

Cayley-Dixon Resultant Matrices of Multi-Univariate Composed Polynomials

Arthur D. Chitcheba¹, Deepak Kapur², and Manfred Minimair³

¹ University of Texas – Pan American, Dept. of Computer Science,
Edinburg TX 78541, USA, cherba@cs.panam.edu

² University of New Mexico, Dept. of Computer Science,
Albuquerque NM 87131, USA, kapur@cs.unm.edu

³ Seton Hall University, Dept. of Mathematics and Computer Science,
South Orange NJ, USA, manfred@minimair.org

Abstract. The behavior of the Cayley-Dixon resultant construction and the structure of Dixon matrices are analyzed for composed polynomial systems constructed from a multivariate system in which each variable is substituted by a univariate polynomial in a distinct variable. It is shown that a Dixon projection operator (a multiple of the resultant) of the composed system can be expressed as a power of the resultant of the *outer* polynomial system multiplied by powers of the leading coefficients of the univariate polynomials substituted for variables in the outer system. The derivation of the resultant formula for the composed system unifies all the known related results in the literature. A new resultant formula is derived for systems where it is known that the Cayley-Dixon construction does not contain any extraneous factors. The approach demonstrates that the resultant of a composed system can be effectively calculated by considering only the resultant of the outer system.

1 Introduction

Problems in many application domains, including engineering and design, graphics, CAD-CAM, geometric modeling, etc. can be modelled using polynomial systems [1–8]. Often a polynomial system arising from an application has a structure. Particularly in engineering and design applications and in geometric modeling, a polynomial system can be expressed as a composition of two distinct polynomial systems, each of which is of much lower degree in comparison to the original system. Furthermore, if the structure of given polynomials is not known a priori, one can efficiently check if they can be decomposed [9].

This paper addresses the resultant computation for such composed polynomial systems [10–14]. The resultant of a polynomial system with symbolic parameters is a necessary and sufficient condition on its parameters for the polynomial system to have a common solution⁴. Resultant computations have been

^{1,2,3} Supported by NSF grant no. CCR-0203051 and a grant from the Computer Science Research Institute at the Sandia National Labs

³ Also supported by NSF grant CCF 0430741

⁴ Resultant depends on an algebraic set for which solutions are sought [15].

found useful in many application domains including engineering and design, robotics, inverse kinematics, manufacturing, design and analysis of nano devices in nanotechnology, image understanding, graphics, solid modeling, implicitization, CAD-CAM design, geometric construction, drug-design, and control theory.

The focus in this paper is on the Cayley-Dixon formulation for multivariate resultants which have been shown to be efficient (both experimentally and theoretically) for computing resultants by simultaneously eliminating many variables from a polynomial system [16]. The behavior of the Cayley-Dixon resultant construction is analyzed for composed polynomial systems constructed from a multivariate system in which each variable is substituted by a univariate polynomial in a distinct variable, referred to as multi-univariate composition in [9]. It is shown that the resultant of the composed system can be expressed as a power of the resultant of the *outer* polynomial system, multiplied by powers of the leading coefficients of the univariate polynomials substituted for variables in the outer system. It is important to point out that the techniques used for deriving resultant formulas in the current paper are different from the techniques used in previous works (such as [10–13, 17, 18]), which seemed not applicable.

A new resultant formula is derived for multi-univariate composed polynomials where it is known that the Cayley-Dixon resultant formulation does not produce any extraneous factors for the outer system. The derivation unifies all known related results in the literature [18, 19]. Such systems include n -degree [8], bivariate corner cut [20] and generalized corner cut systems [21]. Even when extraneous factors are present, a similar formula is derived showing that the extraneous factor of the outer system will be “amplified” in the extraneous factor of composed system. Hence exploiting the composed structure of a polynomial system can reduce the extraneous factors in the resultant computation. Furthermore, it demonstrates that the resultant of a composed system can be effectively calculated by considering only the resultant of the outer system. For practical applications, that is what is needed.

Below, we first state the main result of the paper. This is followed by a section on preliminaries and notation; the generalized Cayley-Dixon formulation as proposed by Kapur, Saxena and Yang [8] is briefly reviewed. Since the Cayley-Dixon formulation involves two disjoint sets of variables, the bilinear form representation of a polynomial in disjoint sets of variables is useful. In section 2, we discuss how bilinear forms are affected by polynomial operations, particularly when two polynomials are multiplied, a polynomial is composed with other polynomials by substituting variables by polynomials etc. To express these relations among bilinear forms, a series of matrix operations is introduced.

We assume that the reader is familiar with the notion of resultant with respect to a given variety (see for example [15]). This notion includes classic resultants like the projective (Macaulay) resultant where the variety is projective space and more recent generalizations like toric resultants where the varieties are suitable toric varieties.

1.1 Main Results

Consider a polynomial system $F = (f_0, f_1, \dots, f_n)$ with symbolic coefficients, where $F \subset \mathbb{K}[\mathbf{c}][y_1, \dots, y_n]$ and

$$f_i = \sum_{\alpha \in \mathcal{F}_i} c_{i,\alpha} \mathbf{y}^\alpha \quad \text{for } i = 0, \dots, n,$$

where $\mathbf{y}^\alpha = y_1^{\alpha_1}, \dots, y_n^{\alpha_n}$ and \mathcal{F}_i is the set of exponent vectors corresponding to the terms appearing in f_i , also called the *support* of f_i . The list \mathbf{c} consists of “other” variables in terms of which polynomial coefficients $c_{i,\alpha} \in \mathbb{K}[\mathbf{c}]$ are defined. They are also sometimes referred as the *parameters* of the polynomial system.

A polynomial system is called *generic* if there is no algebraic relation among coefficients $c_{i,\alpha}$ of F .

