T} *stands for transposition).*

(3) *For* $n > m$ *the polynomials* $p(x)$ *and* $q(x)$ *giving the linear representation of* $\gcd(f,g)$*:*

$$p(x)\,f(x) + q(x)\,g(x) \equiv \gcd(f,g) \tag{3.3}$$

can be obtained from $\mathbf{B}_{n-D}$ *by replacing its last column by*

$$[0, -p_0(x), \ldots, -p_{n-D-2}(x)]^T \quad \textit{and} \quad \left[1, x, \ldots, x^{n-D-1}\right]^T$$

respectively. Here $p_k(x) := (b_{00}x^k + b_{1,0}x^{k-1} + \ldots + b_{k,0})/a_0$.

Proof. The proof follows from the relation (that we show to exist) between $\mathbf{B}_{n-k}$ and the k-th subresultant of $\mathcal{R}(f,g)$ $(k \leq n)$:

$$a_0^{m-k}\mathbf{B}_{n-k} = \mathcal{R}_k := \begin{vmatrix} a_0 & a_1 & a_2 & \ldots & & & \ldots & a_{n+m-2k-1} \\ 0 & a_0 & a_1 & a_2 & \ldots & & \ldots & a_{n+m-2k-2} \\ & & & \ldots & & & & \ldots \\ 0 & \ldots & 0 & a_0 & a_1 & a_2 & \ldots & a_{n-k} \\ 0 & \ldots & 0 & 0 & b_0 & b_1 & \ldots & b_{m-k} \\ 0 & \ldots & 0 & b_0 & b_1 & \ldots & b_{m-k} & b_{m-k+1} \\ & & & \ldots & & & & \ldots \\ b_0 & b_1 & \ldots & & & & \ldots & b_{n+m-2k-1} \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m-k \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n-k \text{ rows} \end{matrix} \tag{3.4}$$

($a_j := 0$ for $j > n$; $b_k := 0$ for $k > m$; $\mathcal{R}_0 := (-1)^{n(n-1)/2}\mathcal{R}(f,g)$). We shall prove (3.4) for the particular case $m = n$. Multiply the determinant from the right-hand side of (3.4) from the left by

$$\begin{vmatrix} I_{n-k} & \mathbf{O} \\ B' & I_{n-k} \end{vmatrix} \text{ where } B' := -\frac{1}{a_0}\begin{pmatrix} 0 & 0 & \dots & 0 & b_0 \\ 0 & 0 & \dots & b_0 & b_{00} \\ \dots & & & & \dots \\ 0 & b_0 & \dots & b_{n-k-4,0} & b_{n-k-3,0} \\ b_0 & b_{00} & \dots & b_{n-k-3,0} & b_{n-k-2,0} \end{pmatrix}_{(n-k)\times(n-k)}$$

and I_{n-k} is the $(n-k)\times(n-k)$-identity matrix. By formulae (3.1), the result of this multiplication (which is equivalent to elementary linear operations applied to the rows of the subresultant) will be the determinant

$$\begin{vmatrix} a_0 & a_1 & a_2 & \dots & & & & \\ 0 & a_0 & a_1 & \dots & & & & \\ \dots & & & & & & & \\ 0 & \dots & a_0 & a_1 & a_2 & \dots & & \\ 0 & \dots & 0 & b_{00} & b_{0,1} & \dots & b_{0,n-k-1} \\ 0 & \dots & 0 & b_{1,0} & b_{1,1} & \dots & b_{1,n-k-1} \\ \dots & & \dots & \dots & & & \dots \\ 0 & \dots & 0 & b_{n-k-1,0} & b_{n-k-1,1} & \dots & b_{n-k-1,n-k-1} \end{vmatrix} = a_0^{n-k}\mathbf{B}_{n-k}$$

and so for this case ($m = n$) formula (3.4) is valid. The other statements of the theorem then follow from the properties of subresultants [1],[23]. To prove, for example, part (3), let us use the easily deduced formulae

$$x^k g(x) = p_{k-1}(x)f(x) + g_k(x), \quad (k = 0, \dots, n-D-1;\ p_{-1}(x) \equiv 0).$$

Multiply the k-th equality by the cofactor to the element of $\mathbf{B}_{n-D}$ standing in its last column and in the k-th row, and add these products. Using then the properties of the determinant expansion and expression for gcd from part (2), we arrive at the desired result. $\square$

Remark. There exists a direct relation of the above approach with the Bézoutiants [19]. Indeed, if instead of taking the remainder of $x^k g(x)$ on division by $f(x)$, one takes for $g_k(x)$ the remainder of $(a_0x^k + a_1x^{k-1} + \dots + a_k)g(x)$ on division by $f(x)$, then the coefficient matrix $\mathbf{B}$ turns out to be the Bézoutiant with $\det \mathbf{B} = \mathcal{R}(f,g)$. The Bézoutiant is a symmetric matrix.

4 The multivariate case

In presentation of the results we will follow [20] and [28]. We use the definition of the resultant given in Section 2 under assumption $\mathcal{A}_0 \neq 0$. Thus the number of common zeros Λ_j of $f_1, \dots, f_L$ equals $N = n_1 \cdots n_L$ (the n_j is the total degree of f_j). Consider the following set of N power products

$$M = \{\mu_k(X)\}_{k=1}^N = \{x_1^{p_1} \cdots x_L^{p_L} \mid 0 \le p_1 < n_1, \dots, 0 \le p_L < n_L\}. \tag{4.1}$$

We call a polynomial $h(X) \in \mathbf{K}[X]$ **reduced** with respect to M if it can be represented as a linear combination (with coefficients from $\mathbf{K}$) of power products from M. Bézout proved that for generic $f_1, \dots, f_L$, it is possible

to reduce any $h(X) \in \mathbf{K}[X]$ **modulo** $f_1, \ldots, f_L$, i.e., to find $\{a_1(X), \ldots, a_L(X)\} \subset \mathbf{K}[X]$ such that the polynomial

$$h_{red}(X) = h(X) - a_1(X)f_1(X) - \cdots - a_L(X)f_L(X)$$

will be reduced with respect to M. We will denote this fact

$$h(X) \to^{M}_{f_1,\ldots,f_L} h_{red}(X) \quad \text{or simply} \quad h(X) \to^{M} h_{red}(X).$$

Evidently, $h_{red}(\Lambda_j) = h(\Lambda_j)$ for $1 \le j \le N$. The reducibility problem will be discussed in subsequent sections, while in the present one we assume any reduction executable.

Reduce now the polynomials $\mu_k(X)\, g(X)$ with respect to M, and denote the result by $g_k(X)$:

$$\mu_k(X)g(X) = a_{k1}(X)f_1(X) + \ldots + a_{kL}(X)f_L(X) + g_k(X), \tag{4.2}$$

$$g_k(X) = b_{k1}\mu_1(X) + \ldots + b_{kN}\mu_N(X). \tag{4.3}$$

Substituting $X = \Lambda_j$ in (4.2) and (4.3), we obtain

$$b_{k1}\mu_1(\Lambda_j) + \ldots + b_{kN}\mu_N(\Lambda_j) = \mu_k(\Lambda_j)g(\Lambda_j). \tag{4.4}$$

Rewriting equalities (4.4) for $1 \le j, k \le N$ in matrix form gives

$$\mathbf{B}\, V = V \left(\begin{array}{ccc} g(\Lambda_1) & & \mathbf{O} \\ & \ddots & \\ \mathbf{O} & & g(\Lambda_N) \end{array} \right) \quad \text{where} \quad V = \left(\begin{array}{ccc} \mu_1(\Lambda_1) & \ldots & \mu_1(\Lambda_N) \\ \ldots & & \ldots \\ \mu_N(\Lambda_1) & \ldots & \mu_N(\Lambda_N) \end{array} \right) \tag{4.5}$$

is the generalized Vandermonde matrix; the $N \times N$ coefficient matrix

$$\mathbf{B} = [b_{kj}]_{k,j=1}^{N} \tag{4.6}$$

will be referred to as the **Bézout matrix**.

The problem of the non-singularity of the matrix V was discussed in [21]. It can be proved (see Section 9) that

$$(\det V)^2 = \Upsilon \mathcal{J}(\Lambda_1) \ldots \mathcal{J}(\Lambda_N) \tag{4.7}$$

where $\mathcal{J}$ stands for the Jacobian of $f_1, \ldots, f_L$ and

$$\Upsilon = \frac{\Omega}{\mathcal{A}_0^{n_1+\cdots+n_L-L+1}}. \tag{4.8}$$

Here Ω is a product of $\sum_{j=1}^{L} n_j - L$ polynomials in the coefficients of the leading forms (2.2) of $f_1, \ldots, f_L$. Thus, Υ is a rational function in these coefficients. In the next section we will detail the structure of Υ and show its relation to the reducibility problem. Obviously $(\det V)^2$ is a symmetric polynomial in the common zeros of $f_1, \ldots, f_L$, hence, by Theorem 2.1, the condition $(\det V)^2 = 0$ is algebraic with respect to the coefficients of $f_1, \ldots, f_L$.

As a preliminary result for the main theorem of this section, we need the following lemma [13] the proof of which one can find in Appendix II.

Lemma 4.1 *Let* $\mathbf{K}$ *be an integral domain containing an infinite number of elements and let* $\{F_1, F_2, H\} \subset \mathbf{K}[y_1, \ldots, y_s]$, $H \not\equiv 0$. *If* $F_1(y_1^*, \ldots, y_s^*) = F_2(y_1^*, \ldots, y_s^*)$ *at every point where* $H(y_1^*, \ldots, y_s^*) \ne 0$, *then* $F_1 \equiv F_2$.

Theorem 4.1 *We have*

(1) *The determinant of the Bézout matrix equals the Poisson product* (2.10)

$$\det \mathbf{B} = \mathcal{R}_X^g(f_1, \ldots, f_L).$$

(2) *If* $\det V \neq 0$ *, then* $\operatorname{rank} \mathbf{B}$ *equals the number of common zeros of* $f_1, \ldots, f_L$ *for which* $g \neq 0$.

(3) *There exist polynomials* $P_1, \ldots, P_L, Q$ *from* $\mathbf{K}[X]$ *giving the linear representation for* $\mathcal{R}_X^g$*:*

$$P_1(X)f_1(X) + \ldots + P_L(X)f_L(X) + Q(X)g(X) = \mathcal{R}_X^g. \tag{4.9}$$

Proof. If $\det V \neq 0$, then the statements (1) and (2) of the theorem follow from (4.5) (and from the fact that the rank of the matrix is unaltered by multiplying it by a non-singular square matrix). The equality $\det \mathbf{B} = \mathcal{R}_X^g(f_1, \ldots, f_L)$ is algebraic with respect to the coefficients of $f_1, \ldots, f_L$, g. Being proved under the assumption $\det V \neq 0$, it remains also valid for $(\det V)^2 = 0$ since the latter is also algebraic with respect to the coefficients of $f_1, \ldots, f_L$, and thus one can apply Lemma 4.1.

To obtain identity (4.9), one should use polynomials $a_{kj}(X)$ from representation (4.2). Let us take, for definiteness, $\mu_1 = 1$, and construct the corresponding matrix $\mathbf{B}$. Multiply equality (4.2) by the cofactor $\mathbf{B}_{k1}$ to the element b_{k1} of $\det \mathbf{B}$, and add these products by $k = 1, \ldots, N$:

$$Q(X) = \mathbf{B}_{11}\mu_1(X) + \ldots + \mathbf{B}_{N1}\mu_N(X), \tag{4.10}$$

$$P_j(X) = -\mathbf{B}_{11}a_{1j}(X) - \ldots - \mathbf{B}_{N1}a_{Nj}(X), \quad (j = 1, \ldots, L). \tag{4.11}$$

By the properties of the determinant expansion:

$$P_1(X)f_1(X) + \ldots + P_L(X)f_L(X) + Q(X)g(X) = \det \mathbf{B}.$$

Notice that the polynomial $Q(X)$ was obtained in a way similar to the polynomial $q(x)$ from Theorem 3.1: it equals the determinant of the matrix obtained from $\mathbf{B}$ by replacing its first column by the column of power products from the set (4.1). □

Rank Conjecture. The assertion (2) of Theorem 4.1 can be replaced by a more general one, namely: the deficiency index of matrix $\mathbf{B}$ (i.e. $N - \operatorname{rank} \mathbf{B}$) equals the number of common zeros of $f_1, \ldots, f_L$ at which g vanishes. If a common zero of (2.4) of multiplicity ℓ_1 is, at the same time, a zero for $g(X) = 0$ of multiplicity ℓ_2, it should be counted $\min(\ell_1, \ell_2)$ times.

The above conjecture is important for the problem of how to find the components of the common zeros of $f_1, \ldots, f_L$ and g in terms of the minors of the Bézout matrix. We will clarify this for the case where $\operatorname{rank} \mathbf{B} = N - 1$.

The Common-Zero-Finding Algorithm. Let $\operatorname{rank} \mathbf{B} = N - 1$ and $X = \Lambda$ be a single common zero. Substitute it in the equations (4.4), and consider the resulting linear homogeneous system

$$b_{k1}\mu_1(\Lambda) + \ldots + b_{kN}\mu_N(\Lambda) = 0, \quad (k = 1, \ldots, N) \tag{4.12}$$

with respect to $\mu_1(\Lambda), \ldots, \mu_N(\Lambda)$. Its rank equals to $N - 1$. Assume, for definiteness, that at least one of the cofactors $\mathbf{B}_{N1}, \ldots, \mathbf{B}_{NN}$ differs from zero. Every non-trivial solution to system (4.12) has to satisfy the ratios

$$\mathbf{B}_{N1} : \mathbf{B}_{N2} : \ldots : \mathbf{B}_{NN} = \mu_1(\Lambda) : \mu_2(\Lambda) : \ldots : \mu_N(\Lambda). \tag{4.13}$$

Assume now, for definiteness, that $\mathbf{B}_{N1} \neq 0$. Then for appropriate values of the index j the formulae

$$\mu_j(\Lambda) = \mathbf{B}_{Nj}/\mathbf{B}_{N1} \quad (j = 2, \ldots, N) \tag{4.14}$$

give the components of the common zero Λ as rational functions of the coefficients of the polynomials $f_1, \ldots, f_L$ and g. Formally, the equations (4.14) could be obtained via the application of Cramer's rule to the system (4.12) (neglecting the last equation, and transferring the first terms onto the right-hand sides). The algorithm can be evidently extended to the case where rank $\mathbf{B} < N - 1$ as will be shown in the examples of the following section.

5 Reducibility

We will discuss here the problem of reduction of a polynomial. Our approach is just a constructive version of the Bézout proof of the reducibility for the *generic case* (see Appendix I); we also provide conditions under which the reduction is possible (in Section 7 we will discuss the use of Gröbner basis for the reduction process). The Laurent treatment of the matter [20] is incorrect. In parallel, we will give some applications of the results from the previous section, in particular, we will consider the problem of how to find zeros of an algebraic system. We will begin with

5.1 The bivariate case

Example 5.1 *Find the Poisson product $\mathcal{R}^g_{x,y}(f_1, f_2)$ and its linear representation* (4.9) *for the polynomials*

$$f_1 := 5x^2 - 6xy + 5y^2 - 16, \;\; f_2 := 2x^2 - xy + y^2 - x - y - 4, \;\; g := x^2 - y + \varepsilon. \tag{5.1}$$

Here ε is a parameter.

Solution. Since $n_1 = n_2 = 2$, one has $M = \{1, x, y, xy\}$. To reduce the polynomials $g, x\,g, y\,g, xy\,g$ with respect to M it is sufficient to construct the reductions for the power products $x^2, y^2, x^3, x^2y, xy^2, x^3y$. To perform these, consider first the equations $f_1 = 0$, $f_2 = 0$ as a linear system with respect to x^2 and y^2. Resolving it, one obtains the identities:

$$x^2 = \left[-\frac{1}{5}f_1 + f_2\right] - \frac{1}{5}xy + x + y + \frac{4}{5}, \tag{5.2}$$

$$y^2 = \left[\frac{2}{5}f_1 - f_2\right] + \frac{7}{5}xy - x - y + \frac{12}{5}. \tag{5.3}$$

Multiplying then (5.2) by y, (5.3) by x, we obtain a linear system with respect to x^2y and xy^2. Resolving it and replacing afterwards x^2 and y^2 by (5.2) and (5.3), we find that

$$x^2y = \left[\frac{1}{32}(-2x - 5y + 9)f_1 + \frac{5}{32}(x + 5y - 4)f_2\right] + 2xy - x + 2, \tag{5.4}$$

$$xy^2 = \left[\frac{1}{32}(10x - 7y + 19)f_1 + \frac{5}{32}(-5x + 7y - 12)f_2\right] + 2xy - y + 2. \tag{5.5}$$

Multiplying now (5.2) by x , and substituting successively (5.4), and then (5.2) and (5.3), we obtain the expression for x^3:

$$x^3 = \left[\frac{1}{160}(-30x + 5y - 41)f_1 + \frac{1}{32}(31x - 5y + 36)f_2\right] + \frac{2}{5}xy + 2x + y + \frac{2}{5}. \tag{5.6}$$

Finally, multiply (5.6) by y, replace xy^2 by formulae (5.5), and then y^2 by (5.3) (the latter is not related to the multipliers of f_1 or f_2 containing y^2 !):

$$\begin{aligned} x^3y &= \left[\frac{1}{160}(5y^2 - 30xy + 20x - 55y + 102)f_1 \right.\\ &\quad \left. + \frac{1}{32}(-5y^2 + 31xy - 10x + 50y - 56)f_2\right] + \frac{21}{5}xy - x - y + \frac{16}{5}. \end{aligned}$$

Remark 1. If one multiplies (5.4) by x, replaces then x^2y by (5.4), and afterwards x^2 by (5.2) (the latter is not related to the multipliers of f_1 or f_2 containing x^2 !), one will obtain another formula:

$$\begin{aligned} x^3y &= \left[\frac{1}{160}(-10x^2 - 25xy + 25x - 50y + 122)f_1 \right.\\ &\quad \left. + \frac{1}{32}(5x^2 + 25xy - 10x + 50y - 72)f_2\right] + \frac{21}{5}xy - x - y + \frac{16}{5}. \end{aligned}$$

With the obtained formulae, we reduce $g, x\,g, y\,g, xy\,g$:

$$\begin{aligned} g &= \left[-\frac{1}{5}f_1 + f_2\right] - \frac{1}{5}xy + x + \left(\frac{4}{5} + \varepsilon\right), \\ x\,g &= \left[\frac{1}{160}(-30x + 5y - 41)f_1 + \frac{1}{32}(31x - 5y + 36)f_2\right] - \frac{3}{5}xy + (\varepsilon + 2)x + y + \frac{2}{5}, \\ y\,g &= \left[-\frac{1}{160}(10x + 25y + 19)f_1 + \frac{1}{32}(5x + 25y + 12)f_2\right] + \frac{3}{5}xy + (\varepsilon + 1)y - \frac{2}{5}, \\ xy\,g &= \left[\frac{1}{160}(5y^2 - 30xy - 30x - 20y + 7)f_1 \right.\\ &\quad \left. + \frac{1}{32}(-5y^2 + 31xy + 15x + 15y + 4)f_2\right] + \left(\varepsilon + \frac{11}{5}\right)xy - x + \frac{6}{5} \end{aligned} \tag{5.7}$$

and place the coefficients of power products $1, x, y, xy$ into matrix $\mathbf{B}$:

$$\mathcal{R}^g_{x,y}(f_1, f_2) = \det \mathbf{B} = \begin{vmatrix} (4/5 + \varepsilon) & 1 & 0 & -1/5 \\ 2/5 & (\varepsilon + 2) & 1 & -3/5 \\ -2/5 & 0 & (\varepsilon + 1) & 3/5 \\ 6/5 & -1 & 0 & (\varepsilon + 11/5) \end{vmatrix} = \varepsilon(\varepsilon + 2)^3. \tag{5.8}$$

Check: the system $f_1 = 0, f_2 = 0$ possesses the following zeros: $(-1, 1); (2, 2)$, and $(1, -1)$, the last one being of multiplicity 2; $\mathcal{R}^g_{x,y}(f_1, f_2) = g(-1, 1)g(2, 2)g(1, -1)^2 = \varepsilon(\varepsilon + 2)^3$.

