On the Complexity of Chow and Hurwitz Forms

M. Levent Dogan, Alperen Ergür, Elias Tsigaridas

ACM Communications in Computer Algebra, Vol. 57, No. 4, Issue 226, December 2023

On the Complexity of Chow and Hurwitz Forms

M. Levent Dogan
Technische Universität Berlin
Berlin, Germany
dogan@math.tu-berlin.de

Alperen A. Ergür
The University of Texas at San Antonio
San Antonio, Texas, U.S.A.
alperen.ergur@utsa.edu

Elias Tsigaridas
INRIA Paris and Sorbonne Université
Paris, France
elias.tsigaridas@inria.fr

Abstract

We consider the bit complexity of computing Chow forms of projective varieties defined over integers and their generalization to multiprojective spaces. We develop a deterministic algorithm using resultants and obtain a single exponential complexity upper bound. Earlier computational results for Chow forms were in the arithmetic complexity model; thus, our result represents the first bit complexity bound. We also extend our algorithm to Hurwitz forms in projective space and we explore connections between multiprojective Hurwitz forms and matroid theory. The motivation for our work comes from incidence geometry where intriguing computational algebra problems remain open.

1 Introduction

Suppose a curve in space is given geometrically, e.g., in parametric form, how can one find an algebraic representation of this curve? This was a question tackled by Cayley [10] and later generalized to arbitrary varieties by van der Waerden and Chow by introducing what is now called the Chow form [56]. The Chow form is now recognized as a fundamental construction in algebraic geometry and it is particularly important in elimination theory. The structural and computational aspects of Chow forms have been an active area of research for several decades, we humbly provide a sample of references: [38, 14, 5, 34, 40]. Despite the large body of literature on the subject, one basic aspect has received little attention: the bit complexity of computing a Chow form. Our paper fills this gap. We also extend our algorithmic results to Hurwitz forms [53] and to the recent generalization of Chow forms for multiprojective varieties [46].

Another motivation for deriving precise complexity bounds for computing Chow forms comes from combinatorics: Let $S_1, S_2 \subset \mathbb{C}^2$ be two finite sets and let p be a 4-variate polynomial. How many zeros of p can be located in $S_1 \times S_2$? It was noticed in [45] that this simple question has surprising consequences in extremal combinatorics and incidence geometry. This question almost entirely looks like a subject for the Schwartz-Zippel-De Millo-Lipton (SZDL) lemma [43], but S_1 and S_2 are two dimensional.

In [18] we developed a multivariate generalization of the SZDL lemma: Suppose $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_m)$ is a partition of n, that is $n = \sum_{i=1}^{m} \lambda_i$. Let $0 \neq p \in \mathbb{C}[x_1, x_2, \ldots, x_n]$ be a polynomial of degree d and assume that for any collection of positive dimensional varieties $V_i \subset \mathbb{C}^{\lambda_i}$, for $i = 1, 2, \ldots, m$, we have $V_1 \times V_2 \times \ldots \times V_m \not\subset \mathbb{V}(p)$. Then, for any collection of finite sets $S_i \subset \mathbb{C}^{\lambda_i}$, any real $\varepsilon > 0$, and $S := S_1 \times S_2 \times \ldots \times S_m$ we have

$$|\mathbb{V}(p) \cap S| = O_{n,d,\varepsilon}\Big(\prod_{i=1}^{m} |S_i|^{1-\frac{1}{\lambda_i+1}+\varepsilon} + \sum_{i=1}^{m} \prod_{j \neq i} |S_j| \Big).$$

Note that the containment assumption on the variety $\mathbb{V}(p)$ is necessary for any non-trivial upper bound to hold: one can simply place any collection of finite sets S_i with arbitrary size on the positive dimensional varieties V_i. For applications in incidence geometry, we need to certify this assumption on the polynomial p that encodes the incidence relation. This brings us to the following problem.

Problem 1.1. *Assume that we are given an n-variate polynomial p and a positive integer vector $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_m)$ where $n = \sum_{i=1}^{m} \lambda_i$. Decide whether there exist positive dimensional varieties $V_i \subset \mathbb{C}^{\lambda_i}$ for $i = 1, 2, 3, \ldots, m$ such that $V_1 \times V_2 \times \cdots \times V_m \subset \mathbb{V}(p)$.*

Note that a variety $\mathbb{V}(p)$ of degree d can contain varieties of arbitrary degree (think of a high degree curve included in an hyperplane). Hence, the problem resists standard computational algebra tools that have to assume a degree bound on V_i. Our paper [18] includes an algorithm to decide if $\mathbb{V}(p)$ contains a cartesian product of hypersurfaces. One can hope to utilize multiprojective Chow form(s) of $\mathbb{V}(p)$ to relate the general containment Problem 1.1 to the special case of hypersurface containment. This was our motivation to develop precise complexity bounds for computing multiprojective Chow forms.

1.1 Previous Works and Our Results

The Chow form of a variety can be computed by using standard tools of elimination theory, e.g., Gröbner basis, in a black-box manner [14]. This black-box approach does not exploit the special structure of the problem and does not yield precise complexity estimates. Instead, we will rely on resultant computations. Roughly speaking, for a (homogeneous) polynomial system of n equations in $m \geq n$ variables, the resultant is a polynomial in $m - n$ variables (and in the coefficients of the original polynomials) that is zero if and only if the original system has a solution; we refer to [22, 12] for further details. Resultants are typically computed using a formula that expresses them as a factor of the determinant of a square matrix. Other factors of this determinant can sometimes be identically zero and might prevent us to compute the resultant. Canny [6] introduced the generalized characteristic polynomial that symbolically perturbs the input polynomials and avoid the unsolicited vanishing of components. Our computations rely on Canny's technique.

To our knowledge, the first algorithm with a precise complexity estimate to compute the Chow form of a pure dimensional variety, say V, is due to Caniglia [5]. Caniglia's algorithm is based on a clever reduction to linear algebra and it admits a single exponential upper bound on the number of arithmetic operations. In the case where the defining polynomials of V are given by straight-line programs, Jeronimo et al. [34] describe a probabilistic algorithm that computes the Chow form of V, see also [35]. This Las Vegas algorithm admits a single exponential time upper bound on a Blum-Shub-Smale (BSS) machine. Its expected complexity is polynomial in terms of the input size and the geometric degree of the variety V and thus; a single exponential time worst case complexity. See [34, Theorem 1] for the exact statement.

Our contribution There is an extensive literature on the complexity of elimination theory procedures in general, and complexity of polynomial system solving in particular; we provide a small sample here [23, 31, 30, 8, 25]. Despite the strong literature on the subject, we were not able to locate any results on the bit complexity of computing Chow forms. We present a single exponential time algorithm to compute the Chow form of a pure dimensional variety where the computational model is the bit model; see Proposition 3.3 for the complete intersection case and Theorem 3.9 for the general case. We further extend our algorithmic techniques to compute Hurwitz forms [53] with precise complexity estimates, see Proposition 3.10.

There is a generalization by Osserman and Trager [46] of Chow forms for varieties in multiprojective space. Our method to compute the Chow form is based on resultant computations and this seamlessly extends to multiprojective space, see Lemma 4.5 for the complete intersection case and Theorem 4.8 for the general case. We should emphasize that the generalization from the projective Chow forms to the multiprojective ones is far from straightforward both from the mathematical and algorithmic complexity

point of views. Even though a multiprojective space is isomorphic to a projective variety via the Segre embedding, this requires adding many more additional variables. To work directly with multiprojective spaces and avoid the use of (many more) additional variables we have to take into account the partition of the variables in blocks, the combinatorics of the supports of the polynomials, and exploit this structure both from a mathematical and an algorithmic point of view. Moreover, the number of blocks (and the variables in each block) should also appear in the corresponding complexity estimates. We refer to Section 4 for a detailed presentation.

In addition, we discuss a multihomogeneous generalization of the Hurwitz form. To the best of our knowledge, our paper provides the first result in this area. Contrary to the homogeneous case, multigraded Chow forms and Hurwitz form require a choice of a non-degenerate multidimension vector for the linear subspace, in a sense that is discussed in Section 4. This set of non-degenerate dimension vectors gives rise to an interesting combinatorial structure, namely a *polymatroid*. In [7], it has been proven that the set of multidegrees of a multiprojective variety forms a polymatroid. In [46], the authors show that the set of non-degenerate dimension vectors for Chow forms equals to the *truncation* of this polymatroid, which is itself a polymatroid. In a similar fashion, we show that non-degenerate dimension vectors for Hurwitz forms also form a polymatroid, which is obtained by the *elongation* of the polymatroid of Chow forms. We discuss this combinatorial structure in Section 5.

Last but not least, our techniques allow us to provide precise bit complexity estimates for the coefficients of the Chow form (both in the projective and in the multiprojective case). These bounds give an estimation on the size of the objects that we compute with and consist a measure of hardness of the corresponding algorithmic problems.

1.2 Outline of the paper

The rest of the paper is structured as follows. In section 2 we present a short overview of Chow forms. Section 3 is on the computation of the Chow form in $\mathbb{P}^n$ and the extension of techniques to compute Hurwitz forms. Section 4 presents algorithms for computing multiprojective Chow forms. Section 5 explores connections between multiprojective Chow & Hurwitz forms and matroid theory.

2 Preliminaries

2.1 Notation

The bold small letters indicate vectors or points; in particular $\boldsymbol{x} = (x_0, \ldots, x_n)$ or $\boldsymbol{x} = (x_1, \ldots, x_n)$ depending on the context. We denote by $\mathcal{O}$, resp. $\mathcal{O}_B$, the arithmetic, resp. bit, complexity and we use $\widetilde{\mathcal{O}}$, resp. $\widetilde{\mathcal{O}}_B$, to ignore (poly-)logarithmic factors. For a polynomial $f \in \mathbb{Z}[\boldsymbol{x}]$, $\mathtt{h}(f)$ denotes the maximum bitsize of its coefficients; we also call it the bitsize of f. We use $[n]$ to denote the set $\{1, 2, \ldots, n\}$. Throughout $\mathbb{C}$ denotes the field of complex numbers, $\mathbb{Z}$ integers, $\mathbb{A}^n$ the *affine space*, and $\mathbb{P}^n$ the *projective space*.

Given polynomials $\boldsymbol{f} \coloneqq (f_1, f_2, \ldots, f_k) \in \mathbb{C}[\boldsymbol{x}]^k$, we call the zero locus

$$\mathbb{V}_{\mathbb{A}}(f_1, f_2, \ldots, f_k) \coloneqq \{\boldsymbol{p} \in \mathbb{A}^n \mid f_1(\boldsymbol{p}) = f_2(\boldsymbol{p}) = \cdots = f_k(\boldsymbol{p}) = 0\},$$

the *affine variety* defined by $\boldsymbol{f}$. In the case that $\boldsymbol{f}$ consists of homogeneous polynomials, the set

$$\mathbb{V}_{\mathbb{P}}(f_1, f_2, \ldots, f_k) \coloneqq \{[\boldsymbol{p}] \in \mathbb{P}^n \mid f_1(\boldsymbol{p}) = f_2(\boldsymbol{p}) = \cdots = f_k(\boldsymbol{p}) = 0\}$$

is well-defined and called the *projective variety* defined by $\boldsymbol{f}$.

A projective variety $V \subset \mathbb{P}^n$ is called *irreducible* if we cannot write it as a non-trivial union of two subvarieties. Otherwise, V is called *reducible*. We can write every reducible variety (in an essentially unique

way) as a finite union of irreducible subvarieties, that is

$$V = \bigcup_{i=1}^{l} V_i, \qquad (V_i \subsetneq \bigcup_{j \neq i} V_j). \tag{1}$$

The irreducible subvarieties V_i are the *irreducible components* (or components for short) and the expression (1) is the *irreducible decomposition* of V.

As a preparation for the discussion on Chow forms, we define the *dimension* of a projective variety *à la Harris* [26, §11]: $\dim V$ of V is the integer r satisfying the property that *every* linear subspace $L \subset \mathbb{P}^n$ of dimension at least $(n-r)$ intersects V and a *generic* subspace $L \subset \mathbb{P}^n$ of dimension at most $(n-r-1)$ is disjoint from V. We call V *pure dimensional* (sometimes also *equidimensional*), if every irreducible component of V has the same dimension. Note that if V is irreducible, then it is trivially pure dimensional.

2.2 Associated hypersurfaces and Chow forms

The main object of our study is the associated hypersurface of a variety V and its defining polynomial, the Chow form. For a detailed introduction on Chow forms, we refer to [13, 14]. For a concise, clear, and deeper exposition we refer to [22].

Let $V \subset \mathbb{P}^n$ be an irreducible variety of dimension r. By the definiton of $\dim V$, if $L \subset \mathbb{P}^n$ is a generic linear subspace of dimension $n-r-1$, then the intersection $L \cap V$ is empty. The *associated hypersurface* of V is the set of non-generic subspaces, i.e., $(n-r-1)$-dimensional subspaces of $\mathbb{P}^n$ that have a non-empty intersection with V. To be more concrete, we consider the *Grassmannian*

$$\mathrm{Gr}(n-r-1, n) = \{L \subset \mathbb{P}^n \mid L \text{ is a subspace of dimension } n-r-1\},$$

of linear subspaces of $\mathbb{P}^n$ of dimension $n-r-1$.

Proposition 2.1. *Let $V \subset \mathbb{P}^n$ be an irreducible variety of dimension r. Then, the set of linear subspaces intersecting V,*

$$\mathcal{CZ}_V \coloneqq \{L \in \mathrm{Gr}(n-r-1, n) \mid V \cap L \neq \varnothing\} \subseteq Gr(n-r-1, n),$$

*is an irreducible hypersurface of $\mathrm{Gr}(n-r-1, n)$ that we call the **associated hypersurface** of V. Moreover, $\mathcal{CZ}_V$ uniquely defines V; that is,*

$$V = \{\boldsymbol{p} \in \mathbb{P}^n \mid \boldsymbol{p} \in L \ \textit{ implies } \ L \in \mathcal{CZ}_V\}.$$

It is known that $\mathrm{Gr}(n-r-1, n)$ has the property that every hypersurface of $\mathrm{Gr}(n-r-1, n)$ is the zero locus of a single element of its coordinate ring (see, for example, [22, Proposition 2.1]). In particular, the associated hypersurface $\mathcal{CZ}_V$ is the zero set of an element in the coordinate ring[1] of $\mathrm{Gr}(n-r-1, n)$ that we call the *Chow form* of V. We write a linear subspace $L \in \mathrm{Gr}(n-r-1, n)$ as the intersection of $r+1$ hyperplanes. For $0 \neq \boldsymbol{u} \in \mathbb{C}^{n+1}$, we consider $U(\boldsymbol{u}, \boldsymbol{x}) = u_0 x_0 + \cdots + u_n x_n$.

Definition 1. *Let $V \subset \mathbb{P}^n$ be a variety. The Chow form of V is the square-free polynomial with the property that*

$$\mathcal{CF}_V(\boldsymbol{u}_0, \ldots, \boldsymbol{u}_r) = 0 \quad \iff \quad V \cap \mathbb{V}(U(\boldsymbol{u}_0, \boldsymbol{x}), \ldots, U(\boldsymbol{u}_r, \boldsymbol{x})) \neq \varnothing$$

for $\boldsymbol{u}_0, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_r \in \mathbb{C}^{n+1}$. The Chow form is defined only up to multiplication with a non-zero scalar.

[1] For a general variety X, it is not true that every hypersurface in X is the zero locus of some element of the coordinate ring of X. The standard example is a plane curve of degree $d > 2$ and a point on the curve.

The previous definition and Proposition 2.1 imply that if V is irreducible, then $\mathcal{CF}_V$ is an irreducible polynomial which defines the irreducible hypersurface $\mathcal{CZ}_V$. More generally,

$$V = V_1 \cup V_2 \cup \cdots \cup V_l \quad \Rightarrow \quad \mathcal{CF}_V = \mathcal{CF}_{V_1} \times \mathcal{CF}_{V_2} \times \cdots \times \mathcal{CF}_{V_l}$$

holds if V is pure dimensional and $V = \bigcup_{i=1}^{l} V_i$ is the irreducible decomposition of V. If V is not pure dimensional, then a linear subspace of complementary dimension generically does not intersect the lower dimensional components so the Chow form forgets these components. We will generally assume that V is pure dimensional.

Lemma 2.2. *Suppose $V \subset \mathbb{P}^n$ is a pure dimensional variety such that $V = X_1 \cap X_2 \cap \cdots \cap X_l$, where the variety X_i is pure dimensional and $\dim V = \dim X_i$, for all $i \in [l]$. Then*

$$\mathcal{CF}_V = \gcd(\mathcal{CF}_{X_1}, \mathcal{CF}_{X_2}, \ldots, \mathcal{CF}_{X_l}).$$

Proof. Since $\dim V = \dim X_i$ for $i \in [l]$, we can see that the irreducible components of V are exactly the common irreducible components of X_i. Hence, both sides are equal to the product of the Chow forms of the components of V and this finishes the proof. □

3 The Chow Form in $\mathbb{P}^n$

In what follows $V \subset \mathbb{P}^n$ denotes an equidimensional projective variety of dimension r. We present an algorithm to compute the Chow form, $\mathcal{CF}_V$, of V.

