Electronic Colloquium on Computational Complexity, Report No. 294 (2026)

Some algebraic and geometric computations in CH via Chow forms

Robert Andrews [*] Abhibhav Garg[†] Rafael Oliveira [‡] Éric Schost[§]

Abstract

The problem of decomposing an algebraic variety into more structured components (such as equidimensional, irreducible, or connected components) is a fundamental problem in computer algebra and algebraic geometry. In this work, we study the computational complexity of computing equidimensional components of algebraic varieties, represented via Chow forms.

We improve the state-of-the-art complexity bounds from PSPACE to CH, the counting hierarchy, for a number of problems related to equidimensional decomposition, including deciding

1. whether the Chow form of the k^{th} equidimensional component of a given projective variety vanishes at a given point,
2. whether a given monomial is in the support of the Chow form of the k^{th} equidimensional component of a given projective variety,
3. membership in a given equidimensional component of a given algebraic variety, and
4. membership in the closure of the image of an irreducible variety under a polynomial map.

As an application of our algorithm to decide membership in the closure of the image of a variety under a polynomial map, we show that the approximate polynomial satisfiability problem can be decided in CH. We also show that the degree of the k^{th} equidimensional component of a given projective variety can be computed in $\mathsf{FP}^{\mathsf{CH}}$.

Our main technical result is the construction of a polylogtime-uniform family of constant-depth, exponential-size threshold circuits that compute the Chow forms of the equidimensional components of a given projective variety. We construct these circuits by combining the machinery of geometric resolutions together with the uniform constant-depth, exponential-size threshold circuits of Andrews, Garg, and Schost (FOCS 2026) for the multivariate resultant.

[*]School of Computing Science, Simon Fraser University. Email: robert_andrews@sfu.ca.
[†]Department of Mathematics, University of Toronto. Email: abhibhav.garg@utoronto.ca.
[‡]Cheriton School of Computer Science, University of Waterloo. Email: rafael@uwaterloo.ca.
[§]Cheriton School of Computer Science, University of Waterloo. Email: eschost@uwaterloo.ca.

ISSN 1433-8092

Contents

1 Introduction **1**
- 1.1 Our results . . . 3
- 1.2 Proof overview . . . 5
- 1.3 Related work . . . 7
- 1.4 Concurrent work . . . 7
- 1.5 AI methodology . . . 8

2 Preliminaries **8**
- 2.1 Notation and conventions . . . 8
- 2.2 Algebraic geometry . . . 9
- 2.3 Uniformity of boolean and arithmetic circuit families . . . 11
- 2.4 Uniform circuits for basic arithmetic operations . . . 13
- 2.5 Uniformity of lifting factorizations . . . 16
- 2.6 Computation and the counting hierarchy . . . 19

3 Chow forms and geometric resolutions **21**
- 3.1 Chow forms . . . 21
- 3.2 Geometric resolutions . . . 22
- 3.3 The relationship between Chow forms and geometric resolutions . . . 26

4 Computing Chow forms of equidimensional components **28**
- 4.1 Chow form of limit subvarieties . . . 28
- 4.2 Constant-depth circuits for the Chow form . . . 33

5 Projections **41**
- 5.1 Projections of equidimensional varieties . . . 42
- 5.2 Approximate polynomial satisfiability . . . 45

1 Introduction

A central quest in computational algebraic geometry and algebraic complexity theory is to understand the computational complexity of deciding or computing geometric properties of algebraic varieties (common zero sets of a collection of polynomials) given the defining collection of polynomials. In this quest, fundamental problems include deciding whether the algebraic variety is empty (known as the Hilbert Nullstellensatz problem), computing the dimension of the variety, computing its degree, and decomposing the variety into more structured components (e.g., equidimensional, irreducible, and connected components).

Some of the above questions can also be (and have been) asked in more general settings, such as the setting of algebraic varieties defined by polynomials over arbitrary rings. To make this introduction more concise and accessible, we will focus on the setting of algebraic varieties defined by polynomials over the complex numbers. However, we will state our results in a more general setting.

In light of the importance of the aforementioned problems, much work has been devoted to them. The earliest works on these problems showed that they can all be solved in doubly-exponential time, as seen in [Las05; Her26; Sei74; GTZ88]. These works used techniques from elimination theory and Gröbner bases to reduce these problems to the task of solving doubly-exponential sized linear systems, or to factoring polynomials of doubly-exponential degree. Together with the work of Csanky [Csa76], this brings the complexity of the Hilbert Nullstellensatz problem down to EXPSPACE. Later, improved degree bounds for the Nullstellensatz (see [Jel05] and references therein) improved the complexity down to PSPACE. Subsequent works have improved the complexity of these problems, and we now give a brief overview of the history and state of the art regarding the complexity-theoretic improvements for them.

Hilbert Nullstellensatz (HN) and Dimension. The complexity of the HN problem has been brought down to the counting hierarchy by Andrews, Garg, and Schost [AGS26], while Koiran [Koi96] proved that this problem lies in AM, assuming an effective prime ideal theorem.[1] Later work by Canny [Can90] and Ierardi [Ier89] reduced HN to the task of computing multivariate resultants. Andrews, Garg, and Schost [AGS26] showed that multivariate resultants can be evaluated in $\mathsf{FP}^{\mathsf{CH}}$, and as a consequence placed HN in the counting hierarchy. Lastly, Koiran [Koi96] gave an AM-protocol for the Hilbert Nullstellensatz problem inspired by Stockmeyer's protocol for approximate counting. With regards to complexity-theoretic lower bounds, it is easy to see that arithmetization of SAT shows that this problem is NP-hard. Under plausible hardness assumptions, Miltersen and Vinodchandran [MV05] showed that NP = AM, so Koiran's result establishes that HN is conditionally NP-complete over $\mathbb{C}$. For a concise yet thorough account of developments on the Hilbert Nullstellensatz problem, we refer the reader to [AGS26] and references therein.

On the geometric front, the computation of the dimension of algebraic varieties was shown to be in the polynomial hierarchy [Koi97], again assuming an effective prime ideal theorem, and unconditionally shown to be in the counting hierarchy by Andrews, Garg, and Schost [AGS26]. Each of these works on computing dimension used similar techniques to those used for the Hilbert Nullstellensatz problem as described above. We once again refer the reader to [AGS26] for more details on works on the dimension of algebraic varieties.

As shown by Bürgisser and Cucker [BC06], the natural setting for obtaining complexity-theoretic lower bounds for several of the aforementioned geometric problems is the setting of counting problems. Thus, before we discuss the complexity of computing the degree and decomposing varieties into

[1] Recent work by Cureton and Thorner [CT26], building on OpenAI's proof of the Quasi-Riemann Hypothesis [Ope26], claims to prove an effective version of the prime ideal theorem, which would yield an unconditional version of Koiran's result.

equidimensional, irreducible, and connected components, we first introduce the notion of geometric counting complexity.

Geometric Counting Complexity. The study of complexity-theoretic lower bounds for more general geometric problems was initiated by Bürgisser and Cucker [BC06], who defined counting variants of the above problems, along with the complexity class GCC (standing for Geometric Counting Complex problems), which they show to be situated between #P and FPSPACE. Moreover, in [BC06], the authors show that the counting version of the Hilbert Nullstellensatz problem is GCC-complete, and that the problem of computing the top-component degree of an algebraic variety[2] is $\mathsf{FP}^{\mathsf{GCC}}$-complete with respect to Turing reductions. Recently, Andrews, Garg, and Schost [AGS26] showed that $\mathsf{GCC} \subseteq \mathsf{FP}^{\mathsf{CH}}$, thereby improving the upper bound for GCC from FPSPACE to $\mathsf{FP}^{\mathsf{CH}}$.

With the above complexity class in mind, and equipped with the results of Bürgisser and Cucker [BC06], we are now ready to discuss the complexity of the remaining geometric problems.

Equidimensional Components and Degree. Decomposing varieties into equidimensional components was first shown to be in exponential time by [CG83; Gri86; GHMP95; Lec00; JKSS04]. Several concepts and techniques used in these works, such as geometric resolutions and the computation of Chow forms representing each equidimensional component, will be used in our work as well, see Sections 3.1 and 3.2. The work of [GH91] shows how to produce an exponential-size and polynomial-depth algebraic circuit that computes the equidimensional components of a given algebraic variety, therefore showing that the problem of computing equidimensional components is in FPSPACE.

Since the degree of an algebraic variety is the sum of the degrees of its equidimensional components, the above results also imply that one can compute the degree of an algebraic variety in FPSPACE. Because these works are able to compute the equidimensional components of an algebraic variety, they are also able to compute the top-component degree of the variety, which is known to be $\mathsf{FP}^{\mathsf{GCC}}$-complete by [BC06]. This places the problem of computing the equidimensional components of an algebraic variety between $\mathsf{FP}^{\mathsf{GCC}}$ and FPSPACE.

Irreducible Components. The problem of decomposing varieties into irreducible components is a fundamental problem in algebraic geometry, being a highly nontrivial generalization of the problem of factoring polynomials (the latter corresponds to the case of decomposing a hypersurface into its irreducible components). The first complexity-theoretic improvement on decomposing varieties into irreducible components was to place this problem in single exponential time by [CG83; Gri86; Chi86; GH91; GHMP95]. These works used geometric resolutions to construct exponential-sized algebraic circuits that compute the equidimensional components of a given algebraic variety, and then used polynomial factorization techniques to decompose each equidimensional component into irreducible components. In [BS09, Theorem 4.1 and Proposition 4.2], the authors show that the problem of counting the number of irreducible components of an algebraic variety is GCC-hard and lies in FPSPACE. Later, an improvement by [Sch10] showed that the problem of computing a representation of the irreducible components is in FPSPACE via a generalization of Stickelberger's theorem for varieties of positive dimension.

[2] In [BC06] the authors denote by "geometric degree" the degree of the top-dimensional component of an algebraic variety. Since we adopt the definition of degree of an algebraic variety as the sum of the degrees of its irreducible components, we will refer to the notion of degree used in [BC06] as "top-component degree".

Connected Components. The problem of counting the number of connected components of an algebraic variety was shown by [BS09, Theorem 3.1] to be in FPSPACE. Subsequently, [Sch07] showed that this counting problem is FPSPACE-hard, therefore establishing FPSPACE-completeness for counting the number of connected components of an algebraic variety.

The complexity of decomposing varieties into connected components was shown to be in FPSPACE by [Sch10, Theorem 1.1]. Scheiblechner's decomposition algorithm for this problem is also based on a generalization of Stickelberger's theorem for varieties of positive dimension.

Summary of the State of the Art. The Hilbert Nullstellensatz problem and the problem of computing the connected components of an algebraic variety are complexity-theoretically well-understood, with (nearly) tight upper and lower bounds for their complexity. In contrast, over the complex numbers, the complexity of the problems of decomposing an algebraic variety into its equidimensional components or irreducible components remain unknown, with a complexity-theoretic gap between the known upper and lower bounds. The same is true for the complexity of the counting versions of these problems.

Given existing results on decompositions of varieties into equidimensional and irreducible components, it is natural to ask whether these decompositions can be computed more efficiently. Among these decompositions, the decomposition into equidimensional components is the simplest problem, as it is a coarser decomposition than (and can be computed from) the decomposition into irreducible components. Moreover, it is a natural first step towards computing the decomposition into irreducible components, as most algorithms for computing irreducible components first compute the equidimensional components and then decompose each equidimensional component into irreducible components via factorization.

1.1 Our results

In this work, we improve the complexity-theoretic upper bounds for the problem of computing the equidimensional components of an algebraic variety, and along the way we obtain improved upper bounds for the problems of computing the degree of an algebraic variety as well as computing projections of an algebraic variety. This also yields applications to the problem of computing coefficients of annihilators, thereby improving the complexity-theoretic upper bounds for the Approximate Polynomial Satisfiability problem, which is also known to be NP-hard via arithmetization of SAT. We now give a more detailed overview of our results.

Before we state our main results, we first give a brief and informal introduction to Chow forms, which are a classical tool in algebraic geometry for representing equidimensional projective varieties. For a more detailed introduction to Chow forms, we refer the reader to Section 3.1 and references therein. From now on, we will refer to homogeneous polynomials as *forms*, and we will refer to the common zero set of a collection of forms as a *projective variety*.

If one is given an equidimensional projective variety $V \subseteq \mathbb{P}^n$ of dimension k, it is well-known that the intersection of V with the zero set of a generic choice of $k+1$ linear forms $L_i = u_{i,0}x_0 + \cdots + u_{i,n}x_n$ for $i = 0, \ldots, k$ is an empty set. As it turns out, there is a unique (up to a scalar multiple) form $C_V(\mathbf{u})$, depending *only on the variables* $\mathbf{u} \coloneqq \{u_{i,j}\}_{0 \leq i \leq k,\ 0 \leq j \leq n}$, such that the intersection of V with the zero set of the linear forms L_i is nonempty if and only if $C_V(\mathbf{u}) = 0$. The form C_V is called the *Chow form* of the equidimensional projective variety V, and it is also known that $\deg(C_V) = (k+1)\deg(V)$, where $\deg(V)$ is the degree of the variety V. This gives a way to represent equidimensional projective varieties by means of a single form (the Chow form), and this form carries important information about the variety. Although we have only defined Chow forms for

projective equidimensional varieties, it is possible to use Chow forms to obtain useful information about equidimensional affine varieties as well (see Remark 4.14 for more details).

We are now ready to state two of our main results, which improve the complexity-theoretic upper bounds for computing Chow forms of equidimensional components of algebraic varieties. To make the statement of our results more concise, we will use the following setup.

Setup. Let $F_1, \ldots, F_m \in \mathbb{Q}[x_0, \ldots, x_n]$ be forms given by constant-free algebraic circuits and let $V \coloneqq \mathrm{V}(F_1, \ldots, F_m)$ be the projective variety defined by these forms. For $0 \leq k \leq n$, denote by V_k the k-equidimensional component of V, and by C_{V_k} the Chow form of V_k.

Theorem 1.1 (Zeros of Chow Form)**.** *Let V be a projective variety given as in the above setup. Let $\mathbf{a} \in \mathbb{Q}^{(n+1)(k+1)}$ and $k \in \mathbb{N}$. Given $V, k, \mathbf{a}$, one can decide whether $C_{V_k}(\mathbf{a}) = 0$ in CH.*

In fact, we can do more than just decide whether the Chow form vanishes at a point.

Theorem 1.2 (Chow Form Coefficients)**.** *Let V be a projective variety given as in the above setup. Let $k \in \mathbb{N}$, and $\mathbf{e} \in \mathbb{N}^{(n+1)(k+1)}$ be the exponent vector of a monomial in the variables of C_{V_k}. Given $V, k, \mathbf{e}$, one can decide if the coefficient of the monomial corresponding to $\mathbf{e}$ in C_{V_k} is zero in CH.*

Remark 1.3. The above two results are a consequence of our main technical result (Theorem 4.9): we construct a polylogtime-uniform family of constant-depth threshold circuits that computes the Chow forms of the equidimensional components of a given projective variety. For more details on our main technical result and its consequences, we refer the reader to Section 4.2. ◊

The above two results allow us to decide membership in equidimensional components of algebraic varieties, as well as to compute the degree of the given variety. This is the content of our next results (see Corollaries 4.12 and 4.13 and Remark 4.14 for proofs of these results).

We now state the first consequence of the above results, which allows us to compute the degree of an algebraic variety.

Theorem 1.4 (Degree)**.** *Given a collection of polynomials $f_1, \ldots, f_m \in \mathbb{Q}[x_1, \ldots, x_n]$ represented as constant-free algebraic circuits and $k \in \mathbb{N}$, one can compute the degree of the k^{th}-equidimensional component of $V \coloneqq \mathrm{V}(f_1, \ldots, f_m)$ in $\mathsf{FP}^{\mathsf{CH}}$. In particular, this implies that one can compute $\deg(V)$, as well as the number of isolated points of V in $\mathsf{FP}^{\mathsf{CH}}$.*

The above result improves the previous best known upper bound of $\mathsf{FPSPACE}$ for computing the degree of an algebraic variety.

The next consequence of the above results is on the problem of deciding membership in equidimensional components of algebraic varieties.

Theorem 1.5 (Equidimensional Component Membership)**.** *Given a collection of polynomials $f_1, \ldots, f_m \in \mathbb{Q}[x_1, \ldots, x_n]$ represented as constant-free algebraic circuits, $\boldsymbol{\alpha} \in \mathbb{Q}^n$, and $k \in \mathbb{N}$, one can decide whether $\boldsymbol{\alpha}$ lies in the dimension-k equidimensional component of $\mathrm{V}(f_1, \ldots, f_m)$ in CH.*

The above result improves the previous best known upper bound of PSPACE for deciding membership in equidimensional components of algebraic varieties [Sch10].

Another consequence of our main technical results is related to deciding membership in the closure of images of irreducible varieties under polynomial maps. This is a basic problem in algebraic geometry, capturing many natural questions, two special cases being the computation of the transcendence degree and the Approximate Polynomial Satisfiability problem (APS) of Guo, Saxena, and Sinhababu [GSS19]. We now state our result on membership in the closure of images of irreducible varieties under polynomial maps, and then discuss its implications for APS.

Theorem 1.6 (Image Closure Membership)**.** *Let $p \in \mathbb{N}$ and $f_1, \ldots, f_m \in \mathbb{Q}[x_1, \ldots, x_n]$ represented as constant-free algebraic circuits be such that the variety $\mathrm{V}(f_1, \ldots, f_m)$ is irreducible and of dimension $p-1$. Let $h_1, \ldots, h_p \in \mathbb{Q}[x_1, \ldots, x_n]$ be represented as constant-free algebraic circuits defining the polynomial map $\Phi_{\mathbf{h}} : \mathbb{C}^n \to \mathbb{C}^p$. Given a point $\boldsymbol{\alpha} \in \mathbb{Q}^p$ and polynomials $f_1, \ldots, f_m, h_1, \ldots, h_p$ as above, where the variety $\mathrm{V}(f_1, \ldots, f_m)$ is irreducible and of dimension $p-1$, one can decide whether $\boldsymbol{\alpha}$ lies in the closure of $\Phi_{\mathbf{h}}(\mathrm{V}(f_1, \ldots, f_m))$ in* CH.

Before we discuss the implications of the above result for APS, we briefly introduce the APS problem. Given a field $\mathbb{F}$, we denote by $\mathbb{A}^n$ the affine n-space over $\overline{\mathbb{F}}$, the algebraic closure of $\mathbb{F}$.

Definition 1.7 (Approximate Polynomial Satisfiability (APS))**.** Let $\mathbb{F}$ be a field, and let $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ be polynomials. This set of polynomials is *approximately satisfiable* if the closure of the image of the map $\phi_{\mathbf{f}} : \mathbb{A}^n \to \mathbb{A}^m$ defined by $\phi_{\mathbf{f}}(\mathbf{a}) = (f_1(\mathbf{a}), \ldots, f_m(\mathbf{a}))$ contains the point $(0, \ldots, 0)$.

The APS problem is the following: given an algebraic circuit that computes polynomials $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$, decide if the polynomials $f_1, \ldots, f_m$ are approximately satisfiable. $\lozenge$

Note that $\{f_1, \ldots, f_m\}$ is *satisfiable* in the usual sense if $(0, \ldots, 0) \in \phi_{\mathbf{f}}(\mathbb{A}^n)$.

Remark 1.8. In the above, if the underlying field $\mathbb{F} = \mathbb{Q}$, then Theorem 1.6 already shows us that we can solve the APS problem in CH, as $\mathbb{A}^n$ is an irreducible variety. However, since the APS problem is a very structured special case of the image closure membership problem, we can actually solve APS in CH over a larger class of fields, as we will show in Section 5. Thus, below we state our result on APS in CH over a larger class of base fields $\mathbb{F}$. $\lozenge$

Theorem 1.9 (APS in CH)**.** *Let $\mathbb{F}$ be one of the fields $\mathbb{F}_{p^a}, \mathbb{F}_{p^a}(t_1, \ldots, t_k)$, a number field $\mathbb{Q}[\alpha]$, or $\mathbb{Q}[\alpha](t_1, \ldots, t_k)$. Then* APS *over $\mathbb{F}$ lies in* CH.

1.2 Proof overview

Having stated our main results, we now give a high-level overview of the challenges and new ideas behind the proof of our main technical result (Theorem 4.9), where we construct a polylogtime-uniform family of constant-depth threshold circuits that compute the Chow forms of the equidimensional components of a given projective variety. Even though the threshold circuits we construct are exponentially large, being polylogtime-uniform and constant depth means they are highly structured. In particular, we can decide the value of an output of such a circuit in CH, the counting hierarchy, which is exactly why CH enters into our complexity bounds. Once we have the circuits Theorem 4.9, we can use them along with the framework of [AGS26] to simulate such circuits in CH and other standard techniques from algebraic geometry to obtain the other results stated above.

It is a classical fact that Chow forms of equidimensional varieties can be computed from resultants (see Lemma 4.2 for a quick proof in the complete intersection case). The recent work of [AGS26] shows that resultants can be computed by a uniform family of algebraic circuits of constant depth and exponential size, so we can directly apply the framework of [AGS26] to prove Theorems 1.1, 1.2 and 1.4 when the variety V is equidimensional. The main difficulty therefore is to reduce the general case (when the variety V has more than one equidimensional component) to the equidimensional case. We begin by asking the following question: can we compute the Chow form of any equidimensional component of a variety V via resultants?

The inspiration and starting point for our approach comes from the work of Canny [Can90] and the subsequent algebraic proof given by Ierardi [Ier89]. The work of [Can90] introduced the concept of the generalized characteristic polynomial (GCP), which allows one to study the solution set of a variety V via a "perturbed system" of equations which "degenerates" to the original system

of equations defining V. This method allows one to argue about the zero-dimensional component of V by studying the zero-set of the perturbed system. In [Can90; Ier89], the authors show that the GCP can be computed by exponential-size algebraic circuits. An important consequence of their result is that they can extract from the GCP a zero-dimensional subvariety of V that *contains* the zero-dimensional component of V. While their result does not give a way to compute the zero-dimensional component of V itself, it makes some important progress towards it. Moreover, they can compute the GCP via resultants, which is a key ingredient in our approach.

The above leads us to the following two challenges:

1. Can we generalize the above GCP-based method to compute a k-equidimensional subvariety of V that *contains* the k-equidimensional component of V?

   The above works only deal with the zero-dimensional case (i.e., $k = 0$), and it is not clear how to generalize their approach to the case of arbitrary k.

2. How do we compute the zero-dimensional component of V from the GCP? Is there an efficient way (in constant depth) to prune the extra points (i.e. components) from the zero-dimensional subvariety of V that contains the zero-dimensional component of V?

   More generally, even if we solve item 1, how do we compute the k-equidimensional component of V by pruning the k-equidimensional subvariety of V that was obtained from item 1?

In this work, we give a positive answer to both of the above questions, and we show that both of these steps (the higher-dimensional generalization of the GCP-based method, and the pruning step for any dimension) can be done in constant depth. With the solution of both items 1 and 2 above and with a bit more work (see Section 4.2), we can compute the Chow form of any equidimensional component of a variety V in constant depth, thereby proving Theorem 4.9.

We now discuss the main conceptual ideas and challenges behind the solution to the above two problems, and how we overcome them.

Solving item 1. The works of Canny [Can90] and Ierardi [Ier89] show that the GCP computes a u-resultant of a zero-dimensional subvariety of V that contains the zero-dimensional component of V. Since the u-resultant of a zero-dimensional variety is the Chow form of that variety, this naturally leads to the approach of using a higher-dimensional generalization of the GCP to compute the Chow form of a k-equidimensional subvariety of V that *contains* the k-equidimensional component of V. We establish this generalization in Section 4.1, and it is our first main technical contribution.

Solving item 2. Once we solved item 1, for any $k \in \{0, 1, \ldots, n\}$, we can compute a k-equidimensional subvariety $W_k \subset V$ that contains the k-equidimensional component of V, which we will denote by V_k. Let us call the irreducible components of W_k that are not in V_k the *excess components* of W_k. Because $W_k \subset V$ and W_k is equidimensional, we know that *all* excess components must lie inside a *higher dimensional component* of V. In particular, if r is the dimension of V, then we know that $W_r = V_r$, as W_r cannot have any excess components due to the dimension of V.

Now that we have one equidimensional component of V (the r-equidimensional component), by the above dimensionality argument, we can prune the excess components of W_{r-1} by removing the intersection of W_{r-1} with V_r. Proceeding inductively, we can prune the excess components of W_k by removing the intersection of W_k with $V_{k+1} \cup V_{k+2} \cup \cdots \cup V_r$. This pruning can be done via a GCD computation, which can be done in constant depth. However, note that this inductive way of pruning the excess components will not yield a constant-depth circuit, as it requires a sequential computation of the equidimensional components of V!

To address this sequentiality issue, we need the following important observations. We definitely know that the excess components of W_k must lie inside a higher-dimensional component of V, that is, inside $V_{k+1} \cup V_{k+2} \cup \cdots \cup V_r$. Since $V_k \subset W_k$, this implies that the excess components of W_k must lie inside $W_{k+1} \cup W_{k+2} \cup \cdots \cup W_r$. Moreover, note that since each $W_k \subset V$, any k-dimensional irreducible component $X \subset V$ *cannot* lie inside $W_{k+1} \cup W_{k+2} \cup \cdots \cup W_r$, as that would imply that X is contained in another irreducible component of V (one of dimension greater than k), which contradicts the fact that X is an irreducible component of V.[3]

This gives us a way to prune the excess components of W_k in constant depth: we first "compute" all the W_k's in parallel, and then we can prune the excess components of each W_k by removing the intersection of W_k with $W_{k+1} \cup W_{k+2} \cup \cdots \cup W_r$, which can be done in constant depth via a GCD computation.

To perform this pruning step, we need to compute both the Chow forms of W_k and a geometric resolution of W_k for all $k \in \{0, 1, \ldots, r\}$. But so far, step 1 only gives us a way to compute the Chow forms of W_k for all $k \in \{0, 1, \ldots, r\}$. To compute the geometric resolutions of W_k for all $k \in \{0, 1, \ldots, r\}$, we show that we can compute a geometric resolution of W_k from the Chow form of W_k (and this can be done in constant depth). The relationship between Chow forms and geometric resolutions is done in Section 3, and the pruning step is done in Section 4.2. This concludes step 2, thereby giving an overview of the proof of Theorem 4.9.

1.3 Related work

In addition to the references mentioned above, a few further comments are in order to compare the approaches used in some of these papers to our work. The algorithm in [GH91] iteratively computes polynomials defining the equidimensional components of V by a succession of projections and saturations; in effect, this reduces the problem to linear algebra in size $d^{n^{O(1)}}$. Follow-up papers such as [GHMP95; GHMMP98] introduced the notion of geometric resolution, on which we rely. In this approach, equidimensional components are described by means of birational projections to hypersurfaces: this yields polynomials with useful algorithmic properties, but in general, they only describe open dense subsets of the components of V. The algorithms in these papers, which culminate with Lecerf's equidimensional decomposition algorithm [Lec00], are based on a formal version of Newton iteration, which makes it possible to store all polynomials by straight-line programs of size $d^{O(n)}$, and perform $d^{O(n)}$ operations altogether.

Inspired in part by these results, the algorithm in [JKSS04] computes Chow forms for the equidimensional components of V. It relies on similar techniques – in particular, straight-line program encoding and Newton iteration and the use of geometric resolutions to perform a pruning step similar to ours – and results in an overall $d^{O(n)}$ operations to compute straight-line programs of size $d^{O(n)}$ for the Chow forms. The algorithms in this paper are instead based on multivariate resultant computations; the bounds on the size of the resulting circuits are slightly inferior, of order $d^{n^{O(1)}}$, but achieving constant-depth through the approach of [JKSS04] remains an open question.

1.4 Concurrent work

Independent of and concurrent to our work, two other sets of authors have obtained similar improvements to the complexity of the approximate polynomial satisfiability problem. Balaji,

[3]The most intuitive way to see this is in the case of $k = 0$, i.e. the case of isolated points of the variety V. By definition, any isolated point of V cannot lie inside a higher-dimensional component of V, as that would contradict the fact that it is an isolated point. Since each $W_\ell \subset V$ is equidimensional of dimension ℓ, for any $\ell > 0$, every irreducible component of W_ℓ is contained in an irreducible component of V of dimension at least ℓ, and thus W_ℓ cannot contain any isolated points of V.

Shirmohammadi, Tavenas, and Worrell [BSTW26] proved $\mathsf{APS} \in \mathsf{CH}$ over the rational numbers and finite fields. Agarwal, Hari, Pandey, and Shukla [AHPS26] likewise gave a proof that $\mathsf{APS} \in \mathsf{CH}$.

1.5 AI methodology

Activity	AI used
Asking the research question	No
Coming up with the approach	No
Proof development	No
Writing and exposition	No
Checking for bugs	No
Other supporting tasks	No

Details No AI was used at any point in the development of this work.

2 Preliminaries

2.1 Notation and conventions

We work over a field $\mathbb{F}$ and use $\overline{\mathbb{F}}$ to denote its algebraic closure. The *coefficient subfield* of $\mathbb{F}$ is the largest algebraic extension of the prime field of $\mathbb{F}$ within $\mathbb{F}$. We use $\mathbb{F}[x_1, \ldots, x_n]$ and $\mathbb{F}(x_1, \ldots, x_n)$, respectively, to denote the ring of polynomials and field of rational functions with coefficients in $\mathbb{F}$ and variables $x_1, \ldots, x_n$. We write vectors as $\mathbf{x} = (x_1, \ldots, x_n)$. Given $\mathbf{a} \in \mathbb{N}^n$, we write $\mathbf{x}^\mathbf{a}$ for the monomial $x_1^{a_1} \cdots x_n^{a_n}$.

A *form* of degree d is a homogeneous polynomial of degree d. We follow the convention that forms are written using capital letters and inhomogeneous polynomials using lowercase letters. We frequently encounter pairs of polynomials where one is the (de-)homogenization of the other. In such instances, we write both polynomials with the same letter to indicate this relationship. As an example, if $F \in \mathbb{F}[x_0, \ldots, x_n]$ is a form, its dehomogenization $F(1, x_1, \ldots, x_n)$ will be denoted by f. Similarly, when $f \in \mathbb{F}[x_1, \ldots, x_n]$ is an inhomogeneous polynomial of degree d, we use F to denote the homogenization $x_0^d f(x_1/x_0, \ldots, x_n/x_0)$.