Now to obtain identity (4.9), one should use the coefficients of f_1 and f_2 (polynomials in brackets) from (5.7). Applying the algorithm from the proof of part (3) of Theorem 4.1, multiply them by the corresponding cofactors of the $\det \mathbf{B}$

$$(\varepsilon + 2)(\varepsilon^2 + 16/5\varepsilon + 8/5); \ -(\varepsilon + 2)(\varepsilon + 1); \ (\varepsilon + 2); \ 1/5(\varepsilon + 2)(\varepsilon - 2)$$

and add these products. For simplicity, consider the case $\varepsilon = -1$:

$$\begin{aligned} P_1(x, y) &= \frac{1}{160}(3y^2 - 18xy - 8x + 13y + 4), \\ P_2(x, y) &= \frac{1}{160}(-15y^2 + 93xy + 20x - 80y + 48), \\ Q(x, y) &= \frac{1}{5}(-3xy + 5y - 3), \\ P_1 \cdot f_1 + P_2 \cdot f_2 + Q \cdot (x^2 - y - 1) &\equiv -1. \end{aligned}$$

(The set of polynomials P_1, P_2 and Q, satisfying the last equality is not unique (see Remark 1).)

Remark 2. This example also confirms the conjecture formulated on page 9: for $\varepsilon = 0$ one has rank $\mathbf{B} = 3$, and, indeed, the system $f_1 = 0, f_2 = 0$ has only one zero common with $g(x, y)$, namely $(-1, 1)$. As for the case $\varepsilon = -2$, here rank $\mathbf{B} = 2$, while $g(x, y)$ vanishes on the **three** zeros of $f_1 = 0, f_2 = 0$: $(2, 2); (1, -1); (1, -1)$. Explanation: zero $(1, -1)$ is of multiplicity $\ell_1 = 2$ for the system $f_1 = 0, f_2 = 0$, but of multiplicity $\ell_2 = 1$ for the polynomial $g(x, y)$. If one had taken $g = (x-1)(y+1)$ or $g = (x-1)^2 + (x-1)(y+1)$, the corresponding matrix $\mathbf{B}$ would have been:

$$\begin{pmatrix} -1 & 1 & -1 & 1 \\ 14/5 & -1 & 1 & 4/5 \\ -2/5 & 1 & -1 & 8/5 \\ 4 & -1 & 1 & 2 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 4/5 & 0 & 0 & 4/5 \\ 8/5 & 0 & 0 & 8/5 \\ 8/5 & 0 & 0 & 8/5 \\ 16/5 & 0 & 0 & 16/5 \end{pmatrix}$$

with the rank equal to 2 and 1 respectively. For both cases $(1, -1)$ is a double zero for $g(x, y)$, in the last case g vanishes also at $(-1, 1)$.

Let us finally illustrate the work of the Common-Zero-Finding Algorithm from Section 4. For $\varepsilon = 0$, one has rank $\mathbf{B} = 3$ and the formulae

$$x = \frac{\mathbf{B}_{4,2}}{\mathbf{B}_{4,1}} = \frac{(\varepsilon+2)(3\varepsilon+2)}{(\varepsilon+2)(\varepsilon-2)}, \quad y = \frac{\mathbf{B}_{4,3}}{\mathbf{B}_{4,1}} = -\frac{(\varepsilon+2)(3\varepsilon+2)}{(\varepsilon+2)(\varepsilon-2)}$$

give the true value of a single common zero. They fail for $\varepsilon = -2$, when rank $\mathbf{B} = 2$. For this case, one may deduce an additional relation between some of the power products from the set M. For example, the condition

$$\begin{vmatrix} (4/5+\varepsilon) & -1/5 \\ 2/5 & -3/5 \end{vmatrix} + x \begin{vmatrix} 1 & -1/5 \\ (\varepsilon+2) & -3/5 \end{vmatrix} + y \begin{vmatrix} 0 & -1/5 \\ 1 & -3/5 \end{vmatrix} = 0$$

remains valid for $\varepsilon = -2$ on all the common zeros of the polynomials. $\square$

Example 5.2 *Find the eliminant in z and evaluate zeros for the system*

$$\begin{aligned} f_1 &= x^2 + xy + y^2 - 2xz - 4yz + 3z^2 + x + 2y - z - 2 = 0, \\ f_2 &= 2x^2 - xy + y^2 - xz - yz - 6z^2 + 2x - y + z + 2 = 0, \\ g &= x^2 - 2xy - y^2 - 2xz + 2yz + 3z^2 + 2x + 3y - 3z - 1 = 0. \end{aligned} \tag{5.9}$$

Solution. We intend to eliminate x and y. The algorithm is similar to that of Example 5.1, though we now do not need to care about the polynomials in brackets. So, we sketch the process:

$$x^2 \to^M 2xy + (-z-1)x + (-3z+3)y + (9z^2 - 2z - 4), \tag{5.10}$$

$$y^2 \to^M -3xy + 3zx + (7z-5)y + (-12z^2 + 3z + 6). \tag{5.11}$$

Multiplying then (5.10) by y, (5.11) by x, we obtain a linear system with respect to x^2y and xy^2. Resolving it and replacing afterwards x^2 and y^2 by (5.10) and (5.11), we find that

$$\begin{aligned} x^2y \to^M & \frac{1}{7}\Big[(34z-20)xy + (-39z^2 + 9z + 12)x + (-30z^2 + 52z - 19)y \\ & +(90z^3 - 57z^2 - 33z + 18)\Big], \end{aligned} \tag{5.12}$$

$$\begin{aligned} xy^2 \to^M & \frac{1}{7}\Big[(-11z+25)xy + (12z^2 - 27z + 6)x + (27z^2 - 93z + 57)y \\ & +(-81z^3 + 129z^2 + 15z - 54)\Big]. \end{aligned} \tag{5.13}$$

Multiplying now (5.10) by x, and using (5.12), (5.10) and (5.11), we obtain the reduction of x^3. Similarly for y^3:

$$\begin{aligned} x^3 \quad &\to^M \quad \frac{1}{7}\Big[(33z-33)xy + (-8z^2+18z+3)x + (-39z^2+104z-59)y \\ &\qquad +(117z^3-163z^2-24z+64)\Big]; \qquad (5.14) \\ y^3 \quad &\to^M \quad \frac{1}{7}\Big[(-93z+30)xy + (111z^2-24z-18)x + (178z^2-190z+46)y \\ &\qquad +(-345z^3+180z^2+144z-48)\Big]. \qquad (5.15) \end{aligned}$$

To reduce x^3y : reduce $y\times(5.14)$ using (5.13) and (5.11). Similarly for xy^3. Finally x^2y^2: reduce $y\times(5.12)$ using (5.13) and (5.11).

With the obtained formulae, we first reduce $g, x\,g, y\,g, xy\,g$ and then place the coefficients of power products into the matrix $\mathbf{B}$:

$$\mathcal{R}^g_{x,y}(f_1,f_2) = \frac{-869814z^7+1156692z^6+399400z^5-1116418z^4+404610z^3+93852z^2-56816z-11506}{49}. \qquad (5.16)$$

The eliminant $\mathcal{Z}(z)$ differs from it by the factor

$$\mathcal{A}_0^2 = [\mathcal{R}(f_{1,2}(z_1,1,0), f_{2,2}(z_1,1,0))]^2 = 49.$$

The roots of (5.16) are the z-components of the zeros of (5.9):

$$z = \left\{1;\ 0.74136_{\pm 10^{-5}};\ -0.94428_{\pm 10^{-5}};\ -0.21498_{\pm 10^{-5}} \ \pm\ i\,0.05478_{\pm 10^{-5}};\ 0.48135_{\pm 10^{-5}} \ \pm\ i\,0.39011_{\pm 10^{-5}}\right\}.$$

The total number of zeros equals 7 and turns out to be less than the Bézout bound : $\deg f_1 \deg f_2 \deg g = 8$. This happens because the leading forms of the polynomials (5.9) have a (non-trivial) common zero $(0,3,1)$:

$$\mathcal{R}(f_{1,2}(z_1,z_2,1), f_{2,2}(z_1,z_2,1), g_2(z_1,z_2,1)) = 0. \qquad (5.17)$$

We can use the Common-Zero-Finding Algorithm to derive the x- and the y-components of the solutions. For this formulae (4.14) can be used. However, we must mention an important

Remark 3. Assume that the eliminant $\mathcal{X}_L(x_L)$ for the system (2.4) has no multiple zeros, which is equivalent to the statement that all the zeros of the system have distinct L-th components. Thus, one should expect that the denominator in (4.14) does not vanish on the roots of the eliminant. Therefore, the condition

$$\mathcal{R}(\mathcal{X}_L(x_L), \mathbf{B}_{N1}) \neq 0$$

has to be true. For the case $n=2$, Dr. E. Kalinina supplied us with the proof of the following equality

$$\mathcal{D}(\mathcal{Y}(y)) = (-1)^{Nn_1(n_1-1)/2}\frac{\mathcal{R}_{x,y}(f_1,f_2,\mathcal{J}(f_1,f_2))\ \mathcal{R}_y(\mathcal{Y}(y),\mathbf{B}_{N1})}{\mathcal{A}_0}.$$

Here $\mathcal{D}$ denotes the **discriminant**.

Formula (4.14) for our example gives

$$x = \frac{\mathbf{B}_{4,2}}{\mathbf{B}_{4,1}} = -\frac{13601z^4-34161z^3+17378z^2+1519z-517}{2277z^4-8581z^3+13522z^2-2995z-2043}$$

Substituting here the values of the roots of (5.16) we obtain the corresponding x-components:

$$x = \left\{1;\ -2.42809_{\pm 10^{-5}};\ -0.97093_{\pm 10^{-5}};\ -0.21886_{\pm 10^{-5}}\ \mp\ i\,0.65557_{\pm 10^{-5}};\ 0.56791_{\pm 10^{-5}}\ \pm\ i\,1.09756_{\pm 10^{-5}}\right\}.$$

The y-components are dealt with analogously:

$$y = \left\{0;\ -0.15702_{\pm 10^{-5}};\ 0.18176_{\pm 10^{-5}};\ 0.67565_{\pm 10^{-5}}\ \pm\ i\,0.33638_{\pm 10^{-5}};\ 1.28693_{\pm 10^{-5}}\ \mp\ i\,0.30635_{\pm 10^{-5}}\right\}.$$

$\square$

The Bivariate Reduction Algorithm for power products of fixed degrees can be performed by solving the succession of linear systems with the coefficients rationally dependent on those of the leading forms f_{1n_1} and f_{2n_2} of f_1 and f_2. The process can be formalized by the following diagram which is relative to the case $n_1 = n_2 = \delta$:

$$\begin{array}{c} f_1 = 0 \\ f_2 = 0 \end{array} \Longrightarrow \left\{ \begin{array}{c} x^\delta \\ y^\delta \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} x^\delta y \\ x y^\delta \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} x^\delta y^2 \\ x^2 y^\delta \end{array} \right\} \hookrightarrow \ldots \hookrightarrow \left\{ \begin{array}{c} x^\delta y^{\delta-1} \\ x^{\delta-1} y^\delta \end{array} \right\}$$

Here $\{\ \}$ means a linear system with respect to the power products included, while $\hookrightarrow$ is a multiplication of the reductions obtained on the previous step by y and x. If the power products of degree $\delta + k - 1$ are reducible and the linear system with respect to $x^\delta y^k, x^k y^\delta$ is consistent, then all power products of degree $\delta + k$ are reducible (with some of them just contained in M). Therefore, for total reducibility in the case $n_1 = n_2$ it is necessary and sufficient to have the n_1 conditions fulfilled.

As for the case $n_1 < n_2$, a modification of the reduction procedure will be illustrated via an example. Let $n_1 = 3,\ n_2 = 5$; so

$$M = \{1, x,\ y,\ x^2,\ xy,\ y^2,\ x^2y,\ xy^2,\ y^3, x^2y^2,\ xy^3,\ y^4,\ x^2y^3,\ xy^4,\ x^2y^4\}. \tag{5.18}$$

Let

$$f_1 := a_{30}x^3 + \underline{a_{21}x^2y} + \underline{a_{12}xy^2} + \underline{a_{03}y^3} + \ldots$$

Here dots and underlined summands mean that the terms are reducible with respect to M. If $a_{30} \ne 0$ then one can obtain the reduction for x^3 from the equation $f_1 = 0$:

$$x^3 \rightarrow^M A_{21}x^2y + A_{12}xy^2 + A_{03}y^3 + \ldots \tag{5.19}$$

Now all the power products of degree 3 are reducible with respect to M. Multiplying (5.19) by y, we can obtain the reduction

$$x^3y \rightarrow^M \underline{A_{21}x^2y^2} + \underline{A_{12}xy^3} + \underline{A_{03}y^4} + \ldots \tag{5.20}$$

since power products of the underlined terms are contained in M. Multiplying (5.19) by x and using (5.20), we obtain the reduction

$$x^4 \rightarrow^M \underline{C_{22}x^2y^2} + \underline{C_{13}xy^3} + \underline{C_{04}y^4} + \ldots \tag{5.21}$$

Now all the power products of degree 4 are reduced with respect to M.

Multiply (5.20) by y:

$$x^3y^2 \rightarrow^M \underline{A_{21}x^2y^3} + \underline{A_{12}xy^4} + A_{03}y^5 + \ldots \tag{5.22}$$

(The power product y^5 is not in M). Multiply (5.20) by x and substitute expression (5.22):

$$x^4y \to^M A_{21}x^3y^2 + \underline{A_{12}x^2y^3} + \underline{A_{03}xy^4} + \ldots \to^M \underline{G_{23}x^2y^3} + \underline{G_{14}xy^4} + G_{05}y^5 + \ldots \tag{5.23}$$

Multiply (5.21) by x and substitute expression (5.22):

$$x^5 \to^M C_{22}x^3y^2 + \underline{C_{13}x^2y^3} + \underline{C_{04}xy^4} + \ldots \to^M \underline{H_{23}x^2y^3} + \underline{H_{14}xy^4} + H_{05}y^5 + \ldots \tag{5.24}$$

Consider now the expansion for f_2:

$$f_2 := b_{50}x^5 + b_{41}x^4y + b_{32}x^3y^2 + \underline{b_{23}x^2y^3} + \underline{b_{14}xy^4} + b_{05}y^5 + \ldots$$

Consider the equation $f_2 = 0$ and replace the non-underlined expression with the help of formulae (5.24), (5.23) and (5.22). One obtains a linear relation connecting the power products x^2y^3, xy^4, y^5. If it is resolvable with respect to the last power product, then it is possible to obtain not only the reduction

$$y^5 \to^M \underline{L_{23}x^2y^3} + \underline{L_{14}xy^4} + \ldots \tag{5.25}$$

but also the reduction for any power product of degree 5, in particular (substituting (5.25) in (5.22)):

$$x^3y^2 \to^M \underline{M_{23}x^2y^3} + \underline{M_{14}xy^4} + \ldots \tag{5.26}$$

The next part of the algorithm is similar to the case $n_1 = n_2$. Multiply (5.25) by x, (5.26) by y:

$$xy^5 \to^M L_{23}x^3y^3 + \underline{L_{14}x^2y^4} + \ldots, x^3y^3 \to^M \underline{M_{23}x^2y^4} + M_{14}xy^5 + \ldots$$

If this system is resolvable with respect to xy^5 and x^3y^3, then any power product of degree 6 is reducible. One more step is needed to obtain the reductions for x^2y^5 and x^3y^4. If this is possible, then any power product of degree 7 is reducible. From these reduction formulae reductions for the power products of the higher degrees can be deduced (without any additional assumptions).

Thus, for the reducibility in the general case when $n_1 \le n_2$, the n_1 conditions have to be fulfilled (aside from the non-vanishing of the leading coefficient of f_1). This is not always the case:

Example 5.3 *Let*

$$f_1 = x^2 + xy + y^2 + \ldots = 0, \ f_2 = 5x^2 - 6xy + 5y^2 + \ldots = 0 \tag{5.27}$$

¿From (5.27), it is impossible to express x^2 and y^2 simultaneously. The situation can be saved by replacing (4.1) by $M_1 = \left\{1, x, y, y^2\right\}$. Generally, apart from (4.1), the following system may be used for the case $n_1 \le n_2$ [31], [32]:

$$M_1 = \{x^py^q \,|\, 0 \le p < n_1, 0 \le q \le n_1 + n_2 - 2p - 2\}. \tag{5.28}$$

However, even this opportunity does not help in the following situation:

Example 5.4 *Find the eliminant in x for the system* (5.9)

We have to eliminate y and z, and $M = \{1, y, z, yz\}$. Using the procedure similar to that from Example 5.2, in the second step we obtain the system

$$y^2z = 3yz^2 + \ldots, \ yz^2 = \frac{1}{3}y^2z + \ldots$$

which cannot be solved with respect to y^2z and yz^2. Moreover, it can be shown that none of the power products y^3, y^2z, yz^2, z^3 can be reduced with respect to any set M of lower degree power products. In fact, for this case the resultant (2.3) vanishes:

$$\mathcal{A}_0 = \mathcal{R}(f_{1,2}(0,z_2,1), f_{2,2}(0,z_2,1)) = \mathcal{R}(z_2^2 - 4z_2 + 3, z_2^2 - z_2 - 6) = 0.$$

As for Example 5.3, $\mathcal{A}_0$ was not zero, whereas one of its minors — a factor in the numerator of expression (4.8) — was.

Now we have collected enough empirical data to clarify the structure of Υ and its influence on the problem of reducibility. To formalize this, it will be convenient to consider first the problem of reducibility with respect to the set (5.28).

Theorem 5.1 *For the given polynomials $f_1(x,y), f_2(x,y) \in \mathbf{K}[x,y]$ let $n_1 \le n_2$. Denote, as usual, $\mathcal{A}_0 := \mathcal{R}(f_{1n_1}(z_1,1), f_{2n_2}(z_1,1)) = (-1)^{n_1(n_1-1)/2}\mathcal{U}$, where*

$$\mathcal{U} := \left| \begin{array}{ccccccccc} a_{n_1,0} & a_{n_1-1,1} & & \dots & a_{0,n_1} & 0 & \dots & 0 \\ & & & \dots & & & \dots & \\ 0 & \dots & 0 & 0 & a_{n_1,0} & a_{n_1-1,1} & \dots & a_{0,n_1} \\ 0 & \dots & 0 & b_{n_2,0} & b_{n_2-1,1} & b_{n_2-2,2} & \dots & b_{0,n_2} \\ & \dots & & & \dots & & & \\ b_{n_2,0} & b_{n_2-1,1} & b_{n_2-2,2} & \dots & \dots & b_{0,n_2} & \dots & 0 \end{array} \right| \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\end{array}}\right\} n_2 \ rows \\ \left.\vphantom{\begin{array}{c}a\\a\\a\end{array}}\right\} n_1 \ rows \end{array} \tag{5.29}$$

and $\mathcal{R}_k(\mathcal{A}_0)$ its k-th subresultant.

(1) *The system of inequalities*

$$\mathcal{A}_0 \ne 0, \mathcal{R}_1(\mathcal{A}_0) \ne 0, \dots, \mathcal{R}_{n_1-1}(\mathcal{A}_0) \ne 0, a_{n_1,0}^{n_2-n_1} \ne 0 \tag{5.30}$$

provides a necessary and sufficient condition for an arbitrary polynomial $g(x,y) \in \mathbf{K}[x,y]$ to be reducible modulo f_1, f_2 with respect to M_1.