Let $G = (g_1, \dots, g_n)$ be a *univariate* polynomial system where

$$g_j(x_j) = d_{j,k_j} x_j^{k_j} + d_{j,k_j-1} x_j^{k_j-1} + \dots + d_{j,0}, \quad \text{for } j = 1, \dots, n.$$

Let $k = (k_1, \dots, k_n)$ be the degree vector of G .

We consider **composed** polynomial system of F with G , written as $F \circ G$, which is the list of polynomials obtained from the list F of polynomials by replacing each y_j by g_j respectively. The operator \circ is called *functional composition* on polynomial systems.

The main results of this paper are:

- (i) The Dixon matrix $\Theta_{F \circ G}$ of a composed system $F \circ G$ is shown to be a product of 3 matrices:

$$\Theta_{F \circ G} = A_L \times \text{Diag}_{k_1 \dots k_n}(\Theta_F) \times A_R,$$

where Θ_F is the Dixon matrix of the outer system F and A_L as well as A_R are triangular matrices which contain only polynomials in terms of the coefficients of the polynomials in G . The matrix $\text{Diag}_{k_1 \dots k_n}(\Theta_F)$ is block diagonal, where Θ_F is repeated $k_1 \dots k_n$ times along the diagonal.

- (ii) If F is a polynomial system for which the determinant of Dixon matrix is $\text{Res}(F)$, then

$$\text{Res}(F \circ G) = d_{1,k_1}^{\epsilon_1} \dots d_{n,k_n}^{\epsilon_n} \text{Res}(F)^\delta,$$

where ϵ_j 's depend on the degrees of G as well as F but δ depends only on the degrees of G .

- (iii) Even if Θ_F is not square or is singular, the *rank submatrix construction* (RSC) introduced in [8] (see also [15]) also works for composed systems. In particular, the projection operator extracted from Θ_F is a factor of the projection operator extracted from $\Theta_{F \circ G}$ raised to the appropriate power; in addition to the leading coefficients d_{j,k_j} of polynomials in G , there are also additional factors introduced in the projection operator extracted from $\Theta_{F \circ G}$.

- (iv) The resultant of composed n -degree system, with degrees (m_1, \dots, m_n) , is

$$\text{Res}(F \circ G) = \left(d_{1,k_1}^{m_1} \dots d_{n,k_n}^{m_n} \right)^{\frac{(n+1)!}{2} m_1 \dots m_n k_1 \dots k_n} \text{Res}(F)^{k_1 \dots k_n}.$$

2 Cayley-Dixon Formulation and Bilinear Form

2.1 The Cayley-Dixon Formulation

In [22], Dixon extended the Bezout-Cayley's construction for computing the resultant of two univariate polynomials to the bivariate case for three polynomials. Kapur, Saxena and Yang [8] generalized this construction to the multivariate case. The concepts of a Dixon polynomial and a Dixon matrix were introduced. Below, the generalized multivariate Dixon formulation for simultaneously eliminating many variables from a polynomial system and computing its resultant are briefly reviewed. Let $\pi_i(\mathbf{y}^\alpha) = \bar{y}_1^{\alpha_1} \cdots \bar{y}_i^{\alpha_i} y_{i+1}^{\alpha_{i+1}} \cdots y_n^{\alpha_n}$, where $i \in \{0, 1, \dots, n\}$, and \bar{y}_i 's are new variables; $\pi_0(\mathbf{y}^\alpha) = \mathbf{y}^\alpha$. π_i is extended to polynomials in a natural way as: $\pi_i(f_j(y_1, \dots, y_n)) = f_j(\bar{y}_1, \dots, \bar{y}_i, y_{i+1}, \dots, y_n)$.

Definition 1. Given a n -variate polynomial system $F = (f_0, f_1, \dots, f_n)$, where $f \in \mathbb{K}[\mathbf{c}][y_1, \dots, y_n]$, define its **Dixon polynomial** as

$$\theta(F) = \prod_{i=1}^n \frac{1}{\bar{y}_i - y_i} \det \begin{pmatrix} \pi_0(f_0) & \pi_0(f_1) & \cdots & \pi_0(f_n) \\ \pi_1(f_0) & \pi_1(f_1) & \cdots & \pi_1(f_n) \\ \vdots & \vdots & \ddots & \vdots \\ \pi_n(f_0) & \pi_n(f_1) & \cdots & \pi_n(f_n) \end{pmatrix} = \bar{Y}^T \times \Theta_F \times Y,$$

where $\bar{Y} = [\bar{\mathbf{y}}^{\beta_1}, \dots, \bar{\mathbf{y}}^{\beta_k}]$ and $Y = [\mathbf{y}^{\alpha_1}, \dots, \mathbf{y}^{\alpha_l}]$ are column vectors. Hence, $\theta(f_0, f_1, \dots, f_n) \in \mathbb{K}[\mathbf{c}][y_1, \dots, y_n, \bar{y}_1, \dots, \bar{y}_n]$, where $\bar{y}_1, \dots, \bar{y}_n$ are new variables. The $k \times l$ matrix Θ_F is called the **Dixon matrix**, and its entries are in $\mathbb{K}[\mathbf{c}]$.

The order in which original variables in \mathbf{y} are replaced by new variables in $\bar{\mathbf{y}}$ is significant in the sense that the computed Dixon polynomial can be different for two different orderings. See [22, 8, 21, 15].

As shown in [8] and [15], Θ_F is a resultant matrix, i.e., the resultant can be computed from the determinant of Θ_F . If Θ_F singular, for example for certain nongeneric polynomial systems, then the resultant is extracted from the determinant of some maximal minor of Θ_F ; this determinant is called a *projection operator* [8, 15].

