The Boolean complexity of computing Chow forms

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

Alperen Ergur
alperen.ergur@utsa.edu
The University of Texas at San Antonio
TX, USA

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

ABSTRACT
We consider the complexity of computing Chow forms 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; our result represents the first Boolean complexity bound. We also extend our algorithm to multiprojective Chow forms and obtain the first computational result in this setting. The motivation for our work comes from incidence geometry where intriguing problems for computational algebraists remain open.

KEYWORDS
Chow form, resultants, multihomogeneous polynomial, incidence geometry

1 INTRODUCTION
Assume a curve in space is given geometrically, how can one find an algebraic representation of this curve? This was a question tackled by Cayley [5] and later generalized to arbitrary varieties by van der Waerden and Chow by introducing what is now called the Chow form [32]. 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 [2, 9, 19, 23, 24]. Despite the large body of literature on the subject one basic aspect has received little attention: the Boolean complexity of computing a Chow form. Our paper aims to fill this gap. We also aim to extend our algorithmic results to multiprojective Chow forms where much less is known [29].

Another motivation for studying 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 [28] that this simple question has surprising consequences in extremal combinatorics and incidence geometry. This question almost entirely looks like a subject for the Schwarz-Zippel-De Millo-Lipton (SZDL) lemma [27], but $S_1$ and $S_2$ are two dimensional.

In [12] we developed a multivariate generalization of SZDL lemma as follows: 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 $V_1 \times V_2 \times \cdots \times V_m \not\subset \mathbb{C}^n$. Then, for any collection of finite sets $S_i \subset \mathbb{C}^{\lambda_i}$, any real $\epsilon > 0$, and $S := S_1 \times S_2 \times \cdots \times S_m$ we have

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

Note that the containment assumption on the variety $V(p)$ 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 $V_1 \times V_2 \times \cdots \times V_m \subset \mathbb{C}^n$.

Note that a variety $V(p)$ 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 [12] includes an algorithm to decide if $V(p)$ contains a cartesian product of hypersurfaces. One can hope to utilize multiprojective Chow form(s) of $V(p)$ to relate the general containment Problem 1.1 to the special case of hypersurface containment. This was our motivation to develop algorithms with 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 [9]. This black-box approach does not exploit the special structure of the problem and does not yield precise complexity estimates.

To our knowledge, the first algorithm with a precise complexity estimate to compute the Chow form of a pure dimensional variety is due to Caniglia [2]. 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. [19] describe a probabilistic algorithm that computes the Chow form of $V$, see also [20]. 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 [19, Theorem 1] for the exact statement.

Our contribution. 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 3.8 for the general case. To our knowledge, our paper is the first one to contain results in this direction.
There is a generalization by Osserman and Trager [29] of Chow forms for varieties in multiprojective space. Our method to compute the Chow form is based on using resultants and it seamlessly extends to multiprojective space, see Lemma 4.5 for the complete intersection case and Theorem 4.8 for the general case. We further extend our algorithmic techniques to compute Hurwitz forms [31], see Proposition 3.9.

Notation. The bold small letters indicate vectors or points; in particular \( x = (x_0, \ldots, x_n) \) or \( x = (x_1, \ldots, x_n) \) depending on the context. We denote by \( \mathcal{O} \), resp. \( \mathcal{O}_B \), the arithmetic, resp. bit, complexity and we use \( \mathcal{O}_B \) to ignore (poly-)logarithmic factors. For a polynomial \( f \in \mathbb{Z}[x], \) \( \text{ht}(f) \) 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, \( \mathbb{A}^n \) affine space and \( \mathbb{P}^n \) the projective space.

Outline. The rest of the paper is structured as follows. In the next section we present a short overview of Chow forms. Section 3 illustrates the computation of the Chow form in \( \mathbb{P}^n \) and extension of techniques to compute Hurwitz forms. Section 4 presents algorithms for computing multiprojective Chow forms.

2 PRELIMINARIES

Given \( f : f_1, f_2, \ldots, f_k \in \mathbb{C}[x] \), we call the zero locus
\[
\mathbb{V}_f(f_1, f_2, \ldots, f_k) \coloneqq \{ p \in \mathbb{A}^n | f_1(p) = f_2(p) = \cdots = f_k(p) = 0 \},
\]
the affine variety defined by \( f \). In the case that \( f \) consists of homogeneous polynomials, the set
\[
\mathbb{V}_p(f_1, f_2, \ldots, f_k) \coloneqq \{ p \in \mathbb{P}^n | f_1(p) = f_2(p) = \cdots = f_k(p) = 0 \}
\]

is well-defined and called the projective variety defined by \( f \).

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. Every reducible variety can be written (in an essentially unique way) as a finite union
\[
V = \bigcup_{i=1}^l V_i, \quad (V_i \subseteq \bigcup_{j \neq i} V_j)
\]
of irreducible subvarieties. The irreducible subvarieties \( V_i \) are called the irreducible components (or components for short) and the expression (1) is called the irreducible decomposition of \( V \).

As a preparation to the discussion on Chow forms, we define the dimension of a projective variety à la Harris [17, §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 \( n - r \) intersect \( V \) and a generic subspace \( L \subset \mathbb{P}^n \) of dimension at most \( n - r - 1 \) is disjoint from \( V \). \( V \) is called pure dimensional (also called equidimensional) if every irreducible component of \( V \) has the same dimension. Note that if \( V \) is irreducible then it is trivially pure dimensional.

2.1 Associated hypersurfaces and Chow forms

The main objects 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 [8, 9]. For a higher level study, we refer to [15].