(2) *Let $\mathcal{A}_0 \ne 0$, and the generalized Vandermonde matrix V be defined similarly as in (4.5) for the power product set M_1. Then for the constant Υ from (4.7) we will have*

$$\Upsilon = (-1)^{n_1(n_1-1)/2} \frac{[\mathcal{R}_1(\mathcal{A}_0)\dots\mathcal{R}_{n_1-1}(\mathcal{A}_0)]^2}{\mathcal{A}_0^{n_1+n_2-1}}. \tag{5.31}$$

Proof. The reduction algorithm outlined above is nothing more than a simplification of the following procedure. Consider, for simplicity, the case $n_1 = n_2 = 3$, so $M_1 = \{1, x, y, x^2, xy, y^2, xy^2, y^3, y^4\}$. Then

$$\begin{aligned} f_1 &= a_{30}x^3 + a_{21}x^2y + \underline{a_{12}xy^2} + \underline{a_{03}y^3} + \dots \\ f_2 &= b_{30}x^3 + b_{21}x^2y + \underline{b_{12}xy^2} + \underline{b_{03}y^3} + \dots \end{aligned}$$

where dots and underlined summands mean that the terms are reducible with respect to M_1. Reductions for power products x^3 and x^2y can be obtained from the equations $f_1 = 0, f_2 = 0$ iff the condition

$$\left| \begin{array}{cc} a_{30} & a_{21} \\ b_{30} & b_{21} \end{array} \right| \ne 0 \tag{5.32}$$

is fulfilled. Then any power product of degree 3 is reducible with respect to M_1, and thus, in the expressions

$$\begin{array}{rcllllll}
x\,f_1 & = & a_{30}x^4+ & a_{21}x^3y & +a_{12}x^2y^2 & +a_{03}xy^3 & & +\ldots \quad , \\
y\,f_1 & = & & a_{30}x^3y & +a_{21}x^2y^2 & +a_{12}xy^3 & +\underline{a_{03}y^4} & +\ldots, \\
y\,f_2 & = & & b_{30}x^3y & +b_{21}x^2y^2 & +b_{12}xy^3 & +\underline{b_{03}y^4} & +\ldots, \\
x\,f_2 & = & b_{30}x^4+ & b_{21}x^3y & +b_{12}x^2y^2 & +b_{03}xy^3 & & +\ldots
\end{array}$$

dots and underlined summands mean that the terms are reducible with respect to M_1. Power products x^4, x^3y, x^2y^2 and xy^3 can be expressed from the 4 last equalities iff the condition

$$\begin{vmatrix} a_{30} & a_{21} & a_{12} & a_{03} \\ 0 & a_{30} & a_{21} & a_{12} \\ 0 & b_{30} & b_{21} & b_{12} \\ b_{30} & b_{21} & b_{12} & b_{03} \end{vmatrix} \neq 0 \tag{5.33}$$

is fulfilled. Then any power product of degree 4 is reducible with respect to M_1, and thus, in the expressions

$$\begin{array}{rcllllll}
x^2\,f_1 & = & a_{30}x^5+ & a_{21}x^4y+ & a_{12}x^3y^2+ & a_{03}x^2y^3+ & \ldots & , \\
xy\,f_1 & = & & a_{30}x^4y+ & a_{21}x^3y^2+ & a_{12}x^2y^3+ & a_{03}xy^4+ \quad \ldots & , \\
y^2\,f_1 & = & & & a_{30}x^3y^2+ & a_{21}x^2y^3+ & a_{12}xy^4+ \quad a_{03}y^5+ & \ldots, \\
y^2\,f_2 & = & & & b_{30}x^3y^2+ & b_{21}x^2y^3+ & b_{12}xy^4+ \quad b_{03}y^5+ & \ldots, \\
xy\,f_2 & = & & b_{30}x^4y+ & b_{21}x^3y^2+ & b_{12}x^2y^3+ & b_{03}xy^4+ \quad \ldots & , \\
x^2\,f_2 & = & b_{30}x^5+ & b_{21}x^4y+ & b_{12}x^3y^2+ & b_{03}x^2y^3+ & \ldots & ,
\end{array}$$

dots mean the power products reducible with respect to M_1. Power products of degree 5 can be expressed from the last equalities iff the condition

$$\begin{vmatrix} a_{30} & a_{21} & a_{12} & a_{03} & 0 & 0 \\ 0 & a_{30} & a_{21} & a_{12} & a_{03} & 0 \\ 0 & 0 & a_{30} & a_{21} & a_{12} & a_{03} \\ 0 & 0 & b_{30} & b_{21} & b_{12} & b_{03} \\ 0 & b_{30} & b_{21} & b_{12} & b_{03} & 0 \\ b_{30} & b_{21} & b_{12} & b_{03} & 0 & 0 \end{vmatrix} \neq 0. \tag{5.34}$$

is fulfilled. Thus, subject to the previous constraints, any power product of degree 5 can be reduced with respect to M_1, i.e., its reduction is a linear combination of the power products of the lower degrees. It can be easily seen that by multiplying these reductions by $x, y, x^2, \ldots$ any power product of a degree higher than 5 can be reduced with respect to M_1.

The expressions on the left-hand sides of (5.32), (5.33) and (5.34) are the subresultants $\mathcal{R}_2(\mathcal{A}_0)$, $\mathcal{R}_1(\mathcal{A}_0)$ and $\mathcal{R}_0(\mathcal{A}_0) = -\mathcal{A}_0$ of

$$\mathcal{A}_0 = \mathcal{R}(a_{30}z_1^3 + a_{21}z_1^2 + a_{12}z_1 + a_{03},\ b_{30}z_1^3 + b_{21}z_1^2 + b_{12}z_1 + b_{03})$$

(see (3.4)). This completes the proof of the part (1).

For the proof of the part (2) we refer to Section 9. $\square$

Let us now modify the conditions of Theorem 5.1 for the case when the power product set is given by (4.1). The statements will be similar, with the only difference that instead of the subresultant $\mathcal{R}_k(\mathcal{A}_0)$ one has to take the following minor[4]

$$\mathcal{R}_k^*(\mathcal{A}_0) := \mathcal{U}\left(\begin{array}{cccccccc} 1 & 2 & \dots & k & n_1+n_2-k+1 & n_1+n_2-k+2 & \dots & n_1+n_2 \\ 1 & 2 & \dots & k & n_2+1 & n_2+2 & \dots & n_2+k \end{array}\right) \tag{5.35}$$

of the determinant (5.29). For the case $n_1 = n_2 = 3$, these minors will be:

$$\mathcal{R}_2^*(\mathcal{A}_0) := \left|\begin{array}{cc} a_{30} & a_{03} \\ b_{30} & b_{03} \end{array}\right| \quad \text{and} \quad \mathcal{R}_1^*(\mathcal{A}_0) := \left|\begin{array}{cccc} a_{30} & a_{21} & a_{03} & 0 \\ 0 & a_{30} & a_{12} & a_{03} \\ 0 & b_{30} & b_{12} & b_{03} \\ b_{30} & b_{21} & b_{03} & 0 \end{array}\right| \tag{5.36}$$

So, the bivariate reducibility conditions are formulated in terms of $\mathcal{A}_0$ and its non-zero minors. Since for the case $\mathcal{A}_0 \neq 0$ a sequence of its non-zero minors with decreasing orders always exists, it is always possible to choose the set of $N = n_1 n_2$ power products with respect to which any polynomial $g(x, y)$ is reducible. The condition $\mathcal{A}_0 \neq 0$ turns out to be the key one; one may notice that the problem of the bivariate resultant construction is reduced — via this condition — to the univariate one considered in Section 3. Even conditions (5.30) can be expressed in terms of the minors of matrix **B** from that section! This idea will be extended later to the trivariate case, but we will first examine how it is possible to modify the reduction algorithm to make it applicable for the case $\mathcal{A}_0 = 0$.

Solution of Example 5.4. To handle this case, let us use the following trick. By Theorem 3.1, it is possible to find a non-trivial linear representation for the resultant $\mathcal{A}_0$:

$$\mathcal{R}(z_2^2 - 4z_2 + 3, z_2^2 - z_2 - 6) \equiv (-z_2 - 2)(z_2^2 - 4z_2 + 3) + (z_2 - 1)(z_2^2 - z_2 - 6).$$

Where it follows that the linear combination

$$(-y - 2z)f_1 + (y - z)f_2 = (-2x - 3)y^2 - yz + (5x + 1)z^2 + (x^2 + x + 4)y + (-4x^2 - 4x + 2)z \tag{5.37}$$

does not contain the terms with y and z of degree higher than 2. Thus, the three relations $f_1 = 0, f_2 = 0$ and (5.37) compose the linear system with respect to the power products y^2, yz, z^2:

$$\begin{aligned} y^2 - 4yz + 3z^2 &= f_1 + (-x - 2)y + (2x + 1)z + (-x^2 - x + 2), \\ y^2 - yz - 6z^2 &= f_2 + (x + 1)y + (x - 1)z + (-2x^2 - 2x - 2), \\ (-2x - 3)y^2 - yz + (5x + 1)z^2 &= (-y - 2z)f_1 + (y - z)f_2 + (x^2 + x + 4)y + (-4x^2 - 4x + 2)z. \end{aligned}$$

The determinant of this system depends on x:

$$A_*(x) := -3(13x + 29) \tag{5.38}$$

and provided that $A_*(x) \neq 0$, one may express y^2, yz, z^2 as the linear combinations of the power products from $M_* = \{1, y, z\}$:

$$y^2 \;=\; -\frac{1}{A_*(x)}\Big(\big[(27y + 54z + 5x + 7)f_1 + (-27y + 27z - 20x - 1)f_2\big]$$

[4] Here the upper (lower) indices give the numbers of rows (columns) to be deleted from (5.29)

$$
\begin{aligned}
&+ \quad (2x^2 - 11x + 93)y + (-118x^2 - 70x + 62)z + (35x^3 + 30x^2 + 45x + 16)\Big),\\
yz &= \ldots,\\
z^2 &= \ldots
\end{aligned}
$$

The further procedure is standard: we reduce $y^2z, yz^2, \ldots$ and then $g, y\,g, z\,g$:

$$
\begin{aligned}
g &= \left[-\frac{1}{3}f_1 - \frac{2}{3}f_2\right] + \left(-\frac{7}{3}x + 3\right) y + \left(-\frac{10}{3}x - \frac{8}{3}\right) z + \left(\frac{8}{3}x^2 + \frac{11}{3}x - \frac{1}{3}\right), \qquad (5.39)\\
y\,g &= -\frac{1}{3A_*(x)}\Big([\ldots] + (248x^3 + 990x^2 - 584x + 270)y +\\
&+ \quad (1436x^3 + 676x^2 - 566x + 470)z + (-535x^4 - 787x^3 - 1023x^2 + 73x + 256)\Big),\\
z\,g &= \ldots
\end{aligned}
$$

Placing the coefficients of $\{1, y, z\}$ into the 3×3 matrix, we obtain:

$$
\det \mathbf{B}_* = \frac{2277x^7 + 3873x^6 - 2752x^5 + 4810x^4 + 2521x^3 - 4407x^2 - 2406x - 3916}{9(13x + 29)}. \qquad (5.40)
$$

The numerator gives the true eliminant $\mathcal{X}(x)$; the Bézout equality for it (if necessary) can be obtained using the polynomials in brackets from (5.39) in a manner similar to that used in Example 5.1.

What is the sense of $A_*(x)$ appearing in this example ? To clarify this, let us form the resultant of f_1 and f_2 eliminating either of the variables y or z:

$$
\mathcal{R}_y(f_1, f_2) = 3(13x + 29)z^3 + \ldots \,, \quad \mathcal{R}_z(f_1, f_2) = 9(13x + 29)y^3 + \ldots
$$

Here dots mean the terms of degree less than 3 in z or y respectively. Thus, A_* is the leading coefficient of both eliminants and therefore it is responsible for the number of zeros of the system $f_1 = 0,\ f_2 = 0$ (it was exactly this situation that was mentioned at the end of Section 2). When $A_* = 0$, the number of zeros of the system $f_1 = 0,\ f_2 = 0$ decreases to 2, and the set M should lose one more power product. □

Example 5.5 *Find the eliminant in x for the system $f_1 = 0, f_2 = 0, g = 0$, where f_1 and f_2 are the same as in* (5.9)*, while*

$$
g := x^2 - 2xy - y^2 - 2xz + 2yz + 3z^2 + 2x + 3y - 3z + \varepsilon = 0.
$$

Here ε is a parameter value satisfying the equation

$$
257049\varepsilon^2 + 283326979\varepsilon + 427778304 = 0.
$$

The **solution** for this example proceeds similarly as for the previous one. For an *arbitrary* ε one obtains

$$
\begin{aligned}
\det \mathbf{B}_* &= \frac{1}{9(13x + 29)}\big[2277x^7 + 3873x^6 + (2143\varepsilon - 609)x^5 + (11021\varepsilon + 15831)x^4\\
&\quad + (1459\varepsilon^2 + 1773\varepsilon + 2835)x^3 + (3421\varepsilon^2 + 3523\varepsilon - 4305)x^2\\
&\quad + (117\varepsilon^3 + +261\varepsilon^3 + 794\varepsilon^2 - 2337\varepsilon - 6786\big];
\end{aligned}
$$

but for the parameter value *specified* the fraction will be reduced by the factor $(13x + 29)$ (since it will appear in the numerator). An additional check shows that a solution of the system corresponding to $x = -29/13$ exists; however it will be lost in the expression for $\det \mathbf{B}_*$. In other words, to modify the suggested reduction algorithm, one has to check every "suspicious" value of a parameter, i.e. any one nullifying the denominator. The expression for the specified Poisson product cannot be obtained from the generic case by analytical continuation. □

In the following example the number of zeros of $f_1 = 0$, $f_2 = 0$ decreases by 3, and the set M loses exactly three power products.

Example 5.6 *Find the eliminant in z for the system*

$$f_1 = (x+y-z)^3 - x - 1 = 0, \; f_2 = (x+y+z)^3 - x^2 - y^2 + \varepsilon - 1 = 0, \; g = -x - y + 3z = 0. \tag{5.41}$$

Solution. For the system $f_1 = 0, f_2 = 0$ the resultant $\mathcal{A}_0$, and both of its minors (5.36) vanish. The leading forms $f_{1,3}(1, z_1, 0)$ and $f_{2,3}(1, z_1, 0)$ have a common zero of multiplicity 3. From the linear representation of the $\mathcal{A}_0$:

$$\mathcal{A}_0 = -f_{1,3} + f_{2,3}$$

the relation follows:

$$f_3 := -f_1 + f_2 = (6z-1)x^2 + (12z)xy + (6z-1)y^2 + x + (2z^3 + \varepsilon) = 0$$

which — together with either of the equations $f_1 = 0$ or $f_2 = 0$ — provides a new system of equations. In the system $f_3 = 0, f_2 = 0$, the first equation is of degree 2 with respect to x and y, but the coefficients of the leading terms depend now on z. We may try to apply the Bivariate Reduction Algorithm. Let us take the set $M_* := \{1, x, y, xy, y^2, xy^2\}$ as a set of independent power products. According to Theorem 5.1, the reduction procedure will be possible iff three conditions are fulfilled, namely

$$6z - 1 \neq 0, \; 2(6z-1) \neq 0, \; A_* = \mathcal{R}((6z-1)x^2 + (12z)x + (6z-1), x^3 + 3x^2 + 3x + 1) = -8 \neq 0.$$

(For the choice $M_* := \{1, x, y, xy, y^2, y^3\}$ the second condition will be $2(6z+1) \neq 0$.) It turns out that A_* has a sense similar to that of the previous example:

$$\mathcal{R}_x(f_1, f_2) = -8y^6 + (24z - 12)y^5 + \ldots$$

and the number of zeros of the system $f_1 = 0$, $f_2 = 0$ considered with respect to the indeterminates x and y does not depend on z. Therefore, for this example one may expect only the power of A_* to occur in the denominator of $\det B_*$. Omitting the intermediate calculations, we obtain finally

$$\det B_* = \frac{128z^6 - 48z^4 - 96z^3 + 9z^2 + 6z + 3 - \varepsilon}{2}$$

which differs from the true eliminant $\mathcal{Z}(z)$ only by the numerical factor (-8). □

Of course, the arguments used in Examples 5.4,5.5 and 5.6 are just speculations. A separate investigation should be carried out in order to make them reliable. We will treat once again the case of violation of conditions (5.30) in Section 7, by means of the Gröbner basis technique.

5.2 The trivariate case

The approach her is similar to that considered in the previous subsection, though some essential differences appear. We will sketch this case only for $n_1 = n_2 = n_3 = \delta$. Let us again begin with an example. Let $\delta = 2$, then the set (4.1) is given by

$$M = \{1, x, y, z, xy, xz, yz, xyz\}. \tag{5.42}$$

Consider the leading forms in the expansions of f_j:

$$
\begin{aligned}
f_1 &:= a_{200}x^2 + \underline{a_{110}xy} + \underline{a_{101}xz} + a_{020}y^2 + \underline{a_{011}yz} + a_{002}z^2 + \ldots, \\
f_2 &:= b_{200}x^2 + \underline{b_{110}xy} + \underline{b_{101}xz} + b_{020}y^2 + \underline{b_{011}yz} + b_{002}z^2 + \ldots, \\
f_3 &:= c_{200}x^2 + \underline{c_{110}xy} + \underline{c_{101}xz} + c_{020}y^2 + \underline{c_{011}yz} + c_{002}z^2 + \ldots
\end{aligned} \tag{5.43}
$$

Here dots and underlined summands mean that, as usual, the terms are reducible with respect to M. Consider the equations $f_1 = 0$, $f_2 = 0$, $f_3 = 0$ as a linear system with respect to x^2, y^2 and z^2. If the condition

$$
\begin{vmatrix} a_{200} & a_{020} & a_{002} \\ b_{200} & b_{020} & b_{002} \\ c_{200} & c_{020} & c_{002} \end{vmatrix} \neq 0 \tag{5.44}
$$

is fulfilled, then it is possible to resolve this system and obtain the reductions

$$x^2 \to^M A_{110}xy + A_{101}xz + A_{011}yz + \ldots, \tag{5.45}$$

$$y^2 \to^M B_{110}xy + B_{101}xz + B_{011}yz + \ldots, \tag{5.46}$$

$$z^2 \to^M C_{110}xy + C_{101}xz + C_{011}yz + \ldots \tag{5.47}$$

Multiply (5.45) by y and z, (5.46) by x and z, (5.47) by x and y respectively, and replace afterwards x^2, y^2 and z^2 on the right-hand sides by formulae (5.45)–(5.47):

$$
\begin{aligned}
x^2y &\to^M A_{110}xy^2 + \underline{A_{101}xyz} + A_{011}y^2z + \ldots, \\
x^2z &\to^M \underline{A_{110}xyz} + A_{101}xz^2 + A_{011}yz^2 + \ldots, \\
xy^2 &\to^M B_{110}x^2y + B_{101}x^2z + \underline{B_{011}xyz} + \ldots, \\
xz^2 &\to^M C_{110}x^2y + C_{101}x^2z + \underline{C_{011}xyz} + \ldots, \\
y^2z &\to^M \underline{B_{110}xyz} + B_{101}xz^2 + B_{011}yz^2 + \ldots, \\
yz^2 &\to^M C_{110}xy^2 + \underline{C_{101}xyz} + C_{011}y^2z + \ldots
\end{aligned}
$$

Consider these equations as a linear system with respect to x^2y, x^2z, xy^2, xz^2, y^2z, yz^2. This system is solvable if the condition

$$
\begin{vmatrix}
1 & 0 & -A_{110} & 0 & -A_{011} & 0 \\
0 & 1 & 0 & -A_{101} & 0 & -A_{011} \\
-B_{110} & -B_{101} & 1 & 0 & 0 & 0 \\
-C_{110} & -C_{101} & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & -B_{101} & 1 & -B_{011} \\
0 & 0 & -C_{110} & 0 & -C_{011} & 1
\end{vmatrix} \neq 0 \tag{5.48}
$$

is fulfilled. Assuming this, one obtains the reductions of the power products mentioned, in particular:

$$x^2y \to^M Dxyz + \ldots, \; x^2z \to^M xy^2 \to^M Fxyz + \ldots, \; xz^2 \to^M Hxyz + \ldots \tag{5.49}$$

One can also find the reductions for x^3 by multiplying (5.45) by x and substituting afterwards formulae (5.49). Similarly for y^3 and z^3. Thus, all the power products of degree 3 are reducible.

To obtain the reductions for the power products of degree 4, one has to multiply the third equation of (5.49) by z and the last by y

$$xy^2z \to^M xyz^2 \to^M Hxy^2z + \dots \tag{5.50}$$

From these equations one can find the reduction for the power products xy^2z, xyz^2 provided that

$$\begin{vmatrix} 1 & -F \\ -H & 1 \end{vmatrix} \neq 0. \tag{5.51}$$

With the help of these reductions, one can always obtain reduction for any other power product of degree 4. Then any power product of degree higher than 4 is reducible with respect to M.

For the general case the procedure is similar.