2.2 Operations on Bilinear Forms

It is easy to see that a multivariate polynomial in terms of two disjoint sets of variables, e.g., the Dixon polynomial above, can be represented in a *bilinear form*. For analyzing how the functional composition of two polynomial systems affects the Dixon polynomials and Dixon matrices of the polynomial systems, bilinear form representations turn out to be useful. Below, we discuss various polynomial operations and their effect on bilinear forms.

A bilinear form of a polynomial p in two disjoint sets of variables is expressed as a matrix, post and pre-multiplied by monomial vectors. That is

$$p(x_1, \dots, x_k, \bar{x}_1, \dots, \bar{x}_l) = \sum_{\alpha, \beta} p_{\alpha, \beta} \mathbf{x}^\alpha \bar{\mathbf{x}}^\beta = \bar{X}_p^T \times M_p \times X_p,$$

where \overline{X}_p and X_p are vectors with entries being monomials in terms of variables $\{\overline{x}_1, \dots, \overline{x}_l\}$ and $\{x_1, \dots, x_k\}$, respectively. M_p is a matrix with the coefficients $p_{\alpha, \beta}$ of terms in p as its entries.

The matrix M_p in the above definition depends on the monomial ordering used. We will assume a total degree ordering on power products, and state explicitly if it is otherwise. Also, implicit in the above definition of M_p are the row labels \overline{X}_p and column labels X_p .

Let \mathcal{P} be the ordered set of the exponent vectors corresponding to X_p ; \mathcal{P} is also called the **support** of the polynomial p w.r.t variables $\{x_1, \dots, x_k\}$. Similarly, let $\overline{\mathcal{P}}$ be the support of p w.r.t. variables $\{\overline{x}_1, \dots, \overline{x}_l\}$. Let $\mathcal{P} + \mathcal{Q}$ stand for the Minkowski sum of the supports \mathcal{P} and \mathcal{Q} . [23]

As stated above, the Dixon polynomial can be conveniently represented in bilinear form using the original variables and the new variables, highlighting the Dixon matrix. Let Δ_F and $\overline{\Delta}_F$ be the supports of the Dixon polynomial $\theta(F)$ in terms of variables \mathbf{y} and $\overline{\mathbf{y}}$, respectively.

Below, we derive the bilinear matrix form of the product of two polynomials in terms of their bilinear matrix forms. For this purpose, we first define the so-called “left” and “right” operators on bilinear forms.

Definition 2. *Given two polynomials p and q admitting bilinear form, i.e. $p = \overline{X}_p \times M_p \times X_p$ and $q = \overline{X}_q \times M_q \times X_q$, consider the following polynomial products*

$$\begin{aligned} p' &= p \cdot \sum_{\overline{e}_q \in \overline{\mathcal{Q}}} \mathbf{z}^{\overline{e}_q} \overline{\mathbf{x}}^{\overline{e}_q} = \overline{X}_{p'} \times M_{p'} \times X_{p'}, \\ q' &= q \cdot \sum_{e_p \in \mathcal{P}} \overline{\mathbf{z}}^{e_p} \mathbf{x}^{e_p} = \overline{X}_{q'} \times M_{q'} \times X_{q'}, \end{aligned} \quad \text{and}$$

where $\overline{z}_1, \dots, \overline{z}_n$ and z_1, \dots, z_n are new variables. Define two matrix operators

$$L_{\overline{\mathcal{Q}}}(M_p) = M_{p'} \quad \text{and} \quad R_{\mathcal{P}}(M_q) = M_{q'},$$

where columns of $M_{p'}$ ordered first by some monomial order on $\{z_1, \dots, z_n\}$ and then by some monomial order on $\{x_1, \dots, x_n\}$. Similarly rows of $M_{q'}$ first ordered by $\{\overline{x}_1, \dots, \overline{x}_n\}$ and then by $\{\overline{z}_1, \dots, \overline{z}_n\}$. To make matrices $M_{p'}$ and $M_{q'}$ “compatible” with each other, we require that monomial order used for columns of $M_{p'}$ on variables $[\{z_1, \dots, z_n\}, \{x_1, \dots, x_n\}]$ be same as for rows of $M_{q'}$ on variables $[\{\overline{x}_1, \dots, \overline{x}_n\}, \{\overline{z}_1, \dots, \overline{z}_n\}]$.

The above matrix operators are defined in such a way that matrix multiplication would coincide with polynomial multiplication. New variables $\overline{z}_1, \dots, \overline{z}_n$ and z_1, \dots, z_n are auxiliary variables for creating block matrix structure, as well as ensuring that the resulting matrix rows and columns are in matching order. Notice that the row indices of $L_{\overline{\mathcal{Q}}}(M_p)$ are $\overline{\mathcal{P}} + \overline{\mathcal{Q}}$ and the column indices are $\overline{\mathcal{Q}} \times \mathcal{P}$, coming from monomials $\mathbf{z}^{\overline{e}_q} \mathbf{x}^{e_p}$ for $\overline{e}_q \in \overline{\mathcal{Q}}$ and $e_p \in \mathcal{P}$.

Matrix $L_{\overline{\mathcal{Q}}}(M_p)$ is quite sparse and its entries are either 0 or the coefficients of the polynomial p . In fact, the entry of $L_{\overline{\mathcal{Q}}}(M_p)$ indexed by row $\overline{\mathbf{x}}^{\overline{e}_p + \overline{e}_q}$ and column $\mathbf{z}^{\overline{e}_q} \mathbf{x}^{e_p + e_q}$ is equal to $p_{\overline{e}_p, e_p}$. All other entries are 0. Also it has a block

matrix structure: $L_{\overline{Q}}(M_p) = \text{RowStack}_{\alpha \in \overline{Q}}(N_\alpha \times M_p)$, where N_α is a matrix which adds zero rows to M_p (depending on α , \overline{Q} and \overline{P}), and operator RowStack stacks matrices columnwise. $R_{\mathcal{P}}(M_q)$ also admits a similar block decomposition.