Let \( V \subset \mathbb{P}^n \) be an irreducible variety of dimension \( r \). By the definition of the dimension, 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 \( (n - r - 1) \)-dimensional subspaces of \( \mathbb{P}^n \) that intersect \( V \). To be more concrete, we consider \( \text{Gr}(n-r-1,n) = \{ L \subset \mathbb{P}^n \mid L \text{ is a subspace of dimension } n-r-1 \} \), the Grassmannian 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 \( V \)
\[
\mathbb{C}Z_V = \{ L \subset \text{Gr}(n-r-1,n) \mid V \cap L \neq \emptyset \} \subset \text{Gr}(n-r-1,n),
\]
is an irreducible hypersurface of \( \text{Gr}(n-r-1,n) \) called the associated hypersurface of \( V \). Moreover, \( \mathbb{C}Z_V \) uniquely defines \( V \). That is,
\[
V = \{ x \in \mathbb{P}^n \mid x \in L \Rightarrow L \subset \mathbb{C}Z_V \}.
\]

The associated hypersurface \( \mathbb{C}Z_V \) is the zero set of an element in the coordinate ring of \( \text{Gr}(n-r-1,n) \) [15, Proposition 2.1]. \(^{1}\) We write a linear subspace \( L \subset \text{Gr}(n-r-1,n) \) as the intersection of \( r+1 \) hyperplanes. For \( 0 \neq u \in \mathbb{C}^{n+1} \), set \( U(u,x) = u_0x_0 + \cdots + u_nx_n \).

Definition 2.2. The Chow form of \( V \) is the square-free polynomial with the property that
\[
\mathcal{C}^F_V(u_0, \ldots, u_r) = 0 \iff V \cap \bigvee(U(u_0, x), \ldots, U(u_r, x)) \neq \emptyset
\]
for \( u_0, u_1, \ldots, u_r \in \mathbb{C}^{n+1} \).

Note that \( \mathcal{C}^F_V \) is defined up to multiplication with a non-zero scalar.

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, \( \mathcal{C}^F_V \), of \( V \).

3.1 The case of a complete intersection

Algorithm 1 ChowForm_CI

Input: \( f_1, \ldots, f_{n-r} \in \mathbb{Z}[x] \).
Precondition: \( V = \bigvee(f_1, \ldots, f_{n-r}) \) 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 \( x_i \)
\[
R = \text{Elim}(\{ f_1, \ldots, f_{n-r}, U_0, \ldots, U_r \}, \{ x \}) \in \mathbb{Z}[u_{i,j}]
\]
(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, thus
\[
V = \bigvee(f_1, f_2, \ldots, f_{n-r}) \subset \mathbb{P}^n
\]
is the common zero locus of \( \text{codim}(V) = n-r \) many polynomials, where \( f_i \in \mathbb{Z}[x] \) and \( \deg(f_i) = d_i \). Let \( d := \max d_i \) denote the maximum of the degrees. Moreover, assume \( h(f_i) \leq r \), i.e., the bitsizes of \( f_i \) are all bounded by \( r \).

\(^{1}\)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.
Let $\mathbf{u} = (u_{ij}, 0 \leq i \leq r, 0 \leq j \leq n)$ be a family of formal variables and consider the system of $r + 1$ formal linear combinations

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

We will regard each element of $U$, $U_i$, as a polynomial in $\mathbb{C}[u][x]$. Observe that if $u \in \mathbb{C}^{(r+1)\times (n+1)}$ is a matrix of full rank, then

$$L = \\text{det}(U(\mathbf{u}, \mathbf{x})) \in \mathbb{P}^n$$

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. Moreover, $V \cap L \neq \emptyset$ if and only if the overdetermined system

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

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

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

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

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

1. $\mathcal{R}$ is invariant under the action of $\text{SL}_{r+1}$ on $\mathbb{C}[\mathbf{u}]$, and
2. $\mathcal{R}(\mathbf{u}) = 0$ if and only if either $u$ has rank $< r + 1$, or $u$ is full rank and $\mathcal{R}(\mathbf{u}, \mathbf{x}) \in \mathbb{C}Z_v$.

**Proof.** By the definition of the resultant, $\mathcal{R}(\mathbf{u}) = 0$ if and only if the system (2) has a common solution in $\mathbb{P}^n$.

For $g \in \text{SL}_{r+1}, \mathcal{R}(U(\mathbf{gu}, \mathbf{x})) = \mathcal{R}(U(\mathbf{u}, \mathbf{x}))$ holds so $\mathcal{R}$ is invariant under the action of $\text{SL}_{r+1}$. Moreover, (2) has a solution if and only if $L = \mathcal{R}(U(\mathbf{u}, \mathbf{x}))$ intersects $V$. As $\text{dim} \ L = n - \text{rk}(u)$, $L$ intersects $V$ precisely when $u$ is rank-deficient, or $u$ is full rank and $L \in \mathbb{C}Z_v$. \hfill $\Box$

**Proposition 3.2.** Let $\mathcal{R} = \mathcal{R}_1 \cap \mathcal{R}_2 \cap \ldots \cap \mathcal{R}_e$ be the irreducible factorization of $\mathcal{R}$. Then $e$ equals the number of irreducible components of $V$ and the square-free part $\mathcal{R}_1 \mathcal{R}_2 \ldots \mathcal{R}_e$ of $\mathcal{R}$ is the Chow form of $V$.