The Trivariate Reduction Algorithm for power products of fixed degree can be performed by solving the succession of linear systems with the coefficients rationally dependent on those of the leading forms f_{1n_1}, f_{2n_2} and f_{3n_3}. The process can be formalized by the following diagram which applies to the case $n_1 = n_2 = n_3 = \delta$

$$\begin{array}{l} f_1 = 0 \\ f_2 = 0 \\ f_3 = 0 \end{array} \Longrightarrow \left\{ \begin{array}{c} x^\delta \\ y^\delta \\ z^\delta \end{array} \right\}_3 \hookrightarrow \left\{ \begin{array}{cc} x^\delta y, & x^\delta z \\ xy^\delta, & y^\delta z \\ xz^\delta, & yz^\delta \end{array} \right\}_6 \hookrightarrow \left\{ \begin{array}{ccc} x^\delta y^2, & x^\delta yz, & x^\delta z^2 \\ y^\delta x^2, & y^\delta xz, & y^\delta z^2 \\ z^\delta x^2, & z^\delta xy, & z^\delta y^2 \end{array} \right\}_9 \tag{5.52}$$

$$\hookrightarrow \dots \hookrightarrow \left\{ \begin{array}{ccc} x^\delta y^{\delta-1}, & x^\delta y^{\delta-2}z, \dots, & x^\delta z^{\delta-1} \\ y^\delta x^{\delta-1}, & y^\delta x^{\delta-2}z, \dots, & y^\delta z^{\delta-1} \\ z^\delta x^{\delta-1}, & z^\delta x^{\delta-2}y, \dots, & z^\delta y^{\delta-1} \end{array} \right\}_{3\delta} \hookrightarrow \left\{ \begin{array}{ccc} y^\delta x^{\delta-1}z, & y^\delta x^{\delta-2}z^2, \dots, & y^\delta xz^{\delta-1} \\ z^\delta x^{\delta-1}y, & z^\delta x^{\delta-2}y^2, \dots, & z^\delta xy^{\delta-1} \end{array} \right\}_{2(\delta-1)}$$

$$\hookrightarrow \left\{ \begin{array}{ccc} y^\delta x^{\delta-1}z^2, & y^\delta x^{\delta-2}z^3, \dots, & y^\delta x^2 z^{\delta-1} \\ z^\delta x^{\delta-1}y^2, & z^\delta x^{\delta-2}y^3, \dots, & z^\delta x^2 y^{\delta-1} \end{array} \right\}_{2(\delta-2)} \hookrightarrow \dots \hookrightarrow \left\{ \begin{array}{c} x^{\delta-1}y^\delta z^{\delta-1} \\ x^{\delta-1}y^{\delta-1}z^\delta \end{array} \right\}_2$$

Here $\{\ \}$ means a linear system with respect to the power products included (the subscript indicates total number of them), while $\hookrightarrow$ means multiplication of the reductions obtained on the previous step by x or y, or z. If the power products of degree $\delta + k - 1$ are reducible and the linear system with respect to the indicated power products of degree $\delta + k$ is consistent, then all power products of degree $\delta + k$ are reducible (with some of them just contained in M). Therefore, for total reducibility it is necessary and sufficient to have $2\delta - 1$ conditions fulfilled. This condition is not always fulfilled:

Example 5.7 *For the polynomials from the system* (5.9) *establish the possibility of reduction with respect to the set* (5.42)*. (For the sake of coordination with the notation of the present subsection, we will set* $f_3(x, y, z) := g(x, y, z)$*).*

Solution. Condition (5.44) is valid ($\det = -24 \neq 0$), and

$$x^2 \to^M \frac{7}{8}xy + \frac{5}{4}xz + \dots, \quad y^2 \to^M -\frac{3}{2}xy + 3yz + \dots, \quad z^2 \to^M -\frac{1}{8}xy + \frac{1}{4}xz + \frac{1}{3}yz + \dots$$

However, the next step is impossible since the determinant from (5.48) vanishes. One may try to use an alternative to the power product system (5.42), namely $M_1 := \{1, x, y, z, xz, yz, z^2, z^3\}$. Generally, the set

$$M_1 = \left\{ x^p y^q z^\ell \mid 0 \le p < \delta, 0 \le q < \min(\delta, 2(\delta - p) - 1),\ 0 \le \ell < 3\delta - 2(p + q + 1) \right\}$$

plays a role similar to (5.28) in the bivariate case. The first of the corresponding conditions is valid:

$$\begin{vmatrix} a_{200} & a_{110} & a_{020} \\ b_{200} & b_{110} & b_{020} \\ c_{200} & c_{110} & c_{020} \end{vmatrix} = 3 \neq 0.$$

Hence, one can obtain the reductions for the power products:

$$x^2 \to^{M_1} 3xz + \frac{7}{3}yz - 7z^2 + \ldots, \; xy \to^{M_1} 2xz + \frac{8}{3}yz - 8z^2 + \ldots, \; y^2 \to^{M_1} -3xz - yz + 12z^2 + \ldots$$

Multiplying them by x,y and z, one can compose a linear system with respect to the power products x^2y, x^2z, xy^2, xyz, xz^2, y^2z, yz (this time, one has 7 power products vs. 6 from the scheme (5.52)), with the determinant equal to $-253/3 \neq 0$. So, the reduction of these power products is possible:

$$x^2y \to^{M_1} 0z^3 + \ldots, \quad x^2z \to^{M_1} 0z^3 + \ldots, \quad xy^2 \to^{M_1} 0z^3 + \ldots,$$
$$xyz \to^{M_1} 0z^3 + \ldots, \quad xz^2 \to^{M_1} 0z^3 + \ldots, \quad y^2z \to^{M_1} 9z^3 + \ldots, \quad yz^2 \to^{M_1} 3z^3 + \ldots$$

Multiplying the first and the fifth of them by z and the fourth by x one can compose a linear system with respect to the power products x^2yz, xz^3, z^4 (this time, one has 3 power products vs. 2 from the scheme (5.52)). However, the determinant of this system vanishes.

It can be shown that none of the power products of degree 4 can be reduced with respect to any set M of lower degree power products. In fact, for the considered polynomials, the resultant (2.3) vanishes (see (5.17)): $\mathcal{A}_0 = \mathcal{R}(f_{1,2}(z_1, z_2, 1), f_{2,2}(z_1, z_2, 1), f_{3,2}(z_1, z_2, 1)) = 0$. Thus, the situation looks somewhat similar to the bivariate case. Unfortunately, we have not been able to prove the following

Choice Conjecture. The condition $\mathcal{A}_0 \neq 0$ is necessary and sufficient for the existence of the set M of $n_1n_2n_3$ power products in x, y and z with respect to which any polynomial $g(x, y, z)$ is reducible.

The main difficulty is that for the trivariate case we do not have an explicit representation of $\mathcal{A}_0$ in terms of the coefficients of the leading forms f_{1n_1}, f_{2n_2} and f_{3n_3}. Therefore, we cannot carry over the proof of Theorem 5.1 to this case. The only fact which we have established is (we formulate it again for the case $n_1 = n_2 = n_3 = \delta$):

Theorem 5.2 *The first δ conditions of the $2\delta - 1$ mentioned in the trivariate reduction algorithm can be rewritten in terms of the nested minors of Macaulay's matrix (see Section 6) formed from the coefficients of $f_{1\delta}$, $f_{2\delta}$, $f_{3\delta}$ for finding the resultant*

$$\mathcal{A}_0 = \mathcal{R}(f_{1\delta}(z_1, z_2, 1), f_{2\delta}(z_1, z_2, 1), f_{3\delta}(z_1, z_2, 1)).$$

The succession of their orders is : $3, 9, \ldots, 3(k + 1)(k + 1)/2, \ldots, 3\delta(\delta + 1)/2$.

Proof. This follows from a reasoning similar to that used in the proof of Theorem 5.1. Assuming that any power product of degree less than or equal to $\delta + k - 1$, $(k \leq \delta - 1)$ is reducible with respect to M, let us multiply the equations $f_1 = 0$, $f_2 = 0$, $f_3 = 0$ by all possible power products of degree k, and use the reductions obtained earlier to reduce all possible terms. In this way, we obtain the $3\binom{k+2}{2}$ linear equations connecting the $\binom{\delta+k+2}{2}$ power products of degree $\delta + k$. Of these, $\binom{\delta+k+2}{2} - 3\binom{k+2}{2}$ are contained in M (see formula (AI.3) from Appendix I). So, the number of the equations coincides with that of the power products to be reduced. To resolve this system, the determinant formed by the coefficients of these power products should be non-zero, and this gives the k-th condition mentioned in the theorem. So, for example, for the case $\delta = 2$, condition (5.48) can be replaced by

$$\begin{vmatrix} a_{200} & a_{110} & a_{101} & a_{020} & a_{002} & 0 & 0 & 0 & 0 \\ 0 & a_{200} & 0 & a_{110} & 0 & a_{020} & a_{011} & a_{002} & 0 \\ 0 & 0 & a_{200} & 0 & a_{101} & 0 & a_{020} & a_{011} & a_{002} \\ b_{200} & b_{110} & b_{101} & b_{020} & b_{002} & 0 & 0 & 0 & 0 \\ 0 & b_{200} & 0 & b_{110} & 0 & b_{020} & b_{011} & b_{002} & 0 \\ 0 & 0 & b_{200} & 0 & b_{101} & 0 & b_{020} & b_{011} & b_{002} \\ c_{200} & c_{110} & c_{101} & c_{020} & c_{002} & 0 & 0 & 0 & 0 \\ 0 & c_{200} & 0 & c_{110} & 0 & c_{020} & c_{011} & c_{002} & 0 \\ 0 & 0 & c_{200} & 0 & c_{101} & 0 & c_{020} & c_{011} & c_{002} \end{vmatrix} \neq 0$$

(provided that condition (5.44) is valid). □

Remark 1. We have not yet been able to establish a relationship between the reducibility conditions and the constant Υ introduced by (4.7). Macaulay claimed in [21] that the structure of Υ remains similar to (5.31); we failed to confirm this even for the case $\delta = 3$.

Remark 2. The last example also reminds one of the case which remains beyond consideration in the present report: when the leading forms of the system (2.4) have a common zero with a zero-component. In Example 5.7, the leading forms have a common zero $(0, 3, 1)$. Their dehomogenization with respect to x "hides" this zero: $\mathcal{A}_0 = \mathcal{R}(f_{1,2}(1, z_2, z_3), f_{2,2}(1, z_2, z_3), f_{3,2}(1, z_2, z_3)) \neq 0$, and the formal application of Poisson's definition of the resultant will lead one to the wrong estimation for the degree of the eliminant in x and, consequently, for the number of zeros for the system $f_1 = 0, f_2 = 0, f_3 = 0$.

5.3 The L-variate case

For $L > 3$ the reduction algorithm works similar to the trivariate case:

The L-Variate Reduction Algorithm for power products of a fixed degree can be performed by solving the succession of linear systems with the coefficients rationally dependent on those of the leading forms $f_{1n_1}, \ldots, f_{Ln_L}$. The process can be formalized by the following diagram which relats to the case

$n_1 = \ldots = n_L = \delta$

$$\begin{array}{c} f_1 = 0 \\ \ldots \\ f_L = 0 \end{array} \Longrightarrow \left\langle \begin{array}{c} x_1^\delta \mu(x_2, \ldots, x_L) \\ \ldots \\ x_L^\delta \mu(x_1, \ldots, x_{L-1}) \end{array} \middle| \; 0 \le \deg \mu \le \delta - 1 \right\rangle_{(\delta)}$$

$$\downarrow$$

$$\left\langle \begin{array}{c} x_2^\delta \mu(x_1, x_3, \ldots, x_L) \\ \ldots \\ x_L^\delta \mu(x_1, \ldots, x_{L-1}) \end{array} \middle| \begin{array}{c} \delta - 1 < \deg \mu \le 2\delta - 2 \\ \\ \mu \in M \end{array} \right\rangle_{(\delta-1)}$$

$$\downarrow$$

$$\left\langle \begin{array}{c} x_3^\delta \mu(x_1, x_2, x_4, \ldots, x_L) \\ \ldots \\ x_L^\delta \mu(x_1, \ldots, x_{L-1}) \end{array} \middle| \begin{array}{c} 2\delta - 2 < \deg \mu \le 3\delta - 3 \\ \\ \mu \in M \end{array} \right\rangle_{(\delta-1)}$$

$$\downarrow$$

$$\ldots$$

$$\downarrow$$

$$\left\langle \begin{array}{c} x_k^\delta \mu(x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_L) \\ \ldots \\ x_L^\delta \mu(x_1, \ldots, x_{L-1}) \end{array} \middle| \begin{array}{c} (k-1)(\delta-1) < \deg \mu \le k(\delta-1) \\ \\ \mu \in M \end{array} \right\rangle_{(\delta-1)}$$

$$\downarrow$$

$$\ldots$$

$$\downarrow$$

$$\left\langle \begin{array}{c} x_{L-1}^\delta \mu(x_1, \ldots, x_{L-2}, x_L) \\ x_L^\delta \mu(x_1, \ldots, x_{L-1}) \end{array} \middle| \begin{array}{c} (L-2)(\delta-1) < \deg \mu \le (L-1)(\delta-1) \\ \mu \in M \end{array} \right\rangle_{(\delta-1)}$$

Here $\langle\ \rangle$ means a finite sequence of linear systems which will be called a **cascade**. The subscript denotes the number of systems. For example, the first of the considered cascades has the structure:

$$\left\{ \begin{array}{c} x_1^\delta \\ \ldots \\ x_L^\delta \end{array} \right\}_L \hookrightarrow \left\{ \begin{array}{c} x_1^\delta x_j,\ 1 < j \le L \\ \ldots \\ x_L^\delta x_j,\ 1 \le j < L \end{array} \right\}_{L(L-1)} \hookrightarrow \left\{ \begin{array}{c} x_1^\delta x_j x_k,\ 1 < j,k \le L \\ \ldots \\ x_L^\delta x_j x_k,\ 1 \le j,k < L \end{array} \right\}_{L\binom{L}{2}} \hookrightarrow$$

$$\hookrightarrow \cdots \hookrightarrow \left\{ \begin{array}{cc} x_1^\delta x_2^{j_2} \ldots x_L^{j_L}, & j_2 + \ldots + j_L = \delta - 1 \\ \ldots & \\ x_1^{j_1} \ldots x_{n-1}^{j_{L-1}} x_L^\delta, & j_1 + \ldots + j_{L-1} = \delta - 1 \end{array} \right\}_{L\binom{L+\delta-3}{\delta-1}} \tag{5.53}$$

The $\{\ \}$ means a linear system with respect to the power products included. The subscript indicates the total number of them; for the system

$$\left\{ \begin{array}{c} x_k^\delta \mu(x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_L) \\ \ldots \\ x_L^\delta \mu(x_1, \ldots, x_{L-1}) \end{array} \middle| \begin{array}{c} \deg \mu = \ell \\ \\ \mu \in M \end{array} \right\} \tag{5.54}$$

it equals

$$(L-k+1)\left[\binom{L+\ell-2}{n-2}-\binom{L-1}{1}\binom{L+\ell-2-\delta}{L-2}+\binom{L-1}{2}\binom{L+\ell-2-2\delta}{L-2}-\dots\right]$$

(see formula (AI.3)). The last system of the diagram contains only two power products:

$$x_1^{\delta-1}\cdots x_{L-2}^{\delta-1}x_{L-1}^{\delta}x_L^{\delta-1} \quad \text{and} \quad x_1^{\delta-1}\cdots x_{L-2}^{\delta-1}x_{L-1}^{\delta-1}x_L^{\delta}.$$

If the power products of degree $\delta+\ell-1$ are reducible and the linear system with respect to indicated power products of degree $\delta+\ell$ is consistent, then all power products of degree $\delta+\ell$ are reducible (with some of them just contained in M). The transfer from the system (5.54) to the next one in the sequence (denoted by $\hookrightarrow$) is performed via multiplication of the reductions obtained in the previous step by any of $x_k,\dots,x_L$ if the new system is contained in the same cascade, and by any of $x_{k+1},\dots,x_L$ if it happens to be the first in the next cascade.

Therefore, for total reducibility it is sufficient to have $(L-1)(\delta-1)+1$ conditions fulfilled. The first δ of them given by the sequence (5.53) can be reformulated in terms of the nested minors of the Macaulay matrix formed for finding the resultant $\mathcal{A}_0$ introduced in (2.3) (see Section 6).

To end this section, let us mention the fact that we are now able to estimate the degrees of the polynomials satisfying the Bézout equalities. Indeed, if every step of the reduction algorithm is executable, then degrees of the polynomials of the linear representation increase "continuously", i.e., if

$$\begin{aligned} h(X) &\equiv h_{red}(X)+a_1(X)f_1(X)+\ldots+a_L(X)f_L(X), \\ h^*(X) &\equiv h^*_{red}(X)+a_1^*(X)f_1(X)+\ldots+a_L^*(X)f_L(X) \end{aligned}$$

and $\deg h^* = 1+\deg h$, then $\deg a_j^* \le 1+\deg a_j$. Restricting, again, ourselves to the case $n_1=\ldots=n_L=\delta$, we arrive at the following

Theorem 5.3 *Provided that the reducibility conditions are fulfilled, one has the following restrictions on degrees of the polynomials from equality* (2.7)*:* $\deg P_j \le N-\delta$*; while for* (2.9) *one has:*

$$\deg P_j \le (L-1)(\delta-1)+m-1, \quad \deg Q \le L(\delta-1).$$

6 Bézout's method versus Macaulay's one

Bézout's method for computing the multivariate resultant has a close relationship with that treated in the book by Macaulay [22]. Both are based on replacement of a given non-linear polynomial system by a linear one with respect to the power products considered as separate indeterminates.

We first recall Macaulay's definition of the resultant for *generic* polynomials. Let $\mathbf{M},\mathbf{M_1},\dots,\mathbf{M_L},\mathbf{M}$ be finite subsets of the set of all the power products in $x_1,\dots,x_L$ such that for every $\tau\in M_j$ (or $\tau\in M$), polynomial $\tau\cdot f_j$ (or $\tau\cdot g$) belongs to the linear subspace of $\mathbf{K}[X]$ spanned by $\mathbf{M}$. In other words, every polynomial $\tau\cdot f_j$ (or $\tau\cdot g$) is a linear combination of the elements of $\mathbf{M}$ ordered somehow. ¿From the coefficient vectors of all these polynomials compose a **coefficient matrix** which will be denoted as

$$\begin{pmatrix} M_1 f_1 \\ \vdots \\ M_L f_L \\ Mg \end{pmatrix} \tag{6.1}$$

Let

$$n_M := n_1 + \ldots + n_L + m - L.$$

The resultant $\mathcal{R}(f_1, \ldots, f_L, g)$ is defined than as the gcd of all the minors of order $\binom{n_M}{L}$ of the matrix (6.1) constructed for the choice

$$\begin{array}{rcl} \mathbf{M} & = & \{\tau(X) \mid \deg \tau \leq n_M\}, \\ M_j & := & \{\tau(X) \mid \deg \tau \leq n_M - n_j\}, \quad (j = 1, \ldots, L) \\ M & = & \{\tau(X) \mid \deg \tau \leq n_M - m\}. \end{array} \tag{6.2}$$

The above algorithm, while possible in theory, is impractical. In order to make it constructive, Macaulay suggested to choose the minor of matrix (6.1) corresponding to the following sequence of the sets:

$$\begin{array}{rcl} M_1 & := & \{\tau(X) \mid \deg \tau(X) \leq n_M - n_1\}, \\ M_j & := & \{\tau(X) = x_1^{p_1} \ldots x_L^{p_L} \mid \deg \tau(X) \leq n_M - n_j,\ p_1 < n_1, \ldots, p_{j-1} < n_{j-1}\}\ (j = 2, \ldots, L), \end{array}$$

where M is defined by (4.1).[5] This minor differs from the resultant only by an extraneous factor A_*, which is polynomially dependent on the coefficients of the leading forms $f_{jn_j}(X)$ of the polynomials $f_1, \ldots, f_L$ only (and independent of the coefficients of $g(X)$). Formally, the coefficient matrix (6.1) represents an analogue of equality (4.9):

$$P_1(X) f_1(X) + \ldots + P_L(X) f_L(X) + Q(X) g(X) = A_* \mathcal{R}_X(f_1, \ldots, f_L, g).$$

Thus, for example, for the bivariate case $(x_1 := x, x_2 := y)$ when $n_1 = n_2 = m = \delta$, one obtains:

$$\begin{array}{rcl} \mathbf{M} & = & \{\tau(x,y) \mid \deg \tau \leq 3\delta - 2\}_{\binom{3\delta}{2}}, \\ M_1 & = & \{\tau(x,y) \mid \deg \tau \leq 2\delta - 2\}_{\binom{2\delta}{2}}, \quad M_2 = \{\tau(x,y) = x^p y^q \mid \deg \tau \leq 2\delta - 2,\ p < \delta\}_{\binom{2\delta}{2} - \binom{\delta}{2}}, \\ M & = & \{\tau(x,y) = x^p y^q \mid \deg \tau \leq 2\delta - 2,\ p < \delta, q < \delta\}_{\delta^2} \end{array}$$

(the subscript denotes the number of power products in the considered set).

The Bézout method can be treated in exactly the same manner, however the coefficient matrix construction is different. For the above example one has to choose:

$$\begin{array}{rcl} M_1 = M_2 & = & \{\tau(x,y) = x^p y^q \mid \deg \tau \leq 2\delta - 2,\ p < \delta\}_{\binom{2\delta}{2} - \binom{\delta}{2}}, \\ \mathbf{M} & = & \{\tau(x,y) = x^p y^q \mid \deg \tau \leq 3\delta - 2,\ p < 2\delta\}_{\binom{3\delta}{2} - \binom{\delta}{2}}, \end{array}$$

while the set M remains the same. The coefficient matrix is now of order $\binom{3\delta}{2} - \binom{\delta}{2}$ and thus smaller than in Macaulay's method. In addition, the coefficients of f_1 and f_2 taken as the entries of the matrix possess

[5] The corresponding coefficient matrix will be a square one of the order $\binom{n_M}{L}$: this fact follows from Theorem AI.1 (Appendix I).

now "equal rights", i.e. the matrix has the same number of rows containing them (Macaulay's one has the predominance of those of f_1). However, this time the "equal rights" of the indeterminates x and y are lost. (The procedure was outlined on Example 5.1, where we were looking for a solution of the Bézout identity (4.9): $P_1 f_1 + P_2 f_2 + Qg \equiv \mathcal{R}^g_{x,y}(f_1, f_2)$. For the sake of coordination with the above scheme one has to replace there x by y.)