Using the above operators, we can express bilinear form of the polynomial product, $pq = \overline{X}_{pq} \times M_{pq} \times X_{pq}$ as matrix multiplication.

Lemma 1. $M_{pq} = L_{\overline{Q}}(M_p) \times R_{\mathcal{P}}(M_q).$

Proof. Directly from the polynomial product of polynomials p and q ,

$$(M_{pq})_{\alpha, \beta} = \sum_{\substack{\alpha = \overline{e}_p + \overline{e}_q, \\ \beta = e_p + e_q}} p_{\overline{e}_p, e_p} q_{\overline{e}_q, e_q},$$

for $\overline{e}_p \in \overline{P}$, $\overline{e}_q \in \overline{Q}$, $e_p \in \mathcal{P}$ and $e_q \in \mathcal{Q}$. On the other hand,

$$\begin{aligned} (L_{\overline{Q}}(M_p) \times R_{\mathcal{P}}(M_q))_{\alpha, \beta} &= \text{Row}_\alpha(L_{\overline{Q}}(M_p)) \cdot \text{Col}_\beta(R_{\mathcal{P}}(M_q)) \\ &= \sum_{\substack{\overline{e}_q \in \overline{Q}, \\ e_p \in \mathcal{P}}} p'_{\alpha, \overline{e}_q e_p} \cdot q'_{\overline{e}_q e_p, \beta}, \end{aligned}$$

where $p'_{\alpha, \overline{e}_q e_p}$ is the coefficient of monomial $\overline{\mathbf{x}}^\alpha \mathbf{z}^{\overline{e}_q} \mathbf{x}^{e_p}$ of p' . But

$$p'_{\alpha, \overline{e}_q e_p} = \begin{cases} p_{\overline{e}_p, e_p} & \text{if } \alpha = \overline{e}_p + \overline{e}_q, \\ 0 & \text{otherwise} \end{cases}, \quad \text{and} \quad q'_{e_p \overline{e}_q, \beta} = \begin{cases} q_{\overline{e}_q, e_q} & \text{if } \beta = e_p + e_q \\ 0 & \text{otherwise} \end{cases}.$$

where $e_p \in \mathcal{P}$, $\overline{e}_p \in \overline{P}$, $q \in \overline{Q}$ and $\overline{e}_q \in \overline{Q}$. Therefore

$$\sum_{\substack{\overline{e}_q \in \overline{Q}, \\ e_p \in \mathcal{P}}} p'_{\alpha, \overline{e}_q e_p} \cdot q'_{\overline{e}_q e_p, \beta} = \sum_{\substack{\alpha = \overline{e}_p + \overline{e}_q, \\ \beta = e_p + e_q}} p'_{\alpha, \overline{e}_q e_p} \cdot q'_{\overline{e}_q e_p, \beta} = \sum_{\substack{\alpha = \overline{e}_p + \overline{e}_q, \\ \beta = e_p + e_q}} p_{\overline{e}_p, e_p} q_{\overline{e}_q, e_q}. \quad \square$$

One of the useful properties of L operator is that the application on matrix product results in the application on one of the matrices times a block diagonal matrix of the other factor.

Lemma 2. *Given a product of two matrices $A \times B$,*

$$L_{\mathcal{P}}(A \times B) = L_{\mathcal{P}}(A) \times \text{Diag}_{\mathcal{P}}(B),$$

where matrix $\text{Diag}_{\mathcal{P}}(B)$ is block diagonal with B repeated $|\mathcal{P}|$ times along the diagonal.

Proof. By definition,

$$\begin{aligned} L_{\mathcal{P}}(A \times B) &= \text{RowStack}_{\alpha \in \mathcal{P}}(N_\alpha \times (A \times B)) = \text{RowStack}_{\alpha \in \mathcal{P}}((N_\alpha \times A) \times B) \\ &= \text{RowStack}_{\alpha \in \mathcal{P}}(N_\alpha \times A) \times \text{Diag}_{\mathcal{P}}(B) = L_{\mathcal{P}}(A) \times \text{Diag}_{\mathcal{P}}(B). \quad \square \end{aligned}$$

Note that if $|\overline{P} + \overline{Q}| = |\overline{P}| \times |\overline{Q}|$, for example when p and q are in terms of different variables, then $L_{\overline{Q}}(M_p) = \text{Diag}_{\overline{Q}}(M_p)$.

Definition 3. Given a support \mathcal{P} and the set of univariate polynomials $G = (g_1, \dots, g_n)$, where each g_i is in x_i , let

$$s = \sum_{\alpha \in \mathcal{P}} \bar{\mathbf{x}}^\alpha G^\alpha = \bar{X}_s \times M_s \times X_s,$$

where $G^\alpha = \prod_{i=1}^n g_i^{\alpha_i}$. Define operator $S_{\mathcal{P}}(G) = M_s$.

$S_{\mathcal{P}}(G)$ is thus the matrix whose rows are indexed by \mathcal{P} and whose columns are indexed by the union over $\alpha \in \mathcal{P}$ of the supports of $\prod_{j=1}^n g_j^{\alpha_j}$. Note that the monomial vector, with support \mathcal{P} composed with G can be expressed as $Y_p \circ G = S_{\mathcal{P}}(G) \times X_s$, where X_s is union of all monomials in G^α for all $\alpha \in \mathcal{P}$. Matrix $S_{\mathcal{P}}(G)$ is also very sparse and it is “step”-triangular (i.e., where in each row, first non-zero entry comes later than in the previous row), i.e.,

$$(S_{\mathcal{P}}(G))_{\bar{e}_s, e_s} = \begin{cases} (d_{1,k_1}, \dots, d_{n,k_n})^{\bar{e}_s} & \text{if } (e_s)_i = k_i(\bar{e}_s)_i, \forall i, \\ 0 & \text{if } \exists i \text{ s.t. } k_i(\bar{e}_s)_i < (e_s)_i. \end{cases} \quad (1)$$

Lemma 3. Let p be a polynomial in the variables $\bar{\mathbf{y}}, \mathbf{y}$, and G a set of univariate polynomials g_i in variable x_i , for $i = 1, \dots, n$. Then

$$M_{p \circ (\bar{G}, G)} = S_{\mathcal{P}}(\bar{G})^T \times M_p \times S_{\mathcal{P}}(G),$$

where $\bar{G} = (\bar{g}_1, \dots, \bar{g}_n)$, and $\bar{g}_i = g_i(\bar{x}_i)$.