**Proof.** By the previous proposition, the zero locus of $\mathcal{R}$ coincides with the zero locus of the Chow form, $\mathcal{C}V$. Thus, the square-free part of $\mathcal{R}$ equals $\mathcal{C}V$ and the number of irreducible factors of $\mathcal{R}$ and $\mathcal{C}V$ are equal. \hfill $\Box$

**Proposition 3.3.** Consider $I = \{f_1, \ldots, f_{n-r}\} \subset \mathbb{Z}[x_0, \ldots, x_n]$ where each $f_i$ is homogeneous of degree $\leq d$ and has bitsize $\tau$; also the corresponding projective variety, $V$, has pure dimension $r$. Let $u_i := (u_{i0}, \ldots, u_{in})$, for $0 \leq i \leq r$, be $(n + 1)(r + 1)$ new variables. The Chow form of $V$, $\mathcal{C}V$, is a multihomogeneous polynomial, it is homogeneous in each block of variables $u_i$, of degree $d^{\tau-1}$ and has bitsize $O(n d^\tau d^{\tau-1})$. CHOWFORM_CI (Alg. 1) computes $\mathcal{C}V$ in

$$O_B(n(n-r)^{\omega+1}(n-r)^{\text{par}}(2d^2)^{\omega+1}n^{\text{par}}(r+n)),$$

where $\omega$ 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 $U_i = u_{i0}x_0 + \cdots + u_{in}x_n$, where $u_i := (u_{i0}, \ldots, u_{in})$, 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 $F = \{f_1, \ldots, f_{n-r}, U_0, \ldots, U_r\}$, say $\mathcal{R}$, where we consider the polynomials in $\mathbb{Z}[\mathbf{u}][x]$ and we eliminate the variables $x_i$; thus $\mathcal{C}F \subset \mathbb{Z}[\mathbf{u}_1, \ldots, \mathbf{u}_{r+1}]$.

The resultant is a multihomogeneous polynomial in the coefficients of the input polynomials [7, Chapter 3]. In our case $\mathcal{R} \subset \mathbb{Z}[u_0, \ldots, u_r]$ is multihomogeneous wrt each block of variables $u_i$. The degree of $\mathcal{R}$ with respect to $u_i$ is given by the Bézout bound of the system when $u_i$ is omitted, and, it is bounded by $d^\tau d^{\tau-1}$.

To estimate the complexity of computing the resultant we adopt accordingly the arguments from [1, Proposition 1]. We consider the Macaulay matrix, $M$, of the system $F$; its elements are polynomials in $\mathbb{Z}[u]$. Then $\mathcal{R}$ is the quotient of two determinants related to $M$, e.g., [7, 11]. The numerator is the determinant of $M$, while the denominator is the determinant of a well defined submatrix of $M$, say $M_1$; thus $\mathcal{R} = \det(M)/\det(M_1) \in \mathbb{Z}[u]$. The dimension of the Macaulay matrix is the number of homogeneous monomials of degree $\sum_{i=0}^r (d-1) + \sum_{i=1}^n (1-1) + 1 = (n-r)(d-1) + 1$ in $n+1$ variables, that is $(n-r)(d-1)^{n-r-1} + \frac{1}{n-r}$.

We compute the evaluation of $\mathcal{R}$ at $O((2d)^{\tau d^\tau})$ points, many say $p$, (these are $(r+1)(n+1)$-tuples) with integer coordinates and we recover it using interpolation. The number of evaluations is driven by the number of monomials in $\mathcal{R}$. The bitsize of the evaluation points is $O(n \log(d))$. Hence, $\mathcal{R}(\mathbf{p})$ corresponds to specialize $u = \mathbf{p}$ in $M$ and $M_1$ and compute the determinants of the specialized matrices and their ratio. It is an overestimation to assume that the entries of $M(\mathbf{p})$ and $M_1(\mathbf{p})$ are integers of bitsize $O((r+n)\log(d))$. Each determinant computation costs $O_B((n-r)(d-1)(\omega+1)(r+n))$ [21]. Since we have to perform it $O((2d)^{\tau d^\tau})$ times, the overall cost of the evaluations is $O_B((n-r)(d-1)(\omega+1)(r+n))$.

The interpolation costs $O_B((2d)^{\omega+1}d^\tau d^{\tau-1})$ using a straightforward algorithm to invert a multivariate Vandermonde matrix, where $\omega \leq 3$ is the exponent of matrix multiplication. More sophisticated algorithm, e.g., [18, 22] and references therein, will decrease the constant $\omega$ in the exponent.

It might happen that $\det(M_1) \equiv 0$. In this case, we have to use the technique of generalized characteristic polynomial by Canny [3]. It introduces one more variable in the computations and will slightly increase the constant in the exponent. We omit this analysis, to simplify the presentation.

Finally, we have to compute the square-free part of $\mathcal{R}$. This amounts, roughly, to one gcd computation. For polynomials in $n$ variables, of degree $\delta$ and bitsize $L$, the gcd costs $O_B(\delta^2 L)$ [28, Lemma 4]. This translates to $O_B(n(rd^{\tau-1})^2(\omega+1)(r+n)(r+n)^{\tau-1})$.

**3.2 The case of an over-determined system**

Now we remove the assumption of complete intersection. Consider

$$V = \mathcal{V}(f_1, f_2, \ldots, f_m) \subset \mathbb{P}^n,$$
where $m \geq n - r = \text{codim} V$. 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 $x$. 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 replace the original system $f$ with a generic system of codimension $V = n - r$ many polynomials $f_i$ that vanish on $V$, by choosing $f_i$ to be generic linear combinations of $f_i$. In this way, the zero locus of the new system is a pure $r$-dimensional variety that contains $V$ (Proposition 3.5). 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 $V$ (Proposition 3.6). Hence, the Chow form of $V$ satisfies

$$C^*V = \gcd(CF_{V_1}, \ldots, CF_{V_k}).$$

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

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

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

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 3.4.** $V = \{f_1, f_2, \ldots, f_m\} \subset \mathbb{P}^n$ 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 homogenous polynomial of degree $d$, and, in particular, it defines a projective hypersurface. More generally, given a matrix $\Lambda = [\lambda_i] \in \mathbb{C}^{k \times m}$ we define the system

$${\Lambda_\tau} := \begin{pmatrix} 1 \lambda_{11} f_1 + \lambda_{12} f_2 + \cdots + \lambda_{1m} f_m \\
\lambda_{21} f_1 + \lambda_{22} f_2 + \cdots + \lambda_{2m} f_m \\
\vdots \\
\lambda_{k1} f_1 + \lambda_{k2} f_2 + \cdots + \lambda_{km} f_m \end{pmatrix},$$

(3)

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

$$\nabla(\Lambda_\tau) = V \cup X,$$

where $X$ is a pure dimensional variety of dimension $n - k$. The proof follows, mutatis mutandis, [16, Section 3.4.1], that considers the case $k = n$.