The reduction algorithm outlined in Section 5 can be interpreted as a procedure of triangularization of the coefficient matrix

$$\left(\begin{array}{c} \left[\begin{array}{c} M_2 \ f_1 \\ M_2 \ f_2 \end{array} \right] \\ M \ g \end{array} \right) \tag{6.3}$$

if we first manipulate with the rows corresponding to its [ ]−part. Let us make the total degree reverse lexicographic ordering of the power products from the set $\mathbf{M}$. Then the reduction algorithm will lead us to the formulae which can be represented in matrix form as

$$\begin{array}{cc} \overbrace{\hphantom{\star \quad \star \quad \ddots \quad \star \quad \star}}^{\mathbf{M}\setminus M} & \overbrace{\hphantom{* \ \dots \ *}}^{M} \\ \end{array}$$
$$\left[\begin{array}{ccccc|ccc} \star & & & & \mathbf{O} & * & \dots & * \\ & \star & & & & * & \dots & * \\ & & \ddots & & & & \dots & \\ & & & \star & & * & \dots & * \\ \mathbf{O} & & & & \star & * & \dots & * \end{array} \right]. \tag{6.4}$$

and thus, it is nothing more than an optimally performed Gaussian elimination for a sparse matrix of a special structure. Evidently, the reducibility conditions mentioned in Section 5 are equivalent to the non-vanishing of the diagonal elements on the left-hand part of (6.4) (marked with $\star$). If these conditions are satisfied, then we may use the reduction formulae to reduce the polynomials $\tau(X) \cdot g(X)$ for $\tau \in M$. In terms of matrices, this means just elimination in the $(M \ g)$-part of matrix (6.3), the entries from the columns not corresponding to the set M. The result is as follows:

$$\begin{pmatrix} \mathbf{D} & * \\ \mathbf{O} & \mathbf{B} \end{pmatrix} \tag{6.5}$$

where $\mathbf{B}$ is the Bézout matrix, and $\mathbf{D}$ is a diagonal one.

Similar algorithms can be applied to the Macaulay matrix too, though for this case we do not have a computationally safe procedure to find the representation (6.4).

7 Application of the Gröbner bases technique

7.1 Extension of the Bézout method to the general case

In previous sections the polynomials $f_1, \dots, f_L, g$ in $\mathbf{K}[X]$ were assumed to be generic. We now look for the resultant in non-generic — also called general — cases. In general cases polynomials may have algebraically dependent coefficients. A universal approach for the general case consideration is provided by a Gröbner basis construction [9], [10], [4].

Let $\mathcal{I}(f_1(X),\dots,f_L(X))$ be the ideal generated by $f_1,\dots,f_L$ over $Qt(\mathbf{K})[X]$. Compute a Gröbner basis $GB(\mathcal{I})$ of this ideal with respect to admissible ordering on the power products in $x_1,\dots,x_L$. Denote by $\operatorname{Init}(GB)$ the set of all the leading power products of the polynomials from $GB(\mathcal{I})$. Let us take the set

$$M = \{\mu(X) = x_1^{p_1}\cdots x_L^{p_L} \mid \mu(X) \text{ is not a multiple of any power product from } \operatorname{Init}(GB)\}\,. \tag{7.1}$$

as a basis for the vector space $Qt(\mathbf{K})[X]/\mathcal{I}$ (the residue class ring modulo $\mathcal{I}$). We will assume this set to be finite ($\mathcal{I}$ is a zero-dimensional ideal) and to contain $N^*>1$ elements:

$$M = \{\mu_1(X)\equiv 1,\dots,\mu_{N^*}(X)\}.$$

Then N^* is the number of common zeros Λ_j of $f_1,\dots,f_L$, counting multiplicities [11].

For any $h(X)\in Qt(\mathbf{K})[X]$, we can compute its **normal form** with respect to $\mathcal{I}$, using GB, i.e. the unique polynomial $h_{red}(X)\in Qt(\mathbf{K})[X]$ with all its power products in M, for which $h(X)-h_{red}(X)\in\mathcal{I}$. We will write $h_{red}(X)=h(X)+\mathcal{I}$. Evidently $h_{red}(\Lambda_j)=h(\Lambda_j)$.

Let us introduce the Bézout matrix as in (4.5). If

$$\mu_k(X)g(X)+\mathcal{I} = b_{k1}\mu_1(X)+\ldots+b_{kN^*}\mu_{N^*}(X) \quad (k=1,\dots,N^*),$$

then the $N^*\times N^*$ matrix

$$\mathbf{B} := [b_{kj}]_{k,j=1}^{N^*} \tag{7.2}$$

with entries in $Qt(\mathbf{K})$ represents the linear mapping of $Qt(\mathbf{K})[X]/\mathcal{I}$:

$$h(X)+\mathcal{I}\mapsto h(X)\cdot g(X)+\mathcal{I}, \quad h(X)\in Qt(\mathbf{K})[X] \tag{7.3}$$

Therefore, one has

$$\mathbf{B}\left(\begin{array}{c}\mu_1\\ \vdots\\ \mu_{N^*}\end{array}\right) = \left(\begin{array}{c}\mu_1\,g+\mathcal{I}\\ \vdots\\ \mu_{N^*}\,g+\mathcal{I}\end{array}\right). \tag{7.4}$$

Substituting the zeros $\Lambda_1,\dots,\Lambda_{N^*}$, we can write down all the equalities obtained in the matrix form:

$$\mathbf{B}V = V\left(\begin{array}{ccc} g(\Lambda_1) & & \mathbf{O}\\ & \ddots & \\ \mathbf{O} & & g(\Lambda_{N^*})\end{array}\right) \quad \text{where} \quad V = \left(\begin{array}{ccc}\mu_1(\Lambda_1) & \ldots & \mu_1(\Lambda_{N^*})\\ \ldots & & \ldots\\ \mu_{N^*}(\Lambda_1) & \ldots & \mu_{N^*}(\Lambda_{N^*})\end{array}\right) \tag{7.5}$$

is what we will call the generalized Vandermonde matrix. Recalling the definition of the Poisson product (2.10), one obtains for matrix (7.2):

$$\det\mathbf{B} = \mathcal{R}_X^g(f_1,\dots,f_L) \tag{7.6}$$

provided that V is non-singular.

We can now compare this approach with that outlined in Section 4. It can be easily noticed that the definition of the normal form is equivalent to the notion of reducedness introduced in that section. The essential difference is that, in Section 4, we have *a priori* foreseen the structure for the basis for $Qt(\mathbf{K})[X]/\mathcal{I}$: it has been assumed to be finite and to coincide with the set (4.1). This assumption is justified by the constructivity of its verification: the validity is established not via the whole set of the coefficients of the polynomials but via its subset of those of the leading forms. For example, the most important condition for reducibility with respect to the set (4.1) is that

$$\mathcal{A}_0 := \mathcal{R}\left(f_{1n_1}(z_1,\dots,z_{L-1},1),\dots,f_{Ln_L}(z_1,\dots,z_{L-1},1)\right) \neq 0.$$

In terms of ideal theory, it is equivalent to

$$\mathcal{I}\left(f_{1n_1}(z_1,\dots,z_{L-1},1),\dots,f_{Ln_L}(z_1,\dots,z_{L-1},1)\right) \ni 1,$$

thus the number of variables decreases. For the *generic* polynomials $f_1,\dots,f_L$ this condition, along with the others necessary for the reduction process (see Section 5), is valid, and therefore the Bézout matrix (4.6) can be constructed. Vanishing of its determinant is then equivalent to

$$g(X) \in \mathcal{I}(f_1(X),\dots,f_L(X)).$$

Let us now come back to equality (7.5) and investigate the condition $\det V \neq 0$. Evidently, it does not hold if there exists a multiple zero for $f_1,\dots,f_L$.

Theorem 7.1 *If $\mathcal{I}$ is a radical ideal, then* $\det V \neq 0$.

Proof. If V is singular, then there exists a linear dependency between the rows of V. This gives a non-zero polynomial $h(X) \in Qt(\mathbf{K})[X]$ with power products among $\mu_1,\mu_2,\dots,\mu_{N^*}$ which vanishes at all the $\Lambda_1,\dots,\Lambda_{N^*}$. Therefore $h(X)$ belongs to the radical ideal of $\mathcal{I}$ but, since $\mathcal{I}$ is a radical one itself, $h(X) \in \mathcal{I}$. Thus the normal form of $h(X)$ is identically zero, which contradicts to the linear independency of the set (7.1). □

To extend Theorem 4.1 to any zero-dimensional ideal $\mathcal{I}$ (not necessarily radical) we will need the following result which in some publications [16], [26] has been assigned to L. Stickelberger [6].

Theorem 7.2 *For any zero-dimensional ideal $\mathcal{I}$ there exists a basis for the vector space $Qt(\mathbf{K})[X]/\mathcal{I}$ in which the matrix of the linear mapping* (7.3) *takes the following block-diagonal form*

$$\left(\begin{array}{ccc} U_1 & & \mathbf{O} \\ & \ddots & \\ \mathbf{O} & & U_{N'} \end{array}\right) \quad \text{where} \quad U_j = \left(\begin{array}{cccc} g(\Lambda_j) & * & \dots & * \\ 0 & g(\Lambda_j) & \dots & * \\ & & \ddots & \\ 0 & 0 & \dots & g(\Lambda_j) \end{array}\right)_{\ell_j\times\ell_j} \tag{7.7}$$

Here $\{\Lambda_1,\dots,\Lambda_{N'}\}$ is the set of all the distinct zeros of $f_1,\dots,f_L$, and ℓ_j stands for the multiplicity of Λ_j.

Theorem 7.3 *Formula* (7.6) *will be true for any basis* (7.1). *One also has $\mathcal{R}_X^g \in Qt(\mathbf{K})$.*

Proof. By Theorem 7.2, there exists a non-singular matrix P such that matrix $P^{-1}\cdot\mathbf{B}\cdot P$ has the form (7.7). For Example 5.1, matrix $\mathbf{B}$ takes the form (5.8). One has:

$$P^{-1}\cdot\mathbf{B}\cdot P = \left(\begin{array}{cccc} \varepsilon & 0 & 0 & 0 \\ 0 & \varepsilon+2 & 1 & 0 \\ 0 & 0 & \varepsilon+2 & 0 \\ 0 & 0 & 0 & \varepsilon+2 \end{array}\right) \quad \text{where} \quad P = \left(\begin{array}{cccc} 2/5 & -2/5 & 3/5 & 1 \\ -1/4 & 1/2 & 1/4 & 0 \\ 1/4 & 1/2 & -1/4 & 0 \\ -1/10 & -2/5 & 1/10 & 1 \end{array}\right).$$

[6] We failed to find an original source for this result. Checking all the papers mentioned in Ludwig Stickelberger's list of publications [30] we decided that the nearest to the subject is the paper [29] on Number Theory.

It is evident that $\det \mathbf{B}$ coincides with the Poisson product:

$$\det \mathbf{B} = \det U_1 \dots \det U_{N'} = \prod_{j=1}^{N'} g(\Lambda_j)^{\ell_j} = \mathcal{R}_X^g(f_1, \dots, f_L).$$

$\square$

Corollary 1 . *The spectrum of the Bézout matrix consists of the numbers $g(\Lambda_j)$ (taken ℓ_j times). The associated eigenvectors coincide with the columns $[\mu_1(\Lambda_j), \dots, \mu_{N^*}(\Lambda_j)]^T$ of the generalized Vandermonde matrix.*

Thus formula (4.13) was nothing more than an algorithm to find an eigenvector associated with the zero eigenvalue of the Bézout matrix.

Remark. Unfortunately Theorem 7.2 does not help in checking the Rank Conjecture formulated on page 9 since it does not give a structure for the entries of the matrix U_j from (7.7) above the leading diagonal. This conjecture can be reformulated in terms of the dependency of the Jordan canonical form for matrix $\mathbf{B}$ on the multiplicity of Λ_j as a zero for $g(X)$.

Example 7.8 *Find the Poisson product $\mathcal{R}_{x,y}^g(f_1, f_2)$ for*

$$f_1 = x^2 - 14xy + 12y^2 + 9x - 18y + 6, \quad f_2 = -9x^2 + 5xy + 2y^2 + 7x - 14y + 12, \quad g = \varepsilon x - y.$$

Solution. Construct first a Gröbner basis for the ideal $\mathcal{I}(f_1(x,y), f_2(x,y))$, e.g. for the total degree ordering $x \succ y$:

$$\{11xy - 10y^2 - 8x + 16y - 6,\ -11x^2 + 8y^2 + 13x - 26y + 18,\ -22y^3 + 50y^2 + 7x - 3y - 25\}.$$

The leading power products are xy, x^2, y^3 respectively, hence one may choose $M = \{1, x, y, y^2\}$. Polynomials f_1 and f_2 has 4 common zeros. The determinant of the Bézout matrix

$$\begin{array}{c} g \\ xg \\ yg \\ y^2 g \end{array} \left(\begin{array}{cccc} 0 & \varepsilon & -1 & 0 \\ (18\varepsilon - 6)/11 & (13\varepsilon - 8)/11 & (-26\varepsilon + 16)/11 & (8\varepsilon - 10)/11 \\ 6\varepsilon/11 & 8\varepsilon/11 & -16\varepsilon/11 & (10\varepsilon - 11)/11 \\ (-14\varepsilon + 25)/22 & (18\varepsilon - 7)/22 & (-14\varepsilon + 3)/22 & (28\varepsilon - 50)/22 \end{array} \right)$$

equals $1/2(\varepsilon - 2)(2\varepsilon - 1)^2$. $\square$

Note that for the example just described, the resultant (2.8) differs from the Poisson product (2.10) by a constant factor because f_1 and f_2 are independent of ε and therefore $\mathcal{A}_0$ is a constant. In the next subsections, we will treat the case where the parameters contained in polynomials affect the number $\mathcal{A}_0$, and thus may alter the order of Bézout's matrix.

7.2 Computation of an eliminant

Let us apply the algorithm described in the previous subsection to find an eliminant for the system (2.4), e.g. the polynomial (2.6) as the Poisson product

$$\mathcal{X}_L(x_L) = \mathcal{R}_{x_1, \dots, x_{L-1}}^{f_L}(f_1, \dots, f_{L-1}). \tag{7.1}$$

In the *generic case* the number of zeros for the system

$$f_1(X)=0,\dots,f_{L-1}(X)=0$$

considered with respect to the indeterminates $x_1,\dots,x_{L-1}$ is independent of x_L, since

$$\mathcal{A}_0:=\mathcal{R}\left(f_{1,n_1}(z_1,\dots,z_{L-2},1,0),\dots,f_{L-1,n_{L-1}}(z_1,\dots,z_{L-2},1,0)\right)\neq 0.$$

Let us consider the exceptional case when the last condition fails.

Example 7.9 *Find the eliminant in x for the system* (5.9).

Solution. For the ideal $\mathcal{I}(f_1(x,y,z),f_2(x,y,z))$ over $\mathbf{K}=Q[x]$ the Gröbner basis computed with respect to the total degree ordering $y\succ z$ will depend on x

$$GB_{x\neq -29/13}=\left\{\begin{array}{l}(39x+87)y^2+(118x^2+70x-62)z+(-2x^2+11x-93)y-35x^3-30x^2-45x-16,\\ (39x+87)yz+(61x^2+76x-11)z-(5x^2+19x+60)y-29x^3-66x^2-45x+14,\\ (39x+87)z^2+(16x^2+7x-23)z+(7x^2+26x+9)y-14x^3-36x^2-42x-34\end{array}\right\}$$

and

$$GB_{x=-29/13}=\{1014z^2-37297z-33573,\ 247y-715z-627\}.$$

The latter cannot be obtained via the specialization of the former. The algorithm from the previous subsection splits:

$$M=\left\{\begin{array}{ll}\{1,y,z\} & \text{for } x\neq -29/13\ ;\\ \{1,z\} & \text{for } x=-29/13.\end{array}\right.$$

The number N^* of the zeros for the system $f_1=0,f_2=0$ is also x-dependent:

$$N^*=\left\{\begin{array}{ll}3 & \text{for } x\neq -29/13\ ;\\ 2 & \text{for } x=-29/13.\end{array}\right.$$

For $x\neq -29/13$, the normal forms of $g,\ g\cdot y,\ g\cdot z$ and the determinant of the 3×3 Bézout matrix were computed on page 19. For $x=-29/13$, the corresponding 2×2 Bézout matrix has the determinant $144708374/257049\neq 0$. Thus the numerator of the fraction (5.40) is the true eliminant for the system. □

Example 5.5 shows that one cannot ignore exceptional cases, even if it is possible to extend analytically the general expression for $\det\mathbf{B}$: it may cause the loss of a zero.

In the Gröbner basis theory the following result is usually utilized as a foundation for solving the system (2.4) [25], [17]:

Theorem 7.1 (Shape Lemma) *For the radical zero-dimensional ideal $\mathcal{I}$ in general position the Gröbner basis with respect to the lexicographical ordering $x_1\succ\ldots\succ x_L$ has the following structure:*

$$GB(\mathcal{I})=\{x_1-F_1(x_L),x_2-F_2(x_L),\dots,x_{L-1}-F_{L-1}(x_L),F_L(x_L)\}\tag{7.2}$$

where $\{F_1,\dots,F_L\}\subset\mathbf{K}[x_L]$, $\deg F_j<\deg F_L,\ (j=1,\dots,L-1)$.

The words "general position" are clear from the structure of the (7.2): the system (2.4) should not have zeros with equal last components.

Although the Shape Lemma is a perfect theoretical result for investigation of the set of zeros of $\mathcal{I}$, its utility is restricted by a necessity of having the Gröbner basis constructed with respect to the lexicographical ordering; often that is not a simple task. So, in recent publications [2], [12], [34] an approach was suggested consisting of replacing the computations of Gröbner basis under lexicographical ordering with that under the total degree. The underlying ideas were similar to that from the previous subsection (though the relationship to the Bézout method was not mentioned). The eliminant was taken to be equal to

$$\mathcal{U}(x_L) = \mathcal{R}_X^{u-x_L}(f_1, \ldots, f_{L-1}, f_L)\Big|_{u:=x_L}. \tag{7.3}$$

Here the notation $|_{u:=x_L}$ means that we substitute $u := x_L$ after computing the Poisson product. Expression (7.3) also contains information about multiplicity ℓ_j of a zero Λ_j: this zero brings the factor $(x_L - \lambda_{Lj})^{\ell_j}$ into $\mathcal{U}(x_L)$. We will refer to (7.3) as the **true eliminant**.

The advantage of using (7.1) over (7.3) is evident: the number of variables and polynomials used in the Gröbner basis computation decreases by 1. The disadvantage is also clear: in some cases the order and the structure of the Bézout matrix constructed for (7.1) might be non-continuous in the "parameter" x_L.

In order to handle this case, we introduce a new definition. Let $\mathbf{K} = Q[t_1, \ldots, t_p]$, i.e., the coefficients of $f_1, \ldots, f_L, g$ be polynomials in parameters $t_1, \ldots, t_p$. These parameters, while specialized (i.e., assuming some particular values), might influence the performability of a Gröbner basis computation utilized in the previous subsection for the Bézout matrix construction. Indeed, it may happen that we divide by an expression in $t_1, \ldots, t_p$ in order either to make some polynomial monic (i.e. with the leading coefficient equal to 1) or to divide out a common multiple in its coefficients. Every such expression — a polynomial in $t_1, \ldots, t_p$ — will be called a **suspicious factor**. Its vanishing might influence the Poisson product evaluation.

The set of all suspicious factors appearing in the computation of the Gröbner basis $GB(\mathcal{I})$ will be denoted by $SF(GB)$. Obviously $SF(GB) = \emptyset$ if there are no parameters in $f_1, \ldots, f_L$. It is easy to modify a Gröbner basis construction in order to gather suspicious factors. Note that every monic $h(X) \in \mathcal{I}$ (in particular, any appearing in the Gröbner basis construction) can be represented as

$$h_1(X)f_1(X) + \ldots + h_L(X)f_L(X).$$

The coefficients of $h_1, \ldots, h_L$ are the rational functions in $t_1, \ldots, t_p$; their denominators have to be treated as suspicious factors. It is evident that, provided that none of them vanishes, the algorithm from the previous subsection works.