The greatest common divisor of any two univariate polynomials with coefficients in a field $\mathbb{F}$ will always be monic. If R is any unique factorization domain with field of fractions $\mathbb{F}$, then the greatest common divisor of two univariate polynomials with coefficients in R will be their greatest common divisor as polynomials in $\mathbb{F}[z]$. For multivariate polynomials $f, g \in \mathbb{F}[x_1, \ldots, x_n]$, we define $\gcd(f, g)$ to be the unique $\mathbb{F}$-multiple of the greatest common divisor that has leading coefficient 1 in the lexicographic order. As in the univariate case, if R is a UFD with field of fractions $\mathbb{F}$, then the GCD of two multivariate polynomials with coefficients in R is their GCD as polynomials with coefficients in $\mathbb{F}$.

Given polynomials $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$, we use $\mathrm{V}(f_1, \ldots, f_m)$ to denote their common zeroes in $\mathbb{A}^n_{\overline{\mathbb{F}}}$, which we will often denote by simply $\mathbb{A}^n$ when the field $\mathbb{F}$ is clear from context. If these polynomials are instead forms $F_1, \ldots, F_m \in \mathbb{F}[x_0, \ldots, x_n]$, then $\mathrm{V}(F_1, \ldots, F_m)$ is taken to be their common zeroes in the projective space $\mathbb{P}^n_{\overline{\mathbb{F}}}$, which we will simply denote by $\mathbb{P}^n$. For us, a variety is any set of solutions to a system of polynomial equations over an algebraically closed field; in particular, varieties may be reducible. The degree of a variety V, denoted $\deg V$, is defined as the sum of the degrees of all irreducible components of V.

We on occasion examine the trailing term and trailing coefficient, defined below, of a polynomial with respect to one of its variables.

Definition 2.1. Suppose $f \in \mathbb{F}[t, y_1, \ldots, y_m]$ is a nonzero polynomial. The *trailing term of f with respect to t*, denoted by $\mathrm{TT}_t\, f(y_1, \ldots, y_m)$, is the coefficient of the lowest-degree term in f when viewed as a polynomial in t. Concretely, if $f = t^i f_i(y_1, \ldots, y_m) + t^{i+1} f_{i+1}(y_1, \ldots, y_m) + \cdots + t^d f_d(y_1, \ldots, y_m)$ where $f_i(\mathbf{y}) \neq 0$, then $\mathrm{TT}_t\, f = f_i$.

The *trailing part of f with respect to t*, written $\mathrm{TP}_t\, f$, is the polynomial obtained by factoring out the highest power of t from f. In the above setting, we have $\mathrm{TP}_t\, f = f_i + t f_{i+1} + \cdots + t^{d-i} f_d$.

The trailing term and the trailing part of the zero polynomial are zero. ◊

The height of an integer $a \in \mathbb{Z}$ is defined to be $\lceil \log(|a|) \rceil$. The height of a polynomial with integer coefficients is the maximum height of its coefficients.

2.2 Algebraic geometry

In this subsection, we list some basic (computational) algebraic geometry facts that we will use throughout this article. The first two facts are standard bounds on the probability that a random hyperplane section of a variety has codimension 1 and on the probability that the variety defined by random linear combinations of a given set of equations has certain nice behaviour.

Lemma 2.2. *Let $B \subseteq \mathbb{F}$ be a finite set. Let $V \subseteq \mathbb{P}^n$ be a projective variety of dimension r and degree D. Suppose ℓ is a linear form with each coefficient picked independently and uniformly at random from B. Then with probability at least $1 - D/|B|$, the intersection $V \cap \mathrm{V}(\ell)$ has dimension $r-1$. If $\ell_1, \ldots, \ell_{r+1}$ are linear forms chosen the same way, then $V \cap \mathrm{V}(\ell_1, \ldots, \ell_{r+1}) = \varnothing$ with probability at least $1 - (r+1)D/|B|$.*

Let $W \subseteq \mathbb{A}^n$ be an affine variety of dimension r and degree D. Suppose ℓ is a linear polynomial with each coefficient picked independently and uniformly at random from B. Then with probability at least $1 - 2D/|B|$, the intersection $W \cap \mathrm{V}(\ell)$ has dimension $r-1$. If $\ell_1, \ldots, \ell_{r+1}$ are linear polynomials chosen the same way, then $W \cap \mathrm{V}(\ell_1, \ldots, \ell_{r+1}) = \varnothing$ with probability at least $1 - 2(r+1)D/|B|$.

Lemma 2.3. *Let $B \subseteq \mathbb{F}$ be a finite set. Let $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ be polynomials of degree at most d. Suppose $g_1, \ldots, g_{n+1}$ are linear combinations of $f_1, \ldots, f_m$, with each coefficient picked independently and uniformly at random from B. Then with probability at least $1 - (n+1)d^n/|B|$, the following is true. For each $s \in [n+1]$, every irreducible component of $\mathrm{V}(g_1, \ldots, g_s)$ of codimension less than s is a component of $\mathrm{V}(f_1, \ldots, f_m)$. As a consequence, $\mathrm{V}(g_1, \ldots, g_{n+1}) = \mathrm{V}(f_1, \ldots, f_m)$. The analogous result in the projective setting also holds.*

The proof of both Lemma 2.2 and Lemma 2.3 are implicit in the methods of Heintz [Hei83]. For an explicit proof of the latter, see for example [KP96, Lemma 36]. The former can be proved using essentially the same arguments.

Next, we list some basic properties of ideals in polynomial rings that are preserved by certain extensions of scalars.

Lemma 2.4. *Let $\mathbb{F}$ be any algebraically closed field. Let $\mathbb{L}$ be an extension of $\mathbb{F}$. Let I and J be ideals in $\mathbb{F}[x_1, \ldots, x_n]$, and let I' and J' denote the extensions $I\mathbb{L}[x_1, \ldots, x_n]$ and $J\mathbb{L}[x_1, \ldots, x_n]$, respectively. The following are true.*

1. *$I' \cap \mathbb{F}[x_1, \ldots, x_n] = I$.*
2. *$(I \cap J)' = I' \cap J'$.*
3. *If I is radical, then I' is radical.*

4. *If I is a prime ideal of dimension r and degree D, then I' is also a prime ideal of dimension r and degree D.*

Proof. Let $\{\alpha_i\}_{i\in S}$ be a basis for $\mathbb{L}$ as a vector space over $\mathbb{F}$, with $\alpha_s = 1$. Given any $f \in I'$, we can write $f = \sum_{i\in S} \alpha_i f_i$, where $f_i \in I$ with only finitely many nonzero f_i. Further, this representation is unique since $\{\alpha_i\}_{i\in S}$ is a basis for $\mathbb{L}[x_1, \ldots, x_n]$ as a free $\mathbb{F}[x_1, \ldots, x_n]$-module. The intersection $I' \cap \mathbb{F}[x_1, \ldots, x_n]$ consists of exactly those elements which, when written in the above representation, only have nonzero f_s. This shows that $I' \cap \mathbb{F}[x_1, \ldots, x_n] = I$.

Given any element $f \in I' \cap J'$, the same argument along with uniqueness shows that we can write $f = \sum_{i\in S} \alpha_i f_i$ with $f_i \in I \cap J$. Therefore we can deduce $f \in (I \cap J)'$, showing $I' \cap J' \subseteq (I \cap J)'$. The reverse containment is immediate from definitions.

If I is radical, then $\mathbb{F}[x_1, \ldots, x_n]/I$ is a reduced $\mathbb{F}$-algebra. The algebra $\mathbb{L}[x_1, \ldots, x_n]/I'$ is exactly $(\mathbb{F}[x_1, \ldots, x_n]/I) \otimes \mathbb{L}$. Since $\mathbb{F}$ is a perfect field, the extension $\mathbb{L}/\mathbb{F}$ is separably generated. Therefore we can invoke [Sta26, Tag 05DS] to deduce that $\mathbb{L}[x_1, \ldots, x_n]/I'$ is reduced, equivalently that I' is radical. Similarly, if I is prime, then we can deduce that I' is prime [Sta26, Tag 020J] .

Suppose now that I is prime. Any transcendence basis of the fraction field of $\mathbb{F}[x_1, \ldots, x_n]/I$ as an $\mathbb{F}$-algebra is also a transcendence basis of the field of fractions of $\mathbb{L}[x_1, \ldots, x_n]/I'$ as an $\mathbb{L}$-algebra. Therefore I and I' have the same dimension.

Finally, when I is prime and has dimension r, then the degree of I is exactly the degree of the field extension $\mathbb{F}(\mathbf{M}, \mathbf{b}) \to \mathbb{F}(\mathbf{M}, \mathbf{b})[x_1, \ldots, x_n]/(I, \mathbf{Mx} + \mathbf{b})$, where $\mathbf{M}$ are the entries of a generic matrix of size $r \times n$, and $\mathbf{b}$ are the entries of a generic vector of size $r \times 1$ ([Hei83, Definition 1]). This degree is unchanged when $\mathbb{F}$ is replaced by $\mathbb{L}$. This shows that the degree of I' agrees with that of I. □

The main setting in which we will invoke the above lemma is when $\mathbb{L}$ is the algebraic closure of $\mathbb{F}(u_0, \ldots, u_m)$, where the u_i are new indeterminates.

Finally, we discuss the notion of the multivariate resultant. For $d \in \mathbb{N}$, we write $M_{n,d}$ for the set of homogeneous degree-d monomials in the $n+1$ variables $x_0, \ldots, x_n$.

Definition 2.5 (see, e.g., [Jou91, Proposition 2.3])**.** Fix positive integers $n, d_0, \ldots, d_n$. Let $\mathbf{u} = \{u_{i,\boldsymbol{\alpha}} \mid i \in \{0, \ldots, n\}, \boldsymbol{\alpha} \in M_{n,d}\}$ be a set of variables corresponding to the coefficients of $n+1$ homogeneous polynomials of degrees $d_0, \ldots, d_n$, respectively. There exists a unique polynomial $\mathrm{Res}_{n,d_0,\ldots,d_n} \in \mathbb{F}[\mathbf{u}]$ with the following properties.

1. *Main property of the resultant:* If $F_0, \ldots, F_n \in \mathbb{F}[x_0, \ldots, x_n]$ are homogeneous polynomials of degrees $d_0, \ldots, d_n$, respectively, then $\mathrm{Res}_{d_0,\ldots,d_n}(F_0, \ldots, F_n) = 0$ if and only if the system of equations $F_0(\mathbf{x}) = \cdots = F_n(\mathbf{x}) = 0$ has a solution in $\mathbb{P}^n_{\overline{\mathbb{F}}}$. By $\mathrm{Res}_{d_0,\ldots,d_n}(F_0, \ldots, F_n)$, we mean the evaluation of $\mathrm{Res}_{d_0,\ldots,d_n}$ obtained by setting $u_{i,\boldsymbol{\alpha}}$ equal to the coefficient of the monomial $\mathbf{x}^{\boldsymbol{\alpha}}$ in F_i.
2. $\mathrm{Res}_{d_0,\ldots,d_n}(x_0^{d_0}, \ldots, x_n^{d_n}) = 1$.
3. The polynomial $\mathrm{Res}_{d_0,\ldots,d_n}$ is irreducible in $\overline{\mathbb{F}}[\mathbf{u}]$.

Moreover, if we write $\mathrm{Res}^{\mathbb{Q}}_{d_0,\ldots,d_n}$ and $\mathrm{Res}^{\mathbb{F}}_{d_0,\ldots,d_n}$ for the resultants over $\mathbb{Q}$ and $\mathbb{F}$, respectively, then the former has integer coefficients and $\mathrm{Res}^{\mathbb{F}}_{d_0,\ldots,d_n}$ is the image of $\mathrm{Res}^{\mathbb{Q}}_{d_0,\ldots,d_n}$ under the natural ring homomorphism $\mathbb{Z}[\mathbf{u}] \to \mathbb{F}[\mathbf{u}]$.

When the degrees of the input polynomials and the field of their coefficients are clear, we write Res in place of $\mathrm{Res}^{\mathbb{F}}_{n,d_0,\ldots,d_n}$ for brevity. ◊

A typical setting in which we invoke the above result is the following. Suppose $F_0, \ldots, F_n \in \mathbb{F}[x_0, \ldots, x_n, y_1, \ldots, y_m]$ are polynomials that are homogeneous in the $\mathbf{x}$ variables. These polynomials

define a variety in $\mathbb{P}^n \times \mathbb{A}^m$. We can treat $F_0, \ldots, F_n$ as polynomials in $\mathbb{F}(y_1, \ldots, y_m)[x_0, \ldots, x_n]$. Let $R := \mathrm{Res}_{d_0,\ldots,d_n}^{\mathbb{F}(y_1,\ldots,y_m)}(F_0, \ldots, F_n)$, where d_i is the degree in $\mathbf{x}$ of F_i. By the universality of the resultant, namely by the fact that the resultant over $\mathbb{F}$ is the image of the resultant over $\mathbb{Z}$ under the natural map $\mathbb{Z}[\mathbf{u}] \to \mathbb{F}[\mathbf{u}]$, we can deduce that $R \in \mathbb{F}[y_1, \ldots, y_m]$. From the universality, we can also deduce that the zeroes of R, or of its squarefree part, form the projection of $\mathrm{V}(F_0, \ldots, F_n)$ onto $\mathbb{A}^m$. Indeed for any setting $\boldsymbol{\gamma} \in \overline{\mathbb{F}}^m$ of the $\mathbf{y}$ variables, the universality implies that $\mathrm{Res}_{d_0,\ldots,d_n}^{\overline{\mathbb{F}}}(F_0(\mathbf{x}, \boldsymbol{\gamma}), \ldots, F_m(\mathbf{x}, \boldsymbol{\gamma})) = R(\boldsymbol{\gamma})$. By definition, the expression on the left vanishes exactly on the image of the projection of $\mathrm{V}(F_0, \ldots, F_n)$ to $\mathbb{A}^m$. One consequence of this property of the resultant is that the projection of $\mathrm{V}(F_0, \ldots, F_n)$ to $\mathbb{A}^m$ is either surjective (which is equivalent to the condition that R is the zero polynomial), empty (when R is a nonzero constant), or has codimension one.

2.3 Uniformity of boolean and arithmetic circuit families

This subsection describes the notions of uniformity we use for both arithmetic and boolean circuits. We start by recalling the definition of arithmetic circuits.

Definition 2.6. Let $\mathbb{F}$ be a field and let $\mathbb{F}(\mathbf{x})$ be the field of rational functions in the variables $x_1, \ldots, x_n$ over $\mathbb{F}$. An *arithmetic circuit over* $\mathbb{F}$ is a directed acyclic graph. The vertices of this graph of in-degree zero are either called *input gates* and are labeled by a variable x_i, or called *constant gates* and are labeled by a field element $\alpha \in \mathbb{F}$. Vertices of positive in-degree are called *internal gates* and are labeled by an operation from $\{+, \times, \div\}$. Vertices of out-degree zero are called *output gates*. Each gate of the circuit naturally computes an element of $\mathbb{F}(\mathbf{x})$, assuming no division by zero takes place in the circuit, which we require. If $\{f_1, \ldots, f_m\}$ are the functions computed by the output gates of the circuit, we say that the circuit *computes* the functions $f_1, \ldots, f_m$. The *size* of the circuit is the number of wires in the circuit. The *depth* of the circuit is the length of the longest path from an input to an output of the circuit.

If the only constants labeling the input gates of the circuit are $0, +1$, and -1, we say that the circuit is *constant-free*. For a fixed variable x_i, if the subcircuits rooted at the denominators of each division gate in the circuit do not contain the input gate corresponding to x_i, then we say that the circuit is *division-free with respect to* x_i. If X' is a subset of variables and the circuit is division-free with respect to every variable in X', we say the circuit is *division-free with respect to* X'. If the circuit is division-free with respect to all variables, we say the circuit is *weakly division-free*. $\Diamond$

For simplicity, we restrict our attention to constant-free arithmetic circuits whenever uniformity is a concern. This avoids the need to impose a uniformity constraint on the field elements appearing as constants in the circuit family. As we shall see, constant-free circuits will be sufficient for our purposes.

We now proceed to define the notion of uniformity we use for families of both boolean and arithmetic circuits. In short, we follow Vollmer [Vol99] and bound the uniformity of a circuit family through the complexity of its direct connection language. To decide the direct connection language of a circuit family $\mathcal{C} = (C_{k,n_1,\ldots,n_k})_{k,n_1,\ldots,n_k \in \mathbb{N}}$, a Turing machine must be able to efficiently answer queries of the form "Is gate a in circuit $C_{k,n_1,\ldots,n_k}$ of type t?" and "Is gate a an ancestor of gate b in circuit $C_{k,n_1,\ldots,n_k}$?" If this language can be decided in polynomial time, we say that the circuit family $\mathcal{C}$ is polylogtime-uniform, as the length of the input to the direct connection language will be logarithmic in the size of the circuit $C_{k,n_1,\ldots,n_k}$.

To keep this work self-contained, we provide a complete definition of the direct connection language and of polylogtime-uniformity. We start with the notion of an admissible encoding, which enforces mild constraints on the manner in which gates of a circuit are indexed.

Definition 2.7 (Admissible encoding)**.** Let $\mathcal{C} = (C_{k,n_1,\ldots,n_k})_{k,n_1,\ldots,n_k \in \mathbb{N}}$ be a family of either threshold or arithmetic circuits of size $s \coloneqq s(k, n_1, \ldots, n_k)$. An *admissible encoding of* $\mathcal{C}$ is a numbering of the gates of each circuit $C = C_{k,n_1,\ldots,n_k}$ in the family with the following properties.

1. If C has m input gates, then they are numbered $0, \ldots, m-1$.
2. If C has m' output gates, then they are numbered $m, \ldots, m+m'-1$.
3. There is a constant c, depending only on the circuit family, such that the binary representation of the number of any gate in C has length at most $c \cdot \log(s)$.

Further, if $\mathcal{C}$ is a family of arithmetic circuits, then for each gate $a \in C$ we fix a numbering of the set of immediate predecessors of a in C. We require that this numbering of predecessors is contiguous, that is, it starts at 1 and ends at the arity of a. For division gates, we require that the numerator occurs before the denominator in the numbering of the predecessors. ◊

We now define the direct connection language of a circuit family.

Definition 2.8 (Direct connection language)**.** Let $\mathcal{C} = (C_{k,n_1,\ldots,n_k})_{k,n_1,\ldots,n_k \in \mathbb{N}}$ be a family of either threshold or arithmetic circuits with an admissible encoding. Suppose a numbering of the gate types is fixed. The *direct connection language of* $\mathcal{C}$, denoted by $L_{DC}(\mathcal{C})$, is the language consisting of binary encodings of tuples $(k, n_1, \ldots, n_k, a, p, b)$, where

1. a is the number of a gate in $C_{k,n_1,\ldots,n_k}$.
2. If $p \neq \epsilon$, then
   (a) If $\mathcal{C}$ is a family of arithmetic circuits, b is the number of the p^{th} predecessor gate in $C_{k,n_1,\ldots,n_k}$ of a.
   (b) If $\mathcal{C}$ is a family of threshold circuits, b is the number of some predecessor gate in $C_{k,n_1,\ldots,n_k}$ of a.
3. If $p = \epsilon$, then b encodes the gate type of a (using the fixed numbering of gate types). ◊

The complexity of the direct connection language provides a way to measure the uniformity of a circuit family.

Definition 2.9 (Polylogtime-uniformity)**.** Let $\mathcal{C} = (C_{k,n_1,\ldots,n_k})_{k,n_1,\ldots,n_k \in \mathbb{N}}$ be a family of either threshold or arithmetic circuits of size $s \coloneqq s(k, n_1, \ldots, n_k)$ with an admissible encoding. We say that the circuit family $\mathcal{C}$ is *polylogtime-uniform* if

1. its direct connection language $L_{DC}(\mathcal{C})$ can be decided in time polynomial in $\log(s) + \log(k) + \sum_{i=1}^{k} \log(n_i)$,
2. the number of inputs and outputs of $C_{k,n_1,\ldots,n_k}$, and an upper bound on the size s can be computed in time polynomial in $\log(s) + \log(k) + \sum_{i=1}^{k} \log(n_i)$, given $(k, n_1, \ldots, n_k)$ as input.
3. when $\mathcal{C}$ is a family of arithmetic circuits, the arity of a gate can be computed in time polynomial in $\log(s) + \log(k) + \sum_{i=1}^{k} \log(n_i)$, given $(k, n_1, \ldots, n_k)$ and the gate name as input. ◊

Remark 2.10. We make a few remarks on the above definitions. For justifications of the following remarks and a more detailed discussion on the above notion of uniformity, we refer the reader to [AGS26, Section 2.2].

- In the above definition, the first index is a count of the remaining indices. In the circuits we design, we extend this slightly and allow the number of indices to be some function of the first index.

- The freedom in numbering the gates afforded by the above definition allows us to number our gates using more than just the integers 1 through s: by using appropriate pairing functions, we can for example number our gates using pairs of integers. To avoid confusion, when we number our gates using more than just natural numbers, we will refer to the name of a gate instead of its number, with the understanding that the actual number is obtained from the name via a pairing function.

- When working with a polylogtime-uniform family of circuits, given an index $(k, n_1, \ldots, n_k)$ and a candidate gate name a, we can test if a is a valid gate name and compute the type of gate a in time polynomial in $\log(s) + \log(k) + \sum_{i=1}^{n} \log(n_i)$. We can also determine if a is an input or output gate. ◊

Remark 2.11. Showing that a given family of circuits is polylogtime-uniform requires checking many details and is rarely insightful. For an example of a proof of uniformity including every detail, we refer the reader to the proofs of [AGS26, Lemma 3.1] and [AGS26, Lemma 3.2]. As discussed in the text following those two proofs, all of our circuits will be constructed using previously-constructed uniform circuit families combined with other simple machinery. The direct connection language of a circuit family constructed this way can be decided by encoding the rules for the simple machinery, and simulating the machines that decide the direct connection languages of the subcircuits. In [AGS26], over the course of the article, the proofs of uniformity became increasingly terse, only highlighting minor differences from earlier proofs. We continue this trend for the sake of readability. ◊

2.4 Uniform circuits for basic arithmetic operations

In this section, we collect a few results that show that basic operations can be performed by uniform families of boolean and arithmetic circuits. These results will used as building blocks throughout our work. Whenever we work with boolean circuits or Turing machines, integers will be represented in base two with a sign bit. Therefore, representing an integer of height h requires $h+1$ bits (accounting for the sign bit). We represent rational numbers as pairs of integers (p, q) with $q \neq 0$, where p and q are not necessarily relatively prime.

We start with some basic results.

Theorem 2.12. *The following functions are in polylogtime-uniform* TC^0.

1. *Iterated Integer Addition: Given n integers $a_1, \ldots, a_n$ as input, each consisting of at most n bits, compute the sum $a_1 + \cdots + a_n$.*

2. *Iterated Integer Multiplication: Given n integers $a_1, \ldots, a_n$ as input, each consisting of at most n bits, compute the product $a_1 \cdots a_n$.*

3. *Integer Division: Given integers a and b as input, with $b \neq 0$, compute $\lfloor a/b \rfloor$, and compute an integer r such that $a = \lfloor a/b \rfloor b + r$.*

4. *Polynomial Division with Remainder: given integers $a_0, \ldots, a_n$ and $b_0, \ldots, b_m$ as input, where $b_m \neq 0$ and $n \geq m$, compute $d \coloneqq b_m^{n-m+1}$ and integers $q_0, \ldots, q_{n-m}, r_0, \ldots, r_{m-1}$ such that for*

$$f(x) \coloneqq a_n x^n + \cdots + a_1 x + a_0 \qquad q(x) \coloneqq q_{n-m} x^{n-m} + \cdots + q_1 x + q_0$$
$$g(x) \coloneqq b_m x^m + \cdots + b_1 x + b_0 \qquad r(x) \coloneqq r_{m-1} x^{m-1} + \cdots + r_1 x + r_0,$$

we have $d \cdot f(x) = q(x)g(x) + r(x)$.

5. *Iterated Polynomial Multiplication: given integers $a_{1,0}, \ldots, a_{m,n}$ as input, compute integers $b_0, \ldots, b_{mn}$ such that*

$$b_{mn}x^{mn} + b_{mn-1}x^{mn-1} + \cdots + b_1 x + b_0 = \prod_{i=1}^{m}(a_{i,n}x^n + a_{i,n-1}x^{n-1} + \cdots + a_{i,1}x + a_{i,0}).$$

6. *Polynomial Greatest Common Divisor: given $2 \cdot (n+1)$ integers as input, representing two univariate polynomials f, g of degree at most n, compute integers $c_0, \ldots, c_n$ and integer d such that for $c(x) = c_n x^n + \cdots + c_0$, the polynomial $c(x)/d$ is the unique monic multiple of the greatest common divisor of f and g in $\mathbb{Q}[x]$.*

7. *Squarefree Part: given $(n+1)$ integers as input, representing an univariate polynomial f of degree at most n, compute integers $c_0, \ldots, c_n$ and integer d such that for $c(x) = c_n x^n + \cdots + c_0$, the polynomial $c(x)/d$ is the unique monic multiple of the squarefree part of f in $\mathbb{Q}[x]$.*

8. *Univariate Polynomial Interpolation: given distinct integers $a_1, \ldots, a_n$ and not necessarily distinct integers $b_1, \ldots, b_n$ as input, compute $d \coloneqq \prod_{1 \le i < j \le n}(a_i - a_j)$ and integers $c_0, \ldots, c_n$ such that $f(x) \coloneqq c_n x^n + \cdots + c_1 x + c_0$ is the unique polynomial in $\mathbb{Z}[x]$ of degree at most n that satisfies $f(a_i) = db_i$ for $1 \le i \le n$.*

9. *Iterated Multivariate Polynomial Multiplication: given $m \cdot \binom{d+n}{d}$ integers as input, representing the coefficients of m polynomials of degree at most d in n variables, compute $\binom{dm+n}{dm}$ integers representing the coefficients of their product.*

10. *Multivariate Polynomial Division with Remainder: given $2 \cdot \binom{d+n}{d}$ integers as input, representing the coefficients of two polynomials f, g degree at most d in n variables, compute integer e and polynomials q, r with integer coefficients in n variables satisfying the following:*

    - $ef = qg + r$.
    - *e is a power of the leading coefficient of g in lexicographic order.*
    - *The leading monomial of r in lexicographic order is smaller than that of g.*

11. *Multivariate Polynomial Interpolation: given $(d+1)^m$ integers $b_1, \ldots, b_{(d+1)^m}$ as input, compute $\binom{d+m}{m}$ integers representing the coefficients of an m-variate polynomial f of degree at most d, and compute $D \coloneqq \prod_{1 \le i < j \le (d+1)^m}(i-j)$ such that*

$$f(k, k^{(d+1)}, \ldots, k^{(d+1)^{m-1}}) = Db_k$$

for every $1 \le k \le (d+1)^m$.

Proof. Item 1 is classical, see [RT92]. Items 2 and 3 are the main result of [HAM02]. Items 4, 5, and 8 are from [HAM02, Corollary 6.5]. Item 6 is a special case of [AGS26, Lemma 6.13]. Item 7 follows from Items 6 and 4, and the fact that the squarefree part of a polynomial $f \in \mathbb{Q}[x]$ is simply $f/\gcd(f, f')$. Item 9 follows from item 5 using Kronecker substitution (see [AGS26, Section 2.3] for details). Item 10 follows from item 4 using Kronecker substitution. Item 11 follows from item 8 using Kronecker substitution. For all items above, the number of input and output bits are easily computable from the index of a circuit in the corresponding family. □

As discussed in [Ebe89] and also [AGS26, Section 2.3], we can use the above circuit families to obtain logtime-uniform families of circuits performing iterated addition and multiplication of rational numbers.

Next, we describe a family of polylogtime-uniform boolean circuits that computes the GCD of two multivariate polynomials. In [AGS26, Theorem 6.13], a family of polylogtime-uniform TC^0 circuits is constructed that computes the greatest common divisor of two polynomials in $\mathbb{Z}[y_1, \ldots, y_k][x]$. This circuit returns the unique monic multiple of the GCD in $\mathbb{Q}(y_1, \ldots, y_k)[x]$. For example, if queried on the inputs y_1y_2x and y_1x, the algorithm returns x as the GCD. To compute the GCD of multivariate polynomials, we will invoke the above algorithm after a random linear transformation of the input variables.

Lemma 2.13. *There exists a polylogtime-uniform family of TC^0 circuits with the following properties.*

- *The circuits take as input $2\binom{d+m}{d}$ integers representing the coefficients of two m-variate polynomials of degree d with integer coefficients f, g. The circuits also take as input $m-1$ integers, denoted $a_2, \ldots, a_m$.*
- *The circuits computes $\binom{d+m}{d}$ integers representing an m-variate polynomial h of degree at most d.*
- *If the integers $a_2, \ldots, a_m$ are independently and uniformly sampled from a set of size b, and if the highest degree parts of f and g depend on the variable x_1, then with probability $1 - 2md^m/b$, the polynomial h is a scalar multiple of the GCD of f and g in $\mathbb{Q}[x_1, \ldots, x_m]$.*

Proof. We use the integers $a_2, \ldots, a_m$ to perform a change of basis for the polynomials f and g. Let

$$\hat{f} \coloneqq f(x_1, x_2 - a_2x_1, \ldots, x_m - a_mx_1)$$
$$\hat{g} \coloneqq g(x_1, x_2 - a_2x_1, \ldots, x_m - a_mx_1).$$

Let $\widetilde{f}$ and $\widetilde{g}$ be the univariate polynomials obtained by applying the Kronecker substitution to $\hat{f}$ and $\hat{g}$, respectively. Given the coefficients of f and g and the integers $a_2, \ldots, a_m$, combined with the arithmetic described in Theorem 2.12, we can compute the evaluations of $\widetilde{f}$ and $\widetilde{g}$ at the integers $1, \ldots, (d+1)^m$. We can then compose with a circuit for multivariate interpolation (item 11 of Theorem 2.12) to obtain the coefficients of $\mathbb{Z}$-multiples of $\hat{f}$ and $\hat{g}$. Next, we compose with the circuit for univariate polynomial GCD in function fields ([AGS26, Lemma 6.13]), treating the polynomials $\hat{f}$ and $\hat{g}$ as univariate polynomials in x_1 with coefficients in $\mathbb{Q}(x_2, \ldots, x_m)$. This returns two polynomials $h_n \in \mathbb{Z}[x_1, \ldots, x_m]$ and $h_d \in \mathbb{Z}[x_2, \ldots, x_m]$ such that h_n/h_d is the GCD of $\hat{f}$ and $\hat{g}$ in $\mathbb{Q}(x_2, \ldots, x_m)[x_1]$. We then compose with the circuits for multivariate polynomial division with remainder to divide every coefficient of x_1 in h_n by h_d, and discard the remainders. We use integer arithmetic to bring the resulting polynomial to common denominator, and discard the denominator. Let the resulting polynomial be denoted by $\hat{h}$. We then compute the coefficients of $h \coloneqq \hat{h}(x_1, x_2 + a_2x_1, \ldots, x_m + a_mx_1)$ using evaluation-interpolation as above. The final output if the circuit are the coefficients of h.