Proof. Since $p = \bar{Y}_p \times M_p \times Y_p$, we have $p \circ (\bar{G}, G) = (\bar{Y}_p^T \circ \bar{G}) \times M_p \times (Y_p \circ G)$ and $Y_p \circ G = S_{\mathcal{P}}(G) \times X_s$ by definition. \square

A very useful property of operators L and S is that in combination, they produce step-triangular matrices⁵. Square step-triangular matrices are triangular.

Proposition 1. Let \bar{Q} be the support of $\prod_{i=1}^n \frac{g_i - \bar{g}_i}{x_i - \bar{x}_i}$, that is $\bar{e}_q \in \bar{Q}$ iff $0 \leq (\bar{e}_q)_i < k_i$ for all $i = 1, \dots, n$. Then for any support \mathcal{P} , the matrix $L_{\bar{Q}}(S_{\mathcal{P}}(\bar{G})^T)$ is (after column reordering) is zero above the step diagonal; moreover, entry in column $\bar{e}_q e_p$ (i.e. indexed by monomial $\mathbf{z}^{\bar{e}_q} \mathbf{x}^{e_p}$) and row α is

$$L_{\bar{Q}}(S_{\mathcal{P}}(\bar{G})^T)_{\alpha, \bar{e}_q e_p} = \begin{cases} (d_{1,k_1}, \dots, d_{n,k_n})^{e_p} & \text{if } \alpha = \bar{e}_p + \bar{e}_q \text{ and } (\bar{e}_p)_i = k_i(e_p)_i, \\ (S_{\mathcal{P}}(\bar{G})^T)_{\bar{e}_p, e_p} & \text{if } \alpha = \bar{e}_p + \bar{e}_q \text{ and } \forall i, (\bar{e}_p)_i < k_i(e_p)_i, \\ 0 & \text{otherwise,} \end{cases}$$

i.e., in every column, first non-zero entry is the product of leading coefficients of G , and all these leading non-zero entries are in different rows.

Proof. Note that the columns of $S_{\mathcal{P}}(\bar{G})^T$ are labelled by \mathcal{P} and rows by \bar{X}_s , which is the set of all monomials in $\bar{G}^\alpha = \bar{g}_1^{\alpha_1} \dots \bar{g}_n^{\alpha_n}$ for all $\alpha \in \mathcal{P}$.

⁵ See the expanded version of this article [24] for many examples illustrating the structure of of these matrices.

Consider the following polynomial,

$$s = \overline{X}_s \times S_{\mathcal{P}}(\overline{G})^T \times X_s, \quad \text{and let} \quad s' = s \cdot \sum_{\overline{e}_q \in \overline{\mathcal{Q}}} \mathbf{z}^{\overline{e}_q} \overline{\mathbf{x}}^{\overline{e}_q},$$

as in definition 2 of $L_{\overline{\mathcal{Q}}}(M_p)$. As in the proof of Lemma 1, $\text{coeff}_{\overline{\mathbf{x}}^{\alpha} \mathbf{z}^{\overline{e}_q} \mathbf{x}^{e_s}}(s') = s_{\overline{e}_s, e_s}$ iff $\alpha = \overline{e}_s + \overline{e}_q$, and 0 otherwise. Since the support of s is \mathcal{P} , we will use labels e_p instead of e_s . Equation (1) and the above observation gives us

$$\text{coeff}_{\overline{\mathbf{x}}^{\alpha} \mathbf{z}^{\overline{e}_q} \mathbf{x}^{e_p}}(s') = \begin{cases} (d_{1,k_1}, \dots, d_{n,k_n})^{e_p} & \text{if } \alpha = \overline{e}_s + \overline{e}_q \text{ and } (\overline{e}_s)_i = k_i(e_p)_i, \\ s_{\overline{e}_s, e_p} & \text{if } \alpha = \overline{e}_s + \overline{e}_q \text{ and } \forall i, (\overline{e}_s)_i < k_i(e_p)_i, \\ 0 & \text{otherwise.} \quad \square \end{cases}$$

In the next section, we use the above operators in expressing the manipulations of bilinear forms of various polynomials arising in the Cayley-Dixon construction to show that Dixon matrix of composed system can be decomposed as a matrix product.