Example 7.10 *Find all the values for the parameter u for which the polynomials*

$$\begin{aligned} f_1 &= y^2z + 2xyu - 2x - z, \ f_2 = 2yzu + xu^2 - x - 2z, \\ f_3 &= -x^3z + 4xy^2z + 4x^2yu + 2y^3u - 10y^2 + 4xz - 10yu + 4x^2 + 2, \\ f_4 &= -xz^3 + 4yz^2u + 4xzu^2 + 2yu^3 + 4xz + 4z^2 - 10yu - 10u^2 + 2 \end{aligned} \tag{7.4}$$

have a common zero.

Solution. Compute the Gröbner basis of $\mathcal{I}(f_1, f_2, f_3)$ over $Q(u)[x, y, z]$ with respect to the total degree ordering $x \succ y \succ z$:

$$\mathrm{Init}(GB) = \left\{2uyz,\ u(3u^2+1)xy,\ (3u^2+1)x^2,\ 6(u+1)(u-1)xz^3, 3u^2(3u^2+1)y^4,\ z^5\right\}$$

provided that none of the factors from

$$SF(GB) = \{u,\ u-1,\ u+1,\ u^2+1/3\}$$

vanishes. Thus, for this case, one may choose the set (7.1):

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

and the system $f_1 = 0, f_2 = 0, f_3 = 0$ (treated with respect to the indeterminates x, y, z) has $N^* = 11$ zeros. The determinant of the 11×11 Bézout matrix equals

$$12^9(u-1)(u+1)(u^2+1)(u^4-10u^2+1)(u^2+1/3)^4(u^2+3)^8. \tag{7.5}$$

Its roots

$$\pm i,\ \pm i\sqrt{3},\ \pm\sqrt{5+2\sqrt{6}},\ \pm\sqrt{5-2\sqrt{6}}$$

give rise to common zeros of (7.4). Those remaining have to be investigated separately, since the corresponding factors are contained in $SF(GB)$. We recompute the Poisson product over the ground fields $Qt(Q[u]/s(u))$ where $s(u)$ is the suspicious factor.

- for $s(u) = u$ ($u = 0$), the 10×10 Bézout matrix is non-singular;
- for $s(u) = u^2 + 1/3$ ($u = \pm i/\sqrt{3}$), the 7×7 Bézout matrix has rank 3;
- for $s(u) = u \pm 1$ ($u = \pm 1$), the Bézout matrix cannot be constructed since the number of common zeros of f_1, f_2 and f_3 becomes infinite.

The true eliminant computed via (7.3) equals

$$\mathcal{U}(u) = (u-1)^9(u+1)^9(u^2+1)(u^4-10u^2+1)(u^2+1/3)^8(u^2+3)^8. \tag{7.6}$$

One may notice the difference in multiplicities with (7.5). □

Multiplicities conjecture. Let SF be the set of suspicious factors obtained from the computation of the Gröbner basis of $\mathcal{I}(f_1, \dots, f_{L-1})$ over $\mathbf{K}[x_L]$, and for every $s(x_L) \in SF$ the $\mathrm{dfc}(s)$ stands for the deficiency index of the Bézout matrix constructed for the specialization $s(x_L) = 0$ (if this construction is possible). Then polynomials (7.1) and (7.3) are connected by the following equality:

$$\mathcal{U}(x_L) = \prod s(x_L)^{\max(\mathrm{mult}(s), \mathrm{dfc}(s))} \tag{7.7}$$

where the product is extended to every suspicious factor from SF and every irreducible factor of the numerator $\mathcal{X}_L(x_L)$ (with mult denoting its multiplicity).

We will call an **extraneous factor** a suspicious one which does not correspond to a zero for the system (2.4). In the last example u was such a factor. The problem of eliminating the extraneous factors is known for several methods for computing the resultant, such as Dixon's or Macaulay's. The advantage of the Bézout method is that it provides a constructive condition for determining whether or not the factor is extraneous (namely it is not in the finite set $SF(GB)$).

7.3 The multiparameter case

Provided that none of the suspicious factors vanishes, the Poisson product gives a necessary and sufficient condition for the system to have a common zero. In order to know what happens if one of the suspicious factors vanishes, we can, in the single parameter case, recompute the Poisson product over the ground field being the quotient field of $Q[t_1]/T(t_1)$ where $T(t_1)$ is the suspicious factor (T_1 should be irreducible because otherwise $Q[t_1]/T_1(t_1)$ is not an integral domain). In this section we show the extra complications that one is faced with in the multiparameter case.

Let $\mathbf{K} = Q[t_1, \dots, t_p], p > 1$ and $T_1(t_1, \dots, t_p)$ be a suspicious factor obtained while computing the Poisson product (2.10). We can proceed by joining this polynomial to the original ones and compute the Poisson product

$$\mathcal{R}^g_{X,t_1}(f_1, \dots, f_L, T_1).$$

This gives a new necessary condition for the existence of a common zero for $f_1, \dots, f_L$ and g — as a polynomial in $t_2, \dots, t_p$, and, probably, a new set of suspicious factors. Let $T_2(t_2, \dots, t_p)$ be one of them. Compute the Poisson product

$$\mathcal{R}^g_{X,t_1,t_2}(f_1, \dots, f_L, T_1, T_2).$$

Finally, after at most p steps, the disjunction of all obtained conditions constitutes a necessary condition, which, however, might be not sufficient.

Example 7.11 *Find all the values for the parameters a, b, c for which the polynomials*

$$f_1 = 2x^2 + axy + y^2 + 4x + c, \quad f_2 = -x^2 + bxy + y^2 - 2x - 3y + 5, \quad g = x - y$$

have a common zero.

Solution. The Gröbner basis computation for $\mathcal{I}(f_1, f_2)$ over $Q(a,b,c)[x,y]$ with respect to the total degree ordering $x \succ y$ furnishes:

$$SF(GB) = \{a + 2b, \mathcal{A}_0 := 2b^2 - a^2 - ab + 9\}, \ M = \begin{cases} \{1, x, y, y^2\} & \text{for } a + 2b \neq 0 \ ; \\ \{1, x, y, xy\} & \text{for } a + 2b = 0. \end{cases}$$

provided that $\mathcal{A}_0 \neq 0$. For $a + 2b \neq 0$, the determinant of the Bézout matrix equals

$$\frac{\varphi_1(a,b,c)}{\mathcal{A}_0}, \text{where } \ \varphi_1(a,b,c) := b^2c^2 + 10b(-ac - c + 8) + 25(a^2 + ac + 10a + 3c + 21) \tag{7.8}$$

while for $a + 2b = 0$ it coincides with the expression obtained from (7.8) via the specialization $a = -2b$.

To treat the case where $\mathcal{A}_0 = 0$, let us compute the Gröbner basis for $\mathcal{I}(f_1, f_2, \mathcal{A}_0)$ over $Q(a,c)[x,y,b]$ with respect to the total degree ordering $x \succ y \succ b$, and find the determinant of the Bézout matrix:

$$SF(GB) = \{a^2 - 12\}, \quad M = \{1, x, y, b, xb, yb\}, \quad \mathcal{R}^g_{x,y,b}(f_1, f_2, \mathcal{A}_0) = \frac{\varphi_2(a,c)}{a^2 - 12}.$$

Here

$$\begin{aligned} \varphi_2(a,c) \quad := \quad & \big[(a+3)(a-3)^2c^4 + 5(2a^3 + 21a^2 - 6a - 180)c^3 + 15(-5a^3 + 33a^2 + 156a + 120)c^2 \\ & +100(-5a^3 + 42a^2 + 441a + 954)c + 100(25a^3 + 465a^2 + 2427a + 4059)\big] \end{aligned}$$

Next, we have to consider the case where $\mathcal{A}_0 = 0, a^2 - 12 = 0$. Compute the Gröbner bases for $\mathcal{I}(f_1, f_2, \mathcal{A}_0, a^2 - 12)$ over $Q(c)[x, y, b, a]$ with respect to the total degree ordering $x \succ y \succ b \succ a$:

$$SF(GB) = \{c+1,\ c+10,\ 13c^2 + 116c + 184\}, \quad M = \{1, x, y, b, a, x\,a, x\,b, y\,a, y\,b, a\,b\},$$

and the Poisson product:

$$\mathcal{R}^g_{x,y,b,a}(f_1, f_2, \mathcal{A}_0, a^2 - 12) = \frac{\varphi_3(c)}{1728(13c^2 + 116c + 184)}$$

where

$$\varphi_3(c) := (c^4 + 20c^3 + 460c^2 + 3600c + 8100)(c^4 + 460c^3 - 1860c^2 - 70400c - 167900).$$

A final check shows that vanishing of any of the suspicious factors does not give rise to a common zero.

Thus a necessary condition for the existence of a common zero is given by

$$\begin{aligned} \varphi_1(a,b,c) &= 0 \wedge \mathcal{A}_0 \neq 0, && (7.9)\\ \bigvee \varphi_2(a,c) &= 0 \wedge \mathcal{A}_0 = 0 \wedge a^2 - 12 \neq 0, && (7.10)\\ \bigvee \varphi_3(c) &= 0 \wedge \mathcal{A}_0 = 0 \wedge a^2 - 12 = 0. && (7.11) \end{aligned}$$

It can readily be verified that this condition is not a sufficient one. Indeed,

$$c^4 + 20c^3 + 460c^2 + 3600c + 8100 \equiv \left(c^2 + 10c + 90(2+\sqrt{3})\right)\left(c^2 + 10c + 90(2-\sqrt{3})\right)$$

and although (7.11) is valid for triples

$$(a,b,c) = \left(2\sqrt{3}, \frac{3+\sqrt{3}}{2}, -5 \pm \sqrt{-90\sqrt{3} - 155}\right),\ (a,b,c) = \left(2\sqrt{3}, \frac{3+\sqrt{3}}{2}, -5 \pm \sqrt{90\sqrt{3} - 155}\right)$$

a common zero exists only for the first specializations.

The condition $\varphi_3(c) = 0 \wedge \mathcal{A}_0 = 0 \wedge a^2 - 12 = 0$ is not a sufficient one, because we only know that $\varphi_3(c) = 0$ is a sufficient condition to let the system $f_1, f_2, g, \mathcal{A}_0, a^2 - 12$ have a common zero in x, y, a, b. Appearantly, the system $f_1, f_2, g, \mathcal{A}_0, a^2 - 12$ imposes conditions on c (for instance that c can be written as rational function in b) that cannot be ignored.

It turns out that the restrictions $\varphi_2(a,c) = 0$ and $\varphi_3(c)$ are particular cases of $\varphi_1(a,b,c) = 0$

$$\varphi_2(a,c) \equiv \frac{\mathcal{R}_b(\varphi_1, \mathcal{A}_0)}{a+3}, \quad \varphi_3(c) \equiv \frac{\mathcal{R}_a(\varphi_2, a^2 - 12)}{-64}.$$

The condition $\varphi_2(a,c) = 0$ is needed to exclude an extraneous condition $a+3 = 0$: $\forall c\ \varphi_1(-3, 0, c) = 0$, however, the common zero exists only for $c = -4$. □

A similar procedure could be designed using specialized Groebner basis. Each suspicious factor stands for a specialization. Again, more than one specialization step might be needed, due to new suspicious factors that may appear during the specialized Gröbner basis computation. We refer to [11] and [18] where the problem of the specialized Gröbner basis is also discussed.

8 Efficiency, applicability, examples

The Bézout matrix has its order bounded by $N := n_1 \cdots n_L$. It is smaller than the matrix from Dixon's method — with the order bounded by $\binom{n\Delta}{n}$, where $\Delta := \max(n_1, \ldots, n_L, m)$. So the order of Bézout matrix is $e^L/\sqrt{L}$ times smaller. However, the Bézout matrix is more complex to construct. Using a Gröbner basis, we face an additional complexity, polynomial in Δ^L.

We have worked out a few more examples using the Computer Algebra system ASIR [24]. For the Gröbner basis computation, the total degree reverse lexicographic ordering $x_1 \succ \ldots \succ x_L \succ x_0$ was used; to check the result we also computed the eliminant via (7.3).

Example 8.12 *Find the eliminant in x_5 for the cyclic 5-roots system*

$$\begin{aligned}
f_1 &= x_1 + x_2 + x_3 + x_4 + x_5 = 0,\\
f_2 &= x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 = 0,\\
f_3 &= x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_5 + x_4x_5x_1 + x_5x_1x_2 = 0,\\
f_4 &= x_1x_2x_3x_4 + x_2x_3x_4x_5 + x_3x_4x_5x_1 + x_4x_5x_1x_2 + x_5x_1x_2x_3 = 0,\\
f_5 &= x_1x_2x_3x_4x_5 - 1 = 0.
\end{aligned} \tag{8.12}$$

Computation of the $GB(\mathcal{I}(f_1, \ldots, f_4))$ does not give suspicious factors. For any value of x_5 the system $f_1 = 0, \ldots, f_4 = 0$ has 18 zeros. The determinant of the 18×18 Bézout matrix equals the true eliminant:

$$(x_5-1)^{10}(x_5^2+3x_5+1)^2(x_5^4-4x_5^3+6x_5^2+x_5+1)^2(x_5^4+x_5^3+6x_5^2-4x_5+1)^2(x_5^4+x_5^3+x_5^2+x_5+1)^{10}.$$

Example 8.13 *Find the eliminant in x_5 for the modified cyclic 5-roots system* [7]*: the polynomials f_1, f_2, f_3, f_5 are the same as in* (8.12)*, but f_4 is replaced by*

$$f_4 = x_2x_3x_4 + x_2x_3x_4x_5 + x_3x_4x_5x_1 + x_4x_5x_1x_2 + x_5x_1x_2x_3.$$

Here $SF(GB) = \{x_5,\ 2x_5-1\}$. The Bézout matrix is smaller (15×15), but the entries are more complicated. The determinant equals a degree 64 polynomial in x_5 (the true eliminant) divided by x_5^5.

Example 8.14 *Find the eliminant in x_0 for the system* [8]*:*

$$\begin{aligned}
f_1 &= x_0 - 1 + 2\textstyle\sum_{j=1}^{n} x_j = 0\ ,\\
f_{k+2} &= x_i - \textstyle\sum_{j=-L}^{L} x_{|k-j|}x_{|j|},\ (k = 0, \ldots, L-1).
\end{aligned} \tag{8.13}$$

Here $SF(GB) = \emptyset$. The determinant of the $2^{L-1} \times 2^{L-1}$ Bézout matrix is the true eliminant of degree 2^L. For example, for the system

$$\begin{aligned}
f_1 &= x_0 + 2x_1 + 2x_2 + 2x_3 - 1 = 0,\\
f_2 &= x_0 - x_0^2 - 2x_3^2 - 2x_2^2 - 2x_1^2 = 0,\\
f_3 &= x_1 - 2x_1x_0 - 2x_2x_3 - 2x_1x_2 = 0,\\
f_4 &= x_2 - 2x_2x_0 - 2x_1x_3 - x_1^2 = 0
\end{aligned} \tag{8.14}$$

[7] This system is used as a benchmark for Gröbner basis computations, and it is considered as much more difficult than the system (8.12)

[8] Known as the Katsura system.

the eliminant equals

$$(3x_0 - 1)(x_0 - 1)(18711x_0^6 - 55728x_0^5 + 67743x_0^4 - 42872x_0^3 + 14805x_0^2 - 2616x_0 + 181).$$

Computations were done for $L = 6, 7, 8$ and 9. For $L \geq 7$, we were only able to compute the determinant modulo a prime number.

The results of our experiments are summarized in the following table. Computing times were measured on a SUN Sparc10 (with 32 Mb) and are reported in seconds (excluding time for garbage collection). The sign ∞ indicates that the computations took more than one day or needed more memory than available.

Example	GB	$\mathbf{B}$	$\det \mathbf{B}$	$\det \mathbf{B}$	$order(\mathbf{B})$
8.12	0.33	2.13	2.19	2.47(17.7)	18
8.13	1.26	9.12	69.1	5.55(57.4)	15
8.14($n = 6$)	5.04	21.0	2120	7.50(469)	32
8.14($n = 7$)	43.3	136	∞	113	64
8.14($n = 8$)	365	1417	∞	1610	128
8.14($n = 9$)	3180	13066	∞	24911	256

The columns 1, 2 and 3 correspond to the Gröbner basis computation, the Bézout matrix construction, and the determinant evaluation respectively. Column 4 gives the time needed for evaluating the determinant modulo a prime number (that in parentheses corresponds to the method using modular computations and lifting); these computations were done using SACLIB. One sees that the Gröbner basis computation and the Bézout matrix construction do not contribute much to the total computation time. The bottleneck is the evaluation of the determinant. Some other examples can be found in [8].

9 Separation of zeros

Let us illuminate here a relationship of the Bézout method with that using block Hankel matrices [31], [32]. This allows one to employ the method for the separation of the zeros of a polynomial system. We will assume here that $\mathbf{K} = \mathbf{R}$.

We first start with the consideration of the univariate case in the notation of Section 3. Construct the following Laurent expansions

$$\frac{1}{f(x)} = \sum_{k=n-1}^{\infty} \frac{d_k}{x^{k+1}}, \quad \frac{g(x)}{f(x)} = \mathbf{L}(\mathbf{x}) + \sum_{k=0}^{\infty} \frac{c_k}{x^{k+1}}. \tag{9.15}$$

The coefficients of the first expansion can be determined by the recurrence formulae

$$d_k = \begin{cases} 1/a_0 & \text{if } k = n-1 \ ; \\ -(d_{n-1}a_1)/a_0 & \text{if } k = n \ ; \\ -(d_{k-1}a_1 + d_{k-2}a_2 + \ldots + d_{n-1}a_{k-n+1})/a_0 & \text{if } k < 2n-1 \ ; \\ -(d_{k-1}a_1 + d_{k-2}a_2 + \ldots + d_{k-n}a_n)/a_0 & \text{if } k \geq 2n-1 \end{cases}$$

while those of the second one can be obtained on multiplication by $g(x)$:

$$c_k = \begin{cases} d_{k+m}b_0 + d_{k+m-1}b_1 + \ldots + d_{n-1}b_{k+m-n+1} & \text{if } k < n-1 \ ; \\ d_{k+m}b_0 + d_{k+m-1}b_1 + \ldots + d_k b_m & \text{if } k \geq n-1. \end{cases} \tag{9.16}$$

On the other hand, these coefficients turn out to be symmetric rational functions of the zeros $\lambda_1, \dots, \lambda_n$ of $f(x)$. Provided that all the zeros are distinct, the Lagrange formulae are valid

$$\sum_{j=1}^{n} \frac{\lambda_j^k g(\lambda_j)}{f'(\lambda_j)} = c_k \qquad \sum_{j=1}^{n} \frac{\lambda_j^k}{f'(\lambda_j)} = \begin{cases} d_k & \text{if } k \geq n-1 \ ; \\ 0 & \text{if } k < n-1. \end{cases} \tag{9.17}$$

Consider the following $n \times n$ Hankel matrices

$$D = \begin{pmatrix} 0 & 0 & \dots & 0 & d_{n-1} \\ 0 & 0 & \dots & d_{n-1} & d_n \\ \dots & & & & \dots \\ 0 & d_{n-1} & \dots & & d_{2n-3} \\ d_{n-1} & d_n & \dots & d_{2n-3} & d_{2n-2} \end{pmatrix}, \quad C = \begin{pmatrix} c_0 & c_1 & \dots & c_{n-2} & c_{n-1} \\ c_1 & c_2 & \dots & c_{n-1} & c_n \\ \dots & & & & \dots \\ c_{n-2} & c_{n-1} & & c_{2n-4} & c_{2n-3} \\ c_{n-1} & c_n & \dots & c_{2n-3} & c_{2n-2} \end{pmatrix} \tag{9.18}$$

and denote by $\mathbf{B}_g$ the matrix obtained from the Bézout matrix (3.2) on reordering its columns:

$$\mathbf{B}_g := [b_{k,n-1-j}]_{k,j=0}^{n-1} \ . \tag{9.19}$$

Theorem 9.2 *The matrices* (9.18) *and* (9.19) *are connected by the following equality:*

$$\mathbf{B}_g D = C. \tag{9.20}$$

Proof. Assuming firstly that all the zeros are distinct, substitute them in the remainders $g_k(x)$:

$$g_k(\lambda_j) = b_{k,n-1} + b_{k,n-2}\lambda_j + \dots + b_{k0}\lambda_j^{n-1} = \lambda_j^k g(\lambda_j) \quad (j = 1, \dots, n; \ k = 0, \dots, n-1).$$

Rewrite these equalities in the matrix form:

$$\mathbf{B}_g \begin{pmatrix} 1 & \dots & 1 \\ \lambda_1 & \dots & \lambda_n \\ \dots & & \dots \\ \lambda_1^{n-1} & \dots & \lambda_n^{n-1} \end{pmatrix} = \begin{pmatrix} 1 & \dots & 1 \\ \lambda_1 & \dots & \lambda_n \\ \dots & & \dots \\ \lambda_1^{n-1} & \dots & \lambda_n^{n-1} \end{pmatrix} \begin{pmatrix} g(\lambda_1) & \dots & \mathbf{O} \\ & \ddots & \\ \mathbf{O} & \dots & g(\lambda_n) \end{pmatrix}$$

Multiplying this from the right by the matrix

$$\begin{pmatrix} 1/f'(\lambda_1) & \lambda_1/f'(\lambda_1) & \dots & \lambda_1^{n-1}/f'(\lambda_1) \\ 1/f'(\lambda_2) & \lambda_2/f'(\lambda_2) & \dots & \lambda_2^{n-1}/f'(\lambda_2) \\ \dots & & & \dots \\ 1/f'(\lambda_n) & \lambda_n/f'(\lambda_n) & \dots & \lambda_n^{n-1}/f'(\lambda_n) \end{pmatrix}$$

and using the Lagrange formulae (9.17) we get the result claimed.