The fact that the above computation can be carried out by a polylogtime-uniform family of TC^0 circuits follows by a simulation argument (see Remark 2.11). We now show that with high probability, the polynomial h is a $\mathbb{Q}$-multiple of the GCD of f and g. To this end, observe that with probability at least $1 - 2md^m/b$, the leading coefficients of $\hat{f}$ and $\hat{g}$ in the variable x_1 are integers. If this holds, then by Gauss's lemma, the GCD of $\hat{f}$ and $\hat{g}$ in $\mathbb{Q}(x_2, \ldots, x_m)[x_1]$ and the GCD in $\mathbb{Z}[x_1, \ldots, x_m]$ are $\mathbb{Q}$-multiples of each other. Specifically, every coefficient of h_n in x_1 is divisible by h_d in $\mathbb{Q}[x_2, \ldots, x_m]$. Therefore, the division step does not produce any remainders and $\hat{h}$ is a $\mathbb{Q}$-multiple of the GCD of $\hat{f}$ and $\hat{g}$. Finally, the last step undoes an invertible linear transformation, so the polynomial h is a $\mathbb{Q}$-multiple of the GCD of f and g as claimed. □

As a corollary, we also obtain a circuit family that computes squarefree parts of multivariate polynomials.

Corollary 2.14. *There exists a polylogtime-uniform family of* TC^0 *circuits with the following properties.*

- *The circuits take as input* $\binom{d+m}{d}$ *integers representing the coefficients of an* m*-variate polynomial of degree* d *with integer coefficients, denoted* f*. The circuits also take as input* $m-1$ *integers, denoted* $a_2, \ldots, a_m$*.*
- *The circuits computes* $\binom{d+n}{d}$ *integers, representing an* m*-variate polynomial* h *of degree at most* d*.*
- *If the integers* $a_2, \ldots, a_m$ *are independent and uniformly sampled from a set of size* b*, and if the highest degree part of* f *depends on the variable* x_1*, then with probability* $1 - 2md^m/b$*, the polynomial* h *is a scalar multiple of the squarefree part of* f *in* $\mathbb{Q}[x_1, \ldots, x_m]$*.*

Theorem 2.15 ([AGS26, Corollary 5.13])**.** *There exists a polylogtime-uniform family of weakly division-free, constant-free circuits* $\mathcal{C}$ *indexed by parameters* $n, d_0, \ldots, d_n, k, D$ *with the following properties.*

- *The circuit* $C_{n,d_0,\ldots,d_n,k,D}$ *has size bounded by* $(PD)^{\mathrm{poly}(n,k)}$*, where* $P = \sum_{i=0}^{n} \prod_{j \neq i} d_j$*, and depth bounded by a universal constant.*
- *The circuit has* $\binom{k+D}{k} \cdot \sum_{i=0}^{n} \binom{n+d_i-1}{d_i}$ *input variables, which we denote by* $u_{i,\boldsymbol{\alpha},\boldsymbol{\beta}}$*, where* $\boldsymbol{\beta} \in \mathbb{N}^k$ *satisfies* $|\boldsymbol{\beta}| \leq D$*, and* $\boldsymbol{\alpha}, i$ *satisfy* $|\boldsymbol{\alpha}| \leq d_i$*. The circuit has* $\binom{DD'+k}{k}$ *outputs, where* D' *is the degree of* $\mathrm{Res}_n(\mathbf{F}_n)$*.*
- *When evaluated at* $\gamma_{i,\boldsymbol{\alpha},\boldsymbol{\beta}}$*, the output gates compute the coefficients of the monomials in* $\mathbf{w}$ *of the resultant of the polynomials*

$$H_i = \sum_{\boldsymbol{\alpha}} \sum_{\boldsymbol{\beta}} \gamma_{i,\boldsymbol{\alpha},\boldsymbol{\beta}} \mathbf{x}^{\boldsymbol{\alpha}} \mathbf{w}^{\boldsymbol{\beta}}$$

with respect to the variables $\mathbf{x}$*, where the ranges of* $\boldsymbol{\alpha}, \boldsymbol{\beta}$ *are the same as above.*

2.5 Uniformity of lifting factorizations

Suppose $\mathbb{F}$ is a field of characteristic 0 and $P \in \mathbb{F}[t, y]$ is a bivariate polynomial. There are a number of different algorithms to compute the irreducible factors of P. We refer the reader to [Gao03, Section 1] for a historical account of these algorithms.

A common approach to bivariate factorization is to lift to the ring $\mathbb{F}[\![t]\!][y]$. Under mild assumptions, Hensel's lemma gives us an algorithm to approximate the roots of the polynomial P in this ring. If P and $P(0, y)$ are both squarefree, then each root of $P(0, y)$ lifts to a unique root of P in $\mathbb{F}[\![t]\!][y]$. Following this, linear algebraic methods can be used to compute which roots of P in $\mathbb{F}[\![t]\!][y]$ combine together to produce factors of P in $\mathbb{F}[t, y]$.

A key observation is that the coefficients of a root $\phi \in \mathbb{F}[\![t]\!]$ of P as an element of $\mathbb{F}[\![t]\!][y]$ are rational functions of the coefficients of P and the root of $P(0, y)$ that lifts to ϕ. As a consequence, we can define the generic bivariate polynomial and construct a universal power series root such that for any bivariate polynomial P with coefficients in $\mathbb{F}$, as long as P satisfies some mild assumptions, the roots of P in $\mathbb{F}[\![t]\!][y]$ can be obtained by specializing the universal power series root. This same observation is used in [Kal95] to derive irreducibility forms.

Let F_d denote the generic bivariate polynomial of degree d with indeterminate coefficients, that is

$$F_d = \sum_{i+j \leq d} c_{i,j} t^i y^j \in \mathbb{Z}[C_d, t, y],$$

where C_d is the set of indeterminates $\{c_{i,j}\}_{i+j\le d}$. Let F'_d denote the partial derivative $\partial_y F_d$. Define

$$\widetilde{F_d}(t,y) := F'_d(0,z)^{-1} \cdot F_d(t, y+z).$$

Define the *universal power series root* $\Phi^{(d)} \in \mathbb{Z}[C_d, z]_{F'_d(0,z)}[\![t]\!]$ by

$$\begin{aligned}
\Phi_N^{(d)} &:= \sum_{i\le 2N} (-1)^i \operatorname{coeff}\left(y\left(\widetilde{F_d}(t,y) - y\right)^i \partial_y \widetilde{F_d}(t,y), t^N y^i \right) \\
&= \sum_{i\le 2N} \frac{(-1)^i}{F'_d(0,z)^{i+1}} \operatorname{coeff}\left(y\big(F_d(t,y+z) - yF'_d(0,z)\big)^i F'_d(t,y+z), t^N y^i \right) \\
&= \frac{1}{F'_d(0,z)^{2N+1}} \sum_{i\le 2N} (-1)^i F'_d(0,z)^{2N-i} \cdot \operatorname{coeff}\left(y\big(F_d(t,y+z) - yF'_d(0,z)\big)^i F'_d(t,y+z), t^N y^i \right)
\end{aligned}$$

and $\Phi^{(d)} := z + \sum_{N\ge 1} \Phi_N^{(d)} t^N$. The universal power series root satisfies the following property. Let $\mathbb{F}$ be any field of characteristic 0, and let $\boldsymbol{\gamma} \in \mathbb{F}^{|C_d|}$. Let P denote the specialization $F_d^{\boldsymbol{\gamma}}$. Suppose $\boldsymbol{\gamma}$ is such that $P(t,y)$ is a degree d squarefree polynomial whose leading coefficient with respect to y lies in $\mathbb{F}$. Suppose $\boldsymbol{\gamma}$ is also such that $P(0,y)$ is a squarefree polynomial. In this setting, the specialization of $F'_d(0,z)$ at $\boldsymbol{\gamma}$ does not vanish, therefore the specialization of $\Phi^{(d)}$ at $\boldsymbol{\gamma}$ is well defined. Let P' denote the specialization of F'_d at $\boldsymbol{\gamma}$, equivalently the derivative of P with respect to y.

Since $P(0,y)$ is squarefree, $P'(0,z)$ is invertible in $\mathbb{K} := \mathbb{F}[z]/P(0,z)$. Therefore, the specialization of $\Phi^{(d)}$ at $\boldsymbol{\gamma}$ is naturally an element of $\mathbb{K}[\![t]\!]$. Call this element ϕ_z. Then $P(t,\phi_z) = 0$ in $\mathbb{K}[\![t]\!]$.

Essentially equivalently, suppose $\alpha \in \overline{\mathbb{F}}$ is a root of $P(0,y)$. Then $P'(0,\alpha) \neq 0$ by assumption. Therefore, the specialization of $\Phi^{(d)}$ at $\boldsymbol{\gamma}$ and α is naturally an element of $\overline{\mathbb{F}}[\![t]\!]$. Call this element ϕ_α. Then $P(t,\phi_\alpha) = 0$ in $\overline{\mathbb{F}}[\![t]\!]$.

The proof of the above is a straightforward application of an explicit version of the implicit function theorem [AY83, Proposition 20.3]. The special case above can also be deduced from the Lagrange inversion formula. That this formula can be used to factor polynomials was first observed by Bhattacharjee, Kumar, Rai, Ramanathan, Saptharishi, and Saraf [BKR+26], and our presentation closely follows theirs. From the description above, combined with the uniform families of algebraic circuits for polynomial interpolation (Theorem 2.12), the following lemma is immediate (see Remark 2.11). For later applications, it will be convenient to compute the denominator and numerator in the final expression for $\Phi_N^{(d)}$ above separately.

Lemma 2.16. *There exists a polylogtime-uniform family of constant-free circuits $\mathcal{C}$ indexed by N, d such that*

- *The circuit $C_{N,d}$ has size polynomial in N and d, and depth bounded by a universal constant.*
- *The circuit $C_{N,d}$ has $\binom{d+2}{2} + 1$ input gates, labeled by variables $c_{i,j}$ for $i + j \le d$ and z. The circuit has two output gates and is weakly division free.*
- *The circuit computes the coefficient $\Phi_N^{(d)}$ of the universal power series root. Specifically, the first output gate computes the sum in the final expression above, and the second output gate computes $F'_d(0,z)^{2N+1}$.*

Fix an integer $e \le d$, and let $b_0, \ldots, b_e$ be new indeterminates. Let H_e denote the generic univariate polynomial of degree d in the variable z, that is, $H_e = b_0 + b_1 z + \cdots + b_e z^e$. Let the definitions of F_d and $\Phi_N^{(d)}$ be as above.

Define the truncated universal power series root $\Psi^{(d)}$ as

$$\Psi^{(d)} := z + \sum_{1 \le N \le d} \Phi_N^{(d)} t^N.$$

From the definition of $\Phi_N^{(d)}$ we deduce that $F_d'(0,z)^{2d+1}\Psi^{(d)} \in \mathbb{Z}[C_d, t, z]$. Further, the degree in z of this polynomial is $2d^2 - d$. Let R_1 denote the resultant of $H(z)$ and $F_d'(0,z)^{2d+1}y - F_d'(0,z)^{2d+1}\Psi^{(d)}$ as univariate polynomials in z. Let R_2 denote the resultant of $H(z)$ and $F_d'(0,z)^{2d+1}$ as univariate polynomials in z.

The polynomials above have the following properties. Let $\boldsymbol{\gamma}$ be a specialization of the variables in C_d with the properties described above. Let $\boldsymbol{\delta}$ be a specialization of the variables $b_0, \ldots, b_e$ such that $Q(z) := H^{\boldsymbol{\delta}}(z)$ has degree e and $Q(z)$ divides $P(0,z)$.

In this setting, the quotient $R_1^{\boldsymbol{\gamma},\boldsymbol{\delta}}/b_e R_2^{\boldsymbol{\gamma},\boldsymbol{\delta}}$ is a polynomial in t and y that is monic in y. The assumptions above ensure that P factors into linear polynomials in $\overline{\mathbb{F}}[\![t]\!]$, and that the quotient $R_1^{\boldsymbol{\gamma},\boldsymbol{\delta}}/b_e R_2^{\boldsymbol{\gamma},\boldsymbol{\delta}}$ is the product of those linear factors whose constant terms are roots of $H^{\boldsymbol{\delta}}$. Specifically, if we are guaranteed that $H^{\boldsymbol{\delta}}$ lifts to a factor of P in $\mathbb{F}[t,y]$, then the truncation of this quotient up to degree d is the lift of $H^{\boldsymbol{\delta}}$. By combining uniform families of algebraic circuits for the resultant (Theorem 2.15) with the circuits for the universal power series roots (Lemma 2.16), we obtain a uniform family of algebraic circuits that computes the polynomials R_1 and R_2 described above.

Lemma 2.17. *There exists a polylogtime-uniform family of constant-free circuits $\mathcal{D}$ indexed by d and e such that*

- *The circuit $D_{d,e}$ has size polynomial in d and e and depth bounded by a universal constant.*
- *The circuit $C_{N,d}$ has $\binom{d+2}{2} + e + 3$ input gates labeled by variables $c_{i,j}$ for $i + j \le d$ and $b_0, \ldots, b_e, t, y$. The circuit has two output gates and is weakly division free.*
- *The circuit computes the truncation of R_1 up to degree d in t, and also computes the polynomial R_2 described above.*

Combining the above lemma with [AGS26, Lemma 6.1], we obtain a polylogtime uniform family of constant-depth threshold circuits that takes as input $\binom{d+2}{2} + e + 1$ integers, and computes the coefficients of R_1 and R_2 in the variables y and t. Using standard reductions from multivariate polynomial factorization to bivariate polynomial factorization, we can also use the above circuits to compute lifts of factors of multivariate polynomials. We reemphasize that the reduction from multivariate polynomial factorization to univariate factorization in the following lemma is folklore, the main content of the following lemma is the uniformity statement.

Lemma 2.18. *There exists a polylogtime-uniform family of TC^0 circuits with the following properties.*

- *The circuit takes as input $\binom{d+m+1}{d} \cdot \binom{e+k}{e}$ integers, representing the coefficients of a polynomial $P \in \mathbb{Z}[w_1, \ldots, w_k][y, x_1, \ldots, x_m]$ of degree at most e in the variables $w_1, \ldots, w_k$ and degree at most d in the variables $y, x_1, \ldots, x_m$. The circuit also takes as input $(d+1) \cdot \binom{e+k}{k}$ integers, representing the coefficients of a polynomial $Q \in \mathbb{Z}[w_1, \ldots, w_k][y]$ of degree at most e in $w_1, \ldots, w_k$ and degree at most d in y.*
- *The circuits computes $\binom{d+m+1}{d} \cdot \binom{e+k}{e}$ integers representing an m-variate polynomial R of degree at most d in $y, x_1, \ldots, x_m$ and at most e in $w_1, \ldots, w_k$.*
- *Suppose the leading term of P in y lies in $\mathbb{Z}$. Suppose that both P and $P(y, 0, \ldots, 0)$ are squarefree, and suppose Q divides $P(y, 0, \ldots, 0)$. Under these assumptions, using Gauss' lemma we can deduce that after scaling, all the factors of P in the ring $\mathbb{Q}(w_1, \ldots, w_k)[y, x_1, \ldots, x_m]$ lie in $\mathbb{Q}[w_1, \ldots, w_k][y, x_1, \ldots, x_m]$. Suppose R' is such a factor of P such that $R'(y, 0, \ldots, 0)$ is a $\mathbb{Q}$-multiple of Q. Then the computed polynomial R is a $\mathbb{Q}$-multiple of R'.*

Proof. Let $\mathbb{K} \coloneqq \mathbb{Q}(w_1, \ldots, w_k, x_1, \ldots, x_m)$. Let $\hat{P}$ denote the polynomial $P(y, tx_1, \ldots, tx_n) \in \mathbb{K}[t, y]$. There exists a polylogtime-uniform family of constant-depth arithmetic circuits with $\binom{d+m+1}{d} \cdot \binom{e+k}{k}$ inputs that takes as input the coefficients of P and computes the coefficients of $\hat{P}$. There also exists a polylogtime-uniform family of arithmetic circuits that computes the coefficients of Q as a polynomial in y. We then compose these with the circuits constructed in Lemma 2.17. The resulting family of circuits is still polylogtime-uniform and constant depth, and it computes two polynomials in y, t with coefficients in $\mathbb{K}$, call them R_1 and R_2. Since $\hat{P}(0, t) \in \mathbb{Q}[y, w_1, \ldots, w_k]$, we can deduce that $R_2 \in \mathbb{Q}[w_1, \ldots, w_e]$. We use [AGS26, Lemma 6.1] to obtain a polylogtime-uniform family of threshold circuits that performs the same computation. We compose with circuits for polynomial division to divide each coefficient of R_1 in t by R_2, and discard the remainders. Finally, we add up all the coefficients in t of the resulting polynomial (equivalently, we evaluate the resulting polynomial at $t = 1$). We then discard all monomials whose degree in $w_1, \ldots, w_k$ is higher than e. This final polynomial is the output polynomial R'. □

2.6 Computation and the counting hierarchy

A key technical tool that is used in [AGS26] that will also be useful in this work is that uniform families of exponentially large constant-depth threshold circuits can be evaluated in the counting hierarchy. Since such a circuit can have exponentially many output gates, we must make precise what we mean by evaluating such a circuit.

Definition 2.19 ([AGS26, Definition 6.2])**.** Let $\mathcal{F} \coloneqq \left(f_{\mathbf{n}} : \{0,1\}^{m'_{\mathbf{n}}} \to \{0,1\}^{m_{\mathbf{n}}}\right)_{\mathbf{n}}$ be a multi-indexed family of boolean functions. The *language $L_{\mathcal{F}}$ corresponding to $\mathcal{F}$* is defined as

$$L_{\mathcal{F}} \coloneqq \{(i, b, x, \mathbf{n}) \mid f_{\mathbf{n}}(x)_i = b\}.$$

If $\mathcal{D}$ is a family of circuits, then we extend notation and use $L_{\mathcal{D}}$ to denote the language corresponding to the family of functions computed by $\mathcal{D}$. ◊

The following simulation result was proved in [AGS26], and is inspired by a similar result in [ABKM09].

Lemma 2.20 ([AGS26, Lemma 6.3])**.** *Let $\mathcal{D} = (D_{\mathbf{n}})_{\mathbf{n}}$ be a polylogtime-uniform family of threshold circuits of size $s_{\mathbf{n}}$ and depth Δ, where $D_{\mathbf{n}}$ has $m_{\mathbf{n}}$ inputs. Let $L_{\mathcal{D}}$ be the language corresponding to the circuit family $\mathcal{D}$ as defined in Definition 2.19. Suppose $s_{\mathbf{n}} \leq \exp(\mathrm{poly}(m_{\mathbf{n}}))$. Then $L_{\mathcal{D}} \in \mathsf{CH}$.*

The next lemma generalizes the above, and shows that an exponential sized circuit with exponentially many inputs can be evaluated in CH, as long as the input bits can themselves be computed in CH.

Lemma 2.21 ([AGS26, Lemma 6.5])**.** *Let $\mathcal{D} = (D_n)_n$ be a polylogtime-uniform family of polynomial-size threshold circuits of depth Δ, where D_n has n inputs. Let $\mathcal{F} = \left(f_{\mathbf{n}} : \{0,1\}^{\ell_{\mathbf{n}}} \to \{0,1\}^{m_{\mathbf{n}}}\right)_{\mathbf{n}}$ be a family of boolean functions. Suppose $m_{\mathbf{n}} \leq \exp(\mathrm{poly}(\ell_{\mathbf{n}}))$ and that a binary representation of $m_{\mathbf{n}}$ can be computed in polynomial time given a unary representation of $\ell_{\mathbf{n}}$ and a binary representation of $\mathbf{n}$. Let $\mathcal{D} \circ \mathcal{F} = (D_{m_{\mathbf{n}}} \circ f_{\mathbf{n}})_{\mathbf{n}}$ denote the family of composed functions. Then $L_{\mathcal{D}\circ\mathcal{F}} \in \mathsf{CH}^{L_{\mathcal{F}}}$. In particular, if $L_{\mathcal{F}} \in \mathsf{CH}$, then $L_{\mathcal{D}\circ\mathcal{F}} \in \mathsf{CH}$.*

For our work, we need a slightly more general version of Lemma 2.21. Lemma 2.21 assumes that the circuit family $\mathcal{D}$ has a single index, that D_n takes exactly n inputs, and that the circuit D_n has size $n^{O(1)}$. We need to relax the requirements of Lemma 2.21 to allow the family $\mathcal{D}$ to be

multi-indexed and for the index to the outer family $\mathcal{D}$ to depend on both the index $\mathbf{n}$ to the inner family $\mathcal{F}$ as well as the input x on which the inner family is evaluated. We omit the proof of this lemma, as it is a straightforward adaptation of the proof of Lemma 2.21. The only change to the proof is that the machine for $L_{\mathcal{D}\circ\mathcal{F}}$ must decide which member of the circuit family $\mathcal{D}$ to invoke. This is easily handled by the assumption that the correct index into $\mathcal{D}$ can be computed in CH.

Lemma 2.22. *Let $\mathcal{F} = \left(f_{\mathbf{n}} : \{0,1\}^{\ell_{\mathbf{n}}} \to \{0,1\}^{m_{\mathbf{n}}}\right)_{\mathbf{n}}$ be a family of boolean functions and let $\mathcal{D} = (D_{\mathbf{n}})_{\mathbf{n}}$ be a polylogtime-uniform family of constant-depth threshold circuits. For every index $\mathbf{n}$ and input $x \in \{0,1\}^{\ell_{\mathbf{n}}}$, let $\mathbf{p}$ be an index such that $D_{\mathbf{p}}$ has $m_{\mathbf{n}}$ inputs. Let $\mathcal{D}\circ\mathcal{F} = (D_{\mathbf{p}} \circ f_{\mathbf{n}})_{\mathbf{n}}$ denote the family of composed functions. Suppose that*

1. *the size of $D_{\mathbf{p}}$ is at most $\exp(\mathrm{poly}(\ell_{\mathbf{n}}))$, and*
2. *given a unary representation of $\ell_{\mathbf{n}}$, a binary representation of $\mathbf{n}$, and an input $x \in \{0,1\}^{\ell_{\mathbf{n}}}$, the binary representation of $\mathbf{p}$ can be decided in CH.*

Then $L_{\mathcal{D}\circ\mathcal{F}} \in \mathsf{CH}^{L_{\mathcal{F}}}$. In particular, if $L_{\mathcal{F}} \in \mathsf{CH}$, then $L_{\mathcal{D}\circ\mathcal{F}} \in \mathsf{CH}$.

We list some functions whose corresponding languages can be computed in CH. We say that a circuit has bounded syntactic degree if the syntactic degree of every output is at most the size of the circuit.

Lemma 2.23. *Let $\mathcal{E}$ be the family of boolean functions that take as input the description of a constant-free, weakly division-free algebraic circuit and compute the coefficient vectors of the polynomials computed by the circuit. Then the language $L_{\mathcal{E}}$ corresponding to $\mathcal{E}$ can be decided in CH.*

Proof. Let C be the given algebraic circuit. We will compute the coefficient vectors of the polynomials computed by C using evaluation-interpolation. To do this, we will show that (1) we can decide the bits of the binary representation of an evaluation of C in CH, and (2) given oracle access to the binary representations of evaluations of C, we can decide the bits of the coefficient vectors in CH.

We first reduce to the univariate case using the Kronecker substitution. Let $d \coloneqq 2^{s+1}$ so that every polynomial computed by C has degree strictly less than d. Define the algebraic circuit $\hat{C}$ via

$$\hat{C}(x) \coloneqq C(x, x^d, x^{d^2}, \ldots, x^{d^{n-1}}).$$

By our choice of d, the binary representation of the coefficients of C may be read off directly from that of the coefficients of $\hat{C}$, so in what remains it suffices to compute the coefficients of $\hat{C}$ in CH. The circuit for $\hat{C}$ can be built from the circuit for C using $O(n \log d) \leq O(s^2)$ additional gates and the polynomials computed by $\hat{C}$ have degree bounded by $d^n \leq 2^{s^2+s}$.

Suppose we want to evaluate $\hat{C}$ on an integer input a of height at most h. We replace the input gate of $\hat{C}$ with a subcircuit that computes the value of a starting from the constants 0 and 1. By writing a in binary, we can implement this subcircuit using $O(h)$ gates. This yields an arithmetic circuit of size $O(s^2 + h)$ that has no inputs and computes $\hat{C}(a)$. Given indices $n, i, j \in \mathbb{N}$, the task of computing the i^{th} bit of the n-bit binary representation of the j^{th} output of $\hat{C}(a)$ is exactly an instance of the problem BitSLP, which lies in CH by [ABKM09, Theorem 4.1]. When our goal is to evaluate $\hat{C}$ on an integer input of height $h \leq s^{O(1)}$, the circuit constructed for $\hat{C}(a)$ is of size $s^{O(1)}$, so we may decide the value of bits of the binary representation of $C(\mathbf{a})$ in CH.

To recover the coefficients of $\hat{C}(x)$ from evaluations, we use the fact that polynomial interpolation can be performed by polylogtime-uniform threshold circuits of constant depth and polynomial size. By [AGS26, Lemma 3.1], there is a family of polylogtime-uniform arithmetic circuits that compute the inverse of the Vandermonde matrix $\mathrm{Vand}(1, \ldots, m)$ in constant depth and $m^{O(1)}$ size.

Multiplying $\mathrm{Vand}(1,\dots,m)^{-1}$ with the evaluations $f(1),\dots,f(m)$ of a univariate polynomial of degree less than m recovers the coefficients of m, which can again be performed by an arithmetic circuit of constant depth and size $m^{O(1)}$. By [AGS26, Lemma 6.1], this yields a polylogtime-uniform family $\mathcal{D} = (D_{m,h})_{m,h\in\mathbb{N}}$ of threshold circuits of constant depth and size $\mathrm{poly}(m,h)$, where $D_{m,h}$ receives evaluations $f(1),\dots,f(m)$, each of height at most h, and computes the coefficients of the unique polynomial $f(x)$ of degree less than m that agrees with these evaluations.

We compose the circuit family $\mathcal{D}$ with the evaluations $\hat{C}(1),\dots,\hat{C}(2^{s^2+s}+1)$. Because each evaluation of $\hat{C}$ can be computed by a constant-free algebraic circuit of size $s^{O(1)}$, the evaluation itself has height bounded by $s^{O(1)}$, so it suffices to invoke the circuit $D_{m,h}$ for $m = 2^{s^2+s}+1$ and $h = s^{O(1)}$. This threshold circuit has constant depth and size $\exp(s^{O(1)})$. Moreover, the index of this circuit can be computed in polynomial time from the value of s. Thus, we may apply Lemma 2.21 to conclude that bits of the evaluation of $D_{m,h}$ on input $\hat{C}(1),\dots,\hat{C}(2^{s^2+s}+1)$—which are precisely the coefficients of $\hat{C}$—can be decided in CH, as desired. □

3 Chow forms and geometric resolutions

In this section, $\mathbb{K}$ is an algebraically closed field. Chow forms and geometric resolutions are two fundamental ways to describe equidimensional affine, or projective, varieties: the former is a single polynomial in several groups of new variables, while the latter involves a family of multivariate polynomials in the ambient coordinates. In order to establish our main result, that Chow forms can be computed in the Counting Hierarchy, we will rely on both encodings. The goal of this section is to introduce both concepts; for convenience, for the latter, existence and basic properties are derived from the ground up.

3.1 Chow forms

All facts about the Chow form that we state here appear in [KPS01, Section 1.2.2], and proofs can be found in [Phi86, Chapter 1].

Let $\mathbb{K}[x_0,\dots,x_n]$ be the homogeneous coordinate ring of $\mathbb{P}^n$. Let $V \subset \mathbb{P}^n$ be an irreducible projective variety of dimension r. Let $\mathbf{u}_0,\dots,\mathbf{u}_r$ be $r+1$ sets of variables, with each $\mathbf{u}_i$ consisting of $n+1$ variables $u_{i,0},\dots,u_{i,n}$. We use $\mathbf{u}$ to denote the union of $\mathbf{u}_0,\dots,\mathbf{u}_r$. We also use U and U_i to denote the size of the sets $\mathbf{u}$ and $\mathbf{u}_i$, respectively. For each $0 \le i \le r$, let L_i denote the polynomial $u_{i,0}x_0 + u_{i,1}x_1 + \cdots + u_{i,n}x_n$. For $\boldsymbol{\gamma} \in \mathbb{A}^{n+1}$, we use $L_{\boldsymbol{\gamma}}$ to denote the linear form $\gamma_0 x_0 + \cdots + \gamma_n x_n$.

The *incidence variety* of the forms $L_0,\dots,L_r$ in V is defined to be the subvariety of $\mathbb{P}^n \times (\mathbb{P}^n)^{r+1}$ consisting of points $(\boldsymbol{\alpha},\boldsymbol{\gamma}_0,\dots,\boldsymbol{\gamma}_r)$ such that $\boldsymbol{\alpha} \in V$ and $L_i(\boldsymbol{\alpha},\boldsymbol{\gamma}_i) = 0$ for all $0 \le i \le r$. We use V_L to denote this incidence variety. Let $\pi_1 : \mathbb{P}^n \times (\mathbb{P}^n)^{r+1} \to \mathbb{P}^n$ denote the projection map onto the first factor, and similarly let π_2 denote the projection map onto $(\mathbb{P}^n)^{r+1}$. It is straightforward to see that $\pi_1(V_L) = V$.

Consider now $W \coloneqq \pi_2(V_L)$. The variety W is a closed proper subvariety of $(\mathbb{P}^n)^{r+1}$ of codimension 1. A defining equation for W is called the *Chow form* of V. We denote this polynomial by $\mathcal{C}_V$. Note that a defining equation for W is only fixed up to a scalar factor. In order to avoid this indeterminacy in the definition of $\mathcal{C}_V$, we will fix the following normalization for $\mathcal{C}_V$: we order the variables $u_{i,j}$ such that $u_{i,j} > u_{i',j'}$ if $i < i'$ or $i = i'$ and $j < j'$. We normalize the Chow form so that its leading coefficient in the lexicographic order extending the variable ordering is always 1.

The points of W correspond to linear subspaces of codimension at most $r+1$ that have nonempty intersection with V. If $(\boldsymbol{\gamma}_0,\dots,\boldsymbol{\gamma}_r) \in W$, then by the definitions of V_L and W, the linear subspace defined by the equations $L_{\boldsymbol{\gamma}_0} = \cdots = L_{\boldsymbol{\gamma}_r} = 0$ has a point that lies in V. The Chow form is homogeneous of degree $\deg V$ in each set of variables $\mathbf{u}_i$.