3 Dixon Matrix Decomposition

The **Cayley-Dixon Construction** of the composed polynomials $F \circ G$ is a generalization of the Cayley-Bézout construction from the univariate case. The Dixon polynomial of the composed system

$$\begin{aligned} \theta_{F \circ G} &= \frac{\det \begin{bmatrix} f_0 \circ (\pi_0(G)) & \dots & f_n \circ (\pi_0(G)) \\ \vdots & \ddots & \vdots \\ f_0 \circ (\pi_n(G)) & \dots & f_n \circ (\pi_n(G)) \end{bmatrix}}{\prod_{i=1}^n (g_i - \overline{g}_i)} \times \frac{\prod_{i=1}^n (g_i - \overline{g}_i)}{\prod_{i=1}^n (x_i - \overline{x}_i)} \\ &= \theta_F \circ (\overline{G}, G) \times \prod_{i=1}^n \frac{g_i - \overline{g}_i}{x_i - \overline{x}_i}. \end{aligned} \quad (2)$$

Let $p = \theta_F \circ (\overline{G}, G)$ and $q = \prod_{i=1}^n \frac{g_i - \overline{g}_i}{x_i - \overline{x}_i}$, where \mathcal{P} is the support of p with respect to the variables x_1, \dots, x_n and $\overline{\mathcal{Q}}$ is the support of q with respect to the variables $\overline{x}_1, \dots, \overline{x}_n$. Using Lemmas 1, 2 and 3 to equation (2) above, we get

$$\Theta_{F \circ G} = L_{\overline{\mathcal{Q}}} \left(S_{\Delta_F}(G)^T \right) \times \text{Diag}_{\overline{\mathcal{Q}}}(\Theta_F) \times \left(\text{Diag}_{\overline{\mathcal{Q}}}(S_{\Delta_F}(G)) \times R_{\mathcal{P}}(M_q) \right).$$

Theorem 1. *For a polynomial system $F = (f_0, f_1, \dots, f_n)$ and a list of univariate polynomials $G = (g_1, \dots, g_n)$, the Dixon matrix $\Theta_{F \circ G}$ is*

$$A_L \times \text{Diag}_{k_1 \dots k_n}(\Theta_F) \times A_R,$$

where A_L and A_R are step triangular matrices with diagonal entries being the product of the leading coefficients of the polynomials in G . Specifically,

$$A_L = L_{\overline{\mathcal{Q}}} \left(S_{\Delta_F}(\overline{G})^T \right), \quad \text{and} \quad A_R = \text{Diag}_{\overline{\mathcal{Q}}}(S_{\Delta_F}(G)) \times R_{\mathcal{P}}(M_q),$$

where $q = \prod_{i=1}^n \frac{g_i - \overline{g}_i}{x_i - \overline{x}_i}$ is the product of the divided differences of G , \mathcal{Q} and $\overline{\mathcal{Q}}$ are, respectively, the supports of q in the variables \mathbf{x} and $\overline{\mathbf{x}}$.

More importantly, for a generic n -degree polynomial system F and a generic system G of n polynomials used to substitute for variables y_1, \dots, y_n in F , the factors, A_L , A_R and Θ_F can be proved to be square and non-singular matrices [8]. We investigate this in Section 4.

More generally, if the factors are square in the above theorem, then we can derive precise expression for the determinant of the Dixon matrix.

Lemma 4. *If $|\overline{\Delta}_F| \cdot \prod_{j=1}^n k_j = |\overline{\Delta}_{F \circ G}|$, i.e., A_L is square, then*

$$\det(A_L) = \pm (d_{1,k_1}, \dots, d_{n,k_n})^{(\sum_{\alpha \in \overline{\Delta}_F} \alpha) k_1 \dots k_n};$$

if $|\Delta_F| = |\overline{\Delta}_F|$, i.e., Θ_F is square, then

$$\det\left(\text{Diag}_{|\overline{\mathcal{Q}}|}(\Theta_F)\right) = (\det(\Theta_F))^{k_1 \dots k_n};$$

and if $|\Delta_F| \cdot \prod_{j=1}^n k_j = |\Delta_{F \circ G}|$, i.e., A_R is square, then

$$\det(A_R) = \pm (d_{1,k_1}, \dots, d_{n,k_n})^{(|\Delta_F| + \sum_{\beta \in \Delta_F} \beta) k_1 \dots k_n}.$$

Proof. When A_L is square, it is triangular with diagonal entries

$$(A_L)_{\alpha, \bar{e}_q, e_p} = (d_{1,k_1}, \dots, d_{n,k_n})^{e_p}$$

in column $\bar{e}_q e_p$, where $e_p \in \mathcal{P} = \overline{\Delta}_F$, by Proposition 1. Since the size of $\overline{\mathcal{Q}}$ is $k_1 \dots k_n$,

$$\det(A_L) = \prod_{\substack{e_p \in \overline{\Delta}_F \\ \bar{e}_q \in \overline{\mathcal{Q}}}} (d_{1,k_1}, \dots, d_{n,k_n})^{e_p} = (d_{1,k_1}, \dots, d_{n,k_n})^{(\sum_{\alpha \in \overline{\Delta}_F} \alpha) k_1 \dots k_n}.$$

Also, for $A_R = \text{Diag}_{|\overline{\mathcal{Q}}|}(\text{S}_{\Delta_F}(G)) \times \text{R}_{\mathcal{P}}(M_q)$, let $s = \overline{Z}_s \times \text{S}_{\Delta_F}(G) \times X_s$, $A_R = M_{sq}$, as in the univariate case. Also note that M_q is triangular, where

$$q_{\bar{e}_q, e_q} = \begin{cases} d_{1,k_1} \dots d_{n,k_n} & \text{if } \forall i \text{ s.t. } (\bar{e}_q)_i + (e_q)_i = k_i - 1, \\ 0 & \text{if } \exists i \text{ s.t. } (\bar{e}_q)_i + (e_q)_i > k_i - 1, \end{cases}$$

and entries of $\text{S}_{\Delta_F}(G)$ by equation 1 are

$$s_{\bar{e}_s, e_s} = \begin{cases} (d_{1,k_1}, \dots, d_{n,k_n})^{\bar{e}_s} & \text{if } \forall i \text{ s.t. } (e_s)_i = k_i (\bar{e}_s)_i, \\ 0 & \text{if } \exists i \text{ s.t. } k_i (\bar{e}_s)_i < (e_s)_i, \end{cases}$$

for $\bar{e}_s \in \Delta_F$ and e_s in support of G^α for all $\alpha \in \Delta_F$. Therefore