**Proposition 3.5.** For a generic choice of $\Lambda \in \mathbb{C}^{k \times m}$, the components of $\nabla(\Lambda_\tau)$ are either the components of $V$ or of dimension $n - k$. More concretely, for each $1 \leq k \leq n$, there exists a hypersurface $H_k \subset \mathbb{C}^{k \times m}$ of degree $\leq kd^{k-1}$ such that for any $\Lambda \not\equiv H_k$, the condition holds.

**Proof.** We will proceed by induction on $k$.

For $k = 1$, the condition is violated if and only if $\Lambda_\tau = \sum_{i=1}^{m} \lambda_i f_i \equiv 0$. This is a linear condition on $\lambda_i$'s. To see this, consider the matrix that has the (coefficients of the) polynomials $f_i$ as rows. Then it suffices to require $\Lambda$ belong to the left kernel of this matrix, which in turn is $H_1$ and is of degree 1.

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

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

is the irreducible decomposition of $X$ and ignore the components that are fully contained in $V$. By the Bézout bound, we have $c \leq d^{k-1}$. Pick arbitrary points

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

so for each $i$ there exists $j$ with $f_j(x_i) \neq 0$.

Form the matrix

$$M = \begin{pmatrix} f_1(x_1) & f_2(x_1) & \cdots & f_m(x_1) \\
\vdots & \ddots & \vdots \\
f_1(x_c) & \cdots & f_m(x_c) \end{pmatrix},$$

If $\mu \in \mathbb{C}^m$ is picked so that each entry of $M\mu \in \mathbb{C}^c$ is non-zero, then the linear combination

$$\bar{f} = \mu_1 f_1 + \mu_2 f_2 + \cdots + \mu_m f_m$$

satisfies

$$\forall i = 1, 2, \ldots, c, \quad \bar{f}(x_i) \neq 0.$$
many times we can construct varieties $V(A_j^r)$, each being a set theoretic complete intersection, where $V$ equals to their intersection.

**Proposition 3.6.** Let $V = V(f_1, f_2, \ldots, f_m)$ be as in Assumption 3.4 and $N = \lfloor \frac{m}{r} \rfloor$. For a generic choice of $A^1, A^2, \ldots, A^N \in \mathbb{C}^{(n-r)\times m}$, each variety $V(A_j^r)$ is a pure dimensional variety of dimension $r$ and $V = \bigcap_{i=1}^N V(A_j^r)$. More concretely, there is a hypersurface $H \subset \mathbb{C}^{N(n-r)\times m}$ of degree $\leq N(n-r)d^{n-r-1} + m$ such that for any $(A^1, \ldots, A^N) \in \mathbb{C}^{N(n-r)\times m} \setminus H$, the condition is satisfied.

**Proof.** Consider the matrix 
$$
\Xi = [A^1, A^2, \ldots, A^N]^T \in \mathbb{C}^{N(n-r)\times m},
$$
and let $V(\Xi) = \bigcap_{i=1}^N V(A_j^r)$. For generic choices of $A_j^r$, the matrix $\Xi$ has full rank. Since $N = \lfloor \frac{m}{r} \rfloor$, we have $N(n-r) \geq m$ so $\Xi$ is injective. Thus, we have
$$
(A_j^r, A_j^r, \ldots, A_j^r) = (f)
$$
which implies that $V = \bigcap_{i=1}^N V(A_j^r)$.

Note that $\Xi$ satisfies the condition if and only if each $A_j^r$ avoids the hypersurface of degree $(n-r)d^{n-r-1}$ from Proposition 3.5 and $\Xi$ is full rank. We can guarantee the second condition by enforcing a particular maximal minor of $\Xi$ to be non-zero. Thus, $\Xi$ 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:** $f_1, \ldots, f_m \in \mathbb{Z}[x], r \in \mathbb{N}$

**Precondition:** Assumption 3.4.

**Output:** $A^1, A^2, \ldots, A^N$.

**Postcondition:** See Proposition 3.6.

1. $N := \lfloor \frac{m}{r} \rfloor$.
2. $S := \lfloor \frac{N(n-r)d^{n-r-1} + m + 1}{n} \rfloor$. \[\text{(2)}\]
3. for $(A^1, A^2, \ldots, A^N) \in S^{N(n-r)\times m}$ do
   if $\dim(V(\Xi)) \leq r$ and $\Xi$ is full-rank then
      return $A^1, A^2, \ldots, A^N$.

**Lemma 3.7.** Alg. 3 returns $A^1, A^2, \ldots, A^N$ satisfying the requirements of Proposition 3.6 in $\text{rm}O(1)\text{d}O(n)$.

**Proof.** $\Xi = (A^1, \ldots, A^N)$ satisfies the requirements of Proposition 3.6 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 $S^{N(n-r)\times m} \subset \mathbb{C}^{N(n-r)\times m}$ where $S \subset \mathbb{C}$ is a finite set of size $|S| > D$. By going through the elements of the grid and testing membership to $H$ at each step, we can generate $\Xi$ satisfying the requirement.

The membership test to $H$ amounts to checking if (i) $V(\Xi)$ has dimension $\leq r$ and (ii) $\Xi$ has rank $m$. If $S$ is chosen to be the list of first $D + 1$ natural numbers, then the entries of $\Xi$ have bitsizes $\log D + 1 = O(\log m + (n-r)\log d)$, so the polynomials in $A_j^r$ have bitsizes bounded by $O((r + \log m + (n-r)\log d))$. Hence, whether $\dim(V(\Xi)) \leq r$ can be tested in $\text{rm}O(1)\text{d}O(n)$ (see [6, 25]). Whether $\Xi$ is full-rank can be tested in $O(\text{rm}O(1)n\log d)$. We repeat this process $|S| = O(md^{n-r})$ times, so the total complexity does not change.