If V is a reducible variety, it is still possible to define the Chow form of V, assuming V is equidimensional. When V is an equidimensional variety of dimension r, the product of Chow forms of the irreducible components of V is the Chow form of V.

The Chow form of a zero-dimensional variety is also called its u-resultant. If V is a zero-dimensional variety with all points at finite distance, then the u-resultant of V has the following factorization: $\mathcal{C}_V = \prod_{\boldsymbol{\alpha} \in V} (u_0 + \boldsymbol{\alpha}_1 u_1 + \cdots + \boldsymbol{\alpha}_n u_n)$, where the points $\boldsymbol{\alpha} \in \mathbb{P}^n$ are written with $\boldsymbol{\alpha}_0 = 1$.

Chow forms behave nicely under linear changes of coordinates. Given the Chow form of a variety V and a linear change of coordinates $\phi : \mathbb{P}^n \to \mathbb{P}^n$, the following lemma describes how to obtain the Chow form of the variety $\phi(V)$.

Lemma 3.1. *Let $M \in \mathbb{K}^{(n+1)\times(n+1)}$ be an invertible matrix and let $\phi : \mathbb{P}^n \to \mathbb{P}^n$ be the linear map given by $\phi(\boldsymbol{\alpha}) = M\boldsymbol{\alpha}$. Let $V \subseteq \mathbb{P}^n$ be an equidimensional variety. If C_V is the Chow form of V, then the Chow form of $\phi(V)$ is obtained by performing the substitution $u_{i,j} \to u'_{i,0} M_{0,j} + u'_{i,1} M_{1,j} + \cdots + u'_{i,n} M_{n,j}$ in C_V, and making the result monic.*

Proof. Let $\mathbb{K}[x_0, \ldots, x_n]$ and $\mathbb{K}[y_0, \ldots, y_n]$ denote the homogeneous coordinate rings of the source and target copies of $\mathbb{P}^n$ in the definition of $\phi : \mathbb{P}^n \to \mathbb{P}^n$ respectively. Corresponding to ϕ, there is a map $\phi^* : \mathbb{K}[y_0, \ldots, y_n] \to \mathbb{K}[x_0, \ldots, x_n]$ defined by $\phi^*(y_i) = M_{i,0}x_0 + \cdots + M_{i,n}x_n$ that satisfies $\phi^{-1}(\mathrm{V}(f(\mathbf{y}))) = \mathrm{V}(\phi^*(f)(\mathbf{x}))$.

Now suppose V has dimension r. Let $\ell_0, \ldots, \ell_r \in \mathbb{K}[y_0, \ldots, y_n]$ be linear forms and let $\beta_{i,j} \in \mathbb{K}$ be such that $\ell_i = \sum \beta_{i,j} y_j$. The variety $\phi(V)$ intersects $\mathrm{V}(\ell_0, \ldots, \ell_r)$ if and only if V intersects $\phi^{-1}(\mathrm{V}(\ell_0, \ldots, \ell_r))$. By the previous discussion, we have $\phi^{-1}(\mathrm{V}(\ell_0, \ldots, \ell_r)) = \mathrm{V}(\phi^*(\ell_0), \ldots, \phi^*(\ell_r))$. By the definition of ϕ^*, we have $\phi^*(\ell_i) = \sum_j \sum_k M_{k,j}\beta_{i,k} x_j$. By the definition of the Chow form $\mathcal{C}_V$, this intersection is nonempty if and only if the evaluation of $\mathcal{C}_V$ at $u_{i,j} = \sum_k M_{k,j}\beta_{i,k}$ is zero. If $\mathcal{C}'$ is the polynomial obtained by substituting $u_{i,j} \to u'_{i,0} M_{0,j} + u'_{i,1} M_{1,j} + \cdots + u'_{i,n} M_{n,j}$, then the above evaluation of $\mathcal{C}_V$ is zero if and only if $\mathcal{C}'$ vanishes at $u'_{i,j} = \beta_{i,j}$. Finally, since $\mathcal{C}_V$ can be obtained from $\mathcal{C}'$ by a similar substitution using the inverse of the matrix M, and since $\mathcal{C}_V$ is squarefree, we can deduce that $\mathcal{C}'$ is squarefree. Therefore, $\mathcal{C}'$, once made monic, is the Chow form for $\phi(V)$. □

3.2 Geometric resolutions

In this subsection, we work with affine varieties. A *geometric resolution* of an equidimensional affine variety is a certain parametric representation of the variety that was introduced in the computer algebra literature in work by Giusti, Heintz, Pardo and their collaborators [GHMP95; GHMMP98]. Similar objects were used in prior work by Grigoriev and his collaborators [Gri87], but the explicit requirement to be in Noether position (see below for the definition) and its consequences appear in the former references. For the convenience of the reader, we provide self contained proofs of all statements about geometric resolutions that we will need, including their existence.

Below, we work with equidimensional varieties of dimension m, for which it will be convenient to divide the variables into two sets. Let $S \coloneqq \mathbb{K}[x_1, \ldots, x_m, y_1, \ldots, y_n]$ be the coordinate ring of the affine space $\mathbb{K}^{m+n}$ and let $\pi_{\mathbf{x}} : \mathbb{K}^{m+n} \to \mathbb{K}^m$ be the projection onto the first m coordinates. We make the following assumption.

Definition 3.2. We say that an equidimensional variety V of dimension m is in *projective Noether position* if there exists a point $\boldsymbol{\alpha} \in \mathbb{K}^m$ such that the fiber $\pi_{\mathbf{x}}^{-1}(\boldsymbol{\alpha}) \cap V$ has cardinality exactly $\deg V$. We say that y_1 *is a primitive element for* V if there is a point $\boldsymbol{\alpha}$ such that the fiber $\pi_{\mathbf{x}}^{-1}(\boldsymbol{\alpha}) \cap V$ has cardinality exactly $\deg V$, and all points in this fiber have distinct y_1 coordinates. ◊

Note that if y_1 is a primitive element for V, then V is in particular in projective Noether position.

Definition 3.3. Let $V \subset \mathbb{A}^{m+n}$ be an equidimensional variety of dimension m such that y_1 is a primitive element for V (Definition 3.2). A *geometric resolution* for V is a set of polynomials $q, r_2, \ldots, r_n \in \mathbb{K}[\mathbf{x}, y_1]$ of degrees at most $\deg V$ with the following properties.

- The polynomial q is monic in y_1. Further, q defines the projection of V onto the first $m+1$ coordinates, that is $\pi_{\mathbf{x},y_1}(V) = \mathrm{V}(q)$.
- The discriminant δ of q with respect to y_1 is nonzero.
- Let q' denote the derivative of q with respect to y_1. Let J denote the ideal generated by $q, q'y_2 - r_2, q'y_3 - r_3, \ldots, q'y_n - r_n$. Then $J : q'^{\infty} = I(V)$. ◊

If y_1 is not a primitive element for V, then we can apply a change of coordinates to ensure that y_1 is a primitive element in the new basis. Consequently, a geometric resolution for an arbitrary variety usually consists of a change of coordinates, along with the above data. For our application, we will not require this more general definition. The rest of this section is devoted to showing that geometric resolutions exist, and along the way, showing some of their useful properties.

For the rest of this subsection, fix an equidimensional variety V of dimension m such that y_1 is a primitive element for V.

Before we begin our proof, we quickly remark on why a geometric resolution is a parametric representation for V. Given a geometric resolution for V as above, we have a map $\phi : \mathbb{A}^{m+1} \setminus \mathrm{V}(q') \to \mathbb{A}^{m+n}$ defined by

$$\phi(a_1, \ldots, a_m, b) = (a_1, \ldots, a_m, b, r_2(\mathbf{a}, b)/q'(\mathbf{a}, b), \ldots, r_n(\mathbf{a}, b)/q'(\mathbf{a}, b)).$$

The conditions that $q, r_2, \ldots, r_n$ are a geometric resolution imply that the image of $\mathrm{V}(q)$ under ϕ is a dense open subset of V. Therefore, a geometric resolution allows us to parametrize a dense open subset of V using a hypersurface. Since we do not use this fact, we do not pursue this further.

Let $W_1, \ldots, W_t$ be the irreducible components of V. Let I denote the ideal of V, and I_j denote the ideal of W_j for each j. Define $X_j \coloneqq \overline{\pi_{\mathbf{x}}(W_j)}$.

Lemma 3.4. *The element y_1 is a primitive element for each of $W_1, \ldots, W_t$. Further, $X_j = \mathbb{K}^m$ for all $j \in [t]$.*

Proof. Let $\boldsymbol{\alpha} \in \mathbb{K}^m$ be a point witnessing the fact that y_1 is primitive element for V. By assumption, the fiber $\pi_{\mathbf{x}}^{-1}(\boldsymbol{\alpha}) \cap V$ has cardinality exactly $\deg V = \sum_{j=1}^{t} \deg W_j$. This implies that each fiber $\pi_{\mathbf{x}}^{-1}(\boldsymbol{\alpha}) \cap W_j$ is finite and therefore of cardinality at most $\deg W_j$. Since

$$\sum_{j=1}^{t} \deg W_j = \deg V = |\pi_{\mathbf{x}}^{-1}(\boldsymbol{\alpha}) \cap V| \leq \sum_{j=1}^{t} |\pi_{\mathbf{x}}^{-1}(\boldsymbol{\alpha}) \cap W_j| \leq \sum_{j=1}^{t} \deg W_j,$$

it follows that the fiber $\pi_{\mathbf{x}}^{-1}(\boldsymbol{\alpha}) \cap W_j$ has cardinality precisely $\deg W_j$, so W_j is in projective Noether position. Since the points in the fiber $\pi_{\mathbf{x}}^{-1}(\boldsymbol{\alpha}) \cap V$ have distinct y_1 coordinates, so do the points in each of the fibers $\pi_{\mathbf{x}}^{-1}(\boldsymbol{\alpha}) \cap W_j$, which shows that y_1 is primitive for each W_j.

The fact that $X_j = \mathbb{K}^m$ follows from the theorem on the dimension of fibers [Sha94, Chapter 1, Theorem 1.25] as follows: Since the map $\pi_{\mathbf{x}} : W_j \to X_j$ is dominant and has a fiber of finite cardinality, the image X_j must have dimension m. Since $X_j \subseteq \mathbb{K}^m$, it follows that $X_j = \mathbb{K}^m$. □

Since y_1 is a primitive element for $W_1, \ldots, W_t$, it also follows that each W_i is in projective Noether position (Definition 3.3). From [Hei83, Proposition 1] we can deduce that the set of points $\boldsymbol{\alpha} \in \mathbb{K}^m$ that witness the fact that V is in projective Noether position (and likewise for each W_i) is a nonempty open subset of $\mathbb{K}^m$.

Let $u_1, \ldots, u_n$ be new indeterminates and let $\mathbb{L}$ denote the algebraic closure of the field $\mathbb{K}(u_1, \ldots, u_n)$. Let I' and I'_j denote the extensions of the ideals I and I_j to $\mathbb{L}[\mathbf{x}, \mathbf{y}]$. Let V' and W'_j denote the zeroes of these ideals in $\mathbb{L}^{m+n}$. From Lemma 2.4 we can deduce that I'_j is prime for all j and that $I' = \bigcap_j I'_j$. In particular, the varieties W'_j are irreducible and V' is their union. Further, W'_j is a variety of dimension m and degree $\deg W_j$. Since y_1 is a primitive element for V (Definition 3.2), it is also a primitive element for V' and W'_j, and any witness for the former is a witness for the latter. By the previous lemma, the maps $\pi_{\mathbf{x}} : W'_j \to \mathbb{L}^m$ are still dominant.

Let ℓ denote the linear form $u_1 y_1 + \cdots + u_n y_n$. Let $\phi : \mathbb{L}^{m+n} \to \mathbb{L}^{m+1}$ be defined by $(\mathbf{p}, \mathbf{q}) \mapsto (\mathbf{p}, \ell(\mathbf{q}))$. The following lemma captures some basic properties of the polynomial that defines the image of each irreducible component of V' under this map.

Lemma 3.5. *For each j, the close of the image $\overline{\phi(W'_j)}$ is an irreducible hypersurface that is defined by an irreducible polynomial $Q_j \in \mathbb{K}[\mathbf{u}, \mathbf{x}, T]$ of degree at most $\deg W_j$ in $\mathbf{x}$ and T.*

Proof. Since W'_j is irreducible and ϕ is continuous, $\phi(W'_j)$ is irreducible. The projection map $\pi_{\mathbf{x}}$ onto the $\mathbf{x}$ coordinates factors through ϕ. Combined with the theorem on the dimension of fibers, we deduce that $\dim W'_j \geq \dim \phi(W'_j) \geq \dim \pi_{\mathbf{x}}(W'_j)$. Since $\dim W'_j = \dim \pi_{\mathbf{x}}(W'_j)$, we can deduce $\dim \phi(W'_j) = m$. This shows that the closure of the image is an irreducible hypersurface.

Let $T := \sum u_i y_i$. After a change of basis, we can treat $x_1, \ldots, x_m, T, y_2, \ldots, y_n$ as the set of variables in our polynomial ring. Since I'_j has generators in $\mathbb{K}[\mathbf{x}, \mathbf{y}]$, it admits generators in $\mathbb{K}(\mathbf{u})[\mathbf{x}, \mathbf{y}]$ in the new coordinates, performing the change of variables $y_1 \leftarrow (T - u_2 y_2 - \cdots - u_n y_n)/u_1$. A defining equation for $\overline{\phi(W'_j)}$ is then obtained by starting from these new equations and constructing a Gröbner basis with any lexicographic order with $y_n, \ldots, y_2$ occurring before $x_1, \ldots, x_m, T$, and eliminating $y_2, \ldots, y_n$.

Since the construction of the Gröbner basis only involves operations with $\mathbb{K}(\mathbf{u})$-coefficients, the resulting Gröbner basis and elimination ideal have generators in $\mathbb{K}(\mathbf{u})[\mathbf{x}, T]$. After clearing denominators and factoring out any content, we can assume that the image is defined by an irreducible polynomial $Q_j \in \mathbb{K}[\mathbf{u}, \mathbf{x}, T]$ as claimed. The degree of Q_j in $\mathbf{x}, T$ is exactly the degree of $\overline{\phi(W'_j)}$, which is at most $\deg W_j$ by [Hei83, Lemma 2]. □

The following lemma further refines the properties of the polynomial Q_j defined above.

Lemma 3.6. *Suppose $Q_j = p_{j,0} + p_{j,1} T + \cdots + p_{j,d_j} T^{d_j}$ with $p_{j,k} \in \mathbb{K}[\mathbf{u}, \mathbf{x}]$, p_{j,d_j} nonzero, and $d_j \leq \deg W_j$. Then $d_j = \deg W_j$ and $p_{j,d_j} \in \mathbb{K}$.*

Proof. Pick $\boldsymbol{\alpha} \in \mathbb{K}^m$ that is witness to W_j being in projective Noether position (Definition 3.2), such that p_{j,d_j} does not vanish when evaluated at $\boldsymbol{\alpha}$. Since the set of all such witnesses is a nonempty open set, and since the set of points in $\mathbb{K}^m$ where p_{j,d_j} does not vanish is also a nonempty open set, such an $\boldsymbol{\alpha}$ exists. This choice of $\boldsymbol{\alpha}$ ensures that $Q_j(\mathbf{u}, \boldsymbol{\alpha}, T)$ is nonzero.

The fiber $\pi_{\mathbf{x}}^{-1}(\boldsymbol{\alpha}) \cap W_j$ has $\deg W_j$ points, say $(\boldsymbol{\alpha}, \boldsymbol{\beta}_1), \ldots, (\boldsymbol{\alpha}, \boldsymbol{\beta}_{\deg W_j})$, with coordinates in $\mathbb{K}$. Considered as points in $\mathbb{L}^{m+n}$, these points have distinct images $(\boldsymbol{\alpha}, t_1), \ldots, (\boldsymbol{\alpha}, t_{\deg W_j})$ under ϕ. The polynomial Q_j vanishes on each $(\boldsymbol{\alpha}, t_i)$, since $(\boldsymbol{\alpha}, \beta_i) \in W'_j$. Therefore the nonzero polynomial $Q_j(\mathbf{u}, \boldsymbol{\alpha}, T)$ has at least $\deg W_j$ many roots as a polynomial in $\mathbb{K}(\mathbf{u})[T]$, hence its degree in T is at least $\deg W_j$. This gives $d_j = \deg W_j$. Since the total degree of Q_j in $\mathbf{x}$ and T is at most $\deg W_j$, we can also deduce $p_{j,d_j} \in \mathbb{K}[\mathbf{u}]$.

Now we show that p_{j,d_j} in fact lies in $\mathbb{K}$. Consider an irreducible factor of p_{j,d_j}, say $f(\mathbf{u})$. Since Q_j is irreducible in $\mathbb{K}[\mathbf{u}, \mathbf{x}, T]$, there is at least one other $p_{j,i}$ such that f does not divide $p_{j,i}$. Therefore, there is an open set of points $\boldsymbol{\alpha} \in \mathbb{K}^m$ such that f does not divide $p_{j,i}(\mathbf{u}, \boldsymbol{\alpha})$. Since each of these conditions are open, we can find a point $\boldsymbol{\alpha} \in \mathbb{K}^m$ that is a witness to W_j being in projective Noether

position, and such that for each factor f of p_{j,d_j}, the polynomial $Q_j(\mathbf{u}, \boldsymbol{\alpha}, T)$ is not divisible by f. In particular, for any such $\boldsymbol{\alpha}$, the polynomial $Q_j(\mathbf{u}, \boldsymbol{\alpha}, T)$ does not have an irreducible factor that depends only on $\mathbf{u}$. Fix such an $\boldsymbol{\alpha}$, and consider again the images of the fiber of $\boldsymbol{\alpha}$ under ϕ. Let these be denoted $(\boldsymbol{\alpha}, s_1), \ldots, (\boldsymbol{\alpha}, s_{\deg W_j})$. We have the factorization $Q_j(\mathbf{u}, \boldsymbol{\alpha}, T) = p_{j,d_j} \prod_{k \le d_j} (T - s_i)$. This, combined with the choice of $\boldsymbol{\alpha}$, implies that p_{j,d_j} must lie in $\mathbb{K}$. □

We normalize Q_j such that $p_{j,d_j} = 1$ for all j. Pick $\boldsymbol{\alpha}$ such that the fibers $\pi_{\mathbf{x}}^{-1}(\boldsymbol{\alpha}) \cap W_i$ and $\pi_{\mathbf{x}}^{-1}(\boldsymbol{\alpha}) \cap W_j$ are disjoint. The polynomials $Q_i(\mathbf{u}, \boldsymbol{\alpha}, T)$ and $Q_j(\mathbf{u}, \boldsymbol{\alpha}, T)$ are coprime. Therefore we can deduce that Q_i and Q_j are themselves coprime for all pairs Q_i, Q_j. The variety $\overline{\phi(V')}$ is the union of $\overline{\phi(W_j')}$ over all j, therefore it is a hypersurface in $\mathbb{L}^{m+1}$ that is defined by the polynomial $Q = Q_1 \cdots Q_t \in \mathbb{K}[\mathbf{u}, \mathbf{x}, T]$. The polynomial Q has total degree $\deg V$ in $\mathbf{x}$ and T and is monic in T. We say that the polynomial Q defines the general projection of the variety V.

Suppose now that $\gamma_1, \ldots, \gamma_n \in \mathbb{K}$ are elements, and consider the map $\mathbb{A}^{m+n} \to \mathbb{A}^{m+1}$ defined by $(\mathbf{p}, \mathbf{q}) \to (\mathbf{p}, \sum_{i=1}^{n} \gamma_i q_i)$. The following lemma states that the specialization of the general projection Q at $\mathbf{u} = \boldsymbol{\gamma}$ vanishes on the image of the above linear map. Since Q is monic, we are guaranteed that this specialization is nonzero. Consequently, we can also deduce that the map $\pi_{\mathbf{x}}$ is a finite map when restricted to V.

Lemma 3.7. *For every $\boldsymbol{\mu} \in \mathbb{K}^n$, the polynomial $Q(\boldsymbol{\mu}, \mathbf{x}, \ell(\boldsymbol{\mu}))$ lies in I. Consequently, $\ell(\boldsymbol{\mu})$ is integral over $\mathbb{K}[\mathbf{x}]$ in the coordinate ring of V. In particular, the map $\pi_{\mathbf{x}} : V \to \mathbb{K}^m$ is finite. For every $\boldsymbol{\alpha}$, and for every $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ in the fiber $\pi_{\mathbf{x}}^{-1}(\boldsymbol{\alpha}) \cap W$, the element $\ell(\boldsymbol{\mu}, \boldsymbol{\beta})$ is a root of $Q(\boldsymbol{\mu}, \boldsymbol{\alpha}, T)$.*

Proof. The polynomial $Q(\mathbf{u}, \mathbf{x}, \ell)$ lies in I'. As in the proof of Lemma 2.4, since I' is the extension of an ideal in $\mathbb{K}[\mathbf{x}, \mathbf{y}]$, every coefficient of $Q(\mathbf{u}, \mathbf{x}, \ell)$ written as a polynomial in $\mathbf{u}$ belongs to the ideal I. Therefore we can write $Q(\mathbf{u}, \mathbf{x}, \ell) = \sum a_i f_i$ where $a_i \in \mathbb{K}[\mathbf{u}]$ and $f_i \in I$. Evaluating this expression at any $\boldsymbol{\mu}$ shows $Q(\boldsymbol{\mu}, \mathbf{x}, \ell(\boldsymbol{\mu})) \in I$. The polynomial $Q(\boldsymbol{\mu}, \mathbf{x}, T)$ is a monic equation satisfied by $\ell(\boldsymbol{\mu})$, which shows that $\ell(\boldsymbol{\mu})$ is integral over $\mathbb{K}[\mathbf{x}]$ in the coordinate ring of V. Invoking this for different choices of $\boldsymbol{\mu}$ we can deduce that y_i is integral over $\mathbb{K}^m$ in the coordinate ring of V for all i, which shows that map $\pi_{\mathbf{x}} : V \to \mathbb{K}^m$ is finite. The final statement follows as in the proof of Lemma 3.6. □

Let $\boldsymbol{\nu}_0 \in \mathbb{K}^n$ denote the point $(1, 0, \ldots, 0)$. Set

$$q \coloneqq Q(\boldsymbol{\nu}_0, \mathbf{x}, y_1), \qquad r_j \coloneqq -\frac{\partial Q}{\partial u_j}(\boldsymbol{\nu}_0, \mathbf{x}, y_1), \quad j = 1, \ldots, n. \tag{1}$$

These are polynomials in $\mathbb{K}[\mathbf{x}, y_1]$ of degree at most $\deg V$. Let $\delta \in \mathbb{K}[\mathbf{x}]$ and $q' \in \mathbb{K}[\mathbf{x}, y_1]$ denote the discriminant and derivative, respectively, of q with respect to y_1. In the rest of this section, we prove that $q, r_2, \ldots, r_n$ are a geometric resolution of V. We break the proof into a series of smaller lemmas.

Lemma 3.8. *The discriminant δ is nonzero. Equivalently, the polynomial q has no multiple factor.*

Proof. Let $\boldsymbol{\alpha}$ be a witness to y_1 being a primitive element for V. The proof of Lemma 3.6 shows that $q(\boldsymbol{\alpha}, y_1) = Q(\boldsymbol{\nu}_0, \boldsymbol{\alpha}, y_1)$ factors as $\prod_{j \le \deg V} (y_1 - \beta_j)$, where $\beta_1, \ldots, \beta_{\deg V}$ are the distinct y_1-coordinates of the fiber above $\boldsymbol{\alpha}$. This shows that $q'(\boldsymbol{\alpha}) \neq 0$, and since q is monic in y_1 this further shows that $\delta \neq 0$. □

Lemma 3.9. *The polynomials $q, q'y_2 - r_2, \ldots, q'y_n - r_n$ are in the ideal I.*

Proof. As in the proof of Lemma 3.7, we can write $Q(\mathbf{u}, \mathbf{x}, \ell) = \sum_i a_i f_i$, for $a_i \in \mathbb{K}[\mathbf{u}]$ and $f_i \in I$. Evaluating this expression at $\boldsymbol{\nu}_0$ shows that $q \in I$. If we take the partial derivative of this expression with respect to u_j we obtain

$$\frac{\partial Q}{\partial T}(\mathbf{u}, \mathbf{x}, \ell) y_j + \frac{\partial Q}{\partial u_j}(\mathbf{u}, \mathbf{x}, \ell) = \sum_i \frac{\partial a_i}{\partial u_j} f_i.$$

Evaluating this expression at $\boldsymbol{\nu}_0$ shows that $q' y_j - r_j \in I$ for all $j \geq 1$. □

Let $J \subset \mathbb{K}[\mathbf{x}, \mathbf{y}]$ be the ideal generated by $q, q'y_2 - r_2, \ldots, q'y_n - r_n$. Since $J \subset I$, we have $\mathrm{V}(J) \supset V$. The next two lemmas will show that the excess components, that is, those components of $\mathrm{V}(J)$ that are not components of V, are exactly those contained in $\mathrm{V}(q')$.

Lemma 3.10. *The polynomial q defines the projection of V onto the first $m+1$ coordinates, equivalently $\pi_{\mathbf{x},y_1}(V) = \mathrm{V}(q)$.*

Proof. The map $\pi_{\mathbf{x}} : V \to \mathbb{K}^m$ is finite. If Y is the Zariski closure of $\pi_{\mathbf{x},y_1}(V)$ then the map $\pi_{\mathbf{x},y_1} : V \to Y$ is also finite, hence surjective. Therefore, Y is a hypersurface of degree at most $\deg V$. Suppose this hypersurface is defined by $P \in \mathbb{K}[\mathbf{x}, y_1]$. The total degree of P is at most $\deg V$. For any $\boldsymbol{\alpha}$ that is a witness to y_1 being a primitive element for V, the polynomial $P(\boldsymbol{\alpha}, y_1)$ has $\deg V$ distinct roots. Therefore P has degree $\deg V$ in y_1, and we can scale by an element of $\mathbb{K}$ to make it monic in y_1.

Since $q \in I$, and since q vanishes on Y, the polynomial P must divide q in $\mathbb{K}[\mathbf{x}, y]$. Since q and P are both monic in y_1, and since q has degree at most $\deg V$, we must have $P = q$. □

Note that the irreducible components of V are in bijection with the irreducible factors of the polynomials q.

Lemma 3.11. *The following equality of ideals holds: $J : q'^{\infty} = I$.*

Proof. First suppose $f \in J : q'^{\infty}$. Then $q'^k f \in J$ for some $k > 0$. Since q and q'^k are coprime in $\mathbb{K}(\mathbf{x})[y_1]$, there exists a polynomial $\delta' \in \mathbb{K}[\mathbf{x}]$ and polynomials $A, B \in \mathbb{K}[\mathbf{x}, y_1]$ such that $Aq + Bq'^k = \delta'$. Multiplying this equation by f and using the fact that $J \subset I$ we deduce $\delta' f \in I$. No minimal prime of I contains any element of $\mathbb{K}[\mathbf{x}]$, since $\pi_{\mathbf{x}}(W_j) = \mathbb{K}^m$ for all j. Therefore, every minimal prime, and hence I itself, contains f.

Conversely, suppose $f \in I$. Define $\widetilde{f} := f(\mathbf{x}, y_1, r_2/q', \ldots, r_n/q') \in \mathbb{K}[\mathbf{x}, y_1]_{q'}$ and write $\widetilde{f} = F/q'^t$ with $F \in \mathbb{K}[\mathbf{x}, y_1]$. Pick a point $(\boldsymbol{\alpha}, \beta_1) \in \pi_{\mathbf{x},y_1}(V)$ such that $\delta(\boldsymbol{\alpha}) \neq 0$. There exists $(\beta_2, \ldots, \beta_n)$ such that $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in V$. Since the polynomials $q'y_j - r_j$ vanish on V and since $q'(\boldsymbol{\alpha}) \neq 0$, we can deduce that $\beta_j = -r_j(\boldsymbol{\alpha})/q'(\boldsymbol{\alpha})$ for all $j \geq 2$. We also have $f(\boldsymbol{\alpha}, \boldsymbol{\beta}) = 0$. Therefore we can deduce $F(\boldsymbol{\alpha}, \beta_1) = 0$.

We have shown that F vanishes on every point in $\mathrm{V}(q) \setminus \mathrm{V}(q')$. No component of $\mathrm{V}(q)$ is contained in $\mathrm{V}(q')$, therefore F must vanish on $\mathrm{V}(q)$. Equivalently, q divides F. To summarize, in the ring $\mathbb{K}[\mathbf{x}, y_1]_{q'}$ we have shown that $f - cq \in (q'y_2 - r_2, \ldots, q'y_n - r_n)$ for some $c \in \mathbb{K}[\mathbf{x}, y_1]_{q'}$. Writing $f = cq + \sum_{j \geq 2} c_j (q'y_2 - r_2)$ for $c_j \in \mathbb{K}[\mathbf{x}, y_1]_{q'}$, and multiplying by a high enough power of q' shows that $f \in J : q'^{\infty}$. □

3.3 The relationship between Chow forms and geometric resolutions

In this section, we show how Chow forms and geometric resolutions are related. We continue to use the same notation as in Section 3.2. First we show how the polynomial defining the general projection, denoted Q, can be computed given the Chow form of the projective closure of an equidimensional

variety. As a consequence, the geometric resolution can also be computed from the Chow form (as long as y_1 is a primitive element).

A similar procedure for the same task appears in [JKSS04, Section 3].

Lemma 3.12. *Let $V \subset \mathbb{K}^{m+n}$ be an equidimensional variety such that y_1 is a primitive element for V. Let $\overline{V} \subset \mathbb{P}^{m+n}$ denote its projective closure (say we homogenize by adding a new variable z) and let $C_{\overline{V}}$ be the Chow form of $\overline{V}$. Let ℓ_i denote the linear form $w_i z - x_i \in \mathbb{K}[\mathbf{w}][z, \mathbf{x}, \mathbf{y}]$ for $i = 1, \ldots, m$. Let ℓ_{m+1} denote the linear form $Tz - \sum_{j=1}^{n} u_i y_i \in \mathbb{K}[T, \mathbf{u}][z, \mathbf{x}, \mathbf{y}]$. Then $C_{\overline{V}}(\operatorname{coeff}(\ell_1), \ldots, \operatorname{coeff}(\ell_{m+1})) = Q(\mathbf{u}, \mathbf{w}, T)$.*

Proof. Let $\boldsymbol{\alpha}$ be a witness to the fact that V is in projective Noether position. Consider the linear forms $x_1 - \alpha_1 z, \ldots, x_m - \alpha_m z$. The variety $\overline{V} \cap \mathrm{V}(x_1 - \alpha_1 z, \ldots, x_m - \alpha_m z)$ contains $\deg V$ points on the chart $z \neq 0$. The projective Bézout's theorem shows that this intersection has degree at most $\deg V$, therefore it cannot contain any other points. In the rest of this proof, $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_{\deg V} \in \mathbb{K}^n$ will be such that $(1, \boldsymbol{\alpha}, \boldsymbol{\beta}_i)$ are the points in $\overline{V} \cap \mathrm{V}(x_1 - \alpha_1 z, \ldots, x_m - \alpha_m z)$.