3.1 The case of a complete intersection

Algorithm 1 ChowForm_CI

Input: $f_1, \ldots, f_{n-r} \in \mathbb{Z}[\boldsymbol{x}]$.
Precondition: $V = \mathbb{V}(f_1, \ldots, f_{n-r})$ is pure r-dimensional.
Output: The Chow form of V.

1. Consider $r+1$ linear forms, $U_i = \sum_{j=0}^{n} u_{ij} x_j$, for $0 \leq i \leq r$.
2. Eliminate the variables $\boldsymbol{x}_i$

$$R = \texttt{Elim}(\{f_1, \ldots, f_{n-r}, U_0, \ldots, U_r\}, \{\boldsymbol{x}\}) \in \mathbb{Z}[u_{i,j}].$$

3. $R_r = \text{SquareFreePart}(R)$.
4. (Optional) Apply the straightening algorithm.
5. return R_r.

Assume that $V \subset \mathbb{P}^n$ is a *set theoretic complete intersection* over $\mathbb{Z}$, i.e., V is the common zero locus of $\operatorname{codim}(V) = n - r$ many polynomials

$$V = \mathbb{V}(f_1, f_2, \ldots, f_{n-r}) \subset \mathbb{P}^n,$$

where $f_i \in \mathbb{Z}[\boldsymbol{x}]$ and $\deg(f_i) = d_i$. Let $d \coloneqq \max_i d_i$ denote the maximum of the degrees. Moreover, assume $\mathtt{h}(f_i) \leq \tau$, i.e., the bitsizes of f_i are all bounded by τ.

Let $\boldsymbol{u} = \{u_{ij} : 0 \le i \le r, 0 \le j \le n\}$ be a set of formal variables and consider the system of $r+1$ formal linear combinations

$$U(\boldsymbol{u}, \boldsymbol{x}) := \begin{cases} U_0 := u_{00}x_0 + u_{01}x_1 + \cdots + u_{0n}x_n = 0 \\ U_1 := u_{10}x_0 + u_{11}x_1 + \cdots + u_{1n}x_n = 0 \\ \vdots \\ U_r := u_{r0}x_0 + u_{r1}x_1 + \cdots + u_{rn}x_n = 0. \end{cases}$$

We will regard each polynomial in U, U_i, as a polynomial in $\mathbb{C}[\boldsymbol{u}][\boldsymbol{x}]$. Suppose for a specialization of the variables $u : u_{ij} \in \mathbb{C}, 0 \le i \le r, 0 \le j \le n$ the matrix that they naturally correspond to, say $M_u \in \mathbb{C}^{(r+1)\times(n+1)}$, is of full rank. Consequently

$$L = \mathbb{V}(U(u, \mathbf{x})) \subset \mathbb{P}^n$$

is an $(n-r-1)$-dimensional linear subspace of $\mathbb{P}^n$. Conversely, every $(n-r-1)$-dimensional subspace of $\mathbb{P}^n$ is of this form; that is, it induces a full rank $(r+1)\times(n+1)$ matrix. Moreover, $V \cap L \neq \varnothing$ holds if and only if the overdetermined system

$$U(\boldsymbol{u}, \boldsymbol{x}) = 0,\ f_1(\boldsymbol{x}) = 0,\ \ldots,\ f_{n-r}(\boldsymbol{x}) = 0 \tag{2}$$

has a solution in $\mathbb{P}^n$.

Proposition 3.1. *Let $\mathcal{R} \in \mathbb{C}[\boldsymbol{u}]$ be the resultant of the system of $n+1$ polynomials*

$$U(\boldsymbol{u}, \boldsymbol{x}) = 0, f_1(\boldsymbol{x}) = 0, \ldots, f_{n-r}(\boldsymbol{x}) = 0,$$

eliminating the variables $x_0, x_1, \ldots, x_n$. Then,

1. *$\mathcal{R}$ is invariant under the action of SL_{r+1} on $\mathbb{C}[\boldsymbol{u}]$ via the left multiplication, and,*
2. *$\mathcal{R}(u) = 0$ if and only if either (the corresponding matrix) M_u has rank $< r+1$, or, M_u is full rank and $\mathbb{V}(U(u, \boldsymbol{x})) \in \mathcal{CZ}_V$.*

Proof. The invariance of the resultant under matrices of determinant 1 is a standard result, see, for example, [12, Section 3.3]. For the second claim, note that the system (2) has a solution if and only if $L = \mathbb{V}(U(u, \boldsymbol{x}))$ intersects V. As $\dim L = n - \mathrm{rk}(u)$, L intersects V precisely when M_u is rank-deficient, or, M_u is full-rank and $L \in \mathcal{CZ}_V$. □

Proposition 3.2. *Let $\mathcal{R} = \mathcal{R}_1^{e_1}\mathcal{R}_2^{e_2}\ldots\mathcal{R}_c^{e_c}$ be the irreducible factorization of $\mathcal{R}$. Then c equals the number of irreducible components of V and the square-free part $\mathcal{R}_1\mathcal{R}_2\ldots\mathcal{R}_c$ of $\mathcal{R}$ is the Chow form of V.*

Proof. By Proposition 3.1, the zero locus of $\mathcal{R}$ coincides with the zero locus of the Chow form, $\mathcal{CF}_V$ (Definition 1). Thus, the square-free part of $\mathcal{R}$ equals $\mathcal{CF}_V$ and the number of irreducible factors of $\mathcal{R}$ and $\mathcal{CF}_V$ are equal. □

Proposition 3.3. *Consider $I = \langle f_1, \ldots, f_{n-r}\rangle \subseteq \mathbb{Z}[x_0, \ldots, x_n]$ where each f_i is homogeneous of degree at most d and has bitsize τ; also the corresponding projective variety, V, has pure dimension r. Let $\boldsymbol{u}_i := (u_{i,0}, \ldots, u_{i,n})$, for $0 \le i \le r$, be $(n+1)(r+1)$ new variables. The Chow form of V, $\mathcal{CF}_V$, is a multihomogeneous polynomial; it is homogeneous in each block of variables $\boldsymbol{u}_i$ of degree at most d^{n-r} and has bitsize $\widetilde{\mathcal{O}}(nd^{r-1}\tau)$. The algorithm* ChowForm_CI *(Alg. 1) correctly computes $\mathcal{CF}_V$ in*

$$\widetilde{\mathcal{O}}_B(n^{n^2+\omega n} d^{2(n-r)(r+1)(n+1)+(\omega+1)n+r-1}(n+d+\tau))$$

bit operations, where ω is the exponent of matrix multiplication.

Proof. The correctness of the algorithm follows from Propositions 3.1 and 3.2.

To compute the Chow form, following Alg. 1, we introduce $r+1$ linear forms, say

$$U_i = u_{i,0}x_0 + \cdots + u_{i,n}x_n,$$

where $\boldsymbol{u}_i := (u_{i,0}, \ldots, u_{i,n})$, for $0 \leq i \leq r$, are $(n+1)(r+1)$ new variables. The Chow form is the square-free part of the resultant of the system

$$\boldsymbol{F} = \{f_1, \ldots, f_{n-r}, U_0, \ldots, U_r\},$$

say $\mathcal{R}$, where we consider the polynomials as elements in $(\mathbb{Z}[\boldsymbol{u}])[\boldsymbol{x}]$ and we eliminate the variables $\boldsymbol{x}$; thus $\mathcal{CF}_V \in \mathbb{Z}[\boldsymbol{u}_0, \ldots, \boldsymbol{u}_r]$.

Bounds on the degree and the bitsize. We compute the resultant $\mathcal{R}$ using the Macaulay matrix, M, corresponding to the system $\boldsymbol{F}$, as quotient of two determinants, that is $\mathcal{R} = \det(M)/\det(M_1)$, where M_1 is a submatrix of M. To avoid the case where the denominator is zero, that is $\det(M_1) = 0$, we apply generalized characteristic polynomial technique of Canny [6]. For this we symbolically perturb the polynomials using a new variable s; that is $\hat{f}_i = f_i + sx_i^{d_i}$, for $i \in [n-r]$. Now the system becomes

$$\hat{\boldsymbol{F}} := \{\hat{f}_1, \ldots, \hat{f}_{n-r}, U_0, U_1, \ldots, U_r\},$$

where we consider the elements in $\hat{\boldsymbol{F}}$ as polynomials in the variables $\boldsymbol{x}$ with coefficients in $\mathbb{Z}[\boldsymbol{u}, s]$.

The resultant of the new system, say $\hat{\mathcal{R}}$, that we obtain after eliminating the variables $\boldsymbol{x}$, is a polynomial in $\mathbb{Z}[\boldsymbol{u}, s]$. We recover $\mathcal{R}$ as the first non-vanishing coefficient of $\hat{\mathcal{R}}$, by interpreting the latter as a univariate polynomial in s. The resultant is a multihomogeneous polynomial in the coefficients of the input polynomials [12, Chapter 3]. In our case, the monomials of $\hat{\mathcal{R}}$ are of the form

$$\varrho\, \boldsymbol{a}_1^{\mathcal{W}_1} \cdots \boldsymbol{a}_{n-r}^{\mathcal{W}_{n-r}} \boldsymbol{b}_0^{\mathcal{W}_{n-r+1}} \cdots \boldsymbol{b}_r^{\mathcal{W}_n},$$

where $\rho \in \mathbb{Z}$. The integer ρ, roughly speaking, corresponds to the lattice points of the Newton polytopes of the input polynomials, we refer to [50] for further details. The interpretation of $\boldsymbol{a}_i$ is that it represents a product of coefficients of $\hat{f}_i$ of total degree $W_i = |\mathcal{W}_i|$, for $i \in [n-r]$. Similarly, $\boldsymbol{b}_j^{\mathcal{W}_{n-r+j}}$ represents a product of coefficients of U_j of total degree $W_{n-r+j} = |\mathcal{W}_{n-r+j}|$, for $0 \leq j \leq r$. Finally, W_k is the Bézout bound on the solutions of the system $\hat{\boldsymbol{F}}$ if we exclude the k-th equation. It holds $W_i \leq d^{n-r-1}$, for $i \in [n-r]$, and $W_{n-r+j} \leq d^{n-r}$, for $0 \leq j \leq r$.

The degree of $\hat{\mathcal{R}}$ w.r.t. s is at most $(n-r)\max\{W_1, W_2, \ldots, W_{n-r}\}$. Its coefficients, and so also $\mathcal{R}$, by interpreting $\hat{\mathcal{R}}$ as a univariate polynomial in s, are multihomogeneous polynomials w.r.t. each block of variables $\boldsymbol{u}_i$ of degree bounded by $W_n \leq d^{n-r}$.

To bound the bitsize of $\hat{\mathcal{R}}$, and thus the bitsize of $\mathcal{R}$, we follow the same techniques as in [21, Theorem 5]. For a worst case bound, it suffices to consider that each $\boldsymbol{a}_i$ is of the form $(s+2^\tau)$. Thus, following Claim A.1, the bitsize of $\boldsymbol{a}_i^{\mathtt{M}_i}$ is at most $\mathcal{O}((n-r)d^{n-r-1}\tau + (n-r)^2 d^{n-r-1}\lg(nd))$ which is $\widetilde{\mathcal{O}}((n-r)d^{n-r-1}(\tau + n - r))$. Hence, the product of all of them has bitsize $\mathcal{O}((n-r)^2 d^{n-r-1}\tau + (n-r)^3 d^{n-r-1}\lg(nd)) = \widetilde{\mathcal{O}}(n^2 d^{n-r-1}(n+\tau))$. Similarly, each $\boldsymbol{b}_j^{\mathtt{M}_{n-r+j}}$ has bitsize $\mathcal{O}((n-r)d^{n-r}\lg d)$ and the product of all of them $\mathcal{O}((n-r)rd^{n-r}\lg d + n(n-r)^2 r\lg(rd)) = \widetilde{\mathcal{O}}(n^2(d^{n-r}+n))$. In addition, it holds that $\mathtt{h}(\rho) = \widetilde{\mathcal{O}}(n^2 d^{n-r})$ [21, Table 1]. Putting all the bounds together, we deduce that the bitsize of $\hat{\mathcal{R}}$, and hence the bitsize of $\mathcal{R}$ is

$$\widetilde{\mathcal{O}}(n^2 d^{n-r-1}(n+d+\tau)).$$

Computing the determinant(s). To actually compute the resultant we exploit Kronecker's trick and efficient algorithms for computing the determinant of matrices with polynomial entries.

Let $D_1 := (n-r)d^{n-r-1}$ be a bound on the degree of s and $D_2 := d^{n-r}$ a bound on the variables $\boldsymbol{u}$ in the polynomial $\hat{\mathcal{R}}$. We perform the following substitutions

$$u_{0,0} \to s^{(D_1+1)}, u_{0,1} \to s^{(D_1+1)(D_2+1)}, u_{0,2} \to s^{(D_1+1)(D_2+1)^2}, \ldots, u_{r,n} \to s^{(D_1+1)(D_2+1)^{(n+1)(r+1)-1}}.$$

In this way the elements of the Macaulay matrix M become univariate polynomials in s of degree at most $(D_1+1)(D_2+1)^{(n+1)(r+1)}$ and bitsize τ. Also M is a square $m \times m$ matrix, where m corresponds to the number of homogeneous monomials of degree $\sum_{i=1}^{n-r}(d-1) + \sum_{i=0}^{r}(1-1)+1 = (n-r)(d-1)+1$ in $n+1$ variables; that is $m = \binom{(n-r)(d-1)+1+n}{n} \leq ((n-r)d)^n$.

Now we compute the quotient $\det(M(s))/\det(M_1(s)) \in \mathbb{Z}[s]$ and we recover $\mathcal{R}$ from the first non-vanishing coefficient of this polynomial. The computation of the determinants costs at most $\widetilde{\mathcal{O}}(m^\omega\,(D_1+1)(D_2+1)^{(n+1)(r+1)})$ operations and if we multiply by the bitsize of the output, then we deduce that the computation of the resultant $\mathcal{R}$ costs

$$\widetilde{\mathcal{O}}_B(2^{(n+1)(r+1)} n^{n^2+\omega n} d^{[(n-r)(r+1)+1](n-r)+(\omega+1)n+r-1}(n+d+\tau))$$

bit operations, where ω is the exponent of the complexity of matrix multiplication.

Square-free factorization. Finally, we have to compute the square-free part of $\mathcal{R}$. This amounts, roughly, to one gcd computation. For polynomials in ν variables, of degree δ and bitsize L, the gcd costs $\widetilde{\mathcal{O}}_B(\delta^{2\nu}L)$ [42, Lemma 4]. This translates to

$$\widetilde{\mathcal{O}}_B(n^2(r+1)^{2(n+1)(r+1)} d^{2(n-r)(n+1)(r+1)+n-r-1}(n+d+\tau)).$$

Combining the two complexity bounds, after some simplifications, we obtain the claimed result. □

3.2 The case of an over-determined system

Algorithm 2 ChowForm

Input: $f_1, \ldots, f_m \in \mathbb{Z}[\boldsymbol{x}], r \in \mathbb{N}$
Precondition: Assumption 3.5.
Output: The Chow form of $\mathbb{V}(f_1, \ldots, f_m)$.

1. $\Lambda^1, \ldots, \Lambda^N :=$ GenericLC$(f_1, f_2, \ldots, f_m)$.
2. **for** $r \in [N]$ **do** $F_i =$ ChowForm_CI$(\Lambda^i_{\boldsymbol{f}})$;
3. return $\gcd(F_1, \ldots, F_N)$

Now we remove the assumption of complete intersection. Consider

$$V = \mathbb{V}(f_1, f_2, \ldots, f_m) \subset \mathbb{P}^n,$$

where $m \geq n - r = \operatorname{codim} V$. Moreover, if $d_i := \deg(f_i)$ we further assume that $d_1 \geq d_2 \geq \cdots \geq d_m$. As before, we want to add to our system $r+1$ linear forms and eliminate the variables $\boldsymbol{x}$. However, if we simply add the linear forms, then we end up with more than $n+1$ polynomials. Thus, we cannot use resultant computations, at least directly, to perform elimination.

To overcome this obstacle we consider the following observation.

Proposition 3.4. *Every pure-dimensional variety $V \subset \mathbb{P}^n$ can be written as the intersection of finitely many complete intersections: $V = V_1 \cap V_2 \cap \cdots \cap V_l$ where $\forall i$, $\dim V_i = \dim V$.*

The proposition offers a strategy to compute $\mathcal{CF}_V$: 1) Compute complete intersections $V_1, V_2, \ldots, V_l$ such that V equals their intersection, 2) compute the Chow form $\mathcal{CF}_{V_i}$ of each X_i by the means of Algorithm 1, 3) compute the gcd of $\mathcal{CF}_{V_i}, i = 1, 2, \ldots, l$. Since V is the intersection of X_i, we have $\mathcal{CF}_V = \gcd(\mathcal{CF}_{V_i} \mid i = 1, 2, \ldots, l)$ by Lemma 2.2.