**Theorem 3.8.** 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 $\tau$; also the corresponding projective variety, $V$, has pure dimension $r$. Let $u_i := (u_{i0}, \ldots, u_{in})$, for $i \in \{r + 1\}$, be $(n + 1)(r + 1)$ new variables. The Chow form of $V$, $\text{CF}_V$, is a multihomogeneous polynomial; it is homogeneous in each block of variables $u_i$ of degree $d^r$ and has bitsize $O(\text{d}^{n-r})$. CHOWFORM (Alg. 2) computes $\text{CF}_V$ in

$$
\tilde{O}(m^\omega n^{\omega n^r}(n-r)(\omega+1)n(2d)^{(\omega+1)n}(\tau+n)),
$$

where $\omega$ is the exponent of matrix multiplication and $\omega$ 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 3.6.

We apply Alg. 3 to generate $A^1, \ldots, A^N$ such that they fulfill the assumptions of Proposition 3.6. The cost of this algorithm is $\text{rm}O(1)\text{d}O(n)$.

The bitsize of the polynomials in $A_j^r$ is $O(\tau + \log m + n\log d) = O(\tau + n)$. Hence, we can compute the Chow form of each $V(A_j^r)$ using Alg. 1 within the complexity

$$
\tilde{O}(m^\omega n^{\omega n^r}(n-r)(\omega+1)n(2d)^{(\omega+1)n}(\tau+n)),
$$

we multiply by the number of systems, $N = O(m)$ to conclude.

Finally, we compute the gcd of $N = O(m)$ Chow forms. As each Chow form has $(r+1)(n+1)$-variables, bitsize $O(\text{d}^{n-r})$ and degree $(r+1)d^r$, this operation costs $\tilde{O}(mn^r\text{d}^{2\omega}(\tau+n))$, 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 [6, 25], without changing the single exponential nature of the complexity of the algorithm.

**3.2.1 Straightening Algorithm.** Let $\mathbb{C}[u]$ denote the ring of regular functions on the space $\mathbb{C}^{(r+1)\times(n+1)}$ of matrices. The Chow form $\text{CF}_V$ of the variety $V$ is invariant under the action of $\text{SL}_{r+1}$ on $\mathbb{C}^{(r+1)\times(n+1)}$ by left multiplication. The first fundamental theorem of invariant theory states that (see, for example, [30, Theorem 3.2.1]) every $\text{SL}_{r+1}$ invariant polynomial can be written as a unique bracket polynomial

$$
F = B\left(\{0, 1, \ldots, r\}, \{n-r+1, n-r+2, \ldots, n+1\}\right)
$$

in the brackets $\{0, 1, \ldots, r\}$. This normal form computation can be done by the means of Rota’s straightening algorithm or the subduction algorithm. We refer to [30, §3] and, in particular, [30, Algorithm 3.2.8] for more information.

**3.3 The Hurwitz polynomial**

Closely related to the Chow form of a projective variety $V \subseteq \mathbb{P}^n$ of dimension $r$ is the Hurwitz form. This is a discriminant that characterizes the linear subspaces of dimension $n-r$ that intersect $V$ in fewer points than its degree. Actually, these linear spaces form a hypersurface in the corresponding Grassmannian. The polynomial
of this hypersurface is the Hurwitz form of $V$ [31]. 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. The resultant of the system when we eliminate the variables $x_i$ using the Poisson formula [7] or the Prime factorization Theorem for principal $A$-determinants [15], 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 $m$ with coefficients in $\mathbb{Z}[u]$ is the Hurwitz polynomial.

**Algorithm 4 HurwitzPoly**

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

1. Let $U_i = \sum_{j=0}^{r} u_i j x_j$, for $i \in [r]$.
2. Let $M = m_0 x_0 + \cdots + m_n x_n$.
3. Eliminate the variables $x_i$.
   \[ R_1 = \text{Elim}(\langle f_1, \ldots, f_{n-r}, U_1, \ldots, U_r, M, x \rangle) \in \mathbb{Z}[u_{i,j}] [m] \]
4. (Consider the discriminant of $R_1$)
   \[ R_2 = \text{Elim}(\langle \partial R_1 / \partial m_0, \ldots, \partial R_1 / \partial m_n \rangle, M) \in \mathbb{Z}[u_{i,j}] \]
5. Deduce the Hurwitz poly from the square-free part of $R_2$.

**Proposition 3.9.** 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 $\tau$; also the corresponding projective variety, $V$, has pure dimension $r$. Let $u_i := (u_{i,0}, \ldots, u_{i,n})$, for $0 \leq i \leq r$, be $(n+1)(r+1)$ new variables.

**Proof Sketch.** The computation of $R_1$ is similar to the computation of the Chow form of $V$ (Lemma 3.8). 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 $O(d^\tau)$ and bitsize $O(d^\tau)$. \( \square \)

## 4 MULTIGRADED CHOW FORMS

$\mathbb{P}^n$ denotes the multiprojective space $\mathbb{P}^{n_1} \times \mathbb{P}^{n_2} \times \cdots \times \mathbb{P}^{n_l}$. For $i = 1, 2, \ldots, l$, $x_i = (x_{i,0}, x_{i,1}, \ldots, x_{i,m_i})$ denotes the coordinates of $\mathbb{P}^{n_i}$. Throughout the section we assume that

\[ V = \mathcal{V}(f_1, f_2, \ldots, f_k) \subseteq \mathbb{P}^n = \mathbb{P}^{n_1} \times \mathbb{P}^{n_2} \times \cdots \times \mathbb{P}^{n_l} \]

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

\[ \text{mdeg}(f_i) = (d_{i,1}, d_{i,2}, \ldots, d_{i,l}). \]

### 4.1 The multidegree and the support of a multiprojective variety

A linear subspace of $\mathbb{P}^n$ is defined to be a product

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

of linear subspaces $L_i \subseteq \mathbb{P}^{n_i}$. We say the format of $L$ is $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_l)$ if $\dim L_i = \alpha_i$. Note that as an abstract variety, $L$ has dimension $|\alpha| = \sum_i \alpha_i$.