Define $C' := C_{\overline{V}}(\operatorname{coeff}(\ell_1), \ldots, \operatorname{coeff}(\ell_{m+1}))$. We now show that $C' \neq 0$. In C', set $w_1 = \alpha_1, \ldots, w_m = \alpha_m$. Set $\mathbf{u}$ to an element $\boldsymbol{\gamma} \in \mathbb{K}^n$ such that $\sum_j \gamma_j \beta_{i,j}$ are distinct for all i. Let this resulting polynomial be denoted by $C''(T)$. Then C'' is nonzero at any τ that is not of the form $\sum_j \gamma_j \beta_{i,j}$ for some i. Indeed by the first step above, $\overline{V} \cap \mathrm{V}(x_1 - \alpha_1 z, \ldots, x_m - \alpha_m z)$ only contains finitely many points, and these choices of τ and $\boldsymbol{\gamma}$ ensure that the hyperplane $z\tau - \sum_j \gamma_j y_j$ avoids these points. Since the Chow form is a homogeneous polynomial of degree $\deg V$ in each set of variables, we can deduce that C'' is monic in T of degree $\deg V$. From this, we can deduce that C' is nonzero, and also that C' has degree $\deg V$ in T.

Next we show $Q(\mathbf{u}, \mathbf{w}, T)$ divides C'. For a general choice of $\boldsymbol{\alpha}' \in \mathbb{K}^m$ and a general choice of $\boldsymbol{\gamma}' \in \mathbb{K}^n$, both $Q(\boldsymbol{\gamma}', \boldsymbol{\alpha}', T)$ and $C'(\boldsymbol{\gamma}', \boldsymbol{\alpha}', T)$ have the same roots. Indeed for a general choice, the fiber $\pi_{\mathbf{x}}^{-1}(\boldsymbol{\alpha}')$ is finite, and the roots of both $Q(\boldsymbol{\gamma}', \boldsymbol{\alpha}', T)$ and $C('\boldsymbol{\gamma}, \boldsymbol{\alpha}', T)$ are $\sum_i \gamma_i' \beta_i'$ where $(\boldsymbol{\alpha}, \boldsymbol{\beta}')$ is a point in the fiber. Along with the statement on the degrees, this shows that $C' = Q \cdot P$ for some polynomial $P \in \mathbb{K}[\mathbf{w}]$. We show $P \in \mathbb{K}$, which will conclude the proof. To this end, assume that $P \notin \mathbb{K}$ and let $\boldsymbol{\mu}$ be a zero of P. The polynomial $C'(\mathbf{u}, \boldsymbol{\mu}, T)$ is zero. By Lemma 3.7, the map $\pi_{\mathbf{x}} : V \to \mathbb{K}^m$ is finite, so the fiber $\pi_{\mathbf{x}}^{-1}(\boldsymbol{\mu}) \cap V$ consists of a finite number of points. Further, these are the only points in $\overline{V} \cap \mathrm{V}(x_1 - \mu_1 z, \ldots, x_m - \mu_m z)$, since

$$\overline{V} \cap \mathrm{V}(x_1 - \mu_1 z, \ldots, x_m - \mu_m z) \cap \mathrm{V}(z) = \overline{V} \cap \mathrm{V}(x_1 - \alpha_1 z, \ldots, x_m - \alpha_m z) \cap \mathrm{V}(z) = \varnothing.$$

We can therefore find a τ and $\boldsymbol{\gamma}$ such that $\tau z - \sum_i y_i \gamma_i$ is nonzero at all of these points. Then the intersection of $\overline{V}$ with $\mathrm{V}(x_1 - \mu_1 z, \ldots, x_m - \mu_m z, \tau z - \sum y_i \gamma_i)$ is empty, so $C'(\boldsymbol{\gamma}, \boldsymbol{\mu}, \tau) \neq 0$, which contradicts the fact that $C'(\mathbf{u}, \boldsymbol{\mu}, T)$ is zero. □

That V is in projective Noether position is crucial in the proof of Lemma 3.12. Without this condition, the specialization of the Chow form vanishes identically.

Finally, we show how a geometric resolution of an affine variety can be used to compute which of its components lie on another variety given by a Chow form.

Lemma 3.13. *Let $V \subset \mathbb{K}^{m+n}$ be an m-equidimensional variety such that y_1 is a primitive element for V. Let $q, r_2, \ldots, r_n \in \mathbb{K}[\boldsymbol{x}, y_1]$ be a geometric resolution for V as above. Let $W \subset \mathbb{P}^{m+n}$ be another equidimensional variety of dimension b, and suppose C_W is the Chow form of W, in the variables $u_{0,0}, \ldots, u_{0,m+n}, u_{1,0}, \ldots, u_{b,m+n}$.*

Consider new variables $w_{i,j}$ (for $0 \leq i \leq b$ and $1 \leq j \leq n+m$), t_j (for $1 \leq j \leq m$) and s, and for $i = 0, \ldots, b$ let g_i denote the following polynomial, which is linear in $\mathbf{x}, \mathbf{y}, z$:

$$g_i \coloneqq \sum_{j=1}^{m} w_{i,j}(x_j - t_j z) + w_{i,m+1}(y_1 - sz) + \sum_{j'=2}^{n} w_{i,m+j'} \left(y_{j'} + \frac{r_{j'}(\mathbf{t}, s)}{q'(\mathbf{t}, s)} z \right).$$

Let $\frac{P(\mathbf{t},s,\mathbf{w})}{q'(\mathbf{t},s)^c} = C_W(\mathrm{coeff}(g_0),\ldots,\mathrm{coeff}(g_b))$*, expressed so that* $P \in \mathbb{K}[\mathbf{t},s,\mathbf{w}]$ *and so that* P *and* q' *are relatively prime. Let* $P' \in \mathbb{K}[\mathbf{t},s]$ *denote the GCD of the coefficients of* P *as a polynomial in* $\mathbf{w}$*. Then* $\gcd(q(\mathbf{t},s),P'(\mathbf{t},s))$ *consists of those factors of* q *that correspond to components of* V *that lie in* W*.*

Proof. Let q_1 denote an irreducible factor of q, and let V_1 be the corresponding component of V.

Suppose first that $V_1 \subset W$. We show $q_1(\mathbf{t},s)$ divides P'. To this end, let $(\boldsymbol{\alpha},\beta_1) \in \mathbb{K}^{m+1}$ be a point in $\mathrm{V}(q_1)\backslash\mathrm{V}(q')$. There exists $\beta_2,\ldots,\beta_n$ such that $(\boldsymbol{\alpha},\boldsymbol{\beta}) \in V_1$ (because the restriction of $\pi_{\boldsymbol{x},y_1}$ to V_1 is closed). Further $\beta_i = -r_i(\boldsymbol{\alpha},\beta_1)/q'(\boldsymbol{\alpha},\beta_1)$ for all $i \geq 2$. After substituting $\boldsymbol{\alpha}$ and β_1 for $\mathbf{t}$ and s, each of the linear forms $x_1-\alpha_1 z, x_2-\alpha_2 z,\ldots,x_m-\alpha_m z, y_1-\beta_1 z, y_2+\frac{r_2(\boldsymbol{\alpha},\beta_1)}{q'(\boldsymbol{\alpha},\beta_1)}z,\ldots,y_n+\frac{r_n(\boldsymbol{\alpha},\beta_1)}{q'(\boldsymbol{\alpha},\beta_1)}z$ vanishes at $(1,\boldsymbol{\alpha},\boldsymbol{\beta}) \in \mathbb{P}^{m+n}$. Therefore $g_0,\ldots,g_b$ also vanish at this point. The evaluation $C_W(\mathrm{coeff}(g_0),\ldots,\mathrm{coeff}(g_b))$ must also vanish, which implies $P(\boldsymbol{\alpha},\beta_1,\mathbf{w}) = 0$. Since this happens for every $(\boldsymbol{\alpha},\beta_1) \in \mathrm{V}(q_1)\setminus\mathrm{V}(q')$, and since q' and q_1 are relatively prime, we can deduce that $q_1(\mathbf{t},s)$ divides every coefficient of P as a polynomial in $\mathbf{w}$, and specifically that $q_1(\mathbf{t},s)$ divides $P'(\mathbf{t},s)$.

Now suppose $V_1 \not\subset W$. Pick a point $(\boldsymbol{\alpha},\beta_1) \in \mathrm{V}(q_1)\setminus\mathrm{V}(q')$ such that the point $(\boldsymbol{\alpha},\boldsymbol{\beta}) \in V$ above $(\boldsymbol{\alpha},\beta_1)$ lies in $V_1 \setminus W$. Such a point exists since W has codimension at least 1 inside V_1. As in the previous case, after substituting $\boldsymbol{\alpha}$ and β_1 for $\mathbf{t}$ and s, each of the linear forms $x_1-\alpha_1 z, x_2-\alpha_2 z,\ldots,x_m-\alpha_m z, y_1-\beta_1 z, y_2+\frac{r_2(\boldsymbol{\alpha},\beta_1)}{q'(\boldsymbol{\alpha},\beta_1)}z,\ldots,y_n+\frac{r_n(\boldsymbol{\alpha},\beta_1)}{q'(\boldsymbol{\alpha},\beta_1)}z$ vanishes at $(1,\boldsymbol{\alpha},\boldsymbol{\beta}) \in \mathbb{P}^{m+n}$. In fact this point is exactly the vanishing set of this collection of linear forms. Since this point is not in W, we can find a specialization $\boldsymbol{\mu}$ of the variables $\mathbf{w}$ such that $W \cap \mathrm{V}(g_0(\boldsymbol{\mu}),\ldots,g_b(\boldsymbol{\mu})) = \varnothing$. Thus $P(\boldsymbol{\alpha},\beta_1,\boldsymbol{\mu}) \neq 0$. Consequently, $q_1(\mathbf{t},s)$ does not divide $P'(\mathbf{t},s)$. □

Remark 3.14. When using Lemma 3.13 to perform computation, we can directly use random linear combinations instead of general linear combinations when defining the polynomials $g_0,\ldots,g_b$. In this case, $\gcd(q(\mathbf{t},s),P(\mathbf{t},s))$ is the factor of q with the claimed properties, with high probability. Indeed as long as the coefficients in the random linear combinations are picked from a set $\mathcal{B} \subset \mathbb{K}$ of size $\mathrm{poly}(n+m,\deg V,\deg W)$, then the required property fails only with probability $1/\mathrm{poly}(n+m,\deg V,\deg W)$. This follows from the above proof by considering the degree of P as a polynomial in $\mathbf{w}$, and also considering the size of $\mathcal{B}$ to ensure that a specialisation $\boldsymbol{\mu}$ with the claimed properties can be found in the second step. ◊

4 Computing Chow forms of equidimensional components

In this section, we start by showing how resultant computations can be used to compute the Chow form of each equidimensional component of a given projective variety. We then show how this can be used to solve the same problem in the affine case

The construction of the Chow form for equidimensional components proceeds in two steps. In the first step, from the defining equations of a projective variety V, we construct the Chow forms for certain subvarieties $V_k \subseteq V$. These are equidimensional subvarieties of V that are obtained via a deformation process. This step generalizes the construction of Ierardi [Ier89, Section 2], where only the isolated points were considered. The second step involves pruning the Chow forms of the varieties V_k to obtain Chow forms for the equidimensional components. This step uses geometric resolutions and the results in Section 3.3.

4.1 Chow form of limit subvarieties

Given a sequence of forms $G_1,\ldots,G_k \in \mathbb{F}[x_0,\ldots,x_n]$ with $k \leq n$, and $d_i := \deg G_i$, we use $\mathrm{V}^p(G_1,\ldots,G_k)$ to denote the variety in $\mathbb{P}^n \times \mathbb{A}^1$ defined by $(1-t)G_1+tx_1^{d_1},\ldots,(1-t)G_k+tx_k^{d_k}$. Since

projective varieties are proper, the projection to $\mathbb{A}^1$ of each irreducible component of $\mathrm{V}^p(G_1,\dots,G_k)$ is an irreducible closed set [Sha94, Chapter 1, Theorem 1.11]. Therefore, the projection is either all of $\mathbb{A}^1$ or a single point. Let $W_1,\dots,W_a$ be those irreducible components of $\mathrm{V}^p(G_1,\dots,G_k)$ whose projection to $\mathbb{A}^1$ is surjective. We use $\mathrm{V}'(G_1,\dots,G_k)$ to denote $\bigcup_{i=1}^a W_i$.

The intersection of $\mathbb{P}^n\times\mathbb{A}^1$ with the hyperplane defined by $t=0$ can be naturally identified with $\mathbb{P}^n$. The image of the intersection of $\mathrm{V}'(G_1,\dots,G_k)$ with the hyperplane defined by $t=0$ under this identification is a subvariety of $\mathbb{P}^n$, which we denote by $\lim_{t\to 0}\mathrm{V}^p(G_1,\dots,G_k)$. More generally, for $\tau\in\mathbb{F}$, we write $\lim_{t\to\tau}\mathrm{V}^p(G_1,\dots,G_k)$ for the subvariety of $\mathbb{P}^n$ corresponding to the intersection of $\mathrm{V}'(G_1,\dots,G_k)$ with the hyperplane defined by $t=\tau$.

The following lemma establishes some basic structural facts about the varieties $\mathrm{V}^p(G_1,\dots,G_k)$ and $\lim_{t\to\tau}\mathrm{V}^p(G_1,\dots,G_k)$. In particular, we compute the dimensions of the varieties $W_1,\dots,W_a$ and $\lim_{t\to\tau}\mathrm{V}^p(G_1,\dots,G_k)$, and show how the variety $\lim_{t\to 0}\mathrm{V}^p(G_1,\dots,G_k)$ is related to $\mathrm{V}(G_1,\dots,G_k)$. In the rest of this subsection, we use π_t and $\pi_{\mathbf{x}}$ to denote the projection maps $\mathbb{P}^n\times\mathbb{A}^1\to\mathbb{A}^1$ and $\mathbb{P}^n\times\mathbb{A}^1\to\mathbb{P}^n$, respectively.

Lemma 4.1. *Every component of $\mathrm{V}^p(G_1,\dots,G_k)$ has codimension at most k and the components $W_1,\dots,W_a$ have codimension exactly k. For every $\tau\in\mathbb{F}$, the variety $\lim_{t\to\tau}\mathrm{V}^p(G_1,\dots,G_k)$ is an equidimensional variety of codimension k. Further,*

$$\lim_{t\to 0}\mathrm{V}^p(G_1,\dots,G_k)\subseteq\mathrm{V}(G_1,\dots,G_k),$$

and every codimension-k component of the latter is an irreducible component of the former.

Proof. That every component of $\mathrm{V}^p(G_1,\dots,G_k)$ has codimension at most k follows from the fact that $\mathrm{V}^p(G_1,\dots,G_k)$ is defined by k equations. Consider now the component W_1. Since $\pi_t(W_1)$ is surjective, $W_1\cap\mathrm{V}(t-1)\neq\varnothing$ and this intersection has codimension 1 within W_1. Further, $W_1\cap\mathrm{V}(t-1)\subseteq\mathrm{V}^p(G_1,\dots,G_k)\cap\mathrm{V}(t-1)=\mathrm{V}\Big(t-1,x_1^{d_1},\dots,x_k^{d_k}\Big)$, and the latter has codimension $k+1$ in $\mathbb{P}^n\times\mathbb{A}^1$. From this we get

$$k+1\geq\operatorname{codim}(W_1)+1=\operatorname{codim}(W_1\cap\mathrm{V}(t-1))\geq k+1,$$

which shows that $\operatorname{codim}(W_1)=k$ in $\mathbb{P}^n\times\mathbb{A}^1$.

Since W_1 is not contained in any hyperplane defined by $t=\tau$, the intersection of W_1 with the hyperplane defined by $t=\tau$ for any τ has codimension $k+1$ in $\mathbb{P}^n\times\mathbb{A}^1$. The same holds for the components $W_2,\dots,W_a$. This proves that $\lim_{t\to\tau}\mathrm{V}^p(G_1,\dots,G_k)$ is an equidimensional variety of codimension k for every τ.

The inclusion $\lim_{t\to 0}\mathrm{V}^p(G_1,\dots,G_k)\subseteq\mathrm{V}(G_1,\dots,G_k)$ follows by construction. Let Y be an irreducible component of the latter of codimension k. Since $Y\times\{0\}\subseteq\mathrm{V}^p(G_1,\dots,G_k)$, there must exist a component Z of $\mathrm{V}^p(G_1,\dots,G_k)$ such that $Y\times\{0\}\subseteq Z$. The component Z has codimension at most k in $\mathbb{P}^n\times\mathbb{A}^1$ by the first paragraph. We will show that $\pi_t(Z)=\mathbb{A}^1$, which implies $Z=W_i$ for some i. As a consequence, we have the inclusion $Z\subseteq\mathrm{V}'(G_1,\dots,G_k)$, and the final statement of the lemma follows.

Towards a contradiction, assume that $\pi_t(Z)\neq\mathbb{A}^1$. Since $\pi_t(Z)$ is closed and irreducible, and since $0\in\pi_t(Z)$, we can deduce $\pi_t(Z)=\{0\}$. Then $Z=Z\cap\mathrm{V}(t)$ in $\mathbb{P}^n\times\mathbb{A}^1$, and this variety has dimension at least $n+1-k$. Further, this variety is contained in $\mathrm{V}(G_1,\dots,G_k)\times\{0\}$ by construction, so it must be contained in one of the irreducible components of $\mathrm{V}(G_1,\dots,G_k)\times\{0\}$ of dimension at least $n+1-k$, say $Z\subseteq Y'\times\{0\}$. We now have $Y\times\{0\}\subsetneq Y'\times\{0\}$ whence $Y\subsetneq Y'$, where these containments are strict since Y' has dimension strictly larger than that of Y. This is a contradiction to the fact that Y is an irreducible component of $\mathrm{V}(G_1,\dots,G_k)$. □

If a set of forms $G_1, \ldots, G_k$ defines an equidimensional variety of codimension k, then the Chow form is easily constructed using the resultant as follows. Let $\{u_{i,j} \mid 0 \le i \le n-k, 0 \le j \le n\}$ be a set of fresh variables. We use $\mathbf{u}_i$ to denote the variables $u_{i,0}, \ldots, u_{i,n}$ and $\mathbf{u}$ to denote all the $u_{i,j}$. Let L_i denote the general linear form $L_i \coloneqq u_{i,0}x_0 + u_{i,1}x_1 + \cdots + u_{i,n}x_n$. If $\gamma_{i,j}$ is a set of elements from $\mathbb{F}$ for $0 \le i \le n-k$ and $0 \le j \le n$ then we use $L_i^{\boldsymbol{\gamma}}$ to denote the specialization of the linear form L_i.

Lemma 4.2. *If $G_1, \ldots, G_k$ are homogeneous forms such that $V = \mathrm{V}(G_1, \ldots, G_k)$ is an equidimensional variety of codimension k, then the squarefree part of $\mathrm{Res}(G_1, \ldots, G_k, L_0, \ldots, L_{n-k})$ (where we treat the polynomials as forms in $x_0, \ldots, x_n$) is a nonzero scalar multiple of the Chow form of V.*

Proof. This is a straightforward consequence of the main property of the resultant (Item 1 of Definition 2.5) as follows. Let $R \in \mathbb{K}[\mathbf{u}]$ denote the resultant of $G_1, \ldots, G_k, L_0, \ldots, L_{n-k}$ as forms in the variables $\mathbf{x}$. Suppose $\gamma_{i,j}$ for $0 \le i \le n-k$ and $0 \le j \le n$ is a set of elements such that $R(\boldsymbol{\gamma}) = 0$. Then by the main property of the resultant, $\mathrm{V}\big(G_0, \ldots, G_k, L_0^{\boldsymbol{\gamma}}, \ldots, L_{n-k}^{\boldsymbol{\gamma}}\big)$ is nonempty, whence $\boldsymbol{\gamma}$ is a zero of the Chow form of V. Conversely, if $\boldsymbol{\gamma}$ is a root of the Chow form, then by definition of the Chow form, $\mathrm{V}\big(G_0, \ldots, G_k, L_0^{\boldsymbol{\gamma}}, \ldots, L_{n-k}^{\boldsymbol{\gamma}}\big)$ is nonempty, and so $R(\boldsymbol{\gamma}) = 0$ by the main property of the resultant. Since R and the Chow form of V have the same zero set, their squarefree parts must be the same (up to a multiple of $\mathbb{K}$). Since the Chow form is squarefree, normalizing the squarefree part of R must yield the Chow form. □

If $\mathrm{V}(G_1, \ldots, G_k)$ is not equidimensional, then it has a component of codimension less than k. In this case, $\mathrm{Res}(G_1, \ldots, G_k, L_0, \ldots, L_{n-k})$ is the zero polynomial, since $\mathrm{V}\big(G_0, \ldots, G_k, L_0^{\boldsymbol{\gamma}}, \ldots, L_{n-k}^{\boldsymbol{\gamma}}\big)$ will be nonempty for every choice of $\boldsymbol{\gamma}$.

As we now prove, even if $\mathrm{V}(G_1, \ldots, G_k)$ is not equidimensional, the resultant

$$\mathrm{Res}\Big((1-t)G_1 + tx_1^{d_1}, \ldots, (1-t)G_k + tx_k^{d_k}, L_0, \ldots, L_{n-k}\Big)$$

remains nonzero. While we cannot recover the Chow forms of the equidimensional components of $\mathrm{V}(G_1, \ldots, G_k)$ directly from this polynomial, we can recover the Chow forms of the varieties $\lim_{t \to \tau} \mathrm{V}^p(G_1, \ldots, G_k)$.

We now prove some intermediate results towards the above facts. The first of these is that certain incidence varieties are irreducible. This is essentially a version of Bertini's theorem.

Lemma 4.3. *Suppose $Z \subseteq \mathbb{P}^n \times \mathbb{A}^1$ is an irreducible variety. Then the incidence variety*

$$Z^H \coloneqq \Big(Z \times (\mathbb{P}^n)^{n-k+1}\Big) \cap \mathrm{V}(L_0, \ldots, L_{n-k})$$

is irreducible in $\mathbb{P}^n \times \mathbb{A}^1 \times (\mathbb{P}^n)^{n-k+1}$.

Proof. Let π denote the projection map from $\mathbb{P}^n \times \mathbb{A}^1 \times (\mathbb{P}^n)^{n-k+1}$ to $\mathbb{P}^n \times \mathbb{A}^1$, restricted to Z^H. The fibre of π at a point $(\boldsymbol{\alpha}, \tau) \in Z$ consists exactly of points of the form $(\boldsymbol{\alpha}, \tau, \boldsymbol{\gamma}) \in \mathbb{P}^n \times \mathbb{A}^1 \times (\mathbb{P}^n)^{n-k+1}$ such that $L_0^{\boldsymbol{\gamma}}, \ldots, L_{n-k}^{\boldsymbol{\gamma}}$ vanish at $\boldsymbol{\alpha}$. These fibres are therefore all nonempty and isomorphic to $\big(\mathbb{P}^{n-1}\big)^{n-k+1}$. In particular, they are also all irreducible. To summarize, the map π is surjective, has irreducible image, and every fibre is irreducible of the same dimension. Therefore we can invoke [Sha94, Chapter 1, Theorem 1.26] to deduce that Z^H is irreducible. We remark that the statement of [Sha94, Chapter 1, Theorem 1.26] assumes that the source and target of the map are projective; however, inspection of the proof shows that it suffices for the map to be closed. □

We now focus on incidence varieties of the above form arising from components of $\mathrm{V}^p(G_1, \ldots, G_k)$. We use $\pi_{t,\mathbf{u}}$ to denote the projection from $\mathbb{P}^n \times \mathbb{A}^1 \times (\mathbb{P}^n)^{n-k+1}$ onto the last two components. Based on whether the projection to $\mathbb{A}^1$ of a given component $Z \subseteq \mathrm{V}^p(G_1, \ldots, G_k)$ is all of $\mathbb{A}^1$ or a single point, we can deduce information about $\pi_{t,\mathbf{u}}(Z^H)$.

Lemma 4.4. *Let Z be an irreducible component of $\mathrm{V}^p(G_1,\dots,G_k)$ such that the projection of Z to $\mathbb{A}^1$ consists of a single point τ. Then $\pi_{t,\mathbf{u}}(Z^H) = \mathrm{V}(t-\tau)$.*

Proof. By Lemma 4.1, the component Z has codimension at most k in $\mathbb{P}^n \times \mathbb{A}^1$. Further Z lies in $\mathrm{V}(t-\tau)$, therefore $Z \cap \mathrm{V}(t-\tau)$ also has codimension at most k in $\mathbb{P}^n \times \mathbb{A}^1$. If we identify $\mathbb{P}^n \times \{\tau\}$ with $\mathbb{P}^n$, then the image of Z under this identification has codimension at most $k-1$ in $\mathbb{P}^n$. As a consequence, this image meets every linear subspace defined by $n-k+1$ equations. This shows that the fibre of $(\tau,\boldsymbol{\gamma})$ under the map $\pi_{t,\mathbf{u}}$ meets Z^H for every choice of $\boldsymbol{\gamma}$, proving the claim. □

Lemma 4.5. *Let Z be an irreducible component of $\mathrm{V}^p(G_1,\dots,G_k)$ such that the projection of Z onto $\mathbb{A}^1$ is surjective. Then $\pi_{t,\mathbf{u}}(Z^H)$ has codimension 1 and is not contained in any hyperplane defined by an equation of the form $t=\tau$.*

Proof. By Lemma 4.1, the component Z has codimension exactly k in $\mathbb{P}^n \times \mathbb{A}^1$, so it has dimension exactly $n+1-k$. Therefore, $Z \times (\mathbb{P}^n)^{n-k+1}$ has dimension $n+1-k+n(n-k+1)$, and $Z^H = \Big(Z \times (\mathbb{P}^n)^{n-k+1}\Big) \cap \mathrm{V}(L_0,\dots,L_{n-k})$ has dimension at least $\dim\Big(Z \times (\mathbb{P}^n)^{n-k+1}\Big) - n + k - 1 = n(n-k+1)$.

Since $\pi_t(Z) = \mathbb{A}^1$, and since

$$Z \cap \mathrm{V}(t-1) \subset \mathrm{V}^p(G_1,\dots,G_k) \cap \mathrm{V}(t-1) = \mathrm{V}(t,x_1,\dots,x_k),$$

and since $\operatorname{codim}(Z) = k$, we have $Z \cap \mathrm{V}(t-1) = \mathrm{V}(x_1,\dots,x_k)$. Pick $\boldsymbol{\gamma}$ such that $L_0^{\boldsymbol{\gamma}} = x_0, L_1^{\boldsymbol{\gamma}} = x_{k+1}, L_2^{\boldsymbol{\gamma}} = x_{k+2}, \dots, L_{n-k}^{\boldsymbol{\gamma}} = x_n$. Then the linear subspace defined by these linear forms does not meet $Z \cap \mathrm{V}(t-1)$. This shows that $\pi_{t,\mathbf{u}}(Z^H) \neq \mathbb{A}^1 \times (\mathbb{P}^n)^{n-k+1}$. Since $\pi_{t,\mathbf{u}}(Z^H)$ is closed ([Sha94, Chapter 1, Theorem 1.11]), we can deduce also that $\dim \pi_{t,\mathbf{u}}(Z^H) \leq \dim(\mathbb{P}^n)^{n-k+1} \times \mathbb{A}^1 - 1 = n(n-k+1)$.

Now we show that there is a point $(\tau,\boldsymbol{\gamma}) \in \pi_{t,\mathbf{u}}(Z^H)$ whose fibre meets Z^H at finitely many points. For this, we can pick $\tau = 1$ and $\boldsymbol{\gamma}$ such that $L_0^{\boldsymbol{\gamma}} = L_1^{\boldsymbol{\gamma}} = x_{k+1}$ and $L_2^{\boldsymbol{\gamma}} = x_{k+2}, \dots, L_{n-k}^{\boldsymbol{\gamma}} = x_n$. The fibre only meets Z^H at the point $((1,0,\dots,0),\tau,\boldsymbol{\gamma})$. By the fibre dimension theorem, since the target and the source are irreducible, we can deduce that $\dim Z^H = \dim \pi_{t,\mathbf{u}}(Z^H)$. Combined with the bounds on $\dim Z^H$ and $\dim \pi_{t,\mathbf{u}}(Z^H)$ shown above, we can deduce that both Z^H and $\pi_{t,\mathbf{u}}(Z^H)$ have dimension exactly $n(n-k+1)$. The final statement, that $\pi_{t,\mathbf{u}}(Z^H)$ is not contained in a hypersurface of the form $\mathrm{V}(t-\tau)$ follows from the fact that for any choice of τ, the intersection $Z \cap \mathrm{V}(t-\tau)$ is nonempty, and therefore we can always find a set of $n-k+1$ linear equations that meet it. □

We can combine the above observations to obtain a defining equation of $\pi_{t,\mathbf{u}}(\mathrm{V}'(G_1,\dots,G_k))$.

Lemma 4.6. *Let $G_1,\dots,G_k$ be forms. Define*

$$R' \coloneqq \operatorname{Res}\Big((1-t)G_1 + tx_1^{d_1}, \dots, (1-t)G_k + tx_k^{d_k}, L_0, \dots, L_{n-k}\Big),$$

where the resultant is computed with respect to $x_0,\dots,x_n$. Let R be the squarefree part of R'. Then the squarefree part of $\mathrm{TT}_t\, R$ is a nonzero scalar multiple of the Chow form for $\lim_{t\to 0} \mathrm{V}^p(G_1,\dots,G_k)$.