Lemma 4.1 allows to extend the result to the case of the existence of a multiple zero. □

Corollary 1 *The leading principal minors of the matrices* $\mathbf{B}$ *and* C *are connected by the equality*

$$\mathbf{B}_j = C_j a_0^j. \tag{9.21}$$

Thus, the Bézout matrix turns out to be "almost" symmetric. The Hankel matrix C is the matrix from Kronecker's theorem on the $\gcd(f,g)$ [32]. Taking into account equality (9.21) let us introduce analogues of the inertia indices and the signature for the (nonsymmetric) Bézout matrix:

$$n_+(\mathbf{B}_g) := P(1, \mathbf{B}_1, \dots, \mathbf{B}_r), \ n_-(\mathbf{B}_g) := V(1, \mathbf{B}_1, \dots, \mathbf{B}_r), \ \sigma(\mathbf{B}_g) := n_+(\mathbf{B}_g) - n_-(\mathbf{B}_g).$$

Here $r = \operatorname{rank} \mathbf{B}$ and P (or V) is the number of permanences (or variations) of sign.[9] For the choice $g(x) := f'(x)$ the signature of the corresponding Hankel matrix gives one the **number** of distinct **real zeros** for $f(x)$

$$\sigma(\mathbf{B}_{f'}) = \operatorname{nrz}\{f(x) = 0\}.$$

This is an analogue of Jacobi's theorem. Now construct the Bézout matrix for the polynomial $f'(x)g(x)$:

$$\mathbf{B}_{f'g} = \mathbf{B}_{f'}\mathbf{B}_g = \mathbf{B}_g\mathbf{B}_{f'}.$$

Then, provided that $\det \mathbf{B}_{f'g} \neq 0$, one has

$$n_+(\mathbf{B}_{f'g}) - n_-(\mathbf{B}_{f'}) = \operatorname{nrz}\{f(x) = 0 \mid g(x) > 0\}$$

(an analogue of the Hermite–Sylvester theorem). Taking here $g(x) := x - t$, one then obtains a counterpart of the Joachimsthal theorem [19],[33], i.e. a system of polynomials which can be treated as the Sturm sequence for $f(x)$:

Theorem 9.3 *Let* $\mathbf{B}$ *be the matrix* (3.2) *constructed for* $g(x) = f'(x)$ *and* $r = \operatorname{rank}\mathbf{B}$. *Then*

$$\operatorname{nrz}\{f(x) = 0 \mid a < x < b\} = V(1, \Delta_1(a), \dots, \Delta_r(a)) - V(1, \Delta_1(b), \dots, \Delta_r(b)).$$

Here

$$\Delta_k(x) = \begin{vmatrix} b_{00} & \dots & b_{0,k-1} & 1 \\ b_{1,0} & \dots & b_{1,k-1} & x \\ \dots & & & \dots \\ b_{k,0} & \dots & b_{k,k-1} & x^k \end{vmatrix}$$

and $\Delta_n(x) = f(x) \det \mathbf{B}/a_0$.

Consider the bivariate case; we begin with the assumption that the resultant $\mathcal{A}_0$ given by (5.29) does not vanish. Compute both eliminants $\mathcal{X}(x) = \mathcal{R}_y(f_1, f_2)$ and $\mathcal{Y}(y) = \mathcal{R}_x(f_1, f_2)$ together with the polynomials of their linear representations:

$$\mathcal{M}(x,y)f_1(x,y) + \mathcal{N}(x,y)f_2(x,y) \equiv \mathcal{X}(x), \quad \mathcal{P}(x,y)f_1(x,y) + \mathcal{Q}(x,y)f_2(x,y) \equiv \mathcal{Y}(y).$$

All the polynomials can be constructed with the aid of Theorem 3.1. Using the estimations for their degrees from this theorem, we can deduce for the function

$$\mathcal{V}(x,y) = \mathcal{M}(x,y)\mathcal{Q}(x,y) - \mathcal{N}(x,y)\mathcal{P}(x,y)$$

the following bounds :

$$\deg \mathcal{V} \leq 2N - n_1 - n_2, \ \deg_x \mathcal{V} \leq N - 1, \ \deg_y \mathcal{V} \leq N - 1. \tag{9.22}$$

With the aid of the expansions of the type (9.15), expand the following fractions in the negative powers of x and y :

$$\frac{\mathcal{V}(x,y)}{\mathcal{X}(x)\mathcal{Y}(y)} = \sum_{j,k=0}^{\infty} \frac{d_{jk}}{x^{j+1}y^{k+1}}, \quad \frac{g(x,y) \cdot \mathcal{V}(x,y)}{\mathcal{X}(x) \cdot \mathcal{Y}(y)} = \mathbf{L}(x,y) + \sum_{j,k=0}^{\infty} \frac{c_{jk}}{x^{j+1}y^{k+1}} \tag{9.23}$$

[9] If some minors vanish, one can use the rule similar to that by Frobenius for computing the signature for a Hankel matrix [14].

Here $\mathbf{L}(x,y)$ is of the form $[A(x,y)\mathcal{X}(x)+B(x,y)\mathcal{Y}(y)]/[\mathcal{X}\mathcal{Y}]$, with $\{A,B\}\subset\mathbf{R}[x,y]$. We will be interested however only in the coefficients of the terms with negative powers of both variables. These coefficients turn out to be symmetric rational functions of the zeros $\Lambda_j=(\alpha_j,\beta_j)$ of $f_1=0, f_2=0$:

Theorem 9.4 (Jacobi) *If $\mathcal{J}(\alpha_p,\beta_p)\neq 0$ for all $p=1,\ldots,N$ (i.e., all zeros are simple), then*

$$\sum_{p=1}^{N}\frac{\alpha_p^j\beta_p^k}{\mathcal{J}(\alpha_p,\beta_p)} = \begin{cases} d_{jk} & \text{if } j+k\geq n_1+n_2-2\ ; \\ 0 & \text{if } j+k<n_1+n_2-2 \end{cases} \tag{9.24}$$

$$\sum_{p=1}^{N}\frac{\alpha_p^j\beta_p^k g(\alpha_p,\beta_p)}{\mathcal{J}(\alpha_p,\beta_p)} = c_{jk}. \tag{9.25}$$

Here the second of equalities (9.24) follows from the bounds (9.22).

Construct the $N\times N$ block Hankel matrices D and C:

$$D := [D_{p,\ell}]_{p,\ell=0}^{n_1-1}, \quad \text{where } D_{p,\ell}:=[d_{p+\ell,j+k}]_{j,k=0}^{n_2-1} \tag{9.26}$$

$$C := [C_{p,\ell}]_{p,\ell=0}^{n_1-1}, \quad \text{where } C_{p,\ell}:=[c_{p+\ell,j+k}]_{j,k=0}^{n_2-1} \tag{9.27}$$

and denote by $\mathbf{B}_g$ the Bézout matrix (4.6) constructed for the purely lexicographical ordering $(y\succ x)$ for the power products μ_j from the set (4.1).

Theorem 9.5 *The matrices* (9.26), (9.27) *and* $\mathbf{B}_g$ *are related by the equality* (9.20).

Proof. Assuming firstly that all the zeros $\Lambda_j=(\alpha_j,\beta_j)$ are distinct, multiply equality (4.5) from the right by the matrix

$$\left(\begin{array}{ccc} \mu_1(\Lambda_1)/\mathcal{J}(\Lambda_1) & \ldots & \mu_N(\Lambda_1)/\mathcal{J}(\Lambda_1) \\ \ldots & & \ldots \\ \mu_1(\Lambda_N)/\mathcal{J}(\Lambda_N) & \ldots & \mu_N(\Lambda_N)/\mathcal{J}(\Lambda_N) \end{array}\right).$$

Using equalities (9.24) and (9.25) we get the result claimed. Extension to the case of the existence of a multiple zero can be done via application of Lemma 4.1. □

Application of Theorem 9.5 to the zero localization problem proceeds in a manner similar to the univariate case. Construct the Bézout matrices $\mathbf{B}_{\mathcal{J}}$ and $\mathbf{B}_{\mathcal{J}\cdot g}$. From the equalities (9.20) and (9.25) we obtain

$$\mathbf{B}_{\mathcal{J}}D=S, \quad \mathbf{B}_{\mathcal{J}\cdot g}D=\mathbf{B}_gS=H. \tag{9.28}$$

Here S and H are block Hankel matrices with a structure similar to (9.27):

$$S := [S_{p,\ell}]_{p,\ell=0}^{n_1-1}, \quad \text{where } S_{p,\ell}:=[s_{p+\ell,j+k}]_{j,k=0}^{n_2-1}, \quad s_{j,k}:=\sum_{p=1}^{N}\alpha_p^j\beta_p^k$$

$$H := [H_{p,\ell}]_{p,\ell=0}^{n_1-1}, \quad \text{where } H_{p,\ell}:=[h_{p+\ell,j+k}]_{j,k=0}^{n_2-1}, \quad h_{j,k}:=\sum_{p=1}^{N}\alpha_p^j\beta_p^k g(\alpha_p,\beta_p)$$

Theorem 9.6 *Provided conditions* (5.30) *are fulfilled, one has:*

$$\operatorname{nrz}\{f_1(x,y)=0, f_2(x,y)=0\}=\sigma(S).$$

If, in addition, $\det H\neq 0$*, then all zeros are distinct and*

$$\operatorname{nrz}\{f_1(x,y)=0, f_2(x,y)=0 \mid g(x,y)>0\}=n_+(H)-n_-(S).$$

One can find the proof of this theorem in [32]. The inertia indices for the matrices S and H can be computed via their leading principal minors. Some of the latter are connected with the minors of the corresponding Bézout matrices via the formulae similar to (9.21). To deduce them, let us detail the structure for the matrix D. Now choose the total degree ordering for the power products of the set (4.1). This causes interchanging of the rows and columns in the matrices $\mathbf{B}_g$, D and C. Because of the equalities (9.24), matrix D takes a very specific form. For the case $n_1 = 3, n_2 = 5$ (the set M was given by (5.18))

$$D = \left(\begin{array}{cccccccccc}
 & & & & & & & & & d_{2,4} \\
 & & & & & & & & d_{1,5}d_{2,4} & \\
 & & & & & & & & d_{2,4}d_{3,3} & \\
 & & \mathbf{O} & & & & & d_{0,6}d_{1,5}d_{2,4} & & \\
 & & & & & & & d_{1,5}d_{2,4}d_{3,3} & & \\
 & & & & & & & d_{2,4}d_{3,3}d_{4,2} & & \\
 & & & & d_{0,6}d_{1,5}d_{2,4} & & & & & \\
 & & & & d_{1,5}d_{2,4}d_{3,3} & & & & & \\
 & & & & d_{2,4}d_{3,3}d_{4,2} & & & & & \\
 & & d_{0,6}d_{1,5}d_{2,4} & & & & & & & \\
 & & d_{1,5}d_{2,4}d_{3,3} & & & & & & & \\
 & & d_{2,4}d_{3,3}d_{4,2} & & & & & & & \\
 & d_{1,5}d_{2,4} & & & & & * & & & \\
 & d_{2,4}d_{3,3} & & & & & & & & \\
d_{2,4} & & & & & & & & &
\end{array} \right)$$

Matrix entries d_{jk} denoted by $*$ have indices with $j + k > n_1 + n_2 - 2 = 6$. Hence,

$$\det D = d_{2,4}^2 \left| \begin{array}{cc} d_{1,5} & d_{2,4} \\ d_{2,4} & d_{3,3} \end{array} \right|^2 \left| \begin{array}{ccc} d_{0,6} & d_{1,5} & d_{2,4} \\ d_{1,5} & d_{2,4} & d_{3,3} \\ d_{2,4} & d_{3,3} & d_{4,2} \end{array} \right|^3 .$$

Theorem 9.7 *For the case $n_1 \le n_2$ we obtain the following formula*

$$\det D = \Upsilon = (-1)^{n_1(n_1-1)/2} \left[D_1^* D_2^* \dots D_{n_1-1}^* \right]^2 \left[D_{n_1}^* \right]^{n_2-n_1+1} . \tag{9.29}$$

Here D_k^* is the order k minor of the matrix

$$\left(\begin{array}{cccc} d_{0,n_1+n_2-2} & d_{1,n_1+n_2-3} & \dots & d_{n_1-1,n_2-1} \\ d_{1,n_1+n_2-3} & d_{2,n_1+n_2-4} & \dots & d_{n_1,n_2-2} \\ \dots & & & \dots \\ d_{n_1-1,n_2-1} & d_{n_1,n_2-2} & \dots & d_{2n_1-2,n_2-n_1} \end{array} \right) \tag{9.30}$$

standing in its upper right corner.

Further investigation of the $\det D$ concerns the elements $d_{j\ell}$ with $j + \ell = n_1 + n_2 - 2$. It turns out that they depend only on the coefficients of f_{1,n_1} and f_{2,n_2}:

Theorem 9.8 *One has:*

$$d_{j\ell} = (-1)^{n_1(n_1+1)/2+1} v_j / \mathcal{A}_0 \quad \text{for} \quad j + \ell = n_1 + n_2 - 2.$$

Here v_j is the coefficient of $x^j y^{n_1+n_2-2-j}$ in the development of

$$\left|\begin{array}{llllll}
a_{n_1,0} & a_{n_1-1,1} & \ldots & a_{0,n_1} 0 & & \ldots 0 \\
 & & & \ldots & & \ldots \\
0 & \ldots & 0 & 0 \quad a_{n_1,0} & a_{n_1-1,1} & \ldots a_{0,n_1} \\
0 & \ldots & 0 & b_{n_2,0} b_{n_2-1,1} b_{n_2-2,2} & \ldots & b_{0,n_2} \\
 & \ldots & & & \ldots & \\
b_{n_2,0} & b_{n_2-1,1} & b_{n_2-2,2} & \ldots \quad b_{0,n_2} & 0 & \ldots 0 \\
y^{n_1+n_2-2} & (xy^{n_1+n_2-3}) & (x^2 y^{n_1+n_2-3}) \ldots & & \ldots & x^{n_1+n_2-2}
\end{array}\right|
\begin{array}{l}
\left.\begin{array}{l} \\ \\ \\ \end{array}\right\} n_2 - 1 \ \mathit{rows} \\
\left.\begin{array}{l} \\ \\ \\ \end{array}\right\} n_1 - 1 \ \mathit{rows} \\
\\
\end{array}$$

The minor D_k^* has a surprising relationship to the minor (5.35) of the resultant $\mathcal{A}_0$:

Theorem 9.9 *One has:*

$$D_k^* = \frac{\mathcal{R}_k^*(\mathcal{A}_0)}{\mathcal{A}_0} \ (k = 1, \ldots, n_1 - 1); \quad D_{n_1}^* = \frac{1}{\mathcal{A}_0} \tag{9.31}$$

Theorems 9.7 and 9.9 proved the structure of the Υ given by formula (5.31). If one had constructed the matrices $\mathbf{B}_g$, D and C for the choice of the set (5.28), one would have obtained the corresponding minors equal to the leading principal ones of the (9.30):

$$D_k^* = [d_{i+j,n_1+n_2-2-i-j}]_{i,j=0}^{k-1} = \frac{\mathcal{R}_k(\mathcal{A}_0)}{\mathcal{A}_0} \quad (k = 1, \ldots, n_1 - 1).$$

Theorem 9.10 *For the orders*

$$\left\{\frac{k(k-1)}{2}\right\}_{k=2}^{n_1}, \quad \left\{\frac{n_1(n_1-1)}{2} + n_1\ell\right\}_{\ell=1}^{n_2-n_1+1}, \quad \left\{n_1 n_2 - \frac{(n_1-p)(n_1-p-1)}{2}\right\}_{p=1}^{n_1-1},$$

the leading principal minors of the matrix (9.27) *are just factors of the minors standing in the upper right corner of the Bézout matrix* $\mathbf{B}_g$.

Proof. Indeed, due to specifical structure of matrix D, one obtains (via application of the Cauchy – Binet formula) the following relationships between these minors

$$D_1^* b_{1,N} = C_1, \ D_1^* D_2^* \left|\begin{array}{lll} b_{1,N-2} & b_{1,N-1} & b_{1,N} \\ b_{2,N-2} & b_{2,N-1} & b_{2,N} \\ b_{3,N-2} & b_{3,N-1} & b_{3,N} \end{array}\right| = C_3, \ldots, \frac{\det D}{D_1^*} \mathbf{B}_{N1} = C_{N-1}, \ \det D \det \mathbf{B}_g = C_N.$$

Other minors of matrix C can be obtained as linear combinations of some minors of matrix $\mathbf{B}_g$, with the coefficients depending only on those of the leading forms f_{1,n_1} and f_{2,n_2}. □

This simplifies computations for Theorem 9.6. One may obtain a bivariate analogue of Theorem 9.3 by setting $g(x, y) = \mathcal{J}(x, y)(x - t)(y - u)$.

10 Conclusions

We have treated Bézout's method for computing the resultant of multivariate polynomials $f_1(X), \ldots, f_L(X), g(X)$. The idea of the method consists of replacing the division algorithm that works for the univariate case by the reduction algorithm with respect to an appropriate power product set. The reduction procedure was given for the generic case when this set of power products can be predicted a priori only via consideration of the leading forms of the polynomials. For the non-generic cases the Gröbner base technique can be used for choosing the set of power products, as well as for proving the general results.

We have compared Bézout's method with Macaulay's and shown some of its applications:

a) for solving system of equations, i.e. for finding an eliminant and for deducing formulae connecting its roots with the zeros of the system (an analogue of the Shape Lemma);

b) for the zero separation problem;

c) for finding polynomials satisfying the Bézout identity.

Some advantages of the method:

a) the resultant-matrix (Bézout's matrix) is square of order never exceeding Bézout's bound (i.e. for $\mathcal{R}(f_1, \ldots, f_L, g)$ it is $\le \deg f_1 \ldots \deg f_L$);

b) for the generic case one does not obtain extraneous factors, while for the non-generic case, the procedure to extract them was worked out;

c) at least for some known examples, the method is more effective than that of using the Gröbner bases under lexicographical ordering.

Several problems have remained for further investigation. Rank, Choice and Multiplicities conjectures from Sections 4, 5.2 and 7.2 respectively have to be verified.

While working on the present investigation we have passed on the usual way of the reader of the classics: one's attitude develops from curiosity to admiration.

AI Appendix I. Bézout's construction for the eliminant

In presentation of the algorithm we follow [23] and [28]; we keep the style and do not comment on the performability of some steps, merely inserting the word *generic* in some places.

AI.1 Counting the power products

Theorem AI.1 *The number of power products of a degree m from L variables equals*

$$N(L,m) := \binom{L+m-1}{n-1}.$$

(We set $N(0,m) = N(L,0) = N(0,0) = 1$ for $m > 0, L > 0$, and $N(L,m) = 0$ for $L < 0$ or $m < 0$). Furthermore, the number of those

(1) *not divisible by $x_1^{n_1}$ equals*

$$\Delta_{n_1} N(L,m) := N(L,m) - N(L, m-n_1);$$

(2) *not divisible by $x_1^{n_1}$ and $x_2^{n_2}$ equals*

$$\Delta_{n_2}\Delta_{n_1} N(L,m) := \Delta_{n_1} N(L,m) - \Delta_{n_1} N(L, m-n_2);$$

(3) *not divisible by any of $x_1^{n_1}, x_2^{n_2}, \ldots, x_k^{n_k}$ equals*

$$\Delta_{n_k}\Delta_{n_{k-1}} \ldots \Delta_{n_1} N(L,m) := \Delta_{n_{k-1}} \ldots \Delta_{n_1} N(L,m) - \Delta_{n_{k-1}} \ldots \Delta_{n_1} N(L, m-n_k).$$

Proof. The part (1) follows from the fact that any power product $\mu(X)$ of a degree m divisible by $x_1^{n_1}$ can be represented as $x_1^{n_1}\mu_1(X)$ where $\mu_1(X)$ is a power product of degree $m-n_1$.