$$(s \cdot q)_{\bar{e}_s \bar{e}_q, e_s + e_q} = \begin{cases} (d_{1,k_1}, \dots, d_{n,k_n})^{\bar{e}_s + 1} & \text{if } e_s = k_i (\bar{e}_s), \bar{e}_q + e_q = k - 1, \\ 0 & \text{if } \exists i \text{ s.t. } k_i (\bar{e}_s)_i < (e_s)_i \\ & \text{or } (\bar{e}_q)_i + (e_q)_i > k_i - 1, \end{cases}$$

i.e., in row $\bar{e}_s \bar{e}_q$ the diagonal element is $(d_{1,k_1}, \dots, d_{n,k_n})^{\bar{e}_s + 1}$. Since $\bar{e}_s \in \Delta_F$ and $\bar{e}_q \in \overline{\mathcal{Q}}$, where $|\overline{\mathcal{Q}}| = k_1 \dots k_n$, we have the determinant of A_R

$$\det(A_R) = \prod_{\substack{\bar{e}_s \in \Delta_F \\ \bar{e}_q \in \overline{\mathcal{Q}}}} (d_{1,k_1}, \dots, d_{n,k_n})^{\bar{e}_s + 1} = (d_{1,k_1}, \dots, d_{n,k_n})^{(|\Delta_F| + \sum_{\beta \in \Delta_F} \beta) k_1 \dots k_n}.$$

□

By Theorem 1 and the above proposition, we have the following main result.

Theorem 2. *Let F be a polynomial system for which the Cayley-Dixon resultant formulation leads to a square and nonsingular resultant matrix Θ_F whose determinant is $\text{Res}(F)$. Then under the multi-univariate composition $F \circ G$,*

$$\text{Res}(F \circ G) = (d_{1, k_1}, \dots, d_{n, k_n})^{(\sum_{\alpha \in \overline{\Delta}_F} \alpha + |\Delta_F| + \sum_{\beta \in \Delta_F} \beta) k_1 \cdots k_n} \text{Res}(F)^{k_1 \cdots k_n}.$$

3.1 Rank Submatrix Construction

In case when the Dixon matrix of the composed polynomials (or any of its factors in Lemma 4) is not square or when the Dixon matrix is rank deficient, one can extract a projection operator from the Dixon matrix by computing the determinant of any maximal minor [8, 15]. Since the Dixon matrix $\Theta_{F \circ G}$ can be factored into a product one obtains a similar factorization of a maximal minor,

$$\det_{\max} [A_L \times \text{Diag}_{k_1 \cdots k_n}(\Theta_F) \times A_R] = \det [M_L \times \text{Diag}_{k_1 \cdots k_n}(\Theta_F) \times M_R],$$

by selecting appropriate rows M_L of A_L and columns M_R of A_R . Furthermore, the well-known Cauchy-Binet formula allows us to expand the determinant of the minor into a sum of products of the form $l \cdot s \cdot r$, where l ranges over determinants of minors of M_L , s ranges over determinants of minors of $\text{Diag}_{k_1 \cdots k_n}(\Theta_F)$ and r ranges over determinants of minors of M_R .

This leads to a formula similar to the square case (Theorem 2). For details, see the expanded version of this paper [24].

Theorem 3. *For a polynomial system $F = (f_0, f_1, \dots, f_n)$, composed with univariate polynomials $G = (g_1, \dots, g_n)$,*

$$\det_{\max}(\Theta_{F \circ G}) = d_{1, k_1}^{\epsilon_1} \cdots d_{n, k_n}^{\epsilon_n} E \left(\gcd_{\max} \det(\Theta_F) \right)^{k_1 \cdots k_n},$$

where E is an extraneous factor dependent on the coefficients of G and F .

The above implies that whenever a resultant can be computed by the Cayley-Dixon construction, the resultant also will be decomposable in a similar fashion.

It is an open question what the values of $\epsilon_1, \dots, \epsilon_n$ are in general and whether the factor E is constant for all selections of maximal minors in $\Theta_{F \circ G}$.

4 Resultant of Composed n -degree polynomial system

In this section, we generalize the McKay and Wang formula [19] for the univariate polynomials to n -degree polynomials systems.

Consider the (m_1, \dots, m_n) -degree generic polynomials f_0, f_1, \dots, f_n where

$$f_j = \sum_{i_1=1}^{m_1} \cdots \sum_{i_n=1}^{m_n} c_{j, i_1, \dots, i_n} y_1^{i_1} \cdots y_n^{i_n}, \quad \text{for } j = 0, 1, \dots, n,$$

with generic coefficients c_{j,i_1,\dots,i_n} and variables y_1, \dots, y_n . The composed polynomials $f_i \circ (g_1, \dots, g_n)$, $i = 0, 1, \dots, n$, are $(m_1 k_1, \dots, m_n k_n)$ -degree as well.

For $\alpha \in \overline{\Delta}_F$, we have $0 \leq \alpha_i < (n - i + 1)m_i$, and for $\beta \in \Delta_F$, we have $0 \leq \beta_i < im_i$ for $i = 1, \dots, n$, [21]. Therefore $|\overline{\Delta}_F| = |\Delta_F| = n! m_1 \cdots m_n$.