Proof. Define $Y \coloneqq \Big(\mathrm{V}^p(G_1,\dots,G_k) \times (\mathbb{P}^n)^{n-k+1}\Big) \cap \mathrm{V}(L_0,\dots,L_{n-k})$. By the main property of the resultant (Item 1 of Definition 2.5), the roots of $\mathrm{V}(R')$ consist of exactly those $(\tau,\boldsymbol{\gamma})$ such that $(1-\tau)G_1 + \tau x_1^{d_1}, \dots, (1-\tau)G_k + \tau x_k^{d_k}, L_0^{\boldsymbol{\gamma}}, \dots, L_{n-k}^{\boldsymbol{\gamma}}$ have a common zero. These are exactly the points in $\pi_{t,\mathbf{u}}(Y)$. Thus $\pi_{t,\mathbf{u}}(Y) = \mathrm{V}(R') = \mathrm{V}(R)$, where the last equality follows since taking

squarefree parts does not change the zero set. Let $R_1 \in \mathbb{F}[t]$ and $R_2 \in \mathbb{F}[t, \mathbf{u}]$ be such that $R = R_1 R_2$ and no factor of R_2 depends only on t (equivalently, $R_2|_{t=\tau} \neq 0$ for all τ).

We show the following three facts regarding R_1 and R_2.

1. $R_1(\tau) = 0$ if and only if $\mathrm{V}^p(G_1, \ldots, G_k)$ has a component whose projection to $\mathbb{A}^1$ consists of the point τ.
2. $\mathrm{V}(R_2) = \pi_{t,\mathbf{u}}\Big(\Big(\mathrm{V}'(G_1, \ldots, G_k) \times (\mathbb{P}^n)^{n-k+1}\Big) \cap \mathrm{V}(L_0, \ldots, L_{n-k})\Big)$.
3. For each τ, the squarefree part of the specialization $R_2|_{t=\tau}$ is a nonzero scalar multiple of the Chow form of $\lim_{t\to\tau} \mathrm{V}^p(G_1, \ldots, G_k)$.

The image $\pi_{t,\mathbf{u}}(Y)$ is the union of the images of the irreducible components of Y under the map $\pi_{t,\mathbf{u}}$. By construction, the irreducible components of Y are exactly the irreducible components of Z^H, where Z is an irreducible component of $\mathrm{V}^p(G_1, \ldots, G_k)$. By Lemma 4.3, the varieties Z^H are themselves irreducible, therefore the irreducible components of Y are exactly Z^H.

Lemma 4.4 and Lemma 4.5 show that the $\operatorname{codim}\big(\pi_{t,\mathbf{u}}(Z^H)\big) = 1$, and therefore each such image either lies in $\mathrm{V}(R_1)$ or $\mathrm{V}(R_2)$. Lemma 4.5 also shows that if Z is a component of $\mathrm{V}'(G_1, \ldots, G_k)$ then the image lies in $\mathrm{V}(R_2)$. Similarly, Lemma 4.4 also shows that if Z is not a component of $\mathrm{V}'(G_1, \ldots, G_k)$ then the image lies in $\mathrm{V}(R_1)$. These two facts prove items 1 and 2.

To prove item 3, note that from item 2 we can deduce

$$\begin{aligned}\mathrm{V}(R_2|_{t=\tau}) &= \pi_{\mathbf{u}}\Big(\Big(\mathrm{V}'(G_1, \ldots, G_k) \times (\mathbb{P}^n)^{n-k+1}\Big) \cap \mathrm{V}(L_0, \ldots, L_{n-k}) \cap \mathrm{V}(t-\tau)\Big) \\ &= \pi_{\mathbf{u}}\Big(\Big(\lim_{t\to\tau} \mathrm{V}^p(G_1, \ldots, G_k) \times (\mathbb{P}^n)^{n-k+1}\Big) \cap \mathrm{V}(L_0, \ldots, L_{n-k})\Big).\end{aligned}$$

By the main property of the resultant (item 1 of Definition 2.5), the zeroes of $\mathrm{V}(R_2|_{t=\tau})$ are exactly those $\boldsymbol{\gamma}$ such that $L_0^{\boldsymbol{\gamma}}, \ldots, L_{n-k}^{\boldsymbol{\gamma}}$ have a common root on $\lim_{t\to\tau} \mathrm{V}^p(G_1, \ldots, G_k)$, therefore the squarefree part of $R_2|_{t=\tau}$ is a nonzero scalar multiple of the Chow form of $\lim_{t\to\tau} \mathrm{V}^p(G_1, \ldots, G_k)$. The conclusion of the lemma now follows from the fact that $R_2|_{t=0}$ and $\mathrm{TT}_t\, R$ are scalar multiples of each other, which can be seen as follows. We have $\mathrm{TT}_t\, R = \mathrm{TT}_t\, R_1 \cdot \mathrm{TT}_t\, R_2$. The first of these terms lies in $\mathbb{F} \setminus \{0\}$, since $R_1 \in \mathbb{F}[t] \setminus \{0\}$. The second term is simply $R_2|_{t=0}$, since no factor of R_2 depends only on t, therefore R_2 is not a multiple of t. □

Using the above results, given any projective variety defined by m equations, and given any k, we can compute a Chow form for some codimension-k equidimensional subvariety of the input that contains every irreducible component of codimension k.

Lemma 4.7. *Let $F_1, \ldots, F_m \in \mathbb{F}[x_0, \ldots, x_n]$ be forms of degrees $d_1, \ldots, d_m$ with $d_1 \geq \cdots \geq d_m$, and let $V \coloneqq \mathrm{V}(F_1, \ldots, F_m)$. Let $B \subseteq \mathbb{F} \setminus \{0\}$ be a subset of the coefficient field of $\mathbb{F}$. Let k be an integer between 1 and n, inclusive. Let $G_1, \ldots, G_k$ and $H_1, \ldots, H_k$ be random linear combinations of $\left\{x_j^{d_1-d_i} F_i\right\}_{i,j}$, where each coefficient is picked independently and uniformly from B. Define*

$$R_G \coloneqq \mathrm{TT}_t \operatorname{Res}\Big((1-t)G_1 + t x_1^{d_1}, \ldots, (1-t)G_k + t x_k^{d_1}, L_0, \ldots, L_{n-k}\Big),$$

and

$$R_H \coloneqq \mathrm{TT}_t \operatorname{Res}\Big((1-t)H_1 + t x_1^{d_1}, \ldots, (1-t)H_k + t x_k^{d_1}, L_0, \ldots, L_{n-k}\Big).$$

Then with probability at least $1 - 4nd^n/|B|$, the squarefree part of the polynomial $\gcd(R_G, R_H)$ is a nonzero scalar multiple of the Chow form for some $V_k \subseteq V$ where V_k is equidimensional of codimension k and contains every component of V of codimension k.

Proof. Let $V_G \coloneqq \mathrm{V}(G_1, \ldots, G_k)$ and $V_H \coloneqq \mathrm{V}(H_1, \ldots, H_k)$. Via a union bound, we can deduce that the following hold with probability at least $1 - 4nd^n/|B|$. By Lemma 2.3, every component of V_G and V_H of codimension less than k is a component of V, and every component of V of codimension k is a component of V_G and V_H. Every codimension-k irreducible variety that is a component of both V_G and V_H is also a component of V: indeed if Z is any irreducible component of V_G that does not lie in $\mathrm{V}(F_1, \ldots, F_m)$ then already Z does not lie in $\mathrm{V}(H_1)$.

Assume now that all the above properties hold. By Lemma 4.6, the squarefree parts of R_G and R_H are nonzero scalar multiples of the Chow forms of $\lim_{t\to 0} \mathrm{V}^p(G_1, \ldots, G_k)$ and $\lim_{t\to 0} \mathrm{V}^p(H_1, \ldots, H_k)$ respectively. Lemma 4.1 says the following about $\lim_{t\to 0} \mathrm{V}^p(G_1, \ldots, G_k)$: it is an equidimensional variety of codimension k that contains every codimension k component of $\mathrm{V}(G_1, \ldots, G_k)$. Further, since $\lim_{t\to 0} \mathrm{V}^p(G_1, \ldots, G_k) \subseteq \mathrm{V}(G_1, \ldots, G_k)$, every component of $\lim_{t\to 0} \mathrm{V}^p(G_1, \ldots, G_k)$ that is not an irreducible component of $\mathrm{V}(G_1, \ldots, G_k)$ actually lies in some higher dimensional component of $\mathrm{V}(G_1, \ldots, G_k)$. In the setting above, these higher dimensional components of $\mathrm{V}(G_1, \ldots, G_k)$ are exactly the components of $\mathrm{V}(F_1, \ldots, F_m)$ of codimension less than k. The same holds for $\lim_{t\to 0} \mathrm{V}^p(H_1, \ldots, H_k)$.

Now since the Chow form of an equidimensional variety is the product of the Chow forms of its components, the squarefree part of $\gcd(R_G, R_H)$ is a nonzero multiple of the Chow form of the union of the those components that are both in $\lim_{t\to 0} \mathrm{V}^p(G_1, \ldots, G_k)$ and in $\lim_{t\to 0} \mathrm{V}^p(H_1, \ldots, H_k)$. From the description of these limit varieties above, and the properties guaranteed by the random choice, every such component lies in some irreducible component of $\mathrm{V}(F_1, \ldots, F_m)$, and further every component of codimension k of $\mathrm{V}(F_1, \ldots, F_m)$ is one of these common components. This completes the proof. □

4.2 Constant-depth circuits for the Chow form

The final step to obtaining the Chow form of the equidimensional components of a given variety is to prune the extra components. This will be carried out using Lemma 3.12 and Lemma 3.13, relying on the interplay between geometric resolutions and Chow forms. These results require in particular that we find a primitive element for the varieties whose geometric resolution we wish to compute (defined in Section 3.2), which we can do by applying a randomly-chosen change of coordinates. The proof of the following lemma is standard, see for example [JKSS04, Section 3.5].

Lemma 4.8. *Let $W \subseteq \mathbb{P}^n$ be an equidimensional projective variety of degree D. Let $B \subseteq \mathbb{F} \setminus \{0\}$ be a subset of the coefficient subfield of $\mathbb{F}$. Let $M \in \mathbb{F}^{(n+1)\times(n+1)}$ be a matrix where each entry is picked uniformly and independently from B. Suppose M is invertible. Let $\phi : \mathbb{P}^n \to \mathbb{P}^n$ be the invertible linear map defined by matrix M, that is, $\phi(\boldsymbol{\alpha}) = M\boldsymbol{\alpha}$.*

Let W' be the restriction of $\phi(W)$ to the affine chart of points at finite distance. With probability at least $1 - 5nD/|B|$, the variety W' is in projective Noether position, and x_{r+1} is a primitive element for $\phi(W')$, where $r = \dim W$. Further, the projective closure of W' is exactly $\phi(W)$.

We now construct a family of circuits that compute the Chow forms of the equidimensional components of a variety, given set-theoretic defining equations for the variety in the dense representation. We will treat part of the input as random bits, but the final output of the circuit is a $\mathbb{Z}$-multiple of the Chow forms, where the exact scaling factor depends in an unspecified manner on these random bits.

The computations of the Chow forms involve multivariate GCD computations and factor-lifting as subroutines, which are only developed over characteristic 0 fields. Consequently, even though the results of Section 4.1 hold over arbitrary fields, the following results are only stated over $\mathbb{Q}$.

Theorem 4.9. *There exists a polylogtime-uniform family of constant-depth threshold circuits $\mathcal{C}^{\mathcal{CHOW}}$ indexed by $n, m, d_1, \ldots, d_m, h$ with the following properties.*

- *The circuit $C^{\mathcal{CHOW}}_{n,m,d_1,\ldots,d_m,h}$ take as input a collection of forms $F_1, \ldots, F_m \in \mathbb{Q}[x_0, \ldots, x_n]$ of degrees $d_1, \ldots, d_m$ and height at most h in the dense representation. The circuit also takes as input $5 \cdot m \cdot (n+1)^3$ integers of height at most h, which we denote by $a_1, \ldots, a_r$.*
- *The output of $C^{\mathcal{CHOW}}_{n,m,d_1,\ldots,d_m,h}$ is a set of $n+1$ polynomials in the dense representation. If the inputs $a_1, \ldots, a_r$ are independently and uniformly sampled from a set of size b, then with probability at least $1 - 100n^2(nd^n)^{n^2}/b$, the computed polynomials are $\mathbb{Z}$-multiples of the Chow forms of the equidimensional components of $\mathrm{V}(F_1, \ldots, F_m)$. Here, d denotes $\max_i d_i$.*
- *The size of $C^{\mathcal{CHOW}}_{n,m,d_1,\ldots,d_m,h}$ is $\mathrm{poly}\Big(h, n, m, (d+1)^{\mathrm{poly}(n)}\Big)$.*

Proof. Let $F_1, \ldots, F_m \in \mathbb{Q}[x_0, \ldots, x_n]$ be the given forms of degrees $d_1, \ldots, d_m$. By rearranging the inputs, we can assume $d_1 \geq \cdots \geq d_m$. For convenience, we let $d \coloneqq d_1$. Let $V \coloneqq \mathrm{V}(F_1, \ldots, F_m)$ be the projective variety defined by $F_1, \ldots, F_m$. If all the F_i are identically zero then $V = \mathbb{P}^n$, and the Chow form of every equidimensional component of V except n is just 1. The Chow form of the component of dimension n is 0. In the rest of this argument, we will assume that at least one of the inputs F_i is nonzero, so $V \neq \mathbb{P}^n$. The Chow form of the component of dimension n is then 1. The rest of the proof will compute the Chow form of the other equidimensional components of V. Let $V = V_0 \cup V_1 \cup \cdots \cup V_{n-1}$ be the equidimensional decomposition of V.

We will first compute, for every $0 \leq k \leq n-1$, the Chow form of a variety $V_k^\star \subseteq V$ that is equidimensional of dimension k and contains V_k, the dimension-k equidimensional component of V. Because $V_k \subseteq V_k^\star$, the Chow form of V_k divides that of $V_k^\star$. Any points in the difference $V_k^\star \setminus V_k$ must lie on a higher-dimensional component of V. In particular, they lie on $V_\ell \subseteq V_\ell^\star$ for some $\ell > k$. We will use the Chow forms of $V_{k+1}^\star, \ldots, V_{n-1}^\star$ to remove these extraneous factors from the Chow form of $V_k^\star$, resulting in the Chow form of V_k.

The varieties $V_0^\star, \ldots, V_{n-1}^\star$ and their Chow forms. We begin by computing Chow forms of the varieties $V_0^\star, \ldots, V_{n-1}^\star$ using Lemma 4.7. As in Lemma 4.7, we define forms $G_1, \ldots, G_{n-k}$ and $H_1, \ldots, H_{n-k}$ each to be linear combinations of the polynomials $\Big\{x_j^{d_1-d_i} F_i : 1 \leq i \leq m, 0 \leq j \leq n\Big\}$, where the coefficients of this linear combination are the first $n(n+1)^2 m/2$ of the integers a_e. Let $\{u_{i,j} \mid 0 \leq i \leq k, 0 \leq j \leq n\}$ be a set of fresh variables and define $L_i \coloneqq u_{i,0}x_0 + \cdots + u_{i,n}x_n$. Let t be a new variable and define the polynomials

$$R_G \coloneqq \mathrm{TT}_t \,\mathrm{Res}\Big((1-t)G_1 + tx_1^{d_1}, \ldots, (1-t)G_{n-k} + tx_{n-k}^{d_1}, L_0, \ldots, L_k\Big)$$
$$R_H \coloneqq \mathrm{TT}_t \,\mathrm{Res}\Big((1-t)H_1 + tx_1^{d_1}, \ldots, (1-t)H_{n-k} + tx_{n-k}^{d_1}, L_0, \ldots, L_k\Big),$$

where the resultants are taken with respect to the variables $x_0, \ldots, x_n$. By Lemma 4.7, under the assumption that the integers $a_1, \ldots, a_r$ are picked uniformly and independently, with high probability the squarefree part of $\gcd(R_G, R_H)$ is a nonzero scalar multiple of the Chow form of an equidimensional dimension-k variety. We assume for the rest of the proof that this event occurs. We let $V_k^\star$ be this variety.

We now bound the cost of computing the Chow form of $V_k^\star$. Computing the coefficients of the forms G_i and H_i can be done using items 1 and 2 of Theorem 2.12 to multiply the coefficients of the polynomials $x_j^{d_1-d_i} F_i$ by the coefficients a_e and then add the resulting polynomials together. The threshold circuits obtained by invoking Theorem 2.12 are of constant depth and size $\mathrm{poly}(h, m, n, (d+1)^{\mathrm{poly}(n)})$. By Theorem 2.15 and [AGS26, Lemma 6.1], the coefficients of

R_G and R_H can be computed by a polylogtime-uniform family of threshold circuits of constant depth and size $\mathrm{poly}(h, n, (d+1)^{\mathrm{poly}(n)})$. To compute $\gcd(R_G, R_H)$, we apply the circuit family of Lemma 2.13, which is a polylogtime-uniform family of TC^0 circuits to compute GCDs of multivariate polynomials. These circuits in turn require "random inputs", for which we use the next few a_e's. In our application, these circuits have size $\mathrm{poly}(h, n, (d+1)^{\mathrm{poly}(n)})$. This follows from the fact that both R_G and R_H are polynomials in $O(nk) \leq O(n^2)$ variables of degree at most nd^n, and hence have at most $\mathrm{poly}(n, (d+1)^{\mathrm{poly}(n)})$ nonzero coefficients; together with the fact that the coefficients of R_G and R_H were obtained by simulating a constant-depth arithmetic circuit of size $\mathrm{poly}(n, (d+1)^{\mathrm{poly}(n)})$ and thus have height at most $h \cdot \mathrm{poly}(n, (d+1)^{\mathrm{poly}(n)})$. The failure probability is at most $2nd^n/b$ for this step. We then apply Corollary 2.14 to compute the squarefree part of $\gcd(R_G, R_H)$, which can be implemented by a polylogtime-uniform family of threshold circuits of constant depth and size $\mathrm{poly}(h, n, (d+1)^{\mathrm{poly}(n)})$, again using the next few a_e's as the random bits. Similar to computing the GCD, the squarefree part computation fails with probability at most $2n^2(nd^n)^{n^2}/b$. Finally, we normalize the coefficients of the squarefree part of $\gcd(R_G, R_H)$ so that it has leading coefficient 1 in the lexicographic order, and thus is the Chow form of $V_k^\star$. In total, this part of the computation can be carried out by a threshold circuit of constant depth and size $\mathrm{poly}(h, n, (d+1)^{\mathrm{poly}(n)})$.

Changing coordinates to projective Noether position. Next, we will change coordinates so that the points of $V_k^\star$ at finite distance are in projective Noether position and have y_1 as a primitive element. To do this, we apply a linear change of coordinates using the next few a_e's as the coefficients of the transformation. Let $W_k^\star$ be the image of $V_k^\star$ under this change of coordinates, and similarly let W_k be the image of V_k. Let $U_k^\star$ and U_k be the points of $W_k^\star$ and W_k, respectively, at finite distance (that is, the points on the open set defined by $x_0 \neq 0$). By Lemma 4.8, if the a_e's are sampled uniformly and independently, then with probability at least $1 - 5nd^k/b$, the variety $U_k^\star$ is in projective Noether position and the variable x_{k+1} is a primitive element for $U_k^\star$. Furthermore, the variety $W_k^\star$ is precisely the projective closure of $U_k^\star$, and likewise W_k is the projective closure of U_k. By Lemma 3.1, the Chow form of $W_k^\star$ is obtained by applying the same change of coordinates to the Chow form of $V_k^\star$.

We can compute the coefficients of the Chow form of $W_k^\star$ from the Chow form of $V_k^\star$ by evaluating the Chow form of $V_k^\star$ at a sufficient number of points and then interpolating the coefficients of the Chow form of $W_k^\star$. The Chow form of $V_k^\star$ is a polynomial of degree at most nd^n in n^2 variables, so $(nd^n+1)^{n^2} \leq \mathrm{poly}(n, (d+1)^{\mathrm{poly}(n)})$ evaluations of the Chow form suffice to recover its coefficients. These evaluations can be performed using a polylogtime-uniform family of threshold circuits of constant depth and size $\mathrm{poly}(h, n, (d+1)^{\mathrm{poly}(n)})$ using items 1 and 2 of Theorem 2.12. We then interpolate back the coefficients of the Chow form of $W_k^\star$ using the threshold circuits in item 11 of Theorem 2.12, which again can be implemented in constant depth and size $\mathrm{poly}(h, n, (d+1)^{\mathrm{poly}(n)})$. Overall, this step can be carried out by threshold circuits of constant depth and $\mathrm{poly}(h, n, (d+1)^{\mathrm{poly}(n)})$ size.

Computing a geometric resolution of $U_k^\star$. Our next goal is to use Chow forms of the varieties $W_k^\star, W_{k+1}^\star, \ldots, W_{n-1}^\star$ to compute the Chow form of W_k. This proceeds in three steps. First, we compute a geometric resolution of the variety $U_k^\star$. We then use the Chow forms of $W_{k+1}^\star, \ldots, W_{n-1}^\star$ to refine this to obtain (part of) a geometric resolution for U_k. Lastly, we lift this (partial) geometric resolution back to a Chow form of W_k.

We start by computing a geometric resolution of $U_k^\star$. Rename the variables $x_{k+1}, \ldots, x_n$ to $y_1, \ldots, y_{n-k}$. Let $u_1, \ldots, u_{n-k}$ be new indeterminates, let $\mathbb{L} = \overline{\mathbb{K}(u_1, \ldots, u_n)}$, and let $\phi : \mathbb{K}^n \to \mathbb{K}^{k+1}$

be the linear map given by

$$\phi(x_1, \ldots, x_k, y_1, \ldots, y_{n-k}) = (x_1, \ldots, x_k, u_1 y_1 + \cdots + u_{n-k} y_{n-k}).$$

By Lemma 3.5, the closure of the image $\overline{\phi(U_k^\star)}$ is a hypersurface defined by a single polynomial $Q_k^\star \in \mathbb{K}[\mathbf{u}][\mathbf{x}, T]$. Because $W_k^\star$ is the projective closure of $U_k^\star$, the polynomial $Q_k^\star$ can be obtained as a specialization of the Chow form of $W_k^\star$ by Lemma 3.12. Because this specialization of the Chow form only involves setting variables to 0, 1, or -1, we can compute the coefficients of $Q_k^\star$ by adding and subtracting the appropriate coefficients of the Chow form of $W_k^\star$. This can be carried out by threshold circuits of constant depth and size $\mathrm{poly}(h, n, (d+1)^{\mathrm{poly}(n)})$ by invoking item 1 of Theorem 2.12.

From the polynomial $Q_k^\star$, we compute a geometric resolution of the variety $U_k^\star$, following Section 3.2. Let $\boldsymbol{\nu}_0 \in \mathbb{K}^k$ be the point $(1, 0, \ldots, 0)$ and define the polynomials

$$\begin{aligned} q^\star(\mathbf{x}, y_1) &\coloneqq Q_k^\star(\boldsymbol{\nu}_0, \mathbf{x}, y_1) \\ r_j^\star(\mathbf{x}, y_1) &\coloneqq -\frac{\partial Q_k^\star}{\partial u_j}(\boldsymbol{\nu}_0, \mathbf{x}, y_1) \qquad\qquad j \in \{1, \ldots, n_k\}. \end{aligned}$$

Together, Lemmas 3.8 to 3.11 imply that $q^\star, r_1^\star, \ldots, r_{n-k}^\star$ are a geometric resolution of $U_k^\star$. These polynomials are obtained by specializing the polynomial $Q_k^\star$ and its first derivatives, so as was the case with $Q_k^\star$, we can compute their coefficients using threshold circuits of constant depth and size $\mathrm{poly}(h, n, (d+1)^{\mathrm{poly}(n)})$ thanks to item 1 of Theorem 2.12.

Removing excess components of $U_k^\star$ in $q^\star$. We now execute the second step of our construction, refining the polynomial $q^\star$ to a polynomial q that corresponds to the components of $U_k^\star$ that lie on W_k. For each $\ell > k$, we will use the Chow form of $W_\ell^\star$ to prune away the factor of $q^\star$ that corresponds to components of $W_k^\star$ that lie on $W_\ell^\star$. To do this, we apply Lemma 3.13. Let $w_{0,1}, \ldots, w_{\ell,n}, t_1, \ldots, t_k, s$ be fresh variables. For $0 \le i \le \ell$, let g_i be the polynomial

$$g_i \coloneqq \sum_{j=1}^{k} w_{i,j}(x_j - t_j x_0) + w_{i,k+1}(y_1 - s x_0) + \sum_{j=2}^{n-k} w_{i,k+j}\left(y_j + \frac{r_j(\mathbf{t}, s)}{q'(\mathbf{t}, s)} x_0\right),$$

where $q'(\mathbf{x}, y_1)$ is the derivative of $q^\star(\mathbf{x}, y_1)$ with respect to y_1. Since $g_0, \ldots, g_\ell$ are linear in the $\mathbf{x}$ and $\mathbf{y}$ variables, we may evaluate the Chow form of $W_\ell^\star$ at the coefficients of $g_0, \ldots, g_\ell$. Letting C_ℓ denote the Chow form of $W_\ell^\star$, write the evaluation $C_\ell(\mathrm{coeff}(g_0), \ldots, \mathrm{coeff}(g_\ell))$ as

$$C_\ell(\mathrm{coeff}(g_0), \ldots, \mathrm{coeff}(g_\ell)) = \frac{P_\ell(\mathbf{t}, s, \mathbf{w})}{q'(\mathbf{t}, s)^{c_\ell}},$$

where the polynomials $P_\ell(\mathbf{t}, s, \mathbf{w})$ and $q'(\mathbf{t}, s)$ are relatively prime. Letting $\hat{P}_\ell(\mathbf{t}, s)$ be the GCD of the coefficients of $P_\ell(\mathbf{t}, s, \mathbf{w})$ viewed as a polynomial in $\mathbf{w}$, Lemma 3.13 implies that

$$q_\ell(\mathbf{t}, s) \coloneqq \gcd(q^\star(\mathbf{t}, s), \hat{P}_\ell(\mathbf{t}, s))$$

consists exactly of those factors of $q^\star$ that correspond to components of $U_k^\star$ lying on $U_\ell^\star$. Equivalently, the polynomial $\frac{q^\star(\mathbf{t}, s)}{q_\ell(\mathbf{t}, s)}$ consists of those factors of $q^\star$ that correspond to components of $U_k^\star$ that do not lie on $W_\ell^\star$.

Consider the polynomial

$$q(\mathbf{t}, s) \coloneqq \gcd\left(\frac{q^\star(\mathbf{t}, s)}{q_{k+1}(\mathbf{t}, s)}, \ldots, \frac{q^\star(\mathbf{t}, s)}{q_{n-1}(\mathbf{t}, s)}\right).$$

The factors of q are precisely the factors of $q^\star$ that correspond to components of $U_k^\star$ not contained in any of the varieties $W_{k+1}^\star, \ldots, W_{n-1}^\star$. Recall that the components of $W_k^\star \setminus W_k$ are contained in $W_{k+1} \cup \cdots \cup W_{n-1} \subseteq W_{k+1}^\star \cup \cdots \cup W_{n-1}^\star$. Since we have removed factors of $q^\star$ that correspond to components lying on $W_{k+1}^\star \cup \cdots \cup W_{n-1}^\star$, it follows that q consists of exactly those factors of $q^\star$ that lie on U_k. Thus, the polynomial $q(\mathbf{t}, s)$ defines the projection of U_k to the first $k+1$ coordinates, as desired.

To compute q, we first compute each of the polynomials q_ℓ in parallel for $k < \ell < n$. For each value of ℓ, we evaluate C_ℓ at the coefficients of $g_0, \ldots, g_\ell$, which results in a rational function $f(\mathbf{t}, s, \mathbf{w})/g(\mathbf{t}, s, \mathbf{w})$. We then compute $\gcd(f(\mathbf{t}, s, \mathbf{w}), g(\mathbf{t}, s, \mathbf{w}))$ and divide both f and g by this GCD, which yields the polynomials $P_\ell(\mathbf{t}, s, \mathbf{w})$ and $q'(\mathbf{t}, s)^{c_\ell}$. Next, we compute $\hat{P}_\ell(\mathbf{t}, s)$ as the GCD of all the $\mathbf{w}$-coefficients of $P_\ell(\mathbf{t}, s, \mathbf{w})$. Finally, we have $q_\ell(\mathbf{t}, s) = \gcd(q^\star(\mathbf{t}, s), \hat{P}_\ell(\mathbf{t}, s))$. Each of these steps can be implemented by a polylogtime-uniform family of threshold circuits of constant depth and size $\mathrm{poly}(h, n, (d+1)^{\mathrm{poly}(n)})$: evaluating C_ℓ and the divisions are carried out using the multivariate polynomial arithmetic of Theorem 2.12, and GCDs are computed using Lemma 2.13. For the multivariate GCD computations, we use the a_e's for the random inputs. Further, to compute the GCD of more than two multivariate polynomials at a time, we can invoke Lemma 2.13 with two distinct formal linear combinations of the polynomials.

After computing the polynomials $q_{k+1}, \ldots, q_{n-1}$, we compute q as $\gcd\left(\frac{q^\star}{q_{k+1}}, \ldots, \frac{q^\star}{q_{n-1}}\right)$. The divisions are carried out in parallel, each implemented with Theorem 2.12. Finally, we compute the GCD of these polynomials once again using Lemma 2.13. In total, this step can be executed by a polylogtime-uniform family of threshold circuits of constant depth and exponential size.

Lifting q to the Chow form of W_k. Finally, we use the polynomial $q(\mathbf{t}, s)$ to compute the Chow form of W_k. If $q(\mathbf{t}, s)$ is a constant Because W_k and $W_k^\star$ are the projective closures of U_k and $U_k^\star$, respectively, we can relate q and $q^\star$ to the Chow forms of W_k and $W_k^\star$. Let C be the Chow form of W_k and recall that C_k is the Chow form of $W_k^\star$. For $1 \le i \le k$, let ℓ_i be the linear form $t_i x_0 - x_i \in \mathbb{K}[\mathbf{t}, s][\mathbf{x}, \mathbf{y}]$, and let ℓ_{k+1} be the linear form $s x_0 - y_1 \in \mathbb{K}[\mathbf{t}, s][\mathbf{x}, \mathbf{y}]$. Then Eq. (1) and Lemma 3.12 imply that

$$C_k(\mathrm{coeff}(\ell_1), \ldots, \mathrm{coeff}(\ell_{k+1})) = q^\star(\mathbf{t}, s)$$
$$C(\mathrm{coeff}(\ell_1), \ldots, \mathrm{coeff}(\ell_{k+1})) = q(\mathbf{t}, s).$$

So far, we have computed the coefficients of C_k, $q^\star$, and q. We know that C is a factor of C_k and likewise that q is a factor of $q^\star$. To compute the coefficients of C, we will invoke Lemma 2.18 to lift q to a factor of C_k, which will be precisely the Chow form C.