If we denote by $\mathbf{N}(L,m)$ the number of power products of degree m not divisible by any of the

$$x_1^{n_1}, x_2^{n_2}, \ldots, x_{k-1}^{n_{k-1}} \tag{AI.1}$$

then the number of those divisible by $x_k^{n_k}$ equals $\mathbf{N}(L, N-n_k)$. Thus the number of power products of degree m not divisible by any of the

$$x_1^{n_1}, x_2^{n_2}, \ldots, x_{k-1}^{n_{k-1}}, x_k^{n_k} \tag{AI.2}$$

equals

$$\Delta_{n_k}\mathbf{N}(L,m) := \mathbf{N}(L,m) - \mathbf{N}(L, m-n_k).$$

Induction completes the proof of part (3). □

Corollary 1 *The set M defined by* (4.1) *contains exactly*

$$N(L,m) - \sum_{1\le j\le L} N(L, m-n_j) + \sum_{1\le j_1<j_2\le L} N(L, m-n_{j_1}-n_{j_2}) - \ldots + (-1)^L N(L, m-n_1-n_2-\ldots-n_L) \tag{AI.3}$$

power products of degree m.

Theorem AI.2 *The following inequality is true :*

$$\sum_{1\le j\le k} N(L, m-n_j) \ge N(L,m) - \Delta_{n_k}\Delta_{n_{k-1}}\ldots\Delta_{n_2}\Delta_{n_1}N(L,m) \tag{AI.4}$$

(generally this inequality is strict).

Remark. All the above results can be reformulated for the problem of counting the terms of a polynomial $V(x_1, x_2, \ldots, x_L)$: in the computations just given one should replace L by $L+1$. Evidently the number of terms of V not divisible by any of the $x_1^{n_1}, \ldots, x_L^{n_L}$ equals

$$N = n_1 n_2 \cdots n_L \tag{AI.5}$$

since all these terms have power products in the set M.

AI.2 Reduction of a polynomial

Consider the polynomials

$$f_1(x_1, \ldots, x_L), \ldots, f_k(x_1, \ldots, x_L) \quad (\deg f_j = n_j,\ k \le L) \tag{AI.6}$$

Theorem AI.3 *A generic polynomial $P(x_1, \ldots, x_L)$ can be reduced modulo $f_1, \ldots, f_k$ with respect to the set*

$$M^{(k)} = \{x_1^{p_1}\cdots x_k^{p_k} \mid 0 \le p_1 < n_1, \ldots, 0 \le p_k < n_k\}.$$

Proof. The statement is equivalent to: there exist polynomials $A_1(x_1, \ldots, x_L), \ldots, A_k(x_1, \ldots, x_L)$ and $P_1(x_1, \ldots, x_L)$, the latter not containing the terms divisible by any of the $x_1^{n_1}, \ldots, x_k^{n_k}$, such that

$$P + A_1 f_1 + A_2 f_2 + \ldots + A_k f_k \equiv P_1. \tag{AI.7}$$

For $k = 1$ that is a triviality. Let $k > 1$. Polynomials A_j are supposed to have indeterminate coefficients. If $\deg P = m$, then one should take $\deg A_j = m - n_j$ (if $m < n_j$, then $A_j \equiv 0$). The number of indeterminate coefficients on the left-hand side of (AI.7) equals

$$N(L+1, m-n_1) + N(L+1, m-n_2) + \ldots + N(L+1, m-n_k),$$

and this polynomial is of degree m with total number of terms equal to $N(L+1, m)$. By Theorem AI.1, among these terms there are

$$\Delta_{n_k}\Delta_{n_{k-1}}\ldots\Delta_{n_2}\Delta_{n_1}N(L+1, m)$$

of those not divisible by any of (AI.2). Thus the number of coefficients of terms on the left-hand side of (AI.7) to be equated to zero equals

$$N(L+1, m) - \Delta_{n_k}\Delta_{n_{k-1}}\ldots\Delta_{n_2}\Delta_{n_1}N(L+1, m).$$

We have obtained the system of linear homogeneous equations for determination of the indeterminate coefficients. By formula (AI.4), the number of these coefficients is greater than the number of linear equations. Such a system, *in general*, is consistent. □

AI.3 Elimination. Bézout's theorem

Now consider the polynomial system

$$f_1(x_1, \ldots, x_L) = 0, \ldots, f_L(x_1, \ldots, x_L) = 0 \quad (\deg f_j = n_j) \tag{AI.8}$$

By Theorem AI.3, we can reduce any of the $x_1^{n_1}, x_2^{n_2}, \ldots, x_{L-1}^{n_{L-1}}$ with respect to the set

$$M^{(L-1)} = \{x_1^{p_1}\cdots x_{L-1}^{p_{n-1}} \mid 0 \le p_1 < n_1, \ldots, 0 \le p_{L-1} < n_{L-1}\}.$$

Let $A_L(x_1, \ldots, x_L)$ be a polynomial of degree $m - n_L$ with yet undefined m. We will show that by a suitable selection of the polynomial A_L it is possible to reduce $A_L f_L$ with respect to the set $M^{(L-1)}$ modulo $f_1, \ldots, f_{L-1}$; the reduction will be a polynomial $F(x_L)$ depending on the single variable x_L.

Being a polynomial of degree m, $A_L f_L$ has $N(L+1, m)$ terms. By Theorem AI.3, one can choose polynomials $A_1, \ldots, A_{L-1}$ ($\deg A_j = m - n_j$) such that the linear combination

$$A_1 f_1 + \ldots + A_{L-1} f_{L-1} + A_L f_L \tag{AI.9}$$

will not contain the terms divisible by any of the

$$x_1^{n_1}, x_2^{n_2}, \ldots, x_{L-1}^{n_{L-1}}. \tag{AI.10}$$

Then by Theorem AI.1 the number of terms in (AI.9) equals $\Delta_{n_{L-1}}\ldots\Delta_{n_2}\Delta_{n_1}N(L+1, m)$. Now A_L has to be chosen such that all the other terms vanish except for those containing only powers of x_L. So the number of terms to be excluded equals

$$\Delta_{n_{L-1}}\ldots\Delta_{n_2}\Delta_{n_1}N(L+1, m) - (m+1). \tag{AI.11}$$

Let us choose A_L in the set of polynomials reduced with respect to the set $M^{(L-1)}$, i.e., with none of its terms divisible by any from (AI.10). Thus by Theorem AI.1 the number of its terms equals $\Delta_{n_{L-1}}\ldots\Delta_{n_2}\Delta_{n_1}N(L+$

$1, m-n_L)$. One of the coefficients of A_L can be fixed. Therefore the total number of coefficients at our disposal equals

$$\Delta_{n_{L-1}} \dots \Delta_{n_2} \Delta_{n_1} N(L+1, m-n_L) - 1. \tag{AI.12}$$

If we succeed now in finding the degree m such that the numbers (AI.11) and (AI.12) are equal, then the problem stated at the beginning of the subsection will be solved (the number of coefficients of A_L will be equal to that of the terms of $A_L f_L$ to be excluded). To determine this m we obtain the following equation

$$\begin{aligned} m &= \Delta_{n_{L-1}} \dots \Delta_{n_2} \Delta_{n_1} N(L+1, m) - \Delta_{n_{L-1}} \dots \Delta_{n_2} \Delta_{n_1} N(L+1, m-n_L) \\ &= \Delta_{n_L} \Delta_{n_{L-1}} \dots \Delta_{n_2} \Delta_{n_1} N(L+1, m) \end{aligned}$$

But the latter equals (AI.5), so $m = N = n_1 n_2 \dots n_L$. Thus $\deg F(x_L) = N$ and this completes the proof of the celebrated "Bézout's theorem". □

It is to be proved, however, that the linear system for determination of the coefficients of A_L is consistent in principle, at least for *generic* polynomials. Non-vanishing of its determinant containing the coefficients of f_L provides a sufficient condition. If at least for a particular choice of f_L this condition is fulfilled, then it cannot also be violated for the *generic* case.

Example AI.1 *Find the eliminant in x_L for the system*

$$x_1^{n_1} - a = 0, x_2^{n_2} - x_1 = 0, x_3^{n_3} - x_2 = 0, \dots, x_L^{n_L} - x_{L-1} = 0.$$

Solution. Here one may take

$$\begin{aligned} A_1 := 1,\ A_2 &:= x_2^{n_2(n_1-1)} + x_2^{n_2(n_1-2)} x_1 + \dots + x_1^{n_1-1}, \\ A_3 &:= x_3^{n_3(n_1 n_2-1)} + x_3^{n_3(n_1 n_2-2)} x_2 + \dots + x_2^{n_1 n_2-1}, \\ &\dots \\ A_L &:= x_L^{(m'-1)n_L} + x_{L-1} x_L^{(m'-2)n_L} + \dots + x_L^{m'-1} \end{aligned}$$

where $m' = N/n_L$. Indeed

$$A_1 f_1 + \dots + A_{L-1} f_{L-1} + A_L f_L \equiv x_L^N - a. \tag{AI.13}$$

Thus for this case the eliminant equals just $x_L^N - a$. □

The existence of a solution (with respect to a polynomial A_L) to the identity (AI.13) is not enough to establish the non-vanishing of the corresponding determinant, since the uniqueness is additionally needed. This was not proved (though examples confirm this).

AII Appendix II. Theorem on the unessentiality of algebraic inequalities

We give here a translation of one result from the book [13] which was used in Section 4.

Let $\mathbf{K}[y_1, \dots, y_s]$ be a polynomial ring over the commutative ring $\mathbf{K}$ with unity.

Definition. Polynomials $F_1, F_2 \in \mathbf{K}[y_1, \ldots, y_s]$ are said to be equal **identically** (functionally) over $\mathbf{K}$ ($F_1 \equiv_{\mathbf{K}} F_2$) if their values coincide at any point $(y_1, \ldots, y_s) \in \mathbf{K}^s$. These polynomials are said to be equal **formally** if their sets of terms coincide.

Definition. A ring $\mathbf{K}$ is referred to as an integral domain (domain of integrity) iff $a_1 a_2 = 0 \Longleftrightarrow a_1 = 0$ or $a_2 = 0$.

Theorem AII.1 *If $\mathbf{K}$ is an integral domain, then $\mathbf{K}[y]$ will also be an integral domain.*

Proof. Let $f(y) = a_0 y^n + \ldots + a_n$, $g(y) = b_0 y^m + \ldots + b_m$ be from $\mathbf{K}[y]$. If $a_0 \neq 0, b_0 \neq 0$, then the product $f(y)g(y)$ contains a non-zero term $a_0 b_0 y^{n+m}$. Thus, $f(y)g(y)$ is a formally-zero polynomial iff any of $f(y)$ or $g(y)$ is a formally-zero polynomial. □

Corollary 2 *If $\mathbf{K}$ is a field, then $\mathbf{K}[y]$ is an integral domain.*

Theorem AII.2 *The polynomial ring $\mathbf{K}[y_1, \ldots, y_s]$ over an integral domain $\mathbf{K}$ is also an integral domain.*

Proof. Use induction on s. For $s = 1$ the statement follows from Theorem AII.1. Suppose that a ring $\mathbf{K}[y_1, \ldots, y_{s-1}]$ is an integral domain. Then $\mathbf{K}[y_1, \ldots, y_s] = \mathbf{K}[y_1, \ldots, y_{s-1}][y_s]$ is a polynomial ring of univariate polynomials over the polynomial ring of polynomials in $s-1$ variables. Thus, by Theorem AII.1, $\mathbf{K}[y_1, \ldots, y_s]$ is also an integral domain. □

Theorem AII.3 *Let $\{F_1, F_2\} \subset \mathbf{K}[y_1, \ldots, y_s]$. If $F_1 \equiv_{\mathbf{K}} F_2$ then the polynomials are formally equal.*

Lemma AII.1 *If $H(y_1, \ldots, y_s) \in \mathbf{K}$ and $H \equiv_{\mathbf{K}} 0$, then it is the formally-zero polynomial.*

Proof. Let us prove the equivalent statement: if H is not the formally-zero polynomial, then there exists a point $(y_1^*, \ldots, y_s^*) \in \mathbf{K}^s$ such that $H(y_1^*, \ldots, y_s^*) \neq 0$.

Use induction on s. For $s = 1$, the statement is true. Let $s > 1$, and H be not the formally-zero polynomial. Rewrite H as a polynomial in y_1 with coefficients from $\mathbf{K}[y_2, \ldots, y_s]$:

$$H(y_1, \ldots, y_s) = a_0(y_2, \ldots, y_s) y_1^n + \ldots + a_n(y_2, \ldots, y_s)$$

Let $a_0(y_2, \ldots, y_s)$ be not the formally-zero polynomial. By the inductive hypothesis, there exists a point $(y_2^*, \ldots, y_s^*) \in \mathbf{K}^{s-1}$ such that $a_0^* := a_0(y_2^*, \ldots, y_s^*) \neq 0$. One then has

$$\begin{aligned} H(y_1, y_2^*, \ldots, y_s^*) &= a_0(y_2^*, \ldots, y_s^*) y_1^n + a_1(y_2^*, \ldots, y_s^*) y_1^{n-1} + \ldots + a_n(y_2^*, \ldots, y_s^*) \\ &= a_0^* y_1^n + a_1^* y_1^{n-1} + \ldots + a_n^* \end{aligned}$$

and $a_0^* \neq 0$. By Theorem AII.1, for $s = 1$ there exists $y_1^* \in \mathbf{K}$ such that

$$H(y_1^*, y_2^*, \ldots, y_s^*) = a_0^* (y_1^*)^n + a_1^* (y_1^*)^{n-1} + \ldots + a_n^* \neq 0.$$

This proves the lemma. □

Now to prove Theorem AII.3, one can apply the above lemma to the difference $H = F_1 - F_2$.

Theorem AII.4 *Let* $\mathbf{K}$ *be an integral domain with an infinite number of elements. Let* $\{F_1, F_2\} \subset \mathbf{K}[y_1, \ldots, y_s]$ *, and*

$$F_1(y_1^*, y_2^*, \ldots, y_s^*) = F_2(y_1^*, y_2^*, \ldots, y_s^*)$$

at any point satisfying the system of inequalities:

$$H_1(y_1^*, y_2^*, \ldots, y_s^*) \neq 0, \ldots, H_k(y_1^*, y_2^*, \ldots, y_s^*) \neq 0$$

where $H_1, \ldots, H_k$ *are non-identically-zero polynomials from* $\mathbf{K}[y_1, \ldots, y_s]$*. Then* $F_1 \equiv_{\mathbf{K}} F_2$ *.*

Proof. Consider the polynomial $(F_1 - F_2)H_1 \ldots H_k$. It is identically zero since whenever $H_1 \neq 0, \ldots, H_k \neq 0$, one has $F_1 = F_2$. Due to Theorem AII.3, this polynomial equals zero formally. But $\mathbf{K}[y_1, \ldots, y_s]$ is an integral domain and $H_1, \ldots, H_k$ are not identically zero. Thus $F_1 - F_2 \equiv_{\mathbf{K}} 0$ and $F_1 \equiv_{\mathbf{K}} F_2$. □

References

[1] A.G. Akritas. *Elements of Computer Algebra with Applications.* J.Wiley & Sons, New-York, 1989.

[2] W. Auzinger and H.J. Stetter. An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations. In *Conference in Numerical Analysis*, volume 86 of *ISNM*, pages 11–30. Birkhäuser, 1988.

[3] S. Barnett. Greatest common divisor of two polynomials. *Linear Algebra and its Applications*, 3:7–9, 1970.

[4] T. Becker and V. Weispfenning. *Gröbner Bases - A Computational Approach to Commutative Algebra.* Springer-Verlag, 1993.

[5] C.A. Berenstein and D.C. Struppa. Small degree solutions for the polynomial bézout equation. *Linear Algebra and Its Applications*, 98:41–56, 1988.

[6] C.A. Berenstein and A. Yger. Analytic bézout identities. *Advances in Applied Mathematics*, 10.1:51–74, 1989.

[7] É. Bézout. *Théorie générale des Équations Algébriques.* P.-D. Pierres, Paris, 1779.

[8] P. Bikker. On bézout's method for computing the resultant. Technical Report 95-36, RISC-Linz, 1995.

[9] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal.* Ph.D. Thesis University of Innsbruck, 1965.

[10] B. Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. In N.K. Bose, editor, *Recent Trends in Multidimensional Systems Theory*, pages 184–232. D. Riedel Publishing Company, 1985.

[11] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms.* Springer-Verlag, 1992.

[12] I.Z. Emiris and A. Rege. Monomial bases and polynomial system solving. In *Proceedings ISSAC '94*, pages 114–122. ACM, 1994.

[13] D.K. Faddeev. *Lectures in Higher Algebra, (in Russian).* Nauka, Moscow, 1984.

[14] F.R. Gantmacher. *The Theory of Matrices.* Chelsea, New York, 1959.

[15] L. González-Vega. An elementary proof of barnett's theorem about the greatest common divisor of several univariate polynomials. *Linear Algebra and Its Applications*, 247:185–202, 1996.

[16] L. González-Vega, G. Trujillo, and J.R. Sendra. Efficient manipulation of the trace matrix via hankel matrices. In *EACA '95*, pages 97–107, 1995.

[17] T. Fujise H. Kobayashi and A. Furukawa. Solving systems of algebraic equations by a general elimination method. *Journal of Symbolic Computation*, 5:303–320, 198.

[18] M. Kalkbrenner. On the stability of gröbner basis under specializations. *Journal of Symbolic Computation*, 24:51–58, 1997.

[19] M.G. Krein and M.A. Naimark. The method of symmetric and hermitian forms in the theory of the separation of the roots of algebraic equations. *Linear and Multilinear Algebra*, 10:265–308, 1981.

[20] H. Laurent. L'élimination. In *Scientia, Phys.-Mathématique*, volume 7. Gauthier–Villars, Paris, 1900.

[21] F.S. Macaulay. On some formulae in elimination. *Proceedings of The London Mathematical Society*, 35:3–27, 1903.

[22] F.S. Macaulay. *The Algebraic Theory of Modular Systems.* Cambridge University Press, 1916.

[23] E. Netto. *Vorlesungen über Algebra*, volume 2. Teubner, Leipzig, 1900.

[24] M. Noro and T. Takeshima. Risa/asir - a computer algebra system. In *Proceedings ISSAC '92*, pages 387–396. ACM, 1992.

[25] B. Trager P. Gianni and G. Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *Journal of Symbolic Computation*, 6:149–167, 1988.

[26] G. Scheja and U. Storch. *Lehrbuch der Algebra.* Teubner, 1988.

[27] L. Schläfli. über die resultante eines systemes mehrerer algebraischer gleichungen (1852). In *Gesammelte Mathematische Abhandlungen*, volume 2, pages 9–112. Birkhäuser, Basel, 1953.

[28] J.-A. Serret. *Cours d'Algèbre Supérieur*, volume 1. Gauthier–Villars, Paris, 1866.

[29] L. Stickelberger. Über eine neue eigenschaft der diskriminante algebraischer zahlkörper. *Verhand. der I internat. Math. Kongresse, 1897, Zürich*, pages 182–193, 1898.

[30] L. Stickelberger. Verzeichnis der schriften von ludwig stickelberger. *Jahresbericht der Deutschen Mathematiker Vereinigung*, 47(5–8):79–86, 1937.

[31] A.Yu. Uteshev and T.M. Cherkasov. Localization of solutions to systems of algebraic equations and inequalities: The hermite's method. *Doklady Math. (English translation)*, 53.2:227–229, 1996.

[32] A.Yu. Uteshev and T.M. Cherkasov. The search for the maximum of a polynomial. *Journal of Symbolic Computation*, 25:587–618, 1998.

[33] A.Yu. Uteshev and S.G. Shulyak. Hermite's method of separation of solutions of systems of algebraic equations and its applications. *Linear Algebra and Its Applications*, 177:49–88, 1992.

[34] K. Yokoyama, M. Noro, and T. Takeshima. Solutions of systems of algebraic equations and linear maps on residue class rings. *Journal of Symbolic Computation*, 14:399–417, 1992.