For a multiprojective variety, the number of intersection points of a linear subspace of complementary dimension may vary with the format of the subspace. As a simple example, one may consider $V = \mathbb{P}^1 \times \{p\} \subseteq \mathbb{P}^1 \times \mathbb{P}^1$ whose 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.

**Definition 4.1.** Let $V \subseteq \mathbb{P}^n$ be a pure dimensional multiprojective variety of dimension $r$. The support $\text{supp}(V)$ of $V$ is defined to be the set of all formats $\alpha \in \mathbb{N}^d$ such that $|\alpha| = \dim V$ 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 $\alpha$ is non-empty.

The multidegree $\text{mdeg}(V)$ of $V$ is defined to be the set of all tuples $(m, \alpha)$ where $\alpha \in \text{supp}(V)$ and $m$ is the number of intersection points of $V$ with a generic linear subspace of $\mathbb{P}^n$ of format $\alpha$.

We note that the number of intersection points, $m$, is finite for dimension reasons.

**Example 1.** Let $V = V_1 \times V_2 \times \cdots \times V_l \subseteq \mathbb{P}^n$ be a variety where $\dim V_i = r_i$. Setting $\beta = (n_1 - r_1, n_2 - r_2, \ldots, n_l - r_l)$, one can observe that $V$ intersects with a generic subspace of format $\beta$ at $\prod_{i=1}^l \deg V_i$ many points. For any other format $\gamma$ with $|\gamma| + \dim V = |\beta|$, there exists $i$ such that $\gamma_i + r_i < n_i$. Since the variety $V_i \subseteq \mathbb{P}^{n_i}$ does not intersect a generic subspace $S_2 \subseteq \mathbb{P}^{n_i}$ of dimension $\gamma_i < n_i - \dim r_i$, $V$ does not intersect with a generic subspace of format $\gamma$. Hence,

\[ \text{supp}(V) = \{ \beta \}, \quad \text{mdeg}(V) = \{ (\prod_{i=1}^l \deg(V_i), \beta) \} \]

holds.

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

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

denote the projection of $\mathbb{P}^n$ onto $\prod_{i \in I} \mathbb{P}^{n_i}$. The main result of [4] is that the support of $V$ can be computed from $\dim \pi_I(V)$.

**Theorem 4.2** ([4]). Assume $V$ is irreducible and let $\beta \in \mathbb{N}^l$ with $\beta_i \leq n_i$ for all $i \in [l]$ and $|\beta| = \dim V$. Then $\beta \in \text{supp}(V)$ if and only if for all $\varnothing \neq I \subseteq [l]$ the following inequality holds

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

The above result can also be generalized to non-irreducible varieties as for a pure dimensional multiprojective variety $V$ with decomposition $V = V_1 \cup V_2 \cup \cdots \cup V_k$,

\[ \text{supp}(V) = \bigcup_{i=1}^k \text{supp}(V_i) \]

holds. See [4, Corollary 3.13] for the exact statement.

### 4.2 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 [29].
Definition 4.3. Let $\alpha \in \mathbb{N}^l$ with $|\alpha| = \text{codim} V - 1$. The associated variety of $V$ of format $\alpha$ is defined to be the multiprojective variety

$$CZ_{V,\alpha} = \{(L_1, L_2, \ldots, L_l) \in \prod_{i=1}^l \text{Gr}(\alpha_i, n_i) \mid V \cap (L_1 \times L_2 \times \cdots \times L_l) \neq \emptyset\},$$

that is, $CZ_{V,\alpha}$ is the set of all linear subspaces of $\mathbb{P}^n$ of format $\alpha$ that intersects $V$.

As the term associated variety suggests, contrary to the projective case, $CZ_{V,\alpha}$ is not always a hypersurface.

Example 2. Let $V_1 \subset \mathbb{P}^{n_1}, V_2 \subset \mathbb{P}^{n_2}$ be codimension 2 varieties and consider

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

Since codim $V = 4$, 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

$$CZ_{V,(3,0)} = \{(L_1, p) \in \text{Gr}(3, n_1) \times \text{Gr}(1, n_2) \mid |L_1 \times L_2 \cap V| \neq \emptyset\}$$

and

$$CZ_{V,(2,1)} = \{(L_1, L_2) \in \text{Gr}(2, n_1) \times \text{Gr}(1, n_2) \mid |L_1 \times L_2 \cap V| \neq \emptyset\}$$

is indeed a hypersurface. However,

$$CZ_{V,(3,0)} = \{(L_1, p) \in \text{Gr}(3, n_1) \times \mathbb{P}^{n_2} \mid |(L_1 \times \{p\}) \cap V| \neq \emptyset\}$$

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

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

\[
\begin{array}{c}
\text{codim}(V) \quad (4, 0) \quad (3, 1) \quad (2, 2) \quad (1, 3) \quad (0, 4) \\
\text{codim}(V) - 1 \quad (3, 0) \quad (2, 1) \quad (1, 2) \quad (0, 3)
\end{array}
\]

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

Proposition 4.4. Let $\alpha \in \mathbb{N}^l$ with $|\alpha| = \text{codim} V - 1$ and $\forall i, \alpha_i \leq n_i$. Then the following are equivalent.

1. $CZ_{V,\alpha}$ is a hypersurface.
2. There exists $\beta \in \text{supp}(V)$ such that $\alpha \leq \beta$.
3. For all $\emptyset \neq I \subset [l]$, we have $\dim \pi_1(V) \geq \sum_{i \in \Theta} (n_i - \alpha_i) - 1$.