To use Lemma 2.18, we need to work with a specialization of the polynomials C_k and C where variables are only set to zero, whereas the specialization above sets some variables to -1. Let $\{u_{i,j} \mid 1 \le i \le k+1, 0 \le j \le n\}$ be the variables of C_k and C. Define the shifted polynomials $\hat{C}_k$ and $\hat{C}$ to be C_k and C, respectively, under the change of coordinates that performs the shift $u_{i,i} \mapsto u_{i,i} - 1$ for $1 \le i \le k+1$ and acts as the identity on the remaining variables. Then we have

$$\hat{C}_k((t_1, 0, \ldots, 0), \ldots, (t_k, 0, \ldots, 0), (s, 0, \ldots, 0)) = q^\star(\mathbf{t}, s)$$
$$\hat{C}((t_1, 0, \ldots, 0), \ldots, (t_k, 0, \ldots, 0), (s, 0, \ldots, 0)) = q(\mathbf{t}, s).$$

To apply Lemma 2.18, we must verify that $\hat{C}_k$ and $q^\star$ are squarefree, and that $\hat{C}_k$ is monic as a polynomial in s. The squarefreeness of $\hat{C}_k$ follows from that fact that it is the Chow form of $W_k^\star$, hence necessarily squarefree, while the squarefreeness of $q^\star$ follows from Lemma 3.8. It is not necessarily the case that $\hat{C}_k$ is monic as a polynomial in s, so to guarantee this, we apply a linear

change of variables $t_i \mapsto t_i + \alpha_i s$, where the scalars α_i are the next few a_e's. The image of $\hat{C}_k$ under this change of coordinates will be monic in s with probability at least $1 - nd^n/b$.

In this new coordinate system, we can apply Lemma 2.18. Let $R(\mathbf{u})$ be the polynomial obtained by applying Lemma 2.18 and then undoing the preceding linear change of variables. The conclusion of Lemma 2.18 guarantees that R is a $\mathbb{Q}$-multiple of C, the Chow form of W_k. By normalizing R to have leading coefficient 1, we obtain the coefficients of the Chow form C.

To carry out this computation, we shift and perform a linear change of variables on the polynomials $\hat{C}_k$ and q. We then apply Lemma 2.18 to $\hat{C}_k$ and q in the new coordinate system. Finally, we change back to the original coordinate system to obtain the coefficients of C, the Chow form of W. The changes of coordinates can both be carried out by threshold circuits of constant depth and size $\mathrm{poly}(h, n, (d+1)^{\mathrm{poly}(n)})$ by evaluating the polynomial in the new coordinate system at sufficiently many points and then interpolating out its coefficients, both of which follow from the arithmetic of Theorem 2.12. The lifting procedure of Lemma 2.18 can likewise be carried out by threshold circuits of constant depth and $\mathrm{poly}(h, n, (d+1)^{\mathrm{poly}(n)})$ size, so this entire step can be implemented by threshold circuits of exponential size and constant depth.

Computing the Chow form of V_k. The variety W_k is the image of V_k under a previously-sampled linear change of coordinates. Using Lemma 3.1, we can compute the Chow form of V_k by composing the Chow form of W_k with the inverse of this change of coordinates. This allows us to compute the coefficients of the Chow form of V_k from the coefficients of the Chow form of W_k. Once more, this change of coordinates can be carried out by evaluating the Chow form of V_k at a sufficient number of points and then interpolating its coefficients, both using the results of Theorem 2.12. This can be done by a threshold circuit of constant depth and $\mathrm{poly}(h, n, (d+1)^{\mathrm{poly}(n)})$ size.

In total, we have computed the coefficients of the Chow form of V_k using a randomized threshold circuit of constant depth and size $\mathrm{poly}(h, m, n, (d+1)^{\mathrm{poly}(n)})$. By our guarantees on the inputs $a_1, \ldots, a_r$, the resulting circuit errs with probability less than $100n^2(nd^n)^{n^2}/b$. Finally, the uniformity of the circuit family follows from the uniformity of each of the subcircuit used throughout the construction, together with the uniformity of the algorithm itself. □

As a corollary of the preceding theorem, we deduce that the coefficients of the Chow form of a variety can be computed in the counting hierarchy.

Corollary 4.10. *The language $L_{\mathcal{CHOW}}$ corresponding to the circuit family $\mathcal{C}^{\mathcal{CHOW}}$ defined in Theorem 4.9 can be decided in* CH.

Proof. This is an immediate consequence of Theorem 4.9 together with Lemma 2.20. □

Corollary 4.10 shows that the Chow forms of the equidimensional components of a projective variety V can be computed in CH when a set of equations that set-theoretically define V are given in the dense representation. Our next corollary extends this result to the case where we are instead given arithmetic circuits that compute equations that set-theoretically define V. This relies on Lemma 2.23, which shows that the coefficients of a polynomial given in the circuit representation can computed in the counting hierarchy.

Corollary 4.11. *There exists a family of boolean functions $\mathcal{G}^{\mathcal{CIRCCHOW}}$ indexed by s with the following properties.*

- *The function $G_s^{\mathcal{CIRCCHOW}}$ takes as input the description of a constant-free, weakly division-free arithmetic circuit of description length at most s, computing a collection of forms $F_1, \ldots, F_m \in \mathbb{Q}[x_0, \ldots, x_n]$. The function also takes as input $5(s+1)^4$ integers of height at most s^5, which we denote by $a_1, \ldots, a_r$.*

- *The output of $G_s^{\mathcal{CIRCCHOW}}$ is a set of polynomials in the dense representation. If the inputs $a_1, \ldots, a_r$ are independently and uniformly sampled from a set of size b, then with probability at least $1 - 100 \cdot 2^{s^4}/b$, the polynomials computed are $\mathbb{Z}$-multiples of the Chow forms of the equidimensional components of $\mathrm{V}(F_1, \ldots, F_m)$, in the dense representation.*
- *The language $L_{\mathcal{CIRCCHOW}}$ corresponding to $\mathcal{G}^{\mathcal{CIRCCHOW}}$ can be decided in CH.*

Proof. We first describe the function $G_s^{\mathcal{CIRCCHOW}}$, which we denote by G_s for brevity. Suppose the input to G_s is a circuit C that computes forms $F_1, \ldots, F_m \in \mathbb{Q}[x_0, \ldots, x_n]$. We can bound both the number of variables n and the number of polynomials m by s. Let $d_1, \ldots, d_m$ denote the degrees of $F_1, \ldots, F_m$. A straightforward induction on s shows that the degrees and heights of the polynomials $F_1, \ldots, F_m$ are both bounded by 2^s. Define $h \coloneqq s^5 \cdot 2^s$. The function G_s, on input $C, a_1, \ldots, a_r$, is defined to be the evaluation of $C^{\mathcal{CHOW}}_{n,m,d_1,\ldots,d_m,h}$ at the coefficients of $F_1, \ldots, F_m$ and the first $5 \cdot m \cdot (n+1)^3$ of the integers $a_1, \ldots, a_r$. From this description, the fact that G_s computes the Chow forms of the equidimensional components of $\mathrm{V}(F_1, \ldots, F_m)$ follows from the guarantees in Theorem 4.9.

We now show that the language $L_{\mathcal{CIRCCHOW}}$ can be decided in CH. First note that given the circuit C, we can compute the integers n, m, and h in polynomial time. We can compute the integers $d_1, \ldots, d_m$ in CH as follows: we nondeterministically guess each d_i, a monomial in F_i of degree d_i with nonzero coefficient, and a bit in this coefficient witnessing the fact that it is nonzero. These guesses can be verified in CH using Lemma 2.23, so we can compute $d_1, \ldots, d_m$ in $\mathsf{NP}^{\mathsf{CH}} = \mathsf{CH}$.

Let $\mathcal{H}$ be the family of boolean functions that takes an arithmetic circuit C as input and computes the coefficients of the polynomials computed by C. Lemma 2.23 shows that the language $L_{\mathcal{H}}$ is in CH. By Lemma 2.22, the description of $\mathcal{G}^{\mathcal{CIRCHOW}}$, and Theorem 4.9, we deduce that the language $L_{\mathcal{CIRCCHOW}}$ is in $\mathsf{CH}^{L_{\mathcal{H}}} \subseteq \mathsf{CH}^{\mathsf{CH}} = \mathsf{CH}$. □

We end with two applications of Corollary 4.10. Our first application is to computing the degree of a projective variety. Because the degree of an equidimensional projective variety can easily be computed from the degree of its Chow form, Corollary 4.11 immediately allows us to compute the degree of both a projective variety and its equidimensional components in CH.

Corollary 4.12. *Given a collection of forms $F_1, \ldots, F_m \in \mathbb{Q}[x_0, \ldots, x_n]$ represented as constant-free, weakly division-free arithmetic circuits, the degree of the projective variety $\mathrm{V}(F_1, \ldots, F_m)$ can be computed in $\mathsf{FP}^{\mathsf{CH}}$.*

Proof. The degree of $\mathrm{V}(F_1, \ldots, F_m)$ is the sum of the degrees of its equidimensional component. For any equidimensional variety of dimension r, the degree of its Chow form as a polynomial is $r+1$ times the degree of the variety.

Let s be the description length of the input circuit C. We sample $5(s+1)^4$ random integers each between 0 and 2^{s^5}, call these $a_1, \ldots, a_r$. Consider the boolean function $G_s^{\mathcal{CIRCCHOW}}$ defined in Corollary 4.11, which we denote by G for the sake of brevity. By Corollary 4.11, with high probability $G(C, a_1, \ldots, a_r)$ computes the Chow forms of the equidimensional components of $\mathrm{V}(F_1, \ldots, F_m)$. Assume for the rest of this proof that this event holds.

Our algorithm now nondeterministically guesses the degree of each of the Chow forms, a monomial with nonzero coefficient of the guessed degree, and a bit witnessing the fact that this coefficient is nonzero. Each equidimensional component of $\mathrm{V}(F_1, \ldots, F_m)$ has degree at most $\exp\left(s^{O(1)}\right)$, and therefore the Chow forms also have degrees bounded by $\exp\left(s^{O(1)}\right)$. Further, the algorithm to compute the Chow form also shows that the heights of the Chow forms are bounded by $\exp\left(s^{O(1)}\right)$. Consequently, all the guesses that the algorithm makes have polynomial length. The algorithm then verifies these guesses using the fact that $L_{\mathcal{CIRCCHOW}}$ can be decided in CH.

Once the degrees of the Chow form are obtained, we can divide the degrees by the respective dimensions and add them up to obtain the degree of the variety. The problem of computing the degree of the variety thus lies in the function version of $\mathsf{BPP}^{\mathsf{CH}}$, which is just $\mathsf{FP}^{\mathsf{CH}}$. □

Our second application is to deciding membership in the equidimensional components of a variety. Suppose we are given a point $\boldsymbol{\alpha} \in \mathbb{F}^{n+1}$ and a list of equations that set-theoretically define a projective variety $V \subseteq \mathbb{P}^n$. Naturally, the equations defining V can be used to test if $\boldsymbol{\alpha} \in V$. Letting $V = V_0 \cup V_1 \cup \cdots \cup V_{n-1}$ be the equidimensional decomposition of V, a natural next question is to decide if $\boldsymbol{\alpha} \in V_k$ for some given k. Using the Chow forms of the equidimensional components of V, we can decide these membership queries in CH.

Corollary 4.13. *Given a collection of forms $F_1, \ldots, F_m \in \mathbb{Q}[x_0, \ldots, x_n]$ represented as constant-free, weakly division-free arithmetic circuits, a point $\boldsymbol{\alpha} \in \mathbb{Q}^{n+1}$, and a natural number $k \in \mathbb{N}$, whether $\boldsymbol{\alpha}$ lies in the dimension-k equidimensional component of $\mathrm{V}(F_1, \ldots, F_m)$ can be decided in CH.*

Proof. If $k > n$ or if $\boldsymbol{\alpha} \notin \mathrm{V}(F_1, \ldots, F_m)$, the algorithm immediately rejects. The latter condition can be checked in randomized polynomial time by evaluating the circuit modulo a random prime [IM83]. Otherwise, we first solve the case $k = 0$. Let V_0 be the zero-dimensional component of $\mathrm{V}(F_1, \ldots, F_m)$. The variety V_0 is a finite set. Let $V_0 = \{\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_d\}$. Then the Chow form $C(u_0, \ldots, u_n)$ of V_0 is a scalar multiple of the polynomial

$$\prod_{i=1}^{d} (u_0\beta_{i,0} + u_1\beta_{i,1} + \cdots + u_n\beta_{i,n}).$$

Thus, to test if $\boldsymbol{\alpha} \in V_0$, it suffices to determine if the Chow form $C(\mathbf{u})$ and the linear form $u_0\alpha_0 + \cdots + u_n\alpha_n$ have a nontrivial GCD. Corollary 4.11 allows us to compute the coefficients of the Chow form $C(\mathbf{u})$ in CH. Together with the polylogtime-uniform TC^0 circuits for multivariate GCD of Lemma 2.13, we conclude by Lemma 2.22 that the coefficients of the GCD can be computed in CH. In particular, we can decide in CH if the GCD is nontrivial, and hence if $\boldsymbol{\alpha} \in V_0$. If $\boldsymbol{\alpha} \in V_0$, we are done and the algorithm accepts.

If $\boldsymbol{\alpha} \notin V_0$, then we will iteratively intersect the variety $\mathrm{V}(F_1, \ldots, F_m)$ with hyperplanes containing $\boldsymbol{\alpha}$ one-by-one until $\boldsymbol{\alpha}$ lies on the zero-dimensional component of the resulting variety. If $\boldsymbol{\alpha}$ is on the dimension-k component of the original variety, then with high probability, $\boldsymbol{\alpha}$ will lie on the zero-dimensional component after k steps.

We now make this argument precise. By performing an invertible linear change of coordinates, we may assume that $\boldsymbol{\alpha} = (1, 0, \ldots, 0)$. Let $B \subseteq \mathbb{Q} \setminus \{0\}$ be a set of size $10n2^{sn}$. Let $L = a_1x_1 + \cdots + a_nx_n$ be a linear form where $a_1, \ldots, a_n$ are chosen independently and uniformly at random from B. We claim that with probability at least $1 - 2^{sn}/|B|$, if $\boldsymbol{\alpha}$ lies on the dimension-k component of $\mathrm{V}(F_1, \ldots, F_m)$, then $\boldsymbol{\alpha}$ lies on the dimension-$(k-1)$ component of $\mathrm{V}(F_1, \ldots, F_m, L)$. To prove this, it suffices to show that L properly intersects each positive-dimensional component of $\mathrm{V}(F_1, \ldots, F_m)$, as this implies that the dimension of each such component drops by 1 on intersecting with L.

Let W be such a component. Because W is positive-dimensional, there is a point $\boldsymbol{\beta} \in W$ different from $\boldsymbol{\alpha}$. The point $\boldsymbol{\beta}$ lies on $\mathrm{V}(L)$ with probability at most $1/|B|$. Since the variety $\mathrm{V}(F_1, \ldots, F_m)$ has degree at most 2^{sn}, it has at most 2^{sn} positive-dimensional components. By a union bound, L properly intersects every positive-dimensional component with probability at least $1 - 2^{sn}/|B|$.

This yields an algorithm to decide on which equidimensional component of $\mathrm{V}(F_1, \ldots, F_m)$ the point $\boldsymbol{\alpha}$ lies. We iteratively sample a linear form L with coefficients in B, add L to our list of equations, and check if $\boldsymbol{\alpha}$ lies on the zero-dimensional component of the resulting variety. With probability at least $1 - n2^{sn}/|B| \geq 9/10$, this procedure decrements the dimension of the component

on which $\boldsymbol{\alpha}$ lies at every step. If $\boldsymbol{\alpha}$ was a point on the dimension-ℓ component of $\mathrm{V}(F_1, \ldots, F_m)$, then this procedure will stop after ℓ steps. At this point, we accept if $\ell = k$ and reject otherwise. □

Finally, we close with two remarks. The first is a remark regarding computing Chow forms of equidimensional components of affine varieties, and the second is regarding the further special case where the affine variety in question is zero-dimensional.

Remark 4.14. Suppose we are given polynomials $f_1, \ldots, f_m \in \mathbb{Q}[x_1, \ldots, x_n]$, and suppose $V \coloneqq \mathrm{V}(f_1, \ldots, f_m)$. The Chow form of the projective closure $\overline{V} \subset \mathbb{P}^n$ can be computed as follows. We consider the equations $F_i := x_0 f_i^h$, where we homogenize with respect to the variable x_0. Because of the additional factor x_0 in each of these equations, the irreducible components of $\mathrm{V}(F_1, \ldots, F_m)$ consist of the hyperplane at infinity $\mathrm{V}(x_0)$, and the projective closures of the irreducible components of $\mathrm{V}(f_1, \ldots, f_m)$. Consequently, for every $k > 1$, the Chow form of the codimension-k equidimensional component of $\mathrm{V}(F_1, \ldots, F_m)$ is exactly the Chow form of the projective closure of the codimension-k equidimensional component of $\mathrm{V}(f_1, \ldots, f_m)$. The Chow form of the codimension-1 equidimensional component of $\mathrm{V}(F_1, \ldots, F_m)$ contains the Chow form of $\mathrm{V}(x_0)$ as a factor, and once we divide by this, we obtain the Chow form of the projective closure of the codimension-1 equidimensional component of $\mathrm{V}(f_1, \ldots, f_m)$. The Chow form of $\mathrm{V}(x_0)$ is simply the determinant of the matrix with i, j entry $u_{i,j}$, therefore it can be computed easily in CH. ◊

Remark 4.15. Suppose we are given polynomials $f_1, \ldots, f_m \in \mathbb{Q}[x_1, \ldots, x_n]$, and suppose $V \coloneqq \mathrm{V}(f_1, \ldots, f_m)$. Suppose further that V is promised to have dimension 0, and that our goal is to compute the u-resultant of V. This can be done using the method discussed in Remark 4.14. However in this case, we can further simplify the calculation as follows. We first compute the Chow form of $\overline{V}_0^\star$ as described in the proof Theorem 4.9 (which is the same as its u-resultant, since $\overline{V}_0^\star$ has dimension 0). The only points in $\overline{V}_0^\star$ that are not in V are those that lie in $\mathrm{V}(x_0)$. Therefore, all we have to do to obtain the u-resultant of V is to identify those factors of $\overline{V}_0^\star$ that depend on u_0. By randomly setting u_0 to two different values and computing a GCD, we can identify the factors that do not depend on u_0, and a final division step gives us the u-resultant of V. In this way, we can avoid the pruning and factor lifting steps that are used in Theorem 4.9. ◊

5 Projections

In this section, we solve the following problem: given an equidimensional variety $V \subset \mathbb{A}^n$ of dimension r, and a linear map $\psi : \mathbb{A}^n \to \mathbb{A}^{r+1}$ described by a matrix $M \in \mathbb{F}^{(r+1)\times n}$ such that $\psi(V')$ has codimension 1 for every irreducible component V' of V, compute a polynomial C such that $\mathrm{V}(C) = \overline{\psi(V)}$. We call this the projection problem. Our treatment of geometric resolutions gave us an answer to this question in the special case when ψ is the projection to the first $r+1$ coordinates and x_{r+1} is a primitive element: this is the content of Lemma 3.10. The computation of the polynomial q described in the statement of Lemma 3.10 is given in Section 4. In this section, we will deal with the more general case described above.

As an application of the projection problem, we give an algorithm for the problem of approximate polynomial satisfiability. While we only give a solution to the projection problem in characteristic zero, our solution to the approximate polynomial satisfiability problem will short-circuit some of the intermediate computations and will in fact be applicable even in fields of finite characteristic.

5.1 Projections of equidimensional varieties

The general case of the projection problem can be reduced to the following case: the map $\psi : \mathbb{A}^n \to \mathbb{A}^{r+1}$ is the projection to the first $r+1$ coordinates, and for every component V' of V, the projection of V' to the first r coordinates is dominant. This is achieved as follows. If M is not full rank, then $\psi(\mathbb{A}^n) \subsetneq \mathbb{A}^{r+1}$. Since we assume that $\psi(V')$ has codimension 1 for every irreducible component V' of V, it must be the case that M has rank r, and that $\overline{\psi(V')} = \psi(\mathbb{A}^n)$ for every irreducible component, therefore the defining equation for $\overline{\psi(V)}$ is easily computed by linear algebra.

Assume now that M is full rank. Pick an invertible linear map $\psi' : \mathbb{A}^{r+1} \to \mathbb{A}^{r+1}$ such that the first r coordinates of ψ' are Noether normalizing for every $\psi(V')$. A random linear map satisfies this property. If we compute the defining equation of $(\psi' \circ \psi)(V)$, then we can use the defining linear equations of ψ' to obtain the defining equation of $\psi(V)$. Since M has rank $r+1$, we can now apply a change of coordinates to $\mathbb{A}^n$ to ensure that $\psi' \circ \psi$ is the projection to the first $r+1$ coordinates. The map $\psi' \circ \psi$ has the two required special properties. Therefore, in the rest of this section, we will assume that ψ is the projection to the first $r+1$ coordinates, and that the projection to the first r coordinates is dominant for every component V' of V.

We start with a fact that relates the projection with the u-resultant of a related variety. We do this by relating both objects to the minimal polynomial of an element of a finite dimensional algebra. The main technical content, and the proof of the following lemma is a slight extension of [Sch03, Proposition 1], the only difference being that we work with a set of polynomials that only generate V set-theoretically, as opposed to ideal-theoretically.

Lemma 5.1. *Let $\mathbb{F}$ be an arbitrary field. Let $V \subset \mathbb{A}^n$ be an equidimensional variety of dimension r such that projection of every irreducible component of V onto the first r coordinates is dense. Let $I \subset \mathbb{F}[x_1, \ldots, x_n]$ denote any ideal such that $\mathrm{V}(I) = V$. Let $\mathbb{K} \coloneqq \overline{\mathbb{F}(x_1, \ldots, x_r)}$, and let $I' \coloneqq I\mathbb{K}[x_{r+1}, \ldots, x_n]$. Let $W \coloneqq \mathrm{V}(I')$. By assumption, W has dimension zero.*

Let $\mathcal{C}_W \in \mathbb{F}(x_1, \ldots, x_r)[\mathbf{u}] \subset \mathbb{K}[\mathbf{u}]$ be a polynomial such that in $\mathbb{K}[\mathbf{u}]$, the squarefree part of $\mathcal{C}_W$ is a nonzero scalar multiple of the u-resultant of W. Let A denote the specialization of $\mathcal{C}_W$ at $u_0 = x_{r+1}, u_1 = -1, u_2 = \cdots = u_{n-r} = 0$. Suppose $A = C/\delta$ where $C \in \mathbb{F}[x_1, \ldots, x_r][x_{r+1}]$ is primitive and $\delta \in \mathbb{F}(x_1, \ldots, x_r)$. Then $\mathrm{V}(C) = \overline{\psi(V)}$.

Proof. The ideal I' has generators in $\mathbb{F}[x_1, \ldots, x_r][x_{r+1}, \ldots, x_n]$. Note that W does not depend on the choice of ideal I used to define V set-theoretically. Let B denote the algebra $\mathbb{K}[x_{r+1}, \ldots, x_n]/I'$. By assumption, B is a finite-dimensional $\mathbb{K}$-algebra.

Let $P \in \mathbb{F}[x_1, \ldots, x_{r+1}]$ be a polynomial that generates the ideal $\mathrm{rad}(I) \cap \mathbb{F}[x_1, \ldots, x_{r+1}]$. Then $\mathrm{V}(P) = \overline{\psi(V)}$. By assumption, every irreducible component V' of V is such that the projection of V' to the first r coordinates is dominant. As a consequence, the polynomial P, when considered as a univariate polynomial in x_{r+1} with coefficients in $\mathbb{F}[x_1, \ldots, x_r]$, is primitive. Indeed, if P has a factor P' in $\mathbb{F}[x_1, \ldots, x_r]$, then no minimal prime of I contains P', and therefore every minimal prime contains P/P', which is a contradiction to the fact that P generates $\mathrm{rad}(I) \cap \mathbb{F}[x_1, \ldots, x_r]$.

Consider the endomorphism of B given by multiplication by x_{r+1}. Let $\mu \in \mathbb{K}[T]$ denote the minimal polynomial of this endomorphism. Since the generators of I' lie in $\mathbb{F}(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$, we deduce that $\mu \in \mathbb{F}(x_1, \ldots, x_r)[T]$. By [CLO05, Chapter 2, Theorem 4.5], the roots of μ are exactly α_1 for $\boldsymbol{\alpha} \in W$. Equivalently, μ factors as $\mu = c \prod_{\boldsymbol{\alpha} \in W} (T - \alpha_1)^{n_{\boldsymbol{\alpha}}}$ for some $c \in \mathbb{F}(x_1, \ldots, x_r)$ and $n_{\boldsymbol{\alpha}} > 0$. Write $\mu = R/d$, where $R \in \mathbb{F}[x_1, \ldots, x_r][T]$ is primitive, and $d \in \mathbb{F}(x_1, \ldots, x_r)$.

We first show that $\overline{\psi(V)} = \mathrm{V}(R(x_{r+1}))$ in $\mathbb{A}^{r+1}_{\mathbb{F}}$. Since P defines $\psi(V)$, we have $P \in \mathrm{rad}(I)$, and therefore $P \in \mathrm{rad}(I')$. Consequently, when P is treated as a univariate polynomial in $\mathbb{K}[x_{r+1}]$, it vanishes on α_1 for every $\boldsymbol{\alpha} \in W$. The roots of $R(x_{r+1})$ are precisely α_1 for each $\boldsymbol{\alpha} \in W$. Therefore we can deduce that $R(x_{r+1})$ divides P^a in $\mathbb{K}[x_{r+1}]$ for some $a \in \mathbb{N} \setminus \{0\}$. Since these polynomials

have coefficients in $\mathbb{F}[x_1, \ldots, x_r][x_{r+1}]$, we can write $P^a = R\eta$ with $\eta \in \mathbb{F}(x_1, \ldots, x_r)[x_{r+1}]$. Since both P and R are primitive, we can deduce by Gauss's lemma that $\eta \in \mathbb{F}[x_1, \ldots, x_r][x_{r+1}]$. This shows $\mathrm{V}(R(x_{r+1})) \subseteq \overline{\psi(V)}$.

Conversely, we have $R(x_{r+1}) \in I' \cap \mathbb{F}[x_1, \ldots, x_{r+1}]$. As seen above, the ideal I' has generators in $\mathbb{F}[x_1, \ldots, x_r][x_{r+1}, \ldots, x_n]$, and is generated by a set of elements that generate I. We can therefore write $R(x_{r+1}) = \sum g_i h_i$ with $g_i \in \mathbb{F}[x_1, \ldots, x_n]$ that are generators of I, and $h_i \in \mathbb{F}(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$. Clearing denominators, we get $c' R(x_{r+1}) = \sum g_i h_i'$ for some $c', h_i' \in \mathbb{F}[x_1, \ldots, x_n]$ such that $h_i = h_i'/c'$ for every i. Therefore, $c' R(x_{r+1}) \in I$. Since no minimal prime of I contains a nonzero element from $\mathbb{F}[x_1, \ldots, x_r]$, we can deduce that $R(x_{r+1}) \in I$. Consequently, $\overline{\psi(V)} \subseteq \mathrm{V}(R(x_{r+1}))$. This completes the proof that $\overline{\psi(V)} = \mathrm{V}(R(x_{r+1}))$.

Finally, consider now the specialization of $\mathcal{C}_W$ at $u_2 = \cdots = u_{n-r} = 0$. By definition of the u-resultant and the property guaranteed by $\mathcal{C}_W$, the resulting polynomial is exactly $e \cdot \prod_{\boldsymbol{\alpha} \in W} (u_0 + u_1 \alpha_1)^{m_{\boldsymbol{\alpha}}}$, for some $e \in \mathbb{K}$ and positive integers $m_{\boldsymbol{\alpha}}$. Further setting $u_1 = -1$ and $u_0 = x_{r+1}$, the resulting polynomial, denoted A, is $e \cdot \prod_{\boldsymbol{\alpha} \in W} (x_{r+1} - \alpha_1)^{m_{\boldsymbol{\alpha}}}$. Since $\mathcal{C}_W$ lies in $\mathbb{F}(\mathbf{x})[\mathbf{u}]$, we can deduce that $e \in \mathbb{F}(\mathbf{x})$. The polynomial C defined in the statement of the lemma is therefore a primitive polynomial in $\mathbb{F}[x_1, \ldots, x_r][x_{r+1}]$ with roots α_1 for $\boldsymbol{\alpha} \in W$. The polynomial $R(x_{r+1})$ also satisfies this property. Therefore $\mathrm{V}(C) = \mathrm{V}(R(x_{r+1}))$. Combined with the fact that $\mathrm{V}(R(x_{r+1})) = \overline{\psi(V)}$ proved above, the proof is complete. □

In fact by factoring an arbitrary polynomial map through its graph, we can use the above lemma to compute the image of V under an arbitrary polynomial map to $\mathbb{A}^{r+1}$, as long as the map preserved the dimension of every irreducible component of V. Since the computation requires computing multivariate GCDs and squarefree parts, and since we have only developed the machinery for these operations in characteristic zero, the following lemma applies in a more restrictive setting than Lemma 5.1. Before we state and prove the lemma, we make a quick remark about Tseitin encodings, and show that we can work in the dense representation while solving this problem of computing the image.

Remark 5.2. Suppose C is a constant-free, weakly division-free arithmetic circuit of bit complexity s that computes polynomials $f_1, \ldots, f_m \in \mathbb{Q}[x_1, \ldots, x_n]$. Let $V \subset \mathbb{A}^n$ be the variety defined by $f_1, \ldots, f_m$. The Tseitin encoding of C is constructed as follows. First, we modify C to ensure that it has fan-in two. This increases the size and bit complexity of C by a polynomial factor. Next, we introduce one new variable w_v for each gate v in the circuit. We then construct the following set of equations, which we denote by S. For each addition gate v in the circuit, we add the equation $w_v - w_{v_1} - w_{v_2} = 0$ to our set S, where v_1, v_2 are the inputs to v. For each multiplication gate v in the circuit, we add the equation $w_v - (w_{v_1} \times w_{v_2}) = 0$ to our set S, where v_1, v_2 are the inputs to v. If v is an input gate with input x_i, then we add $w_v - x_i = 0$ to our set S, and if v is a constant gate with constant c, we add $x_v - c = 0$ to our set. For each output gate v, we also add $w_v = 0$ to our set S.

Suppose the circuit C had r gates, and we added a total of r equations to our set. Then S defines a variety $W \subset \mathbb{A}^{n+r}$, where the first n coordinates correspond to the variables $x_1, \ldots, x_n$. Consider the map $\phi : V \to W$ defined as follows. Given a point $\boldsymbol{\alpha} \in V$, construct a point $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathbb{A}^{n+r}$, by setting the w_v variables to the value obtained at gate v when the circuit C is evaluated at $\boldsymbol{\alpha}$. By the construction of the equations above, we see that $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ satisfies all the equations in S. An inverse to the map ϕ is given by projection to the first n coordinates. Once again, by the construction of the equations, it is easy to check that the projection of a point in W to the first n coordinates is a root of $f_1, \ldots, f_m$.