In order to compute complete intersections V_i whose intersection is V, we will proceed as follows: We replace the original system $\boldsymbol{f}$ with a generic system of $\operatorname{codim}(V) = n - r$ many polynomials $\tilde{f}_i$ that vanish on V, by choosing $\tilde{f}_i$ to be generic linear combinations of f_i. We will prove that the zero locus of the new system is a pure r-dimensional variety that contains V (Proposition 3.6). By repeating this process, say k times, we obtain a number of pure dimensional varieties, $V_1, V_2, \ldots, V_k$, all containing V. For large enough k, the intersection $V_1 \cap \cdots \cap V_k$ is exactly V. What the exact number of required pure-dimensional varieties itself is an interesting question. Proposition 3.7 gives the upper bound $k = \lceil \frac{m}{n-r} \rceil$. The Chow form of V satisfies

$$\mathcal{CF}_V = \gcd(\mathcal{CF}_{V_1}, \ldots, \mathcal{CF}_{V_k}).$$

Moreover, each V_i is a set theoretic complete intersection and so we can use Alg. 1 to compute its Chow form $\mathcal{CF}_{V_i}$.

First, we modify the set of polynomials $\boldsymbol{f}$ so that it contains only polynomials of the same degree. Let $d = \max_i d_i$. We replace each f_i satisfying $d_i < d$ with the set of polynomials

$$x_0^{d-\deg f_i} f_i,\ x_1^{d-\deg f_i} f_i,\ \ldots,\ x_n^{d-\deg f_i} f_i.$$

The zero locus of the new system, which has less than $(n+1)m$ polynomials, equals the zero locus of the original system, but now the polynomials all have the same degree. So in what follows we make the following assumption:

Assumption 3.5. *$V = \mathbb{V}(f_1, f_2, \ldots, f_m) \subset \mathbb{P}^n$ is a pure dimensional variety of dimension $\dim(V) = r$, where $f_1, f_2, \ldots, f_m$ are homogeneous polynomials of the same degree d.*

The assumption that f_i all have the same degree allows us to consider linear combinations of f_i. That is, for $\lambda_1, \lambda_2, \ldots, \lambda_m \in \mathbb{C}$, the polynomial $\sum_{i=1}^m \lambda_i f_i$ is also a homogeneous polynomial of degree d, and, in particular, it defines a projective hypersurface. More generally, for an arbitrary k and a matrix $\Lambda = [\lambda_{ij}] \in \mathbb{C}^{k \times m}$ we define the system

$$\Lambda_{\boldsymbol{f}} := \begin{cases} \lambda_{11} f_1 + \lambda_{12} f_2 + \cdots + \lambda_{1m} f_m \\ \lambda_{21} f_1 + \lambda_{22} f_2 + \cdots + \lambda_{2m} f_m \\ \qquad\qquad \vdots \\ \lambda_{k1} f_1 + \lambda_{k2} f_2 + \cdots + \lambda_{km} f_m, \end{cases} \tag{3}$$

that consists of k linear combinations of f_i's. Let $\mathbb{V}(\Lambda_{\boldsymbol{f}})$ denote the zero locus of this system. The next proposition shows that for generic $\Lambda \in \mathbb{C}^{k \times m}$, the variety $\mathbb{V}(\Lambda_{\boldsymbol{f}})$ is of the form

$$\mathbb{V}(\Lambda_{\boldsymbol{f}}) = V \cup X,$$

where X is a pure dimensional variety of dimension $n - k$. The proof follows, mutatis mutandis, [24, Section 3.4.1] which considers the case $k = n$.

Proposition 3.6. *For a generic choice of $\Lambda \in \mathbb{C}^{k \times m}$, the components of $\mathbb{V}(\Lambda_{\boldsymbol{f}})$ are either the components of V or of dimension $n - k$. More concretely, there exists a hypersurface $H \subset \mathbb{C}^{k \times m}$ of degree at most kd^{k-1} such that the condition holds for any $\Lambda \in \mathbb{C}^{k \times m} \setminus H$.*

Proof. We will proceed by induction on k. For $k = 1$, the condition is violated if and only if $\Lambda_{\boldsymbol{f}} = \sum_{i=1}^{m} \lambda_i f_i \equiv 0$. This is a linear condition on λ_i's. To see this, consider the matrix that has the (coefficients of the) polynomials f_i as rows. Then it suffices to require Λ not belong to the left kernel of this matrix. Let H_1 be an arbitrary hyperplane (i.e., hypersurface of degree 1) containing the left kernel. Then any $\Lambda \notin H_1$ satisfies the condition and this proves the base case.

Let $k > 1$ and assume that the claim holds for $k-1$. Let $\Lambda \in \mathbb{C}^{(k-1)\times m} \setminus H_{k-1}$ so $\mathbb{V}(\Lambda_{\boldsymbol{f}}) = V \cup X$ for some pure $(n-k+1)$-dimensional variety X. Let

$$X = X_1 \cup X_2 \cup \cdots \cup X_c$$

be the irreducible decomposition of X and disregard the components that are fully contained in V. By the Bézout bound, we know that the number of irreducible components are at most $c \leq d^{k-1}$. Now we pick arbitrary points

$$x_i \in X_i \setminus V,$$

so for each i there exists j with $f_j(x_i) \neq 0$, and form the matrix

$$M = \begin{bmatrix} f_1(x_1) & f_2(x_1) & \dots & f_m(x_1) \\ f_1(x_2) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ f_1(x_c) & \dots & \dots & f_m(x_c) \end{bmatrix}.$$

Suppose $\boldsymbol{\mu} \in \mathbb{C}^m$ is a vector such that each entry of $M\boldsymbol{\mu} \in \mathbb{C}^c$ is non-zero. Then the linear combination $\tilde{f} := \mu_1 f_1 + \mu_2 f_2 + \cdots + \mu_m f_m$ satisfies $\tilde{f}(x_i) \neq 0$ for all $i = 1, 2, \dots, c$. In particular we have $X_i \not\subset \mathbb{V}(\tilde{f})$. By Krull's principal ideal theorem, (see, for example, [19, Theorem 10.1]) the intersection $\mathbb{V}(\tilde{\boldsymbol{f}}) \cap X_i$ is either empty or pure dimensional of dimension $\dim X_i - 1$. Hence, the system $\Lambda_{\boldsymbol{f}}$ together with $\tilde{f}$ satisfies the assertion.

The condition that each entry of $M\boldsymbol{\mu} \in \mathbb{C}^c$ being non-zero amounts to $\boldsymbol{\mu}$ avoiding c (not necessarily distinct) hyperplanes, hence a hypersurface H' of degree at most $c \leq d^{k-1}$. In particular, the pairs $(\Lambda, \boldsymbol{\mu})$ with $Z(\Lambda_{\boldsymbol{f}}, \tilde{\boldsymbol{f}})$ not satisfying the condition are contained in the hypersurface

$$\big(H_{k-1} \times \mathbb{C}^m\big) \cup \big(\mathbb{C}^{(k-1)\times m} \times H'\big),$$

which has degree $(k-1)d^{k-2} + d^{k-1} \leq kd^{k-1}$ by induction. □

We apply the procedure in Proposition 3.6 with $k = n - r$ and obtain a pure r dimensional variety $\mathbb{V}(\Lambda_{\boldsymbol{f}})$ that contains V. We use ChowForm_CI (Alg. 1) to compute its Chow form. If V is not a *set theoretic complete intersection*, then $\mathbb{V}(\Lambda_{\boldsymbol{f}}) \neq V$ (since $\mathbb{V}(\Lambda_{\boldsymbol{f}})$ is a set theoretic complete intersection by its construction) so $\mathbb{V}(\Lambda_{\boldsymbol{f}})$ contains V properly. In this case, by repeating the process of Proposition 3.6 sufficiently many times we can construct varieties $\mathbb{V}(\Lambda^i_{\boldsymbol{f}})$, each being a set theoretic complete intersection, where V equals to their intersection. The next proposition implies that we only need $\lceil \frac{m}{n-r} \rceil$ many complete intersections.

Proposition 3.7. *Let $V = \mathbb{V}(f_1, f_2, \dots, f_m)$ be as in Assumption 3.5 and $N = \lceil \frac{m}{n-r} \rceil$. For a generic choice of $\Lambda^1, \Lambda^2, \dots, \Lambda^N \in \mathbb{C}^{(n-r)\times m}$, the corresponding varieties $\mathbb{V}(\Lambda^i_{\boldsymbol{f}})$ are pure dimensional varieties of dimension r and $V = \bigcap_{i=1}^{N} \mathbb{V}(\Lambda^i_{\boldsymbol{f}})$. More concretely, there is a hypersurface $H \subset \mathbb{C}^{N(n-r)\times m}$ of degree at most $N(n-r)d^{n-r-1} + m = \mathcal{O}(md^{n-r-1})$ such that for any $(\Lambda^1, \dots, \Lambda^N) \in \mathbb{C}^{N(n-r)\times m} \setminus H$, the condition is satisfied.*

Proof. Consider the matrix

$$\Xi = [\Lambda^1, \Lambda^2, \cdots, \Lambda^N]^\top \in \mathbb{C}^{N(n-r)\times m},$$

and let $\mathbb{V}(\Xi_{\boldsymbol{f}}) = \bigcap_{i=1}^{N} \mathbb{V}(\Lambda^i_{\boldsymbol{f}})$. For generic choices of Λ^i, the matrix Ξ has full rank. Since $N = \lceil \frac{m}{n-r} \rceil$, we have $N(n-r) \geq m$ so Ξ is injective. Thus, we have

$$\langle \Lambda^1_{\boldsymbol{f}}, \Lambda^2_{\boldsymbol{f}}, \ldots, \Lambda^N_{\boldsymbol{f}} \rangle = \langle \boldsymbol{f} \rangle$$

which implies that $V = \bigcap_{i=1}^{N} \mathbb{V}(\Lambda^i_{\boldsymbol{f}})$.

Note that Ξ satisfies the condition if and only if each Λ^i avoids the hypersurface of degree $(n-r)d^{n-r-1}$ from Proposition 3.6 and Ξ is full rank. We can guarantee the second condition by enforcing a particular maximal minor of Ξ to be non-zero. Thus, Ξ satisfies the condition if it avoids N hypersurfaces of degree $(n-r)d^{n-r-1}$ and a hypersurface of degree m. □

Algorithm 3 GenericLC

Input: $f_1, \ldots, f_m \in \mathbb{Z}[\boldsymbol{x}], r \in \mathbb{N}$
Precondition: Assumption 3.5.
Output: $(\Lambda^1, \Lambda^2, \ldots, \Lambda^N)$.
Postcondition: See Proposition 3.7.

1. $N \coloneqq \lceil \frac{m}{n-r} \rceil$.
2. $S \coloneqq [N(n-r)d^{n-r-1} + m + 1] \subset \mathbb{N}$
3. **for** $(\Lambda^1, \Lambda^2, \ldots, \Lambda^N) \in S^{N(n-r)\times m}$ **do**
   if $\dim(\mathbb{V}(\Lambda^i_{\boldsymbol{f}})) \leq r$ and Ξ is full-rank **then**
   return $(\Lambda^1, \ldots, \Lambda^N)$;

Lemma 3.8. *Algorithm 3 returns N matrices $\Lambda^1, \Lambda^2, \ldots, \Lambda^N \in \mathbb{C}^{(n-r)\times m}$ satisfying the requirements of Proposition 3.7 in $\tau m^{2m^2+\mathcal{O}(1)}(2d)^{m^2 n+\mathcal{O}(n)}$ bit operations.*

Proof. The matrix $\Xi = (\Lambda^1, \ldots, \Lambda^N)$ satisfies the requirements of Proposition 3.7 if and only if it avoids a hypersurface $H \subset \mathbb{C}^{N(n-r)\times m}$ of degree $\leq D = N(n-r)d^{n-r-1} + m$. By the bound on its degree, H cannot contain a grid $S^{N(n-r)m} \subset \mathbb{C}^{N(n-r)\times m}$ where $S \subset \mathbb{C}$ is a finite set of size $|S| > D$. By going through all $|S^{N(n-r)m}| \leq (2md^{n-r-1})^{2m^2}$ points of the grid and testing membership to H at each step, we can generate Ξ satisfying the requirement.

The membership test to H amounts to checking if (i) $\mathbb{V}(\Lambda^i_{\boldsymbol{f}})$ has dimension $\leq r$ and (ii) Ξ has rank m. If S is chosen to be the list of first $D+1$ natural numbers, then the entries of Ξ have bitsizes $\log D + 1 = \mathcal{O}(\log m + (n-r)\log d)$, so the polynomials in $\Lambda^i_{\boldsymbol{f}}$ have bitsizes bounded by $\mathcal{O}(\tau + \log m + (n-r)\log d)$. Hence, whether $\dim \mathbb{V}(\Lambda^i_{\boldsymbol{f}}) \leq r$ can be tested in $\tau m^{\mathcal{O}(1)} d^{\mathcal{O}(n)}$ (see [41, 11]). Whether Ξ is full-rank can be tested in $\mathcal{O}(\tau m^{\mathcal{O}(1)} n \log d)$. We repeat this process $(2md^{n-r-1})^{2m^2}$ times, so the total complexity becomes $\tau m^{m^2+\mathcal{O}(1)}(2d)^{m^2 n+\mathcal{O}(n)}$. □

Theorem 3.9. *Consider the ideal $I = \langle f_1, \ldots, f_m \rangle \subseteq \mathbb{Z}[x_0, \ldots, x_n]$, where each f_i is homogeneous of degree d and bitsize τ; also the corresponding projective variety, V, has pure dimension r. Let $\boldsymbol{u}_i \coloneqq (u_{i,0}, \ldots, u_{i,n})$, for $i \in [r+1]$, be $(n+1)(r+1)$ new variables. The Chow form of V, $\mathcal{CF}_V$, is a multihomogeneous polynomial;*

it is homogeneous in each block of variables $\boldsymbol{u}_i$ of degree d^r and has bitsize $\widetilde{\mathcal{O}}(nd^{r-1}\tau)$. ChowForm *(Alg. 2) computes $\mathcal{CF}_V$ in*

$$\widetilde{\mathcal{O}}_B(m^{2m^2+\kappa}\, n\, r^{6nr}(n-r)^{(\omega+1)n}\,(2d)^{2m^2n+\omega n^2r+(\omega+1)n)}\,(\tau+n)),$$

bit operations where ω is the exponent of matrix multiplication and κ is a small constant, depending on the precise complexity estimate of the dimension test in Alg. 3.

Proof. The correctness of the algorithm follows from the previous discussion and Proposition 3.7.

We apply Alg. 3 to generate $\Lambda^1, \ldots, \Lambda^N$ such that they fulfill the assumptions of Proposition 3.7. The cost of this algorithm is $\tau m^{2m^2+\kappa}(2d)^{m^2n}$.

The bitsize of the polynomials in $\Lambda^i_{\boldsymbol{f}}$ is $\mathcal{O}(\tau + \log m + n\log d) = \widetilde{\mathcal{O}}(\tau+n)$. Hence, we can compute the Chow form of each $\mathbb{V}(\Lambda^i_{\boldsymbol{f}})$ using Alg. 1 within the complexity

$$\widetilde{\mathcal{O}}_B(n(n-r)^{(\omega+1)n}r^{6nr}(2d)^{\omega n^2r+(\omega+1)n}(\tau+n)).$$

We multiply by the number of systems, $N = \mathcal{O}(m)$ to conclude.

Finally, we compute the gcd of $N = \mathcal{O}(m)$ Chow forms. As each Chow form has $(r+1)(n+1)$-variables, bitsize $\widetilde{\mathcal{O}}(nd^{r-1}(\tau+n))$ and degree $(r+1)d^r$, this operation costs $\widetilde{\mathcal{O}}_B(mnr^2d^{3r}(\tau+n))$, which is less than the claimed cost. □

Remark 1. *We have assumed in Alg. 2 that $r = \dim V$ is part of the input. We could also compute r using the algorithms in [41, 11], without changing the single exponential nature of the complexity of the algorithm.*

3.2.1 Straightening Algorithm

Let $\mathbb{C}[\boldsymbol{u}]$ denote the ring of regular functions on the space $\mathbb{C}^{(r+1)\times(n+1)}$ of matrices. The Chow form $\mathcal{CF}_V$ of the variety V is invariant under the action of SL_{r+1} on $\mathbb{C}^{(r+1)\times(n+1)}$ by left multiplication. The first fundamental theorem of invariant theory states that (see, for example, [52, Theorem 3.2.1]) every SL_{r+1} invariant polynomial can be written as a unique bracket polynomial

$$F = B([0,1,\ldots,r],\ldots,[n-r+1,n-r+2,\ldots,n+1])$$

in the bracket $[i_0,\ldots,i_r]$ polynomials. The computation of this representation of $\mathcal{CF}_V$ can be done by the means of Rota's straightening algorithm or the subduction algorithm. We refer to [52, § 3] and, in particular, [52, Algorithm 3.2.8] for more information.

3.3 The Hurwitz polynomial

Closely related to the Chow form of a projective variety $V \subseteq \mathbb{P}^n$ is its Hurwitz form. This is a discriminant that characterizes the linear subspaces of dimension $n-r$ that intersect V non-transversally. When $\deg(V) \geq 2$, these linear spaces form a hypersurface in the corresponding Grassmannian. The polynomial of this hypersurface is named as the Hurwitz form of V by Sturmfels [53].

Remark 2. *The assumption $\deg(V) \geq 2$ is necessary to have a hypersurface. Intuitively, if V is a linear subspace, then the condition that another linear space intersects V in less than $\deg(V)$ many points actually implies that the intersection is empty. We should consider this case as a degenerate case of the general situation.*

The computation of the Hurwitz form goes along the same lines as the computation of the Chow form. We assume that V is a complete intersection. We introduce r linear forms U_i and one linear form M, see Alg. 4. As V is a complete intersection, if the linear forms are generic, then the resulting system does not

have any solution and hence its resultant is not zero. The resultant of the system when we eliminate the variables $\boldsymbol{x}$, using the Poisson formula [12], corresponds to the evaluation of M over all the roots of the system $\{f_1 = \cdots = f_{n-r} = U_1 = \cdots = U_r = 0\}$.

The (square-free part of the) discriminant of this multivariate polynomial, by considering it as a polynomial in $\boldsymbol{m}$, the generic coefficients of the linear form M, with coefficients in $\mathbb{Z}[\boldsymbol{u}]$ is the Hurwitz polynomial.

Algorithm 4 HurwitzPoly

Input: $f_1, \ldots, f_{n-r} \in \mathbb{Z}[\boldsymbol{x}]$ (complete intersection)
Output: The Hurwitz polynomial of $\mathbb{V}(f_1, \ldots, f_{n-r})$.

1. Let $U_i = \sum_{j=0}^{n} u_{ij} x_j$, for $i \in [r]$
2. Let $M = m_0 x_0 + \cdots + m_n x_n$
3. Eliminate the variables $\boldsymbol{x}_i$

$$R_1 = \texttt{Elim}(\{f_1, \ldots, f_{n-r}, U_1, \ldots, U_r, M\}, \boldsymbol{x}) \in \mathbb{Z}[u_{i,j}][\boldsymbol{m}]$$

4. Consider the discriminant of R_1

$$R_2 = \texttt{Elim}(\{\partial R_1/\partial m_0, \ldots, \partial R_1/\partial m_n\}, \boldsymbol{m}) \in \mathbb{Z}[u_{i,j}]$$

5. The Hurwitz polynomial is the square-free part of R_2.

Proposition 3.10. *Consider $I = \langle f_1, \ldots, f_{n-r} \rangle \subseteq \mathbb{Z}[x_0, \ldots, x_n]$ where each f_i is homogeneous of degree d and has bitsize τ; also the corresponding projective variety, V, has pure dimension r. Let $\boldsymbol{u}_i := (u_{i,0}, \ldots, u_{i,n})$, for $i \in [r]$, be $(n+1)r$ new variables. The algorithm* HurwitzPoly *(Alg. 4) correctly computes the Hurwitz polynomial, in the variables $\boldsymbol{u}_i$, of V in $\widetilde{\mathcal{O}}_B((rd)^{(n^2r^2)}\tau)$ bit operations.*

Proof sketch. The dimension of the variety, V, defined by the polynomials f_i is r. Thus, by introducing r linear forms, U_i, if they are sufficiently generic, then the (augmented) system becomes zero dimensional and the number of solutions is the degree of V. Furthermore, the introduction of one more linear form, M, results a system of $n+1$ polynomials in $n+1$ variables; we concetrate on the $\boldsymbol{x}$ variables. The polynomial M plays the role of the u-resultant (also appear with the term separating linear form). If we eliminate the variables $\boldsymbol{x}$ from this system, then we obtain a polynomial in coefficients of M, R_1, that factors to linear forms. The coefficients of the linear forms in this factorization correspond to the solutions of the zero dimensional system. To force (some) of these solutions to have multiplicities we compute the discriminant R_2 of R_1. If this is zero, then there are roots with multiplicities. The square-free part of R_2, that is a polynomial in $\boldsymbol{u}$ (and in the coefficients of the polynomials f_i) is the Hurwitz form: The reason for this is the prime factorization theorem of [22] and the fact that the support set of the polynomials we are working with is a simplex. The computation of R_1 is similar to the computation of the Chow form of V (Lemma 3.9). Then, the computation of R_2 results in computing the resultant of a square system with polynomials having coefficients polynomials in $\mathbb{Z}[u]$ in $r(n+1)$ variables, of degree $\mathcal{O}(d^r)$ and bitsize $\mathcal{O}(d^r\tau)$. □

4 Multigraded Chow forms

In [46], Osserman and Trager gave a generalization of Chow forms to multiprojetive varieties, i.e., varieties in the *multiprojective space* $\mathbb{P}^{\boldsymbol{n}} \coloneqq \prod_{i=1}^{l} \mathbb{P}^{n_i}$, given as the zero locus of *multihomogeneous polynomials*. The construction of a Chow form in the multiprojective space is similar to the projective case in the sense that the multiprojective Chow form is simply defined as the defining polynomial of the set of linear subspaces of $\mathbb{P}^{\boldsymbol{n}}$ that intersects the variety. On the other hand, this intersection is dependent on the intersection theory of the variety, i.e., its class in the Chow ring of $\mathbb{P}^{\boldsymbol{n}}$, which leads to degenerate and non-degenerate cases.

In this section, we will introduce the multigraded associated varieties and provide algorithms to compute them. Moreover, we extend the results of [46] to the multigraded versions of Hurwitz forms.

Throughout $\mathbb{P}^{\boldsymbol{n}}$ denotes the multiprojective space $\mathbb{P}^{\boldsymbol{n}} = \mathbb{P}^{n_1} \times \mathbb{P}^{n_2} \times \cdots \times \mathbb{P}^{n_l}$. For $i = 1, \ldots, l$, $\boldsymbol{x}_i = (\boldsymbol{x}_{i0}, \boldsymbol{x}_{i1}, \ldots, \boldsymbol{x}_{in_i})$ denotes the coordinates of $\mathbb{P}^{n_i}$. We assume that

$$V = \mathbb{V}(f_1, f_2, \ldots, f_k) \subset \mathbb{P}^{\boldsymbol{n}} = \mathbb{P}^{n_1} \times \mathbb{P}^{n_2} \times \cdots \times \mathbb{P}^{n_l} \tag{4}$$

is an r-dimensional *multiprojective variety* where each f_i is a *multihomogeneous* polynomial of *multidegree*

$$\boldsymbol{d}_i \coloneqq \operatorname{mdeg}(f_i) = (d_{i1}, d_{i2}, \ldots, d_{il}).$$

For a vector $\boldsymbol{\alpha} \in \mathbb{N}^l$, $|\boldsymbol{\alpha}| \coloneqq \sum_{i=1}^{l} \alpha_i$ denotes the 1-norm of $\boldsymbol{\alpha}$. In particular, $|\boldsymbol{n}|$ is the dimension of $\mathbb{P}^{\boldsymbol{n}}$ and $|\boldsymbol{d}_i|$ is the total degree of f_i. For $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{N}^l$, we write $\boldsymbol{\alpha} \leq \boldsymbol{\beta}$ if $\boldsymbol{\beta}$ *dominates* $\boldsymbol{\alpha}$, i.e., $\forall i \in [l]$, $\alpha_i \leq \beta_i$ holds.

4.1 The multidegree and the support of a multiprojective variety

A linear subspace of $\mathbb{P}^{\boldsymbol{n}} = \mathbb{P}^{n_1} \times \mathbb{P}^{n_2} \times \cdots \times \mathbb{P}^{n_l}$ is defined to be a product of linear subspaces:

$$L = L_1 \times L_2 \times \cdots \times L_l.$$

We say the *format* of L is $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_l)$ if $\dim L_i = \alpha_i$. Note that as an abstract variety, L has dimension $|\boldsymbol{\alpha}| = \sum_i \alpha_i$.

Contrary to the projective case, for a multiprojective variety, the number of intersection points of a linear subspace of complementary dimension may vary with the format of the subspace. Recall that a projective variety of degree d has d intersection points with a linear subspace of complementary dimension. The simplest counter-examples in the multiprojective space occur when one considers the multiprojective varieties that are products of projective varieties. For example, if $V = \mathbb{P}^1 \times \{p\} \subset \mathbb{P}^1 \times \mathbb{P}^1$ then the intersection with linear subspaces of format $(1, 0)$ is generically empty whereas for a linear subspace of format $(0, 1)$, the intersection is a singleton.

This observation leads to the following definition which aims to capture the intersection theoretic properties of the multiprojective variety V.

Definition 2. *Let $V \subset \mathbb{P}^{\boldsymbol{n}}$ be a pure dimensional multiprojective variety of dimension r. The support* $\operatorname{supp}(V)$ *of V is the set of all formats $\boldsymbol{\alpha} \in \mathbb{N}^l$ such that $|\boldsymbol{\alpha}| = \operatorname{codim} V$ and the intersection*

$$V \cap (L_1 \times L_2 \times \cdots \times L_l)$$

of V with a generic linear subspace $L = (L_1, L_2, \ldots, L_l)$ of format $\boldsymbol{\alpha}$ is non-empty.

The multidegree[2] $\operatorname{mdeg}(V)$ *of V is the set of all tuples $(m_{\boldsymbol{\alpha}}, \boldsymbol{\alpha})$ where $\boldsymbol{\alpha} \in \operatorname{supp}(V)$ and $m_{\boldsymbol{\alpha}}$ is the number of intersection points of V with a generic linear subspace of $\mathbb{P}^{\boldsymbol{n}}$ of format $\boldsymbol{\alpha}$.*

[2]This concept is also called the *dimension* or the *multidimension* of a multiprojective variety in the literature. We reserve the term dimension for the dimension of V as a projective variety, e.g., the dimension of its Segre embedding.

We note that the number of intersection points, $m_{\boldsymbol{\alpha}}$, is finite for dimension reasons.

Example 1. *For $i \in [l]$, let $V_i \subset \mathbb{P}^{n_i}$ be projective varieties of dimension r_i and set*

$$V \coloneqq V_1 \times V_2 \times \cdots \times V_l \subset \mathbb{P}^{\boldsymbol{n}}.$$

For a linear subspace $L = L_1 \times L_2 \times \cdots \times L_l$, the equality

$$V \cap L = (V_1 \cap L_1) \times (V_2 \cap L_2) \times \cdots \times (V_l \cap L_l)$$

clearly holds. Hence, setting $\boldsymbol{\beta} \coloneqq (n_1 - r_1, n_2 - r_2, \ldots, n_l - r_l)$, one can observe that V intersects with a generic subspace of format $\boldsymbol{\beta}$ at $\prod_{i=1}^{l} \deg V_i$ many points. For any other format $\boldsymbol{\gamma}$ with $|\boldsymbol{\gamma}| = \operatorname{codim} V = |\boldsymbol{n}| - \dim V$, there exists i such that $\gamma_i + r_i < n_i$ and, thus; the intersection $V_i \cap L_i$ is generically empty. The equalities

$$\operatorname{supp}(V) = \{\boldsymbol{\beta}\}, \quad \operatorname{mdeg}(V) = \{(\prod_{i=1}^{l} \deg(V_i), \boldsymbol{\beta})\}$$

follow.

Remark 3. *The multidegree of V can be also seen as the class of V in the Chow ring of $\mathbb{P}^{\boldsymbol{n}}$. Informally, the Chow ring of $\mathbb{P}^{\boldsymbol{n}}$is the set of all formal linear combinations of the subvarieties of $\mathbb{P}^{\boldsymbol{n}}$, modulo the relations given by rational equivalences (see, for example, [20, Definition 1.3]). In the case of the multiprojective space $\mathbb{P}^{\boldsymbol{n}}$, the Chow ring is generated by the cycles of the form*

$$[L] = [L_1 \times L_2 \times \cdots \times L_l]$$

where each L_i is a linear subspace of $\mathbb{P}^{n_i}$. Two cycles $[L]$ and $[L']$ are equal if L and L' have the same format.

For a multiprojective variety $V \subset \mathbb{P}^{\boldsymbol{n}}$, the statement

$$\operatorname{mdeg}(V) = \{(d_1, \boldsymbol{\beta}_1), (d_2, \boldsymbol{\beta}_2), \ldots, (d_k, \boldsymbol{\beta}_k)\},$$

is equivalent to the statement that

$$[V] = \sum_{i=1}^{k} d_i [L_i]$$

in the Chow ring of $\mathbb{P}^{\boldsymbol{n}}$, where $L_i = [L_{i1} \times L_{i2} \times \cdots \times L_{il}]$ has format $\boldsymbol{\beta}_i$.

For an index set $\varnothing \neq I \subset [l]$, let

$$\pi_I : \prod_{i=1}^{l} \mathbb{P}^{n_i} \to \prod_{i \in I} \mathbb{P}^{n_i}$$

denote the projection of $\mathbb{P}^{\boldsymbol{n}}$ onto $\prod_{i \in I} \mathbb{P}^{n_i}$. The main result of [7] is that the support of V can be easily computed if one is given $\dim \pi_I(V)$ for each index set $\varnothing \neq I \subset [l]$.

Theorem 4.1 ([7])**.** *Assume V is an irreducible variety in $\mathbb{P}^{\boldsymbol{n}}$. Let $\boldsymbol{\beta} \in \mathbb{N}^l$ with $\boldsymbol{\beta} \leq \boldsymbol{n}$ and $|\boldsymbol{\beta}| = \operatorname{codim} V$. Then, $\boldsymbol{\beta} \in \operatorname{supp}(V)$ if and only if for all $\varnothing \neq I \subset [l]$ we have*

$$\sum_{i \in I} (n_i - \beta_i) \leq \dim \pi_I(V).$$

The above result can also be generalized to non-irreducible varieties as for a pure-dimensional multiprojective variety V with decomposition $V = V_1 \cup \cdots \cup V_k$, one has $\operatorname{supp}(V) = \cup_{i=1}^{k} \operatorname{supp}(V_i)$. See [7, Corollary 3.13] for the exact statement.

Remark 4. *Assume V is irreducible. Define the function δ from the power set $2^{[l]}$ of $[l]$ to $\mathbb{N}$ via $\delta(I) = \dim \pi_I(V)$ for $\varnothing \neq I \subset [l]$ and $\delta(\varnothing) = 0$. Then δ is a **submodular function**, meaning δ satisfies the following properties:*

1. *$\delta(\varnothing) = 0$,*
2. *for $I \subset J$, $\delta(I) \leq \delta(J)$, and,*
3. *for $I, J \subset [l]$, $\delta(I) + \delta(J) \geq \delta(I \cap J) + \delta(I \cup J)$.*

The proof of this fact can be found in [7]. We also refer to [29] for more on the combinatorial structure of $\operatorname{supp}(V)$. *We note that together with Theorem 4.1, the submodularity of* $\dim \pi_I(V)$ *implies that* $\operatorname{supp}(V) \subset \mathbb{N}^l$ *is a polymatroid. We will discuss more on this in Section 5.*

4.2 Computing the support of a multiprojective variety

In this section, we provide algorithms to compute $\operatorname{supp}(V)$ by the means of Theorem 4.1. The idea is to compute $\dim \pi_I(V)$ for every $I \subset [l]$ and iterate through each possible format $\alpha \in \mathbb{N}^l$ of dimension $\operatorname{codim}(V)$ and test membership to $\alpha \in \operatorname{supp}(V)$. Here, we emphasize the crucial observation that we do not have access to the defining equations of $\pi_I(V)$, since this requires elimination of variables and significantly increases the complexity. Instead, we will show that a small modification of the original dimension algorithms ([41, 11]) can be used to compute the dimension of any linear projection $\pi(V)$ of a variety, V.

For simplification, we will assume that $V \subset \mathbb{C}^n$ is an affine variety. To compute the dimension, there is no harm in working with affine varieties compared to projective/multiprojective ones since we can always consider the (multi)affine cone

$$V_{\mathbb{A}} \subset \prod_{i=1}^{l} \mathbb{C}^{n_i+1} = \mathbb{C}^{|n|+l}$$

over $V \subset \prod_{i=1}^{l} \mathbb{P}^{n_i}$, defined as the zero set of the same set of polynomials, $f_1, f_2, \ldots, f_k$. Then the dimension of the (multi)affine cone and the multiprojective variety is related by the formulas $\dim V_{\mathbb{A}} = \dim V + l$ and $\dim \pi_I(V_{\mathbb{A}}) = \dim \pi_I(V) + |I|$, and, in particular, we can compute $\dim \pi_I(V)$ from $\dim \pi_I(V_{\mathbb{A}})$.

The dimension algorithms in [41, 11] rely on the observation that a variety $Z \subset \mathbb{C}^n$ has dimension at least s if and only if a generic affine subspace $L \subset \mathbb{C}^n$ of dimension $n - s$ intersect Z. Now we take $Z = \pi_I(V)$. Assume $m \leq n$ and $\pi : \mathbb{C}^n \to \mathbb{C}^m$ denotes the orthogonal projection onto the first m coordinates. Then, for an affine subspace $L \subset \mathbb{C}^m$ we have

$$\pi(V) \cap L \neq \varnothing \iff V \cap \pi^{-1}(L) \neq \varnothing.$$

In particular, $\dim \pi(V) \geq s$ if and only if for a generic affine subspace $L \subset \mathbb{C}^m$ of dimension $m - s$ we have $V \cap \pi^{-1}(L) \neq \varnothing$. Note that $\pi^{-1}(L)$ is an affine subspace of dimension $n - s$ and can be given as the zero locus of s linear polynomials. The complexity of computing $\dim \pi_I(V)$ is hence equivalent to the complexity of constructing a generic linear subspace $L \subset \mathbb{C}^m$ (see [41, Lemma 5.5, Theorem 5.6]) and checking if $f_1, f_2, \ldots, f_k$ have a common zero in L. Following [41], the complexity of these tasks is bounded by $k^{\mathcal{O}(1)} d^{\mathcal{O}(n)} \mathcal{O}(\tau)$.

Theorem 4.2. *Assume $V \subset \mathbb{C}^n$ is given as the zero set of polynomials $f_1, f_2, \ldots, f_k \in \mathbb{C}[\boldsymbol{x}]$ of degree $\leq d$ with integer coefficients of bitsize $\leq \tau$. Let $m \leq n$. Then, the dimension of the image $\pi(V)$ of V under the orthogonal projection $\pi : \mathbb{C}^n \to \mathbb{C}^m$ onto the first $m \leq n$ coordinates can be computed in*

$$k^{\mathcal{O}(1)}\, d^{\mathcal{O}(n)}\, \mathcal{O}(\tau)$$

bit operations.

Theorem 4.3. *Assume $V \subset \mathbb{P}^{\boldsymbol{n}} = \prod_{i=1}^{l} \mathbb{P}^{n_i}$ is an irreducible multiprojective variety of dimension r, given as the zero set of multihomogeneous polynomials $f_1, f_2, \ldots, f_k$, of multidegrees $\boldsymbol{d}_1, \boldsymbol{d}_2, \ldots, \boldsymbol{d}_k$ and with integral coefficients of bitsize bounded by τ.*

Then, we can compute $\operatorname{supp}(V)$ *in time*

$$k^{\mathcal{O}(1)}\, D^{\mathcal{O}(|\boldsymbol{n}|)}\, 2^l\, \mathcal{O}(\tau) + 2^l \mathcal{O}(\binom{|\boldsymbol{n}| - r}{l})$$

bit operations where $D = \max_i\{|\boldsymbol{d}_i|\}$ is the maximum total degree of f_i.

Proof. Using the previous theorem, for each $I \subset [l]$ we can compute $\dim \pi_I(V)$ in

$$k^{\mathcal{O}(1)}\, D^{\mathcal{O}(|\boldsymbol{n}|)}\, \mathcal{O}(\tau).$$

Iterating through the power set $2^{[l]}$, the family $(\dim \pi_I(V) \mid I \subset [l])$ can be computed in the claimed complexity. Using Theorem 4.1, we can now compute $\operatorname{supp}(V)$ by iterating through each possible format α with $|\alpha| = |\boldsymbol{n}| - r$ and decide whether for every $I \subset [l]$ $\sum_{i \in I} n_i - \alpha_i \leq \dim \pi_I(V)$ holds. The number of possible formats is bounded by $\binom{|\boldsymbol{n}|-r}{l}$ and the number of constraints to be checked is bounded by 2^l. □

4.3 Associated varieties of multiprojective varieties

In this section, we introduce the generalization of associated hypersurfaces to multiprojective varieties. The definitions and the results of this section follow [46].

Definition 3. *Let $\alpha \in \mathbb{N}^l$ be a format such that $\alpha \leq \boldsymbol{n}$, i.e., $\forall i \in [l]$, $\alpha_i \leq n_i$, and $|\alpha| = \operatorname{codim} V - 1$. The associated variety of V of format α is defined to be the multiprojective variety*

$$\mathcal{CZ}_{V,\alpha} = \Big\{ (L_1, L_2, \ldots, L_l) \in \prod_{i=1}^{l} \operatorname{Gr}(\alpha_i, n_i) \;\mid\; V \cap (L_1 \times L_2 \times \cdots \times L_l) \neq \varnothing \Big\}.$$

That is, $\mathcal{CZ}_{V,\alpha}$ is the set of all linear subspaces of $\mathbb{P}^{\boldsymbol{n}}$ of format α that intersect V.

As the term *associated variety* suggests, $\mathcal{CZ}_{V,\alpha}$ is not always a hypersurface.

Example 2. *Assume $n_1, n_2 \geq 3$, let $V_1 \subset \mathbb{P}^{n_1}, V_2 \subset \mathbb{P}^{n_2}$ be arbitrary varieties of codimension 2 and consider $\tilde{V} \coloneqq V_1 \times V_2 \subset \mathbb{P}^{n_1} \times \mathbb{P}^{n_2}$. Since* $\operatorname{codim} \tilde{V} = 4$*, there are four possible formats for the associated varieties, namely $\alpha = (3,0), (2,1), (1,2), (0,3)$. By the symmetry of V_1, V_2, we will only consider $(3,0)$ and $(2,1)$. Note that*

$$\begin{aligned}
\mathcal{CZ}_{\tilde{V},(2,1)} &= \{(L_1, L_2) \in \operatorname{Gr}(2, n_1) \times \operatorname{Gr}(1, n_2) \mid L_1 \times L_2 \cap V \neq \varnothing\} \\
&= \{(L_1, L_2) \in \operatorname{Gr}(2, n_1) \times \operatorname{Gr}(1, n_2) \mid L_2 \cap V_2 \neq \varnothing\} \\
&= \operatorname{Gr}(2, n_1) \times \mathcal{CZ}_{V_2}
\end{aligned}$$

is indeed a hypersurface. However,

$$\begin{aligned}\mathcal{CZ}_{\tilde{V},(3,0)} &= \{(L_1,p) \in \mathrm{Gr}(3,n_1) \times \mathbb{P}^{n_2} \mid (L_1 \times \{p\}) \cap V \neq \varnothing\} \\ &= \{(L_1,p) \in \mathrm{Gr}(3,n_1) \times \mathbb{P}^{n_2} \mid p \in V_2\} \\ &= \mathrm{Gr}(3,n_1) \times V_2\end{aligned}$$

is a codimension 2 *variety in* $\mathrm{Gr}(3,n_1) \times \mathbb{P}^{n_2}$.

The formats in $\mathrm{supp}(V)$ and the formats for which the associated variety is a hypersurface are closely related. If we consider the previous example, the support $\mathrm{supp}(V)$ of V is $\{(2,2)\}$ by Example 1, and the formats α for which $\mathcal{CZ}_{V,\alpha}$ is a hypersurface are $(2,1)$ and $(1,2)$. If we mark the formats in the support of V and the formats where $\mathcal{CZ}_{V,\alpha}$ is a hypersurface, we arrive at the following diagram in the partially ordered set of the formats:

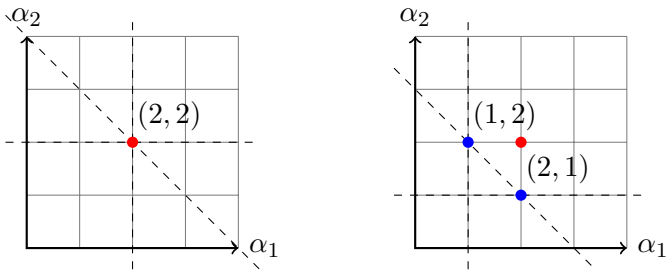

Figure 1: Example 2. On the left, we have $\mathrm{supp}(V)$, cut out by $\alpha_1+\alpha_2 = 4, \alpha_1 \geq 2, \alpha_2 \geq 2$, as described in Theorem 4.1. On the right, we have the set of formats such that the associated variety is a hypersurface which is cut out by $\alpha_1 + \alpha_2 = 3, \alpha_1 \geq 1, \alpha_2 \geq 1$.

This example is no coincidence and the next proposition clarifies the relation between $\mathrm{supp}(V)$ and the formats of associated varieties.

Proposition 4.4. *Assume* $\alpha \leq \boldsymbol{n}$ *and* $|\alpha| = \operatorname{codim} V - 1$. *Then the following are equivalent.*

1. $\mathcal{CZ}_{V,\alpha}$ *is a hypersurface.*
2. *There exists* $\beta \in \mathrm{supp}(V)$ *such that* $\alpha \leq \beta$.
3. *For all* $\varnothing \neq I \subset [l]$, *we have* $\dim \pi_I(V) \geq \sum_{i\in I}(n_i - \alpha_i) - 1$.

Proof. See Proposition 3.1 and Corollary 5.11 of [46]. □

4.4 Computing the Chow form of a multiprojective variety

In this section, we provide algorithms to compute associated varieties of multiprojective varieties. For the rest of the section, $V \subset \mathbb{P}^{\boldsymbol{n}} = \mathbb{P}^{n_1} \times \mathbb{P}^{n_2} \times \cdots \times \mathbb{P}^{n_l}$ is a pure dimensional multiprojective variety of dimension r.

4.4.1 The complete intersection case

As in the case of projective varieties, we first assume that V is a complete intersection, i.e.,

$$V = Z(f_1, f_2, \ldots, f_{|\boldsymbol{n}|-r})$$

is the zero locus of $k = |\boldsymbol{n}| - r$ many multihomogeneous polynomials. To simplify notation for the next lemma, we will denote $n = |\boldsymbol{n}| = \sum_{i=1}^{l} n_i$ and assume that $\forall i \in [k], j \in [l], \deg(f_i; \boldsymbol{x}_j) \leq d$.

Algorithm 5 MULTICHOWFORM_CI

Input: $f_1, \ldots, f_{|\boldsymbol{n}|-r} \in \mathbb{Z}[\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_l], \alpha \in \mathbb{N}^l$
Precondition: $V = \mathbb{V}(f_1, \ldots, f_{|\boldsymbol{n}|-r})$ is pure r-dimensional. $\mathcal{CZ}_{V,\alpha}$ is a hypersurface.
Output: The Chow form of V corresponding to format α.

1. Consider linear forms,
$$U_j^i \coloneqq \sum_{k=0}^{n_i} u_{jk}^i x_{ij}, \text{ for } 0 \leq j \leq n_i - \alpha_i - 1$$
for $i = 1, 2, \ldots, l$.
2. Eliminate the variables $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_l$.
$$R = \texttt{Elim}(\{f_1, \ldots, f_{|\boldsymbol{n}|-r}, U_j^i\}, \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_l\}) \in \mathbb{Z}[u_{jk}^i]$$
3. $R_r = \text{SQUAREFREEPART}(R)$.
4. RETURN R_r.

Lemma 4.5. *Let V be a r-dimensional complete intersection, i.e., V is the zero locus $\mathbb{V}(f_1, f_2, \ldots, f_{n-r})$ of $k \coloneqq n - r$ many multihomogeneous polynomials and assume that $\deg(f_i; \boldsymbol{x}_j) \leq d$ for $i \in [k], j \in [l]$ and the bitsizes of f_i are bounded by τ. Set $B_r \coloneqq (dl)^{n-r} \sum_{i=1}^{l} \binom{n-r}{\alpha_1, \ldots, \alpha_i+1, \ldots, \alpha_l}$, where the summands in the second factor are the multinomial coefficients. If α is a format that satisfies the equivalent conditions of Proposition 4.4, then the Chow form of V corresponding to α is a multihomogeneous polynomial in $A = \sum_{i=1}^{l}(n_i - \alpha_i)(n_i + 1)$ new variables of total degree at most B_r and bitsize $\widetilde{\mathcal{O}}(nB_r\tau)$.* MULTICHOWFORM_CI *(Alg. 5) computes $\mathcal{CF}_{V,\alpha}$ in*

$$\widetilde{\mathcal{O}}_B(n^{\omega+1} 2^{(\omega+1)n} B_r^{(\omega+1)r^2+2A+\omega+1} (\tau + n^3))$$

bit operations (Las Vegas) where ω is the exponent of matrix multiplication,

Proof. The proof is similar to the proof of Proposition 3.3. To exploit the multihomogeneity, we use sparse/multiprojective resultant computations and the multihomogeneous Bézout bound. We have $n - r$ multihomogeneous polynomials, each having (total) degree at most dl. To compute the $\mathcal{CF}_{V,\alpha}$ we add $(n_i - \alpha_i)$ linear forms in $\boldsymbol{x}_i$, U_j^i; their coefficients are the variables u_{jk}^i, for $i \in [l]$. The sparse resultant is an irreducible polynomial in the coefficients of f_i and u_{jk}^i, which vanishes if and only if V and the linear subspace described by U_j^i intersects.

The sparse resultant is homogeneous in each set of variables $\boldsymbol{u}_j^i$. Its degree with respect to $\boldsymbol{u}_j^i$ equals to the generic number of solutions of the remaining system when $\boldsymbol{u}_j^i$ is omitted, hence bounded by the multihomogeneous Bézout bound $(dl)^{n-r}\binom{n-r}{\alpha_1, \ldots, \alpha_i+1, \ldots, \alpha_l}$ where the second factor is the *multinomial coefficient*:

$$\binom{N}{a_1, \ldots, a_l} \coloneqq \frac{N!}{a_1!\, a_2! \ldots\, a_l!}$$

Thus, the resultant has total degree at most B_r. The coefficients are integers of bitsize $\widetilde{\mathcal{O}}(nB_r\tau)$. The number of monomials is bounded by $\widetilde{\mathcal{O}}(B_r^{r^2})$. Following [15], we compute the sparse resultant as a ratio of two determinants using the sparse resultant matrix. The sparse resultant matrix has dimension $M \times M$,

where $M = \mathcal{O}(ne^n B_r)$ and each entry of M is a coefficient of one of the input polynomials f_i or the linear forms U_j^i.

It suffices to specialize u_{jk}^i to numbers of bitsize $\mathcal{O}(n^3 \lg(d))$. So the specialized matrix contains numbers of bitsize $\widetilde{\mathcal{O}}(\tau + n^3)$. We compute each determinant in $\widetilde{\mathcal{O}}_B(M^{\omega+1}(\tau + n^3))$. We need to perform this computations $\widetilde{\mathcal{O}}(B_r^{r^2})$ many times and then we recover the resultant using interpolation. The cost of all the evaluations is $\widetilde{\mathcal{O}}_B(n^{\omega+1}2^{(\omega+1)n}B_r^{r^2+\omega+1}(\tau + n^3))$. The cost of interpolation is $\widetilde{\mathcal{O}}_B(B_r^{\omega r^2+1}(\tau + n^3))$. Finally, the cost of computing the square-free part is $\widetilde{\mathcal{O}}_B((nB_r)^{2A+1}\tau)$.

The algorithm is of Las Vegas type becauce of the construction of the resultant matrix (see the remark that follows). □

Remark 5. *In the previous complexity estimate, we should also take into account the cost for constructing the sparse resultant matrix. Following [9, Thm. 11.6] there is a Las Vegas algorithm for this computation with cost $\widetilde{\mathcal{O}}_B(M)$, where M is the size of the matrix and the number of lattice points in the Minkowski sum of the Newton polytopes of the input polynomials. In our case, as the polynomials are multihomogeneous, the corresponding Newton polytopes are product of simplices. Therefore, we can also afford to construct the resultant matrix using the lower hull of an appropriate (sufficiently generic) lifting of the lattice points of the Minkowski sum of the Newton polytopes; this costs $\widetilde{\mathcal{O}}(M^{\lfloor n/2 \rfloor})$ [48]. Neither complexity bound dominates the overall complexity; this is so because the resultant matrix contains polynomials in many variables, that is the $\boldsymbol{u}_j^i$'s.*

The Las Vegas characterization is due to the sufficiently generic lifting but also due to the random perturbation needed in order to assign the lattice points to the appropriate polynomials. We refer to [9, 15] for further details.

To avoid the case that the denominator is zero in the resultant computations, we can apply the technique of the generalized characteristic polynomial [6], similarly to the projective case. Now, we can apply a symbolic perturbation to all the terms of all the polynomials [49] or only to the terms that appear in the diagonal of the resultant matrix [44]. In both cases, we introduce one additional variable that does not affect the single exponential behavior of the complexity bound.

4.4.2 The general case

Algorithm 6 MultiChowForm

Input: $f_1, \ldots, f_m \in \mathbb{Z}[\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_l], r \in \mathbb{N}, \alpha \in \mathbb{N}^l$
Precondition: $V = \mathbb{V}(f_1, \ldots, f_m)$ is pure r-dimensional and $\mathcal{CZ}_{V,\alpha}$ is a hypersurface.
Output: The Chow form of V.

1. $\Lambda^1, \ldots, \Lambda^N :=$ MultiGenericLC$(f_1, f_2, \ldots, f_m)$.
2. **for** $r \in [N]$ **do** $F_i =$ ChowForm_CI$(\Lambda^i_{\boldsymbol{f}})$;
3. return $\gcd(F_1, \ldots, F_N)$

Now we remove the assumption that V is a complete intersection and assume

$$V = Z(f_1, f_2, \ldots, f_m) \subset \mathbb{P}^{\mathbf{n}},$$

where $m \geq |\boldsymbol{n}| - r$. Consider the multidegrees $\boldsymbol{d}^i = \mathrm{mdeg}(f_i)$ and set

$$\boldsymbol{d} = (\max_i d_1^i, \max_i d_2^i, \ldots, \max_i d_m^i).$$

Note that for all $i = 1, 2, \ldots, m$ we have $\boldsymbol{d}^i \leq \boldsymbol{d}$ by construction. For each $i = 1, 2, \ldots, m$ with $\boldsymbol{d}^i < \boldsymbol{d}$, we replace the polynomial f_i with the collection $\boldsymbol{x}_1^{\alpha_1}\boldsymbol{x}_2^{\alpha_2}\cdots\boldsymbol{x}_l^{\alpha_l} f_i$ where $\boldsymbol{x}_j$ denotes the j-th block of variables of the multiprojective space $\mathbb{P}^{\boldsymbol{n}}$ and α_j runs over the all possible monomials with $|\alpha_j| = \boldsymbol{d}_j - \boldsymbol{d}_j^i$. The new collection $\tilde{\boldsymbol{f}}$ has the property that each polynomial in it has the same multidegree, $\boldsymbol{d}$. Hence, without loss of generality, we will assume throughout the rest of the section that $V = Z(f_1, f_2, \ldots, f_m)$ where each f_i has the same multidegree, $\mathrm{mdeg}(f) = \boldsymbol{d}$.

As in the projective case, for $\Lambda \in \mathbb{C}^{k\times m}$ we consider k linear combinations $\Lambda_{\boldsymbol{f}}$ of $\boldsymbol{f}$, defined as in (3). By the assumption that each f_i has the same multidegree, each linear combination has multidegree $\boldsymbol{d}$, and, thus; has a well-defined zero locus in $\mathbb{P}^{\boldsymbol{n}}$.

For generic $\Lambda \in \mathbb{C}^{k\times m}$ we have $Z(\Lambda_{\boldsymbol{f}}) = V \cup X$ for some pure dimensional variety X of dimension $|\boldsymbol{n}| - k$. The proof is essentially the same as the projective case, Proposition 3.6 and Proposition 3.7. The only change in the proof is the bound on the number of irreducible components of a variety, where the Bézout bound is replaced by the multihomogeneous Bézout bound.

Proposition 4.6. *Let $N = \lceil \frac{m}{|\boldsymbol{n}|-r} \rceil$. For generic choices of matrices $\Lambda^1, \ldots, \Lambda^N \in \mathbb{C}^{(|\boldsymbol{n}|-r)\times m}$, each variety $\mathbb{V}(\Lambda^i_{\boldsymbol{f}})$ is a pure dimensional variety of dimension r and $V = \cap_{i=1}^N \mathbb{V}(\Lambda^i_{\boldsymbol{f}})$. More concretely, there is a hypersurface $H \subset \mathbb{C}^{N(|\boldsymbol{n}|-r)\times m}$ of degree $\leq N(|\boldsymbol{n}| - r)|\boldsymbol{d}|^{|\boldsymbol{n}|-r-1} + m$ such that for any $(\Lambda^1, \ldots, \Lambda^N) \in \mathbb{C}^{N(|\boldsymbol{n}|-r)\times m} \setminus H$, the condition is satisfied.*

The proposition allows us to consider the following algorithm to generate $(\Lambda^1, \ldots, \Lambda^N)$ satisfying the condition of Proposition 4.6.

Algorithm 7 MultiGenericLC

Input: $f_1, \ldots, f_m \in \mathbb{Z}[\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_l], r \in \mathbb{N}$
Precondition: $\mathbb{V}(f_1, f_2, \ldots, f_m)$ is pure r-dimensional.
Output: $\Lambda^1, \Lambda^2, \ldots, \Lambda^N$.
Postcondition: See Proposition 4.6.

1. $N \coloneqq \lceil \frac{m}{|\boldsymbol{n}|-r} \rceil$.
2. $S \coloneqq [N(|\boldsymbol{n}| - r)|\boldsymbol{d}|^{|\boldsymbol{n}|-r} + m + 1] \subset \mathbb{N}$.
3. **for** $(\Lambda^1, \Lambda^2, \ldots, \Lambda^N) \in S^{N(|\boldsymbol{n}|-r)m}$ **do**
   if $\dim(\mathbb{V}(\Lambda^i_{\boldsymbol{f}})) \leq r$ and Ξ is full-rank **then**
   return $\Lambda^1, \ldots, \Lambda^N$;

Lemma 4.7. *Algorithm 7 returns a tuple $(\Lambda^1, \Lambda^2, \ldots, \Lambda^N)$ satisfying the requirements of Proposition 4.6 in $\tau m^{2m^2+\mathcal{O}(1)}|2\boldsymbol{d}|^{m^2 n+\mathcal{O}(|\boldsymbol{n}|)}$.*

Proof. The proof goes as in Lemma 3.8. To test dimension of $\mathbb{V}(\Lambda^i_{\boldsymbol{f}})$, we consider the affine cone $C = \mathbb{V}_{\mathbb{A}}(\Lambda^i_{\boldsymbol{f}})$ over $\mathbb{V}(\Lambda^i_{\boldsymbol{f}})$. We have $\dim C = \dim \mathbb{V}(\Lambda^i_{\boldsymbol{f}}) + l$, so we can compute the dimension of $\mathbb{V}(\Lambda^i_{\boldsymbol{f}})$ from $\dim C$. □

For the simplicity of notation, we will assume for the next theorem that $d = \max_i \boldsymbol{d}_i$ and $n = |\boldsymbol{n}|$.

Theorem 4.8. *Consider $I = \langle f_1, \ldots, f_m \rangle \subseteq \mathbb{Z}[\boldsymbol{x}_1, \ldots, \boldsymbol{x}_l]$, where each f_i is multihomogeneous of degree $\boldsymbol{d}$ and bitsize τ; also the corresponding multiprojective variety, V, has pure dimension r. Also, $B_r = (dl)^{n-r} \sum_{i=1}^{l} \binom{n-r}{\alpha_1,\ldots,\alpha_i+1,\ldots,\alpha_l}$.*

The Chow form of V corresponding to a format α is a multihomogeneous polynomial in $A = \sum_{i=1}^{l}(n_i - \alpha_i)(n_i + 1)$ new variables of total degree $\leq B_r$ and bitsize $\widetilde{\mathcal{O}}(nB_r\tau)$.

MULTICHOWFORM *(Alg. 6) computes $\mathcal{CF}_V$ in*

$$\widetilde{\mathcal{O}}_B(m^{2m^2+\kappa}n^{\omega+1}2^{(\omega+1)n}\,B_r^{m^2n+(\omega+1)r^2+2A+\omega+1}\,(\tau+n^3)),$$

bit operations where ω is the exponent of matrix multiplication and κ is a small constant, depending on the precise complexity of the dimension test in Alg. 7.

Proof. The cost of generating $\Lambda^1, \ldots, \Lambda^N$ is $\tau m^{2m^2+\mathcal{O}(1)}(2d)^{m^2n+\mathcal{O}(n)}$ by the previous lemma.

$\Lambda^i_{\boldsymbol{f}}$ have bitsizes bounded by $\mathcal{O}(\lg m + n\lg d + n\lg l + \tau) = \widetilde{\mathcal{O}}(\tau + n)$. As there are $N = \mathcal{O}(m)$ Chow forms to compute, the second step costs $\widetilde{\mathcal{O}}_B(mn^4 2^{4n} B_r^{(\omega+1)r^2+2A+6}\,(\tau^2 + n^6))$.

For the last step, we need to compute the gcd of N Chow forms. As in the proof of Theorem 3.9, the cost of this step is less than the claimed complexity, therefore we can omit it. □

4.5 The multiprojective Hurwitz form

Recall that for a projective variety $V \subset \mathbb{P}^n$ of dimension r, the Hurwitz form is defined to be the defining polynomial of the set of all linear forms $L \in \mathrm{Gr}(n-r, n)$ such that the intersection $L \cap V$ is non-generic, i.e., either $L \cap V$ is infinite, or, $L \cap V$ is finite but $|L \cap V| < \deg V$. As in the case of the Chow forms, one readily generalizes the Hurwitz form to multiprojective varieties.

Definition 4. *Assume $V \subset \mathbb{P}^{\boldsymbol{n}}$ is an irreducible multiprojective variety of dimension r and $\alpha \in \mathbb{N}^l$ is a format with $|\alpha| = \operatorname{codim} V$. We define the higher associated variety $\mathcal{HZ}_{V,\alpha} \subset \mathbb{P}^{\boldsymbol{n}}$ as the set of all linear subspaces L of format α which intersects V in non-generic way. That is, for $\alpha \in \operatorname{supp}(V)$, $\mathcal{HZ}_{V,\alpha}$ is the set of all linear subspaces L of format α such that $V \cap L$ is either infinite, or, $|L \cap V| < \operatorname{mdeg}(V, \alpha)$. Similarly, if $\alpha \notin \operatorname{supp}(V)$, then we define $\mathcal{HZ}_{V,\alpha}$ as the set of all linear subspaces L of format α such that $L \cap V \neq \varnothing$.*

As in the case of the Chow forms, the higher associated variety is not always a hypersurface.

Example 3. *Recall Example 2, where*

$$\tilde{V} = V_1 \times V_2 \subset \mathbb{P}^{n_1} \times \mathbb{P}^{n_2}$$

for codimension 2 varieties V_1, V_2. Moreover, assume that $\deg V_1, \deg V_2 > 1$. Note that we have $\operatorname{supp}(V) = \{(2,2)\}$. For $\alpha = (4,0)$,

$$\begin{aligned}\mathcal{HZ}_{\tilde{V},(4,0)} &= \{L_1 \times \{p\} \in \mathrm{Gr}(4, n_1) \times \mathrm{Gr}(0, n_2) \mid (L_1 \times \{p\}) \cap \tilde{V} \neq \varnothing\} \\ &= \{L_1 \times \{p\} \in \mathrm{Gr}(4, n_1) \times \mathrm{Gr}(0, n_2) \mid p \in V_2\} \\ &= \mathrm{Gr}(4, n_1) \times V_2\end{aligned}$$

has codimension 2. For $\alpha = (3,1)$, on the other hand,

$$\begin{aligned}\mathcal{HZ}_{\tilde{V},(3,1)} &= \{L_1 \times L_2 \in \mathrm{Gr}(3, n_1) \times \mathrm{Gr}(1, n_2) \mid L_2 \cap V_2 \neq \varnothing\} \\ &= \mathrm{Gr}(3, n_1) \times \mathcal{CZ}_{V_2}\end{aligned}$$

is a hypersurface. For $\alpha = (2,2)$,

$$\begin{aligned}\mathcal{HZ}_{\tilde{V},(2,2)} &= \{L_1 \times L_2 \in \mathrm{Gr}(2, n_1) \times \mathrm{Gr}(2, n_2) \mid \sharp(L_1 \times L_2 \cap \tilde{V}) \neq \deg V_1 \deg V_2\} \\ &= \Big(\mathcal{HZ}_{V_1} \times \mathrm{Gr}(2, n_2)\Big) \cup \Big(\mathrm{Gr}(2, n_1) \times \mathcal{HZ}_{V_2}\Big)\end{aligned}$$

is again a hypersurface.

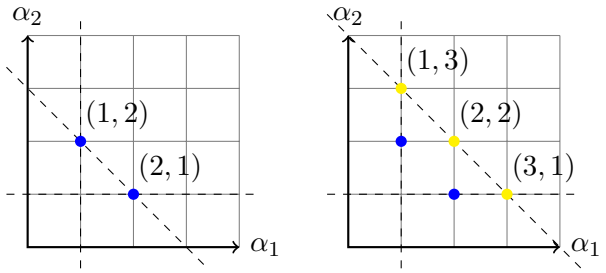

Figure 2: Example 3. The blue points are the formats for which the associated variety $\mathcal{CZ}_{\tilde{V},\alpha}$ is a hypersurface. The yellow points are the ones with $\mathcal{HZ}_{\tilde{V},\alpha}$ a hypersurface and cut out by the inequalities and the equality $\alpha_1+\alpha_2=4, \alpha_1 \geq 1, \alpha_2 \geq 1$.

Similar to the case of associated varieties of multiprojective varieties, we can classify all formats α where $\mathcal{HZ}_{V,\alpha}$ is a hypersurface.

Theorem 4.9. *Let $V \subset \mathbb{P}^{\boldsymbol{n}}$ be an irreducible multiprojecive variety of dimension r and let $\alpha \leq \boldsymbol{n}$ be a format with $|\alpha| = \operatorname{codim} V$. If $\alpha \notin \operatorname{supp}(V)$, then the following are equivalent.*

1. *$\mathcal{HZ}_{V,\alpha} \subset \prod_{i=1}^{l} \operatorname{Gr}(\alpha_i, n_i)$ is a hypersurface.*
2. *For every $\varnothing \neq I \subset [l]$ we have*
$$\sum_{i \in I} n_i - \alpha_i \leq \dim \pi_I(V) + 1.$$
3. *There exists a format $\gamma \leq \alpha$ such that $|\gamma| = \operatorname{codim} V - 1$ and $\mathcal{CZ}_{V,\gamma}$ is a hypersurface.*

If $\alpha \in \operatorname{supp}(V)$, then $\mathcal{HZ}_{V,\alpha}$ is a hypersurface if and only if $\operatorname{mdeg}(V,\alpha) \neq 1$.

Proof. The proof is similar to the proof of [46, Proposition 3.1], and it takes about two pages. ($1 \Rightarrow 2$) For $\alpha \notin \operatorname{supp}(V)$, we have

$$\mathcal{HZ}_{V,\alpha} = \{L \in \prod_{i=1}^{l} \operatorname{Gr}(\alpha_i, n_i) \mid L \cap V \neq \varnothing\}.$$

Consider the incidence variety

$$Z = \{(p, L) \in V \times \prod_{i=1}^{l} \operatorname{Gr}(\alpha_i, n_i) \mid p \in L\}$$

and the double filtration

$$V \leftarrow Z \rightarrow \mathcal{HZ}_{V,\alpha}.$$

Note that both projections are surjective. For a point $p \in V$, the fiber over p is given by

$$\{L \in \prod_{i=1}^{l} \operatorname{Gr}(\alpha_i, n_i) \mid p \in L\}$$

which is itself a product of Grassmannians and has dimension $\sum_{i=1}^{l} \alpha_i(n_i - \alpha_i)$. Hence, the incidence variety Z has dimension

$$r + \sum_{i=1}^{l} \alpha_i(n_i - \alpha_i) = \sum_{i=1}^{l} (\alpha_i + 1)(n_i - \alpha_i) = \dim(\prod_{i=1}^{l} \operatorname{Gr}(\alpha_i, n_i)).$$

In particular, $\mathcal{HZ}_{V,\alpha}$ is a hypersurface if and only if the generic fiber over a linear subspace $L \in \mathcal{HZ}_{V,\alpha}$ has dimension 1. Note that for $L \in \prod_{i=1}^{l} \mathrm{Gr}(\alpha_i, n_i)$, the fiber over L equals $L \cap V$.

Assume that the inequalities in (2) are not satisfied, i.e., there exists $\varnothing \neq I \subset [l]$ such that $\sum_{i\in I} n_i - \alpha_i > \dim \pi_I(V) + 1$. Then

$$r - \dim \pi_I(V) > r - (\sum_{i\in I} n_i - \alpha_i) + 1 = 1 + \sum_{i\notin I} n_i - \alpha_i$$

holds. In this case we will prove that $\dim(V \cap L)$ is at least 2 for a generic linear subspace $L \in \mathcal{HZ}_{V,\alpha}$. For such L, denote by L_I the product $\prod_{i\in I} L_i$ and similarly $L_{I^c} = \prod_{i\notin I} L_i$. Then, we have

$$V \cap L = \big(V \cap \pi_I^{-1}(L_I)\big) \cap \pi_{I^c}^{-1}(L_{I^c}).$$

Since $L \in \mathcal{HZ}_{V,\alpha}$, we have $V \cap \pi_I^{-1}(L_I) \neq \varnothing$. This implies that $\pi_I(V) \cap L_I \neq \varnothing$ so $V \cap \pi_I^{-1}(L_I)$ has dimension at least the generic fiber dimension of π_I, i.e.,

$$\dim(V \cap \pi_I^{-1}(L_I)) \geq r - \dim \pi_I(V) > 1 + \sum_{i\notin I} n_i - \alpha_i.$$

Since $\operatorname{codim} \pi_{I^c}^{-1}(L_{I^c}) = \sum_{i\notin I} n_i - \alpha_i$, we get $\dim(V \cap L) = \dim(V \cap \pi_I^{-1}(L_I) \cap \pi_{I^c}^{-1}(L_{I^c})) > 1$. Therefore, $\mathcal{HZ}_{V,\alpha}$ is not a hypersurface in this case.

(2 $\Rightarrow$ 3) Assume that for each $\varnothing \neq I \subset [l]$ the required inequality holds. We will show that there exists an index $j \in [l]$ such that $j \in I$ implies $\sum_{i\in I} n_i - \alpha_i \leq \dim \pi_I(V)$. Then, setting $\gamma = \alpha - \boldsymbol{e}_j = (\alpha_1, \ldots, \alpha_{j-1}, \alpha_j - 1, \alpha_{j+1}, \ldots, \alpha_l)$, for any $I \subset [l]$ we have

$$\sum_{i\in I} n_i - \gamma_i = \begin{cases} \sum_{i\in I} n_i - \alpha_i & \text{if } j \notin I \\ (\sum_{i\in I} n_i - \alpha_i) + 1 & \text{if } j \in I \end{cases} \leq \dim \pi_I(V) + 1.$$

By Proposition 4.4, we deduce that $\mathcal{CZ}_{V,\gamma}$ is a hypersurface.

To prove the existence of the index j, we set

$$S_\alpha \coloneqq \{I \subset [l] \mid \sum_{i\in I} n_i - \alpha_i = \dim \pi_I(V) + 1\}.$$

Note that $S_\alpha \neq \varnothing$ since $\alpha \notin \operatorname{supp}(V)$. We recall that the function $I \mapsto \dim \pi_I(V)$ has the property that for $I, J \subset [l]$,

$$\dim \pi_I(V) + \dim \pi_J(V) \geq \dim \pi_{I\cup J}(V) + \dim \pi_{I\cap J}(V)$$

holds (Remark 4). Then, for $I, J \in S_\alpha$, we have

$$\begin{aligned} \sum_{i\in I\cup J} n_i - \alpha_i &= \sum_{i\in I} n_i - \alpha_i + \sum_{i\in J} n_i - \alpha_i - \sum_{i\in I\cap J} n_i - \alpha_i \\ &\geq \dim \pi_I(V) + 1 + \dim \pi_J(V) + 1 - \dim \pi_{I\cap J}(V) - 1 \\ &\geq \dim \pi_{I\cup J}(V) + 1. \end{aligned}$$

Thus, $I \cup J \in S_\alpha$. On the other hand, for $I = [l]$ we have

$$\sum_{i\in[l]} n_i - \alpha_i = |\boldsymbol{n}| - |\boldsymbol{\alpha}| = r = \dim(V),$$

which implies that $[l] \notin S_\alpha$. Since S_α is closed under taking unions and $[l] \notin S_\alpha$, we deduce that there is an index $j \in [l]$ such that $I \in S_\alpha$ implies $j \notin I$. The result follows.

$(3 \Rightarrow 1)$ By permuting the indices if necessary we may assume without loss of generality that

$$\alpha = \gamma + \boldsymbol{e}_1 = (\gamma_1 + 1, \gamma_2, \ldots, \gamma_l).$$

Consider the incidence variety

$$Z = \{(L, \tilde{L}) \in \mathcal{CZ}_{V,\gamma} \times \mathcal{HZ}_{V,\alpha} \mid L \subset \tilde{L}\}$$

and the double filtration

$$\mathcal{CZ}_{V,\gamma} \leftarrow Z \rightarrow \mathcal{HZ}_{V,\alpha}.$$

Note that both projections are surjective. For $L \in \mathcal{CZ}_{V,\gamma}$, the fiber over L equals

$$\{\tilde{L} \in \prod_{i=1}^{l} \mathrm{Gr}(\alpha_i, n_i) \mid L_1 \subset \tilde{L}_1, L_2 = \tilde{L}_2, \ldots, L_l = \tilde{L}_l\}$$

which is isomorphic to the Grassmannian $\mathrm{Gr}(\alpha_1 - \gamma_1 - 1, n_1 - \gamma_1 - 1) \cong \mathbb{P}^{n_1 - \gamma_1 - 1}$. Thus, Z has dimension

$$\dim \mathcal{CZ}_{V,\alpha} + n_1 - \gamma_1 - 1 = \sum_{i=1}^{l} (\gamma_i + 1)(n_i - \gamma_i) + n_1 - \gamma_1 - 2.$$

Similarly, for $\tilde{L} \in \mathcal{HZ}_{V,\alpha}$, the fiber over $\tilde{L}$ is isomorphic to the Grassmannian $\mathrm{Gr}(\gamma_1, \alpha_1)$ with dimension $\alpha_1 = \gamma_1 + 1$. Thus, we have

$$\begin{aligned}\dim \mathcal{HZ}_{V,\alpha} &= \dim Z - \alpha_1 = \sum_{i=1}^{l} (\gamma_i + 1)(n_i - \gamma_i) + n_1 - 2\gamma_1 - 3 \\ &= \sum_{i=1}^{l} (\alpha_i + 1)(n_i - \alpha_i) - 1 = \dim(\prod_{i=1}^{l} \mathrm{Gr}(\alpha_i, n_i)) - 1.\end{aligned}$$

□

Example 4. *The condition that* $\mathrm{mdeg}(V, \alpha) \neq 1$ *is necessary and reminisces the condition* $\deg(V) \neq 1$ *in the projective case. For a linear subspace* $L = L_1 \times L_2 \times \cdots \times L_l$ *of format* α *we have*

$$\mathcal{HZ}_{L,\boldsymbol{n}-\alpha} = \Big\{ K_1 \times K_2 \times \cdots \times K_l \in \prod_{i=1}^{l} \mathrm{Gr}(n_i - \alpha_i, n_i) \ \mid \ \exists j \in [l],\, \dim(K_j \cap L_j) \geq 1 \Big\}.$$

This variety is simply the union of higher associated varieties of each factor L_i*, each having codimension* 2*. Hence,* $\mathcal{HZ}_{L,\boldsymbol{n}-\alpha}$ *has itself codimension* 2*.*

For a slightly more interesting example let $V \subset \mathbb{P}^n \times \mathbb{P}^n$ *be the multiprojective variety given as the zero set of the standard bilinear product,* $V = \mathbb{V}(\langle x, y \rangle)$*. That is,* $(x, y) \in V$ *iff* $\sum_{i=0}^{n} x_i y_i = 0$*. By direct computation we can see that for a linear subspace* $L = l \times \{[v]\}$ *of format* $(1, 0)$ *we have*

$$V \cap L = (l \cap [v^\perp]) \times \{[v]\},$$

where $[v^\perp] = \{[w] \in \mathbb{P}^n \mid \langle v, w \rangle = 0\}$*. For a generic* L*, the projective line* l *intersects the hyperplane* $[v^\perp]$ *at a single point. Hence,* $\mathrm{mdeg}(V, (1, 0)) = 1$*. On the other hand,* $V \cap L$ *is infinite if and only if* $l \subset [v^\perp]$*. Consider the variety*

$$\mathcal{HZ}_{V,(1,0)} = \{l \times \{[v]\} \in \mathrm{Gr}(1, n) \times \mathrm{Gr}(0, n) \mid l \subset [v^\perp]\}$$

and the projection $\pi : \mathcal{HZ}_{V,(1,0)} \to \mathbb{P}^n$ *onto the second coordinate. Then* π *is surjective and the fiber over a point* $[v]$ *is isomorphic to* $\mathrm{Gr}(1, [v^\perp])$ *which has dimension* $2n - 4$*. Hence,*

$$\dim \mathcal{HZ}_{V,(1,0)} = n + 2n - 4 = 3n - 4$$

holds. Since $\dim \mathrm{Gr}(1, n) \times \mathrm{Gr}(0, n) = 3n - 2$*, we deduce that* $\mathcal{HZ}_{V,(1,0)}$ *is not a hypersurface.*

5 Combinatorial structure of the support of a multiprojective variety

In this section, we outline an interesting connection between multiprojective varieties and the polymatroid theory.

Recall from Theorem 4.1 that the support $\operatorname{supp}(V)$ of an irreducible multiprojective variety $V \subset \prod_{i=1}^{l} \mathbb{P}^{n_i}$ are cut out by the inequalities of the form

$$\sum_{i \in I} (n_i - \beta_i) \leq \dim \pi_I(V), \tag{5}$$

where I runs over all possible subsets of $[l]$. It is immediate from the inequalities that $\operatorname{supp}(V)$, i.e. the set of β that satisfies (5), is the set of lattice points of a rational polytope. Remark 4 shows that the function $I \mapsto \dim \pi_I(V)$ has special properties, i.e., it is *submodular*, which further makes $\operatorname{supp}(V)$ a polymatroid. See Definition 5 below for the definition of a polymatroid.

As demonstrated in Figure 1, the set of formats α for which $\mathcal{CZ}_{V,\alpha}$ is a hypersurface equals to the set of lattice points that lie "below" $\operatorname{supp}(V)$. Furthermore , the set of formats for which the higher associated variety is a hypersurface are the lattice points that lie "above" the set of non-degenerate Chow formats as in Figure 2. The exact meaning of lying below and above were given in Proposition 4.4 and Theorem 4.9. In this section, we will translate these results to the language of polymatroid theory. More specifically, we will show that the operations of taking points below or above a polymatroid correspond to *truncation* and *elongation* of polymatroids, respectively, which also implies that the set of non-degenerate formats of Chow/Hurwitz forms are polymatroids as well.

Definition 5. *Let $l \in \mathbb{N}$ and $\delta : 2^{[l]} \to \mathbb{N}$. Then, δ is called **submodular** if*

1. *$\delta(\varnothing) = 0$,*
2. *for $I \subset J \subset [l]$, $\delta(I) \leq \delta(J)$, and,*
3. *for $I, J \subset [l]$, $\delta(I) + \delta(J) \geq \delta(I \cup J) + \delta(I \cap J)$.*

For a submodular function δ, the set

$$\mathcal{P}(\delta) \coloneqq \{\alpha \in \mathbb{N}^l \mid \sum_{i \in I} \alpha_i \leq \delta(I),\ I \subset [l]\}$$

*is called the (discrete) **polymatroid** associated to δ.*

In the case that $\delta(I) \leq |I|$ for $I \subset [l]$, $\mathcal{P}(\delta)$ is called a *matroid* with the *rank function* δ. Note that in this case $\mathcal{P}(\delta)$ consists of binary vectors (by simply taking $I = \{i\}$ we get $\alpha_i \leq 1$) so we can associate the elements of $\mathcal{P}(\delta)$ to the subsets of $[l]$. In the general case, we can associate the elements of a polymatroid with *multisubsets* of $[l]$, i.e., subsets where the repetition of elements are allowed.

The polymatroids admit properties reminiscent to matroids. We refer to [28, Section 18] for proofs.

Proposition 5.1. *Assume that $\mathcal{P}$ is a polymatroid.*

1. *$\mathcal{P}$ is **downward closed**, i.e., if $\alpha \in \mathcal{P}$ and $\beta \leq \alpha$ then $\beta \in \mathcal{P}$. A vector $\alpha \in \mathcal{P}$ which is not dominated by any other vector in $\mathcal{P}$ is called a **basis**.*
2. *If $\alpha, \beta \in \mathcal{P}$ with $|\beta| < |\alpha|$, then there exists an index $i \in [l]$ such that $\beta + \boldsymbol{e}_i \in \mathcal{P}$.*
3. *If $\alpha \in \mathcal{P}$ is a basis then $|\alpha| = \delta([l])$.*

Remark 6. *For the remainder of the section, the chief example of a polymatroid to us is the support of a multiprojective variety (and its downward closure). The polymatroids of this form are now called Chow polymatroids,*[3] *an interesting (and proper) subclass of polymatroids.*

Now we turn our attention to multiprojective varieties and their supports. To describe the submodular function of $\mathrm{supp}(V)$, we need the following definition.

Lemma 5.2 (Dual polymatroid)**.** *Assume $\mathcal{P} \subset \mathbb{N}^l$ is a polymatroid associated to the submodular function $\delta : 2^{[l]} \to \mathbb{N}$. Let $\boldsymbol{n} \in \mathbb{N}^l$ be such that $\forall I \subset [l]$, $\delta(I) \leq \sum_{i\in I} n_i$. Then,*

1. *The function*
$$\delta^*(I) \coloneqq \delta([l] \setminus I) - \delta([l]) + \sum_{i\in I} n_i$$
is submodular.

2. *The set*
$$\mathcal{P}^* \coloneqq \boldsymbol{n} - \mathcal{P} = \{\boldsymbol{n} - \alpha \mid \alpha \in \mathcal{P}\}$$
*is a polymatroid, associated to the submodular function δ^*, called the **dual** of $\mathcal{P}$ with respect to $\boldsymbol{n}$.*

Proof. To prove (1), we simply check the conditions of submodularity. First, we observe that for $I \subset [l]$,

$$\begin{aligned}\delta^*(I) &= \delta([l] \setminus I) - \delta([l]) + \sum_{i\in I} n_i \\ &\geq -\delta(I) + \sum_{i\in I} n_i \\ &\geq 0\end{aligned}$$

where in the second line we used $\delta(I) + \delta([l] \setminus I) \geq \delta([l])$. If $I \subset J$, then

$$\begin{aligned}\delta^*(I) &= \delta([l] \setminus I) - \delta([l]) + \sum_{i\in I} n_i \\ &\leq \delta([l] \setminus J) + \delta(J \setminus I) - \delta([l]) + \sum_{i\in J} n_i - \sum_{i\in J\setminus I} n_i \\ &= \delta([l] \setminus J) - \delta([l]) + \sum_{i\in J} n_i + \big(\delta(J \setminus I) - \sum_{i\in J\setminus I} n_i\big) \\ &\leq \delta^*(J).\end{aligned}$$

Lastly, for $I, J \subset [l]$, we have

$$\begin{aligned}\delta^*(I) + \delta^*(J) &= \delta([l] \setminus I) + \delta([l] \setminus J) - 2\delta([l]) + \sum_{i\in I} n_i + \sum_{i\in J} n_i \\ &\geq \delta([l] \setminus (I \cup J)) + \delta([l] \setminus (I \cap J)) - 2\delta([l]) + \sum_{i\in I\cup J} n_i + \sum_{i\in I\cap J} n_i \\ &= \delta^*(I \cup J) + \delta^*(I \cap J).\end{aligned}$$

[3]This naming is unfortunate for us because we will later associate a polymatroid to the formats of non-degenerate Chow forms of a variety, which are not themselves Chow polymatroids.

Hence, δ^* is submodular and this finishes the proof of (1). To prove the second claim, we note that a vector $\beta \in \mathbb{N}^l$ is in $\mathcal{P}^*$ if and only if

$$\forall I \subset [l], \quad \sum_{i\in I} \beta_i \ \leq \ \delta([l] \setminus I) - \delta([l]) + \sum_{i\in I} n_i.$$

Rearranging the inequality we obtain $\sum_{i\in I}(n_i - \beta_i) \leq \delta([l]) - \delta([l] \setminus I)$. Note that $\delta([l]) - \delta([l] \setminus I) \leq \delta(I)$ holds by the submodularity of δ so we have $\forall I, \sum_{i\in I} n_i - \beta_i \leq \delta(I)$ which implies that $\boldsymbol{n} - \beta \in \mathcal{P}$ and $\boldsymbol{n} - \mathcal{P}^* \subset \mathcal{P}$. On the other hand, $(\delta^*)^* = \delta$ so applying the same argument with the roles of $\mathcal{P}, \mathcal{P}^*$ swapped, we deduce that $\mathcal{P}^* = \boldsymbol{n} - \mathcal{P}$ and this finishes the proof. □

Remark 7. *Note that by the definiton of δ^* it is immediate that for any $I \subset [l]$, the inequality $\delta^*(I) \leq \sum_{i\in I} n_i$ holds. This allows us to take dual again, i.e., we can take the dual of $\mathcal{P}^*$ with respect to $\boldsymbol{n}$. By Lemma 5.2 (2), it is easy to see that $(\mathcal{P}^*)^* = P$.*

With this definition, Theorem 4.1 translates to the following.

Theorem 5.3 ([7])**.** *Let $\boldsymbol{n} = (n_1, n_2, \ldots, n_l) \subset \mathbb{N}^l$ be a vector and let $V \subset \mathbb{P}^{\boldsymbol{n}}$ be an irreducible multiprojective variety. Then,* $\mathrm{supp}(V)$ *is the set of basis vectors of a polymatroid, which is dual (with respect to $\boldsymbol{n}$) to the polymatroid associated to the submodular function $\delta(I) = \dim \pi_I(V)$ where $\pi_I(V)$ denotes the projection of V onto the multiprojective space $\prod_{i\in I} \mathbb{P}^{n_i}$.*

Proposition 4.4 and Theorem 4.9 describe two interesting combinatorial sets related to $\mathrm{supp}(V)$. In the case of Chow forms, the formats α where $\mathcal{CZ}_{V,\alpha}$ is a hypersurface are all of the form $\beta - e_i$ where $i = 1, 2, \ldots, l$ and $\beta \in \mathrm{supp}(V)$. In the case of Hurwitz forms, the formats are of the form $\alpha + e_i$, $i = 1, 2, \ldots, l$ where α is a format and $\mathcal{CZ}_{V,\alpha}$ is a hypersurface. In particular, both of these sets also have a combinatorial structure that is closely related to $\mathrm{supp}(V)$. Indeed, both of these sets are also polymatroids, obtained by applying structure preserving operations to $\mathrm{supp}(V)$.

Proposition 5.4. *Let $\mathcal{P} \subset \mathbb{N}^l$ be a polymatroid associated to the submodular function δ and $\boldsymbol{n} \in \mathbb{N}^l$ be a vector with $\forall I \subset [l]$, $\sum_{i\in I} n_i \geq \delta(I)$. Then, the sets*

$$\mathcal{P}_T \coloneqq \{\alpha - \boldsymbol{e}_j \mid \alpha \in \mathcal{P},\, j \in [l],\, \alpha_j \geq 1\}$$
$$\mathcal{P}^E \coloneqq \{\alpha + \boldsymbol{e}_j \mid \alpha \in \mathcal{P},\, j \in [l],\, \alpha_j < n_j\}$$

are also polymatroids, called the ***truncation*** *and* ***elongation*** *of $\mathcal{P}$, respectively. Moreover, we have $((\mathcal{P}^*)_T)^* = \mathcal{P}^E$, i.e., the elongation of $\mathcal{P}$ is the dual of the truncation of the dual of $\mathcal{P}$ where the dual is taken with respect to $\boldsymbol{n}$.*

Proof. Define a new submodular function δ' as

$$\forall I \subset [l],\ \delta'(I) \coloneqq \min\{\, \delta(I)\,,\, \delta([l]) - 1\,\}.$$

It is straightforward to show that $\delta'(I)$ is submodular. We claim that $\mathcal{P}_T$ is the polymatroid associated to δ'. We first prove that $\mathcal{P}(\delta') \subset \mathcal{P}_T$. Suppose $\beta \in \mathbb{N}^l$ satisfies $\forall I, \sum_{i\in I} \beta_i \leq \delta'(I)$. In particular, we have $|\beta| \leq \delta'([l]) = \delta([l]) - 1$. By Proposition 5.1 (2) and (3), there exists $\boldsymbol{e}_i$ such that $\beta + \boldsymbol{e}_i \in \mathcal{P}$ so $\beta \in \mathcal{P}_T$.

For the reverse inclusion, we assume that $\beta = \alpha - \boldsymbol{e}_j \in \mathcal{P}_T$ where $\alpha \in \mathcal{P}$ and $\alpha_j \geq 1$. We need to prove that β satisfies the inequalities $\sum_I \beta_i \leq \delta'(I)$ for $I \subset [l]$. There are two cases. If $j \in I$ then

$$\sum_{i\in I} \beta_i = \sum_{i\in I} \alpha_i - 1 \leq \delta(I) - 1 \leq \delta'(I).$$

Hence we may assume that $j \notin I$. To reach a contradiction, assume that $\sum_{i\in I} \beta_i = \sum_{i\in I} \alpha_i > \delta'(I)$. Then we must have $\delta(I) = \delta([l])$ and $\delta'(I) = \delta([l]) - 1$. This implies that $\sum_{i\in I} \alpha_i = \delta([l])$. Since $|\alpha| \leq \delta([l])$ also holds, we deduce that $\sum_{i\notin I} \alpha_i = 0$. This contradicts $\alpha_j \geq 1$ and finishes the proof that $\mathcal{P}_T = \mathcal{P}(\delta')$.

The claim $((\mathcal{P}^*)_T)^* = \mathcal{P}^E$ follows from Lemma 5.2 (2) and implies that $\mathcal{P}^E$ is a polymatroid since the dual and the truncation operators preserve being a polymatroid. □

Now we state Proposition 4.4 and Theorem 4.9 in the language of polymatroids.

Theorem 5.5. *Let $V \subset \mathbb{P}^{\boldsymbol{n}}$ be an irreducible multiprojective variety and assume that* $\mathrm{mdeg}(V, \alpha) \neq 1$ *for* $\alpha \in \mathrm{supp}(V)$*. If $\mathcal{P}$ denotes the polymatroid with basis vectors in* $\mathrm{supp}(V)$*, then*

1. *the set of basis vectors of the truncation $\mathcal{P}_T$ of $\mathcal{P}$ equals the set of all formats α such that the associated variety $\mathcal{CZ}_{V,\alpha}$ is a hypersurface, and,*
2. *the set of basis vectors of the elongation $\mathcal{P}_T^E$ of $\mathcal{P}_T$ equals the set of all formats β such that the higher associated variety $\mathcal{HZ}_{V,\beta}$ is a hypersurface.*

6 Acknowledgments

The authors would like to thank Matías Bender, Kathlén Kohn, Jonathan Leake, and Jorge Alberto Olarte for useful discussions. We also thank the anonymous referee for suggesting improvements. A.E. is supported by NSF CCF 2110075, M.L.D. is supported by ERC Grant 787840, E.T. is supported by ANR JCJC GALOP (ANR-17-CE40-0009), the PGMO grant ALMA, and the PHC GRAPE.

References

[1] John Abbott, Manuel Bronstein, and Thom Mulders. Fast deterministic computation of determinants of dense matrices. In *Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation*, ISSAC '99, pages 197-204, New York, NY, USA, 1999. Association for Computing Machinery.

[2] Saugata Basu, Richard Pollack, and Marie-Françoise Coste-Roy. *Algorithms in Real Algebraic Geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer Berlin / Heidelberg, Berlin, Heidelberg, 2006.

[3] Laurent Bernardin. *Factorization of multivariate polynomials over finite fields*. PhD thesis, ETH Zurich, 1999.

[4] Cornelius Brand and Michael Sagraloff. On the complexity of solving zero-dimensional polynomial systems via projection. In *Proc. ACM International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 151–158, 2016.

[5] Leandro Caniglia. How to compute the chow form of an unmixed polynomial ideal in single exponential time. *Applicable Algebra in Engineering, Communication and Computing*, 1(1):25–41, 1990.

[6] John Canny. Generalised characteristic polynomials. *Journal of Symbolic Computation*, 9(3):241–250, March 1990.

[7] Federico Castillo, Yairon Cid-Ruiz, Binglin Li, Jonathan Montaño, and Naizhen Zhang. When are multidegrees positive? *Advances in Mathematics*, 374:107382, 2020.

[8] David Castro, Marc Giusti, Joos Heintz, Guillermo Matera, and Luis Miguel Pardo. The hardness of polynomial equation solving. *Foundations of Computational Mathematics*, 3:347–420, 2003.

[9] John Canny and Ioannis Emiris. A subdivision-based algorithm for the sparse resultant. *Journal of the ACM (JACM)* 47(3):417–451, 2000.

[10] Arthur Cayley. On a new analytical representation of curves in space. *The Quarterly Journal of Pure and Applied Mathematics*, 3:225–236, 1860.

[11] Alexander L. Chistov. Polynomial-time computation of the dimension of algebraic varieties in zero-characteristic. *Journal of Symbolic Computation*, 22(1):1–25, 1996.

[12] David Cox, John Little, and Donal O'Shea. *Using algebraic geometry*. Graduate texts in mathematics BV000000067 185. Springer, New York u.a., 1998.

[13] John Dalbec. *Geometry and Combinatorics of Chow Forms*. PhD thesis, Cornell University, 1995.

[14] John Dalbec and Bernd Sturmfels. *Introduction to Chow Forms*. In NeilL. White, editor, *Invariant Methods in Discrete and Computational Geometry*, pages 37–58. Springer Netherlands, 1995.

[15] Carlos D'Andrea. Macaulay style formulas for sparse resultants. *Transactions of the American Mathematical Society*, 354(7):2595–2629, 2002.

[16] J. Désarménien. An algorithm for the rota straightening formula. *Discrete Mathematics*, 30(1):51–68, 1980.

[17] Alicia Dickenstein and Ioannis Z Emiris. Solving polynomial equations, volume 14 of. *Algorithms and Computation in Mathematics*, 2005.

[18] M. Levent Dogan, Alperen A. Ergür, Jake D. Mundo, and Elias Tsigaridas. The multivariate Schwartz–Zippel lemma. *SIAM Journal on Discrete Mathematics*, 36(2):888–910, 2022.

[19] David Eisenbud. *Commutative algebra with a view toward algebraic geometry*. Graduate texts in mathematics BV000000067 150. Springer, New York u.a., 1995.

[20] David Eisenbud and Joe Harris. *3264 and all that : a second course in algebraic geometry*. Cambridge University Press, Cambridge, 2016.

[21] Ioannis Emiris, Bernard Mourrain, and Elias Tsigaridas. Separation bounds for polynomial systems. *Journal of Symbolic Computation*, 101:128–151, 2020.

[22] Israel M Gelfand, Mikhail Kapranov, and Andrei Zelevinsky. *Discriminants, Resultants, and Multidimensional Determinants*. Modern Birkhäuser Classics. Birkhäuser Boston, Boston, MA, 1st ed. 1994. edition, 1994.

[23] Nardo Giménez and Guillermo Matera. On the bit complexity of polynomial system solving. *Journal of Complexity*, 51:20–67, 2019.

[24] Marc Giusti, Joos Heintz, and Contre Le Conicet. La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial, 1991.

[25] Bruno Grenet, Pascal Koiran, and Natacha Portier. On the complexity of the multivariate resultant. *Journal of Complexity*, 29(2):142–157, 2013.

[26] Joe Harris. *Algebraic geometry : a first course*. Graduate texts in mathematics BV000000067 133. Springer, New York u.a., corr. 2. printing edition, 1993.

[27] Robin Hartshorne. *Algebraic geometry*. Graduate texts in mathematics 52. Springer, New York u.a., 1977.

[28] Dominic Welsh. *Matroid Theory*. London u.a.: Acad. Press, 1976. Print.

[29] Jonathan Hauenstein, Anton Leykin, Jose Rodriguez, and Frank Sottile. A numerical toolkit for multiprojective varieties. *Mathematics of Computation*, 90(327):413–440, 2021.

[30] Joos Heintz, Guillermo Matera, and Ariel Waissbein. On the time–space complexity of geometric elimination procedures. *Applicable Algebra in Engineering, Communication and Computing*, 11:239–296, 2001.

[31] Joos Heintz and Jacques Morgenstern. On the intrinsic complexity of elimination theory. *Journal of Complexity*, 9(4):471–498, 1993.

[32] J. van der Hoeven and G. Lecerf. Sparse polynomial interpolation. Exploring fast heuristic algorithms over finite fields. Technical report, HAL, 2019.

[33] James E Humphreys. *Linear algebraic groups*. Graduate texts in mathematics BV000000067 21. Springer, New York u.a., 1975.

[34] Gabriela Jeronimo, Teresa Krick, Juan Sabia, and Martín Sombra. The computational complexity of the Chow form. *Foundations of Computational Mathematics*, 4(1):41–117, 2004.

[35] Gabriela Jeronimo, Susana Puddu, and Juan Sabia. Computing chow forms and some applications. *Journal of Algorithms*, 41(1):52–68, 2001.

[36] Erich Kaltofen and Gilles Villard. On the complexity of computing determinants. *Computational complexity*, 13(3):91–130, 2005.

[37] Erich Kaltofen and Lakshman Yagati. Improved sparse multivariate polynomial interpolation algorithms. In *International Symposium on Symbolic and Algebraic Computation*, pages 467–474. Springer, 1988.

[38] Mikhail M Kapranov, Bernd Sturmfels, and Andrei V Zelevinsky. Chow polytopes and general resultants. *Duke Mathematical Journal*, 67(1):189–218, 1992.

[39] Jürgen Klose. Binary segmentation for multivariate polynomials. *Journal of Complexity*, 11(3):330–343, 1995.

[40] Kathlén Kohn. Coisotropic hypersurfaces in Grassmannians. *Journal of Symbolic Computation*, 103:157–177, March 2021.

[41] Pascal Koiran. Randomized and deterministic algorithms for the dimension of algebraic varieties. In *Proceedings of the 38th Annual Symposium on Foundations of Computer Science*, FOCS '97, page 36, USA, 1997. IEEE Computer Society.

[42] Sylvain Lazard, Marc Pouget, and Fabrice Rouillier. Bivariate triangular decompositions in the presence of asymptotes. *Journal of Symbolic Computation*, 82:123–133, 2017.

[43] Richard Lipton. The curious history of the Schwartz-Zippel lemma. https://rjlipton.wpcomstaging.com/2009/11/30/the-curious-history-of-the-schwartz-zippel-lemma.

[44] Angelos Mantzaflaris, Éric Schost, and Elias Tsigaridas. Sparse rational univariate representation. In *Proc. ACM on International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 301–308, 2017.

[45] Hossein Nassajian Mojarrad, Thang Pham, Claudiu Valculescu, and Frank de Zeeuw. Schwartz-Zippel bounds for two-dimensional products. *arXiv preprint arXiv:1507.08181*, 2015.

[46] Brian Osserman and Matthew Trager. Multigraded Cayley-Chow forms. *Advances in Mathematics*, 348:583–606, May 2019.

[47] Oskar Perron. Beweis und verschärfung eines satzes von Kronecker. *Mathematische Annalen*, 118(1):441–448, Dec 1941.

[48] Franco Preparata and Michael Shamos. Computational geometry: an introduction. Springer Science & Business Media, 2012.

[49] Maurice Rojas. *Solving degenerate sparse polynomial systems faster.* Journal of Symbolic Computation, 28(1-2), 155–186, 1999.

[50] Martin Sombra. The height of the mixed sparse resultant. *American Journal of Mathematics*, 126(6):1253–1260, 2004.

[51] Arne Storjohann. The shifted number system for fast linear algebra on integer matrices. *Journal of Complexity*, 21(4):609–650, 2005.

[52] Bernd Sturmfels. *Algorithms in invariant theory.* Texts and monographs in symbolic computation. Springer, Wien u.a., 2. ed. edition, 2008.

[53] Bernd Sturmfels. The Hurwitz form of a projective variety. *Journal of Symbolic Computation*, 79:186–196, March 2017.

[54] Bartel Leendert Van der Waerden. On Hilberts function, series of composition of ideals and a generalization of the theorem of Bezout. In *Proc. Roy. Acad. Amsterdam*, volume 31, pages 749–770, 1929.

[55] B.L. Van der Waerden. On varieties in multiple-projective spaces. *Indagationes Mathematicae (Proceedings)*, 81(1):303–312, January 1978.

[56] Bartel L. Waerden van der and Wei-Liang Chow. Zur algebraischen geometrie. ix. Über zugeordnete formen und algebraische systeme von algebraischen mannigfaltigkeiten. *Mathematische Annalen*, 113:DCXCII–DCCIV, 1937.

[57] Chee-Keng Yap. *Fundamental problems of algorithmic algebra.* Oxford University Press, New York, 2000.

A Auxiliary results

The proof of Proposition 3.3 relies on the following that bounds on the bitsize of multivariate polynomial multiplication; see [44].

Claim A.1 (Polynomial multiplication)**.** *The following bounds holds:*

(i) Consider two multivariate polynomials, f_1 and f_2, in ν variables of total degrees δ, having bitsize τ_1 and τ_2, respectively. Then $f = f_1 f_2$ is a polynomial in ν variables, of total degree 2δ and bitsize $\tau_1 + \tau_2 + 2\,\nu\,\lg(\delta)$.

(ii) Using induction, the product of m polynomials in ν variables, $f = \prod_{i=1}^{m} f_i$, each of total degree δ_i and bitsize τ_i, is a polynomial of total degree $\sum_{i=1}^{m} \delta_i$ and bitsize $\sum_{i=1}^{m} \tau_i + 12\,\nu\,m\,\lg(m)\,\lg(\sum_{i=1}^{m} \delta_i)$.

(iii) Let f be a polynomial in ν variables of total degree δ and bitsize τ. The m-th power of f, f^m, is a polynomial of total degree $m\delta$ and bitsize $m\tau + 12\nu m \lg(\delta)$.