Proof. See Proposition 3.3 and Corollary 5.11 of [29].

4.3 Computing the Chow form of a multiprojective variety

For the rest of the section, $V \subset \mathbb{P}^n$ is a pure dimensional multiprojective variety of dimension $r$.

Algorithm 5 MultiChowForm_CI

**Input:** $f_1, \ldots, f_{|n| - r} \in \mathbb{Z}[x_1, x_2, \ldots, x_l], \alpha \in \mathbb{N}^l$

**Precondition:** $V = \mathbb{V}(f_1, \ldots, f_{|n| - r})$ is pure $r$-dimensional.

**Output:** The Chow form of $V$ corresponding to format $\alpha$.

1. Consider linear forms,
\[
U^i_j = \sum_{k=0}^{n_i} u_{jk} x_{ij}, \quad 0 \leq j \leq n_i - \alpha_i - 1
\]
for $i = 1, 2, \ldots, l$.

2. Eliminate the variables $x_1, \ldots, x_l$.
\[
R = \text{Elim}\{f_1, \ldots, f_{|n| - r}, U^i_j, \{x_1, \ldots, x_l\}\} \subset \mathbb{Z}[u_{jk}]
\]

3. $R_r = \text{SquareFreePart}(R)$.

4. RETURN $R_r$.

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

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

is the zero locus of $|n| - r$ many multihomogeneous polynomials. To simplify notation for the next lemma, we will denote $n = |n|$ and assume that $\forall i \in [n], j \in [l], \deg(f_i; x_j) \leq d$.

Lemma 4.5. Let $V$ be a complete intersection, i.e., the zero locus $V = \mathbb{V}(f_1, f_2, \ldots, f_{|n| - r})$ of $n - r$ many multihomogeneous polynomials and assume that $\deg(f; x_j) \leq d$ for $i \in [n], j \in [l]$ and the bitizes of $f_i$ are bounded by $\tau$. Also, $B_r = d^{n-r} \sum_{a} (n-r \times a)^{\tau+1}$. The Chow form of $V$ corresponding to a format $\alpha$ is a multihomogeneous polynomial in $\Lambda = \sum_{i=1}^l (n_i - \alpha_i)(n_i + 1)$ new variables of total degree $\leq B_r$ and bitizes $O(nB_r)$.

**Proof.** The proof is similar to the proof of Proposition 3.3. To exploit the multihomogeneity, we use sparse resultant computations and the multihomogeneous Bézout bound. We have $n - r$ multihomogeneous polynomials, each having (total) degree $\leq d$. To compute the Chow form of $V$, we add $(n_i - \alpha_i)$ linear forms in $x_i$, $U^i_j$; their coefficients are the variables $u_{jk}$ for $i \in [l]$.

The sparse resultant is homogeneous in each set of variables $u_{jk}$. Its degree with respect to $u_{jk}$ equals to the generic number of solutions of the remaining system when $u_{jk}$ is omitted, hence bounded by the multihomogeneous Bézout bound $d^{n-r}(n-r \times a)^{\tau+1}$. Thus, the resultant has total degree $\leq B_r$. The coefficients are integers of bitize $O(nB_r)$. The number of monomials is bounded by $O(nB_r^2)$. Following [10], 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 $M = O(n^d B_r)$.

It suffices to specialize $u_{jk}$ to numbers of bitize $O(n^3 \lg(d))$. So the specialized matrix contains numbers of bitize $O(n)$.
compute each determinant in $\tilde{O}(m^{n+1}(r+n^3))$. We need to perform this computations $\tilde{O}(B_m^r)$ many times and then we recover the resultant using interpolation. The cost of all the evaluations is $\tilde{O}(m^{n+1}r^{n+1}B_m^{r+1}(r+n^3))$. The cost of interpolation is $\tilde{O}(B_m^{r+1}(r+n^3))$. Finally, the cost of computing the square-free part is $\tilde{O}(m(B_m^{r+1}(r+n^3)))$. □

**Algorithm 6 MultIChowForm**

**Input:** $f_1, \ldots, f_m \in \mathbb{Z}[x_1, x_2, \ldots, x_r], r \in \mathbb{N}, \alpha \in \mathbb{N}^l$

**Precondition:** $V = \mathbb{V}(f_1, \ldots, f_m)$ is pure $r$-dimensional and $C\subset Z_{V, \alpha}$ is a hypersurface.

**Output:** The Chow form of $V$.

1. $\Lambda^1, \ldots, \Lambda^N := \text{MultiGENERICLC}(f_1, f_2, \ldots, f_m)$.
2. for $r \in |N|$ do $F_r = \text{ChowForm}\_C\_I(\Lambda^j_r)$;
3. **return** $\gcd(F_1, \ldots, F_N)$

### 4.3.2 The general case

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

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

where $m \geq |n| - r$. Consider the multidegrees $d_i = \max_{f_j} \deg(f_j)$ and set

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

Note that for all $i = 1, 2, \ldots, m$ we have $d_i \leq d$ by construction. For each $i = 1, 2, \ldots, m$ with $d_i < d$, we replace the polynomial $f_i$ with the collection $x_1^{a_1^i}x_2^{a_2^i} \cdots x_r^{a_r^i} f_i$ where $x_j$ denotes the $j$-th block of variables of the multiprojective space $\mathbb{P}^m$ and $a_j$ runs over all the possible monomials with $|a_j| = d_j - d_i$. The new collection $\tilde{f}$ has the property that each polynomial in it has the same multidegree, $d$. 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, $\max_i \deg(f_j) = d$.