The main advantage of the Tseitin encoding is that the polynomials in the set S are all quadratic polynomials, and therefore can be expressed in the dense representation with a total bit complexity

that is only polynomially larger than s. For any questions regarding the variety V where the answer does not change under isomorphism, this allows us to work in the dense representation without loss of generality. An example of such a problem is deciding if V is empty, computing the dimension of V, or computing the size of V (if it is promised to be finite). This is what enables [Koi96; Koi97; AGS26] to work in the dense representation.

However, if we are deciding some property of V that is extrinsic, that is, that depends on how V is embedded in $\mathbb{A}^n$, we cannot always use the Tseitin encoding. For example, the Chow forms of the equidimensional components of V are not invariant under isomorphisms, and it is not clear how to compute these from the Chow forms of the equidimensional components of W. Consequently, most results in Section 4 worked in the circuit representation.

Consider now the problem of computing the image of a variety under a polynomial map. Suppose we have two circuits C_1 and C_2 computing polynomials $f_1, \dots, f_m$ and $h_1, \dots, h_p$, respectively. Let $\phi_{\mathbf{h}}$ be the map $\mathbb{A}^n \to \mathbb{A}^p$ with coordinate functions h_i. Suppose that $\mathrm{V}(f_1, \dots, f_m)$ is equidimensional of dimension $p-1$, and that the image of every irreducible component of $\mathrm{V}(f_1, \dots, f_m)$ under $\phi_{\mathbf{h}}$ has dimension $p-1$. In this case, we can construct the graph $\Gamma_{\mathbf{h}}$ of the map $\phi_{\mathbf{h}}$ restricted to $\mathrm{V}(f_1, \dots, f_m)$. This is a variety in $\mathbb{A}^{n+p}$, defined by the polynomials $f_1, \dots, f_m, y_1 - h_1, \dots, y_p - h_p$. The image of V under $\phi_{\mathbf{h}}$ is the same as the projection of $\Gamma_{\mathbf{h}}$ to the coordinates corresponding to the $\mathbf{y}$ variables.

Now the graph $\Gamma_{\mathbf{h}}$ is itself defined by equations computed by the circuits C_1 and C_2. We can then construct the Tseitin encodings of C_1 and C_2, obtaining a variety W that is isomorphic to $\Gamma_{\mathbf{h}}$ such that W is defined by quadratic polynomials. The equations for W are obtained from the circuits C_1, C_2 as defined above. Since the isomorphism $W \to \Gamma_{\mathbf{h}}$ is given by a projection, the image of W under the projection to the coordinates corresponding to $\mathbf{y}$ is the same as the image of $\Gamma_{\mathbf{h}}$ under the projection to the same coordinates. As a consequence, for the problem of computing the equation of the image of a variety under a polynomial map with the above guarantees, we can assume without loss of generality that the input is in the dense representation. ◊

Lemma 5.3. *There exists a family of boolean functions $\mathcal{G}^{\mathcal{IM}}$ with the following properties.*

- *The function $G^{\mathcal{IM}}$ takes as input collections of polynomials $f_1, \dots, f_m \in \mathbb{Q}[x_1, \dots, x_n]$ and $h_1, \dots, h_p \in \mathbb{Q}[x_1, \dots, x_n]$ in the dense representation. The function also takes as input $10(n+2)^2(m+p)$ integers, which we denote by $a_1, \dots, a_e$.*
- *The output of $G_s^{\mathcal{IM}}$ is a polynomial in the dense representation. If $V \coloneqq \mathrm{V}(f_1, \dots, f_m)$ is equidimensional of dimension $p-1$, and the image of every irreducible component of V under the map $\phi_{\mathbf{h}} : \mathbb{A}^n \to \mathbb{A}^p$ with coordinate functions $h_1, \dots, h_p$ has codimension 1, and the inputs $a_1, \dots, a_r$ are independently and uniformly sampled from a set of size b, then with probability at least $1 - 100n^{10}d^{n^{10}}/b$, where $d = \max(1, \max_i \deg f_i, \max_j \deg h_j)$, the polynomial computed is a $\mathbb{Z}$-multiple of the generator of the ideal of $\overline{\phi_{\mathbf{h}}(V)}$*
- *The language $L_{\mathcal{IM}}$ corresponding to $\mathcal{G}^{\mathcal{IM}}$ can be decided in CH.*

Proof. We start by describing the function $G^{\mathcal{IM}}$, which we denote by G for brevity. Let $g_1, \dots, g_c$ denote the set of polynomials $f_1, \dots, f_m, y_1 - h_1, \dots, y_p - h_p$. Our goal is to compute the image of $\mathrm{V}(g_1, \dots, g_c)$ under the projection to the coordinates corresponding to the $\mathbf{y}$ variables. In the rest of this proof, all homogenizations will be done by introducing a variable x_0, and only with respect to the variables $y_p, x_1, \dots, x_n$. Let d_i denote the degree of g_i in the variables $y_p, x_1, \dots, x_n$, and let d denote $\max_i d_i$. Let $P_1, \dots, P_{c'}$ denote the set of polynomials $\left\{x_j^{d-d_i} g_i^h\right\} \cup \left\{y_p^{d-d_i} g_i^h\right\}$.

For $1 \le i \le Q$, define $Q_{i,1} \coloneqq t \cdot x_i^d + \sum_k \alpha_{k,i} P_k$, where the coefficients $\alpha_{k,i}$ are the first few a_e's. Define $Q_{n+1,1} \coloneqq t \cdot y_p^d + \sum_k \alpha_{k,n+1} P_k$, where again the $\alpha_{k,n+1}$ are the next few a_e's. Let

$Q_{1,2}, \ldots, Q_{n+1,2}$ be another set of polynomials defined the same way, using the next few a_e's as coefficients. Let L denote the polynomial $u_0 x_0 + \cdots + u_n x_n + v y_p$, where $\mathbf{u}$ and v are new variables. For $i = 1, 2$, let R_i denote $\mathrm{TT}_t \operatorname{Res}(Q_{1,i}, \ldots, Q_{n+1,i}, L)$, where the resultant is computed with respect to $y_p, x_0, \ldots, x_n$. Let R denote the polynomial obtained by first applying Lemma 2.13 to R_1 and R_2 using the next few a_e's as the random inputs, and then applying Corollary 2.14 to the resulting polynomial, using the next few a_e's as the random inputs. By Lemma 4.7 we can deduce that as long as the a_e's are sampled uniformly, the product of those factors of R that depend on the variable u_0 are the u-resultant of $\mathrm{V}(g_1, \ldots, g_c)$ in $\overline{\mathbb{Q}(y_1, \ldots, y_{p-1})}^{n+1}$.

Let S_1 be the polynomial obtained by setting u_0 to the next a_e in R, and similarly S_2 be the polynomial obtained by setting u_0 to the next a_e in R. Let S_3 be the polynomial obtained by applying Lemma 2.13 to S_1 and S_2, as usual using the next few a_e's for the random inputs. Let S_4 be the polynomial obtained by using the multivariate polynomial division circuit Theorem 2.12 to divide R by S_3, and then setting u_0 to y_p, and v to -1, and $u_1, \ldots, u_n$ to 0. As long as all the a_e's are picked uniformly and independently, by Lemma 5.1 we can deduce that with high probability, the squarefree-part of the y_p-primitive part of polynomial S_4 is the generator of the ideal of $\overline{\phi_{\mathbf{h}}(V)}$. To compute the y_p-primitive part, we again define S_5 to be the polynomial obtained by setting y_p to the next a_e, define S_6 to be the polynomial obtained by applying Lemma 2.13 to S_5 and S_4, define S_7 to be the quotient when dividing S_4 by S_6, and finally setting S_8 to be the polynomial obtained by applying Corollary 2.14 to S_7.

The boolean function G is defined so that $G(f_1, \ldots, f_m, h_1, \ldots, h_p, a_1, \ldots, a_r) = S_8$. Over the course of the construction of G, we have also shown that it computes the image of the projection. That the language $L_{\mathcal{IM}}$ can be computed in CH is at this point a routine argument. □

5.2 Approximate polynomial satisfiability

In this subsection, we solve the APS problem (Definition 1.7) by reducing it to a special structured instance of the projection problem defined above. If the underlying field $\mathbb{F}$ is $\mathbb{Q}$, then Lemma 5.3 already allows us to solve the APS problem in CH. The goal of the rest of this section is to solve APS over a larger class of fields, for example when $\mathbb{F}$ is a finite field. To this end, we will reduce an instance of APS to a very structured instance of the projection problem. We will also crucially use the fact that solving APS only requires us to compute the constant term of the equation defining the projection. Essentially, we want to avoid the multivariate GCD computations that are used within the proof of Lemma 5.3, since the machinery to perform these is only developed in characteristic 0.

In the rest of this section, we will allow the input circuits to use constants, but the encoding of the circuit will include the bit complexity of the constants. For circuits over fields of the type $\mathbb{Q}(y_1, \ldots, y_k)$ and $\mathbb{F}_{p^a}(y_1, \ldots, y_k)$, we will assume that the constants on the wires are encoded in the dense representation. We use $|C|$ to denote the length of encoding the circuit C in binary. The Tseitin encoding of our circuits will be appropriately modified to account for these constants: for example, if gate w_v computes the sum of w_{v_1} and w_{v_2} with constants α, β on the wires, then the equation we add is $w_v - \alpha w_{v_1} - \beta w_{v_2} = 0$. Before we give the reduction, we will need a subroutine to compute transcendence degrees.

Lemma 5.4. *Let $\mathbb{F}$ be a field of the form $\mathbb{F}_{p^a}(y_1, \ldots, y_k)$. Given a circuit C computing $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$, the transcendence degree of $f_1, \ldots, f_m$ can be computed in $\mathsf{FP}^{\mathsf{CH}}$.*

Proof. We first show that the algebraic independence of $f_1, \ldots, f_m$ can be decided in CH. Let d be a bound on the maximum degrees of $f_1, \ldots, f_m$, such a bound can be obtained from C. If $m > n$ then the polynomials are always algebraically dependent, so we focus on the case $m \leq n$. Fix a set B in the coefficient subfield of $\mathbb{F}$ of size $n^3 d^{2n^2}$. If $p^a \leq n^3 d^{2n^2}$, then we pass to a field extension of

size at least $n^3 d^{2n^2}$ (see [AGS26, Lemma 2.13]). Pick $\alpha_1, \ldots, \alpha_m$ each independently and uniformly from B. We claim that with probability at least $1 - 1/n^2$, the polynomials $f_1 - \alpha_1, \ldots, f_m - \alpha_m$ are satisfiable if and only if $f_1, \ldots, f_m$ are algebraically independent.

Indeed if $f_1, \ldots, f_m$ are algebraically dependent, then the closure of the image of $\mathbb{A}^n$ under the map $\phi_{\mathbf{f}} = (f_1, \ldots, f_m)$ is a proper subvariety of $\mathbb{A}^m$ of degree at most d^m. Therefore, the probability that $(\alpha_1, \ldots, \alpha_m)$ lies in the image of $\phi_{\mathbf{f}}$, or equivalently that $f_1 - \alpha_1, \ldots, f_m - \alpha_m$ is satisfiable, is at most $d^m/|B|$.

Conversely, suppose $f_1, \ldots, f_m$ are algebraically independent. The key observation is that $\overline{\phi_{\mathbf{f}}(\mathbb{A}^n)} = \mathbb{A}^m$, therefore the set of points with nonempty fiber is dense. We control the degree of the bad set of the points that do not have any point in the fiber. To this end, consider the polynomials $f_1 - z_1, \ldots, f_m - z_m$, where $z_1, \ldots, z_m$ are new variables. Consider the linear system of equations over the field $\mathbb{F}(z)$ obtained by considering each $\mathbf{x}$ monomial in the identity $1 = (f_1 - z_1)g_1 + \cdots + (f_m - z_m)g_m$, where we treat each coefficient of each g_i as a variable, and restrict the g_i to have degrees at most d^m. Write this linear system as $Mu = v$, where M is the coefficient matrix, u is the vector of unknowns (corresponding to the coefficients of g), and b is the v is the vector with 1 in the entry corresponding to the constant term and 0 everywhere else. Let Δ be any maximal nonzero minor of the matrix M. As a polynomial in $z_1, \ldots, z_m$, it has degree at most nd^{2n^2}. Let r be the size of the submatrix to which Δ corresponds. Finally, let $\Delta_1, \ldots, \Delta_t$ be the minors of the augmented matrix $[M|v]$ of size $r + 1$.

For a general choice of elements $\gamma_1, \ldots, \gamma_m \in \mathbb{F}$, the specialization of Δ at $(\gamma_1, \ldots, \gamma_k)$ is nonzero. Further, for this general choice, $f_1 - \gamma_1, \ldots, f_m - \gamma_m$ is satisfiable, therefore by the effective Nullstellensatz [Jel05], the rank of the augmented matrix $[M|v]$ after specialization is the same as the rank of M after specialization. Specifically, this implies that $\Delta_1(\boldsymbol{\gamma}), \ldots, \Delta_t(\boldsymbol{\gamma}) = 0$, and since $\boldsymbol{\gamma}$ is general, we can deduce that $\Delta_1, \ldots, \Delta_t$ vanish identically. From these two facts and another application of the effective Nullstellensatz, we can deduce that for any point $\boldsymbol{\alpha} \in \mathbb{F}^m$, as long as $\Delta(\boldsymbol{\alpha}) \neq 0$, the system $f_1 - \alpha_1, \ldots, f_m - \alpha_m$ is satisfiable. If the coordinates of $\boldsymbol{\alpha}$ are picked independently from B, then the above happens with probability at least $1 - nd^{2n^2}/|B|$, which is at least $1 - 1/n^2$ as claimed.

Once $\alpha_1, \ldots, \alpha_m$ have been picked randomly, to verify if the fiber is empty or not, we can use the satisfiability algorithm of [AGS26]. To invoke this algorithm, we must switch to the dense representation. For this, we switch to the Tseitin encoding of the circuit C as described in Remark 5.2. Note that in the remark, we only described the Tseitin encoding for constant-free circuits, but the required changes to handle the case of circuits with constants are straightforward. We can now use the satisfiability algorithm [AGS26, Theorem 6.9] on this system, and decide if $f_1 - \alpha_1, \ldots, f_m - \alpha_m$ is satisfiable in CH.

Once we have the above algorithm for checking independence as a subroutine, the transcendence degree can be computed as follows. We start with $\mathcal{B} \coloneqq \varnothing$. For each i from 1 to m, we do the following: add the polynomial f_i to the set $\mathcal{B}$, and check if the elements of $\mathcal{B}$ are algebraically independent. If they are, then we move on to the next i. If they are not, then we remove f_i from $\mathcal{B}$ and move on to the next i. It is clear that the set $\mathcal{B}$ that we end up with at the end of this algorithm is a transcendence basis for $\{f_1, \ldots, f_m\}$, and therefore the size of $\mathcal{B}$ is the required transcendence degree. □

We now give the claimed reduction. Our reduction requires computation of the transcendence degree of the input equations.

Lemma 5.5. *Let $\mathbb{F}$ be one of the fields $\mathbb{F}_{p^a}, \mathbb{F}_{p^a}(t_1, \ldots, t_k)$, a number field $\mathbb{Q}[\alpha]$, or $\mathbb{Q}[\alpha](t_1, \ldots, t_k)$. There exists a randomized polynomial-time algorithm that takes as input an instance of* APS *over*

a field $\mathbb{F}$ in the form of an algebraic circuit C, along with the transcendence degree of the input polynomials, and returns a set of polynomials $g_1, \ldots, g_m \in \mathbb{K}[y_1, \ldots, y_{r+1}, x_1, \ldots, x_{m-1}]$ with the following properties.

- *The number of variables $r+m$, the number of polynomials m, and the heights of the coefficients of g_i are bounded by $\mathrm{poly}(|C|)$. Further, each g_i is has degree at most 2.*
- *If $\mathbb{F}$ has characteristic 0 then $\mathbb{K} = \mathbb{Q}$. If $\mathbb{F} = \mathbb{F}_{p^a}(t_1, \ldots, t_k)$ then $\mathbb{K} = \mathbb{F}_{p^b}(t_1, \ldots, t_k)$ with $b/a = \mathrm{poly}(|C|)$.*
- *$V \coloneqq \mathrm{V}(g_1, \ldots, g_m) \subset \mathbb{A}^{r+m}$ is an irreducible variety of dimension r.*
- *The projection of V onto the coordinates corresponding to $y_1, \ldots, y_r$ is dominant. The projection of V onto the coordinates corresponding to $y_1, \ldots, y_{r+1}$ has dimension r. Further, the polynomial that generates the ideal $\mathrm{rad}(g_1, \ldots, g_m) \cap \mathbb{F}[y_1, \ldots, y_{r+1}]$, which we denote by A, is such that the leading coefficient of A with respect to y_{r+1} lies in $\mathbb{F}$.*
- *The constant term of the polynomial A is zero if and only if the given input to* APS *is a YES instance, namely if and only if the given polynomials are approximately satisfiable.*

Proof. This reduction takes place in two steps. In the first step we transform the instance of APS into another instance of APS with some additional structure. We then reduce this to an instance of projection, and then further transform the instance of the projection problem to obtain the final structure.

Let $f_1, \ldots, f_a \in \mathbb{F}[u_1, \ldots, u_b]$ denote the polynomials computed by C, and let d be a bound on their maximum degree. Let r denote the transcendence degree of $f_1, \ldots, f_a$, equivalently the dimension of $\overline{\phi_{\mathbf{f}}(\mathbb{A}^b)}$. By assumption, the integer r is part of the input to the algorithm. For the rest of this argument, we will assume that the coefficient subfield of $\mathbb{F}$ is larger than $100bd^b$, by passing to a field extension if required (see for example [AGS26, Lemma 2.13]). Let B a finite subset of the coefficient subfield of $\mathbb{F}$ of size $100bd^b$.

Let $f'_1, \ldots, f'_{r+1}$ denote random linear combinations of $f_1, \ldots, f_a$, where each coefficient is picked uniformly and independently from B. By [GSS19, Theorem 17], the following two facts hold with probability at least $1 - (r+1)d^r/|B|$: the set $\{f'_1, \ldots, f'_{r+1}\}$ has transcendence degree exactly r, and further $f_1, \ldots, f_a$ are approximately satisfiable if and only if $f'_1, \ldots, f'_{r+1}$ are approximately satisfiable. With probability at least $1 - 2bd^b/|B|$, the defining equation of the variety $\overline{\phi_{\mathbf{f}'}(\mathbb{A}^b)}$ will also be such that its leading coefficient with respect to every variable is a scalar.

Next, we pick $b - r$ random linear polynomials $\ell_i \coloneqq b_{i,0} + \sum_{j=1}^{b} b_{i,j} u_j$ where each $b_{i,j}$ is picked independently and uniformly from B. Let H denote the linear subspace $\mathrm{V}(\ell_1, \ldots, \ell_{b-r})$. We claim that $\overline{\phi_{\mathbf{f}'}(H)} = \overline{\phi_{\mathbf{f}'}(\mathbb{A}^b)}$ holds with high probability. With probability at least $1 - b/|B|$, the polynomials $\ell_1, \ldots, \ell_{b-r}$ are linearly independent. We assume that this holds for the rest of the argument. Let $\boldsymbol{\alpha} \in \phi_{\mathbf{f}'}(\mathbb{A}^b)$ be any point such that the fiber $Y \coloneqq \phi^{-1}_{\mathbf{f}'}(\boldsymbol{\alpha})$ has dimension $b - r$. Such a point exists by the fiber dimension theorem and the fact that $\overline{\phi_{\mathbf{f}'}(\mathbb{A}^b)}$ is an irreducible variety of dimension r. The variety Y has degree at most d^{r+1} by Bézout's theorem. By Lemma 2.2, with probability at least $1 - 2bd^{r+1}/|B|$, the intersection $Y \cap H$ has dimension 0. We can now apply the fiber dimension theorem to the map $\phi_{\mathbf{f}'}|_H : H \to \mathbb{A}^{r+1}$. Since $\boldsymbol{\alpha}$ is a point in the image of this restricted map whose fiber has dimension 0, and since H has dimension r, we can deduce that $\overline{\phi_{\mathbf{f}'}(H)}$ has dimension r. Since $\overline{\phi_{\mathbf{f}'}(H)} \subseteq \overline{\phi_{\mathbf{f}'}(\mathbb{A}^b)}$ is a containment of irreducible varieties of the same dimension, we can deduce that these varieties are the same.

We now compute a linear map $\psi : \mathbb{A}^r \to \mathbb{A}^b$ such that $\psi(\mathbb{A}^r) = H$. This requires elementary linear algebra over $\mathbb{F}$. If ψ^* is the corresponding map of coordinate rings $\mathbb{F}[u_1, \ldots, u_b] \to \mathbb{F}[v_1, \ldots, v_r]$, then the polynomials $h_1 \coloneqq \psi^*(f'_1), \ldots, h_{r+1} \coloneqq \psi^*(f'_{r+1})$ are such that $\overline{\phi_{\mathbf{h}}(\mathbb{A}^r)} = \overline{\phi_{\mathbf{f}'}(\mathbb{A}^a)}$. Therefore, $(0, \ldots, 0) \in \overline{\phi_{\mathbf{h}}(\mathbb{A}^r)}$ if and only if $(0, \ldots, 0) \in \overline{\phi_{\mathbf{f}'}(\mathbb{A}^a)}$. Equivalently, $h_1, \ldots, h_{r+1}$ are approximately

satisfiable if and only if $f'_1, \ldots, f'_{r+1}$ are approximately satisfiable. We can thus deduce that $h_1, \ldots, h_{r+1}$ are approximately satisfiable if and only if $f_1, \ldots, f_a$ are approximately satisfiable. A union bound shows that if B has size at least $100bd^b$, then the above holds with probability at least $2/3$. Observe that from the circuit C, we can easily compute a circuit C' that computes the polynomials $h_1, \ldots, h_{r+1}$.

With this structured instance of APS at our disposal, we proceed to construct an instance of the projection problem. For this, we simply factor the map $\phi_{\mathbf{h}}$ through its graph. Specifically, we consider the variety $\Gamma_{\mathbf{h}} \subset \mathbb{A}^{2r+1}$ defined by the equations $y_1 - h_1(\mathbf{v}), \ldots, y_{r+1} - h_{r+1}(\mathbf{v})$. The graph of any morphism is isomorphic to the source, therefore $\Gamma_{\mathbf{h}} \cong \mathbb{A}^r$ is an irreducible variety of dimension r. Further, the projection of $\Gamma_{\mathbf{h}}$ onto the variables $y_1, \ldots, y_{r+1}$ is exactly $\phi_{\mathbf{h}}(\mathbb{A}^r)$. By the properties guaranteed above, we can deduce that the projection of $\Gamma_{\mathbf{h}}$ onto $y_1, \ldots, y_r$ is dominant, that the projection onto $y_1, \ldots, y_{r+1}$ is a hypersurface defined by a polynomial whose leading term with respect to y_{r+1} is a scalar, and that this polynomial has zero constant term if and only if the original instance $f_1, \ldots, f_a$ is approximately satisfiable. Therefore, we can solve the original instance of APS by computing any polynomial Q such that $\mathrm{rad}(Q) = \mathrm{rad}(y_1 - h_1(\mathbf{v}), \ldots, y_{r+1} - h_{r+1}(\mathbf{v})) \cap \mathbb{F}[y_1, \ldots, y_{r+1}]$, and checking if the constant term of Q vanishes. At this stage, the equations $y_i - h_i(\mathbf{v})$ are still given by algebraic circuits. We now further simplify this instance and reduce to the case where the defining equations are given by quadratic polynomials. This will allow us to work in the dense representation, as opposed to having to work in the circuit representation.

To reduce to this dense representation, we again use the Tseitin encoding. We repeat the construction of the encoding here, since we want to keep track of the number of variables and equations introduced. Given the circuit C', we first convert it into a circuit where every gate has fan-in at most 2. This increases the size by a polynomial factor. Let e denote the number of gates in the resulting circuit. For each gate c in the circuit, we introduce a variable x_c. We now construct a set of polynomials in the variables $y_1, \ldots, y_{r+1}, v_1, \ldots, v_r$ and x_c. If a gate c_i computes the sum of gates c_j and $c_{j'}$ with weights $\alpha, \beta \in \mathbb{F}$, we add the polynomial $x_{c_i} - \alpha x_{c_j} - \beta x_{c_{j'}}$ to our set of polynomials. We do the same for product gates. If c_i is an input gate corresponding to variable v_j, we add $x_{c_i} - v_j$ to our set of polynomials, and similarly if c_i is an output gate computing $\mathbf{f}'_j$ then we add $y_i - x_{c_j}$. Therefore, our set consists of a total of $e + r + 1$ polynomials in $e + 2r + 1$ variables. Let W denote the zero set of these polynomials. As in Remark 5.2, we have $W \cong \Gamma_{\mathbf{h}}$, and also that the projection of W onto $\mathbf{y}$ is the same as the projection of $\Gamma_{\mathbf{h}}$ onto $\mathbf{y}$.

This instance of projection from W onto $\mathbf{y}$ is the final output of our reduction. We rename the variables and indices and call the defining equations of W constructed above $g_1, \ldots, g_m$, and call the non $\mathbf{y}$ variables $x_1, \ldots, x_{m-1}$. The polynomials g_i by construction have the claimed degree and height bounds, and by the arguments in the previous paragraphs, the original input equations $f_1, \ldots, f_a$ are approximately satisfiable if and only if the equation defining the projection of W to the $\mathbf{y}$ variables has nonzero constant term. □

Now that we have reduced the instance of APS to a structured instance of projection, we show how this lets us solve the APS problem in CH. Note that the APS problem only requires us to decide if the constant term of the equation defining the projection is zero or not. We do not have to compute the constant term exactly, nor do we have to compute any other coefficient. This gives us two advantages that we will exploit. The first is that we can perform partial substitutions throughout the computation to simplify, as long as we ensure that zero/nonzeroness of the constant term remains unchanged. The second is that it suffices to compute the defining equation up to a radical, since this also does not affect the constant term. Further, since the variety whose projection we are computing is a complete intersection, we also compute the u-resultant of the limit subvariety using a single resultant calculation, thus avoiding a multivariate GCD calculation. Putting all these together, we

obtain the following.

Theorem 5.6. *Let $\mathbb{F}$ be one of the fields $\mathbb{F}_{p^a}, \mathbb{F}_{p^a}(t_1, \ldots, t_k)$, a number field $\mathbb{Q}[\alpha]$, or $\mathbb{Q}[\alpha](t_1, \ldots, t_k)$. Then* APS *over $\mathbb{F}$ lies in* CH*.*

Proof. Let C be the input to the APS instance. The circuit C computes the polynomials whose approximate satisfiability we must decide. We first compute the transcendence degree of the polynomials computed by C. If $\mathbb{F}$ has characteristic 0, then the transcendence degree can be computed in RP ([DGW09]). If $\mathbb{F}$ is a finite field, then the transcendence degree can be computed in $\mathsf{FP}^{\mathsf{PH}}$ ([GSS19]). Otherwise, the transcendence degree can be computed in $\mathsf{FP}^{\mathsf{CH}}$ (Lemma 5.4). We then invoke Lemma 5.5 on the circuit C, using the transcendence degree computed above. This gives us polynomials $g_1, \ldots, g_m \in \mathbb{F}[y_1, \ldots, y_{r+1}, x_1, \ldots, x_{m-1}]$. If the coefficient subfield of $\mathbb{F}$ has size less than $100(m+r)^2 2^{2(m+r)}$, we pass to a field extension of size at least $100(m+r)^2 2^{2(m+r)}$ (see [AGS26, Lemma 2.13]). We assume for the rest of the proof that the coefficient subfield is larger than this number, and we fix a subset B of the coefficient subfield $\mathbb{F}$ of size $100(m+r)^2 2^{2(m+r)}$.

Let $V \subset \mathbb{A}^{m+r}$ denote the zero set of $g_1, \ldots, g_m$. By Lemma 5.5, we know that V has dimension r. Our goal is to decide if the constant term of the defining equation of the projection of V onto the variables $y_1, \ldots, y_{r+1}$ is zero or not. We know from the reduction also that this defining equation is monic in y_{r+1}.

Following Lemma 5.1, we must first compute the u-resultant of $g_1, \ldots, g_m$, treated as polynomials in $\mathbb{L}[y_{r+1}, x_1, \ldots, x_{m-1}]$, where $\mathbb{L} \coloneqq \overline{\mathbb{F}(y_1, \ldots, y_r)}$. In $\mathbb{A}^m_{\mathbb{L}}$, the zero set of $g_1, \ldots, g_m$ is zero dimensional. Consequently, we can directly apply the method of generalized characteristic polynomials to $g_1, \ldots, g_m$ as follows. We define $G_i \coloneqq g_i^h + t \cdot x_i^{\deg g_i}$ for $1 \le i \le m-1$, and define $G_m \coloneqq g_m^h + t \cdot y_{r+1}^{\deg g_m}$, where the degree is computed only with respect to the variables $x_1, \ldots, x_{m-1}, y_{r+1}$, and we homogenize by introducing a new variable z. We define $L \coloneqq u_0 z + v y_{r+1} + \sum_{i=1}^{m-1} u_i x_i$, where $u_0, \ldots, u_{m-1}, v$ are new variables. Define $R \coloneqq \mathrm{TT}_t \operatorname{Res}(G_1, \ldots, G_m, L)$. By [Ier89, Lemma 2.6], we can deduce the following about the polynomial R: in the ring $\mathbb{L}[y_{r+1}, x_1, \ldots, x_{m-1}]$, the squarefree part of R is a $\mathbb{L}$-multiple of the u-resultant of a limit variety $\lim_{t \to 0} \mathrm{V}^p(g_1^h, \ldots, g_m^h)$. Specifically, if we consider the product of those factors of R that do not depend on u_0, then the squarefree part of this product in $\mathbb{L}[y_{r+1}, x_1, \ldots, x_{m-1}]$ is a $\mathbb{L}$-multiple of the u-resultant of $g_1, \ldots, g_m$.

Suppose $R = R_1 R_2$, where R_1 is the product of those factors of R that do not depend on u_0, and R_2 is the product of the factors that depend on u_0. Let R_3 be the polynomial obtained by specializing R_2 at $u_0 = y_{r+1}$ and $v = -1$ and $u_1, \ldots, u_{m-1} = 0$. The polynomial R_