To apply Lemma 4, in the above support, the sum of all points in the support for a particular coordinate $i \in \{1, \dots, n\}$ is

$$\sum_{\alpha \in \overline{\Delta}_F} \alpha_i = n! m_1 \cdots m_n \frac{(n - i + 1)m_i - 1}{2}, \quad \sum_{\beta \in \Delta_F} \beta_i = n! m_1 \cdots m_n \frac{im_i - 1}{2}.$$

Substituting into Lemma 4, $\det [\text{Diag}_{\overline{\mathcal{Q}}}(\Theta_F)] = (\det(\Theta_F))^{k_1 \cdots k_n}$, and

$$\det [A_L] = \prod_{i=1}^n d_{i, k_i}^{n! m_1 \cdots m_n \frac{(n-i+1)m_i-1}{2} k_1 \cdots k_n},$$

$$\det [A_R] = \prod_{j=1}^n d_{j, n_j}^{(n! m_1 \cdots m_n + n! m_1 \cdots m_n \frac{im_i-1}{2}) k_1 \cdots k_n}.$$

Note that if F and G are generic, then the coefficients of $F \circ G$ will still not have any algebraic relations, and therefore the system $F \circ G$ is generic. By Theorem 2 and the fact that the Dixon matrix is exact for generic n -degree systems [8], we have another main result of the paper.

Theorem 4. *For the unmixed n -degree case,*

$$\text{Res}(F \circ G) = \left(d_{1, k_1}^{m_1} \cdots d_{n, k_n}^{m_n} \right)^{\frac{(n+1)!}{2} m_1 \cdots m_n k_1 \cdots k_n} \text{Res}(F)^{k_1 \cdots k_n}.$$

5 Conclusion

This paper studied the behavior of the Cayley-Dixon construction of resultants for multi-univariate composed polynomials. It gave a factorization of the Cayley-Dixon matrix induced by the structure of the composed polynomials and it showed how to efficiently extract the Dixon projection operator utilizing the factorization of the Cayley-Dixon matrix.

In a special case, when polynomials substituted for the variables are $g_i = x_i^k$, the composition problem in the context of Cayley-Dixon construction was analyzed in [18], where it was studied as support scaling. Under this setting, the main result of that paper coincides with Theorem 2. Results presented here are thus a strict generalization.

A new resultant formula has also been derived for multi-univariate composition of n -degree systems.

References

1. Sederberg, T., Goldman, R.: Algebraic geometry for computer-aided design. IEEE Computer Graphics and Applications **6** (1986) 52–59

2. Hoffman, C.: Geometric and Solid modeling. Morgan Kaufmann Publishers, Inc., San Mateo, California 94403 (1989)
3. Morgan, A.: Solving polynomial systems using continuation for Scientific and Engineering problems. Prentice-Hall, Englewood Cliffs, NJ (1987)
4. Chionh, E.: Base points, resultants, and the implicit representation of rational Surfaces. PhD dissertation, Univ. of Waterloo, Dept. of Computer Science (1990)
5. Zhang, M.: Topics in Resultants and Implicitization. PhD thesis, Rice University, Dept. of Computer Science (2000)
6. Bajaj, C., Garrity, T., Warren, J.: On the application of multi-equational resultants. Technical Report CSD-TR-826, Dept. of Computer Science, Purdue (1988)
7. Ponce, J., Kriegman, D.: Elimination Theory and Computer Vision: Recognition and Positioning of Curved 3D Objects from Range. In: Symbolic and Numerical Computation for AI. Academic Press (1992) Donald, Kapur and Mundy (eds.).
8. Kapur, D., Saxena, T., Yang, L.: Algebraic and geometric reasoning using the Dixon resultants. In: ACM ISSAC 94, Oxford, England (1994) 99–107
9. Rubio, R.: Unirational Fields. Theorems, Algorithms and Applications. PhD thesis, University of Cantabria, Santander, Spain (2000)
10. Cheng, C.C., McKay, J.H., Wang, S.S.: A chain rule for multivariable resultants. Proceedings of the American Mathematical Society **123** (1995) 1037–1047
11. Jouanolou, J.P.: Le formalisme du résultant. Adv. Math. **90** (1991) 117–263
12. Minimair, M.: Factoring resultants of linearly combined polynomials. In Sendra, J.R., ed.: Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, New York, NY, ACM (2003) 207–214 ISSAC 2003, Philadelphia, PA, USA, August 3-6, 2003.
13. Minimair, M.: Computing resultants of partially composed polynomials. In Ganzha, V.G., Mayr, E.W., Vorozhtsov, E.V., eds.: Computer Algebra in Scientific Computing. Proceedings of the CASC 2004 (St. Petersburg, Russia). TUM München (2004) 359–366
14. Hong, H., Minimair, M.: Sparse resultant of composed polynomials I. J. Symbolic Computation **33** (2002) 447–465
15. Buse, L., Elkadi, M., Mourrain, B.: Generalized resultants over unirational algebraic varieties. J. Symbolic Computation **29** (2000) 515–526
16. Kapur, D., Saxena, T.: Comparison of various multivariate resultants. In: ACM ISSAC 95, Montreal, Canada (1995)
17. Hong, H.: Subresultants under composition. J. Symb. Comp. **23** (1997) 355–365
18. Kapur, D., Saxena, T.: Extraneous factors in the Dixon resultant formulation. In: ISSAC, Maui, Hawaii, USA (1997) 141–147
19. McKay, J.H., Wang, S.S.: A chain rule for the resultant of two polynomials. Arch. Math. **53** (1989) 347–351
20. Zhang, M., Goldman, R.: Rectangular corner cutting and sylvester \mathcal{A} -resultants. In: Proc. of the ISSAC, (St. Andrews, Scotland)
21. Chtcherba, A.D.: A new Sylvester-type Resultant Method based on the Dixon-Bézout Formulation. PhD dissertation, University of New Mexico, Department of Computer Science (2003)
22. Dixon, A.: The eliminant of three quantics in two independent variables. Proc. London Mathematical Society **6** (1908) 468–478
23. Cox, D., Little, J., O’Shea, D.: Using Algebraic Geometry. first edn. Springer-Verlag, New York (1998)
24. Chtcherba, A.D., Kapur, D., Minimair, M.: Cayley-dixon construction of resultants of multi-univariate composed polynomials. Technical Report TR-CS-2005-15, Dept. of Computer Science, University of New Mexico (2005)