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

For generic $\Lambda \in \mathbb{C}^{k \times m}$ we have $Z(A_f) = V \cup X$ for some pure dimensional variety $X$ of dimension $|n| - k$. The proof is essentially the same as the projective case, Proposition 3.5 and Proposition 3.6. 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 $N = \lceil \frac{m}{|n| - r} \rceil$. For generic choices of matrices $\Lambda^1, \ldots, \Lambda^N \in \mathbb{C}^{(|n| - r) \times m}$, each variety $\mathbb{V}(\Lambda^j)$ is a pure dimensional variety of dimension $r$ and $V = \bigcap_{j=1}^N \mathbb{V}(\Lambda^j)$. More concretely, there is a hypersurface $H \subset \mathbb{C}^{N(|n| - r) \times m}$ of degree $\leq N(|n| - r)|d|^{(n|n| - r - 1) + m}$ such that for any $(\Lambda^1, \ldots, \Lambda^N) \in \mathbb{C}^{N(|n| - r) \times m} \setminus H$, 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:** $f_1, \ldots, f_m \in \mathbb{Z}[x_1, x_2, \ldots, x_r], r \in \mathbb{N}$

**Precondition:** $V(f_1, f_2, \ldots, f_m)$ is pure $r$-dimensional.

**Output:** $\Lambda^1, \Lambda^2, \ldots, \Lambda^N$.

**Postcondition:** See Proposition 4.6.

1. $N := \lceil \frac{m}{|n| - r} \rceil$.
2. $S := \lceil N(|n| - r)|d|^{(n|n| - r) + m + 1} \rceil \in \mathbb{N}$.
3. for $(\Lambda^1, \Lambda^2, \ldots, \Lambda^N) \in \mathbb{C}^{N(|n| - r) \times m}$ do

   if dim($\mathbb{V}(\Lambda^j)$) $\leq r$ and $\mathbb{E}$ is full-rank then
   return $\Lambda^1, \ldots, \Lambda^N$.

**Lemma 4.7.** Alg. 7 returns $\Lambda^1, \Lambda^2, \ldots, \Lambda^N$ satisfying the requirements of Proposition 4.6 in $\tilde{O}(m(|n|))$.

**Proof.** The proof goes as in Lemma 3.7. To test dimension of $\mathbb{V}(\Lambda^j)$, we consider the affine cone $C = \mathbb{V}(\Lambda^j) \cap \mathbb{V}(\Lambda^j)$.

We have dim($C$) = dim($\mathbb{V}(\Lambda^j)$) + l, so we can compute the dimension of $\mathbb{V}(\Lambda^j)$ from dim($C$). □

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

**Theorem 4.8.** Consider $I = \langle f_1, \ldots, f_m \rangle \subset \mathbb{Z}[x_1, \ldots, x_r]$, where each $f_i$ is homogeneous of degree $d$ and bitsize $\tau$; also the corresponding projective variety, $V$, has pure dimension $r$. Also, $B_r = \sum_{i=1}^m (d_i - 1)^{n-1}$.

The Chow form of $V$ corresponding to a format $\alpha$ is a multihomogeneous polynomial in $A = \sum_{i=1}^m (n_i - a_i)(n_i + 1)$ new variables of total degree $\leq B_r$ and bitsize $\tilde{O}(\beta B_r \tau)$. 

**MultiGENERICLC (Alg. 6) computes $C\_V$ in $\tilde{O}(m^{\kappa \cdot n \cdot (\beta + 1) + n} \cdot \tilde{O}(\beta^{n-1} n^{\kappa-1} + 2^4 \cdot 24^4 + 1 \cdot \tau^2 + n^2))$, where $\omega$ is the exponent of matrix multiplication and $\kappa$ 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 $\tilde{O}(m(|n|))$ by the previous lemma.

$\Lambda^j$ have bitsizes bounded by $O(n \cdot \log m \cdot \log d \cdot \log l + r) = \tilde{O}(r + n)$. As there are $N = O(m)$ Chow forms to compute, the second step costs $\tilde{O}(m^{\kappa \cdot n \cdot (\beta + 1) + n} \cdot \tilde{O}(\beta^{n-1} n^{\kappa-1} + 2^4 \cdot 24^4 + 1 \cdot \tau^2 + n^2))$.

For the last step, we need to compute the gcd of $N$ Chow forms. As in the proof of Theorem 3.8, the cost of this step is less than the claimed complexity, therefore we can omit it. □

**Acknowledgments.** The authors would like to thank Matthias Bender and Kathlén Kohn for useful discussions.

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] C. Brand and M. Sagraloff. On the complexity of solving zero-dimensional polynomial systems via projection. In Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation, pages 151–158, 2016.
[2] L. 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):23–41, 1990.

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

[4] F. Castillo, Y. Cid-Ruiz, B. Li, J. Montaño, and N. Zhang. When are multidegrees positive? *Advances in Mathematics*, 374:187382, 2020.

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

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

[7] D. Cox, J. Little, and D. O'Shea. *Using algebraic geometry*. Graduate texts in mathematics. Springer, New York u.a., 1998.

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

[9] J. Dalbec and B. Sturmfels. *Introduction to Chow Forms*, pages 37–58. Springer Netherlands, Dordrecht, 1995.

[10] C. D’Andrea. Macaulay style formulas for sparse resultants. *Transactions of the American Mathematical Society*, 357(7):2595–2629, 2002.

[11] A. E. Z. E. Z. Emiris. Solving polynomial equations, volume 14 of *Algorithms and Computation in Mathematics*, 2005.

[12] M. L. Dogan, A. A. Ergür, J. D. Mundo, and E. Tsagirdas. The multivariate Schwartz-Zippel Lemma. *arXiv preprint arXiv:1910.01095*, 2019.

[13] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*. Graduate texts in mathematics. Springer, New York u.a., 2. ed. edition, 1995.

[14] I. Emiris, B. Mourrain, and E. Tsigaridas. Separation bounds for polynomial systems. *Journal of Symbolic Computation*, 82:123–133, 2017.

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

[16] B. Osserman and M. Trager. Multigraded Cayley-Chow forms. *Advances in Mathematics*, 348:583–606, May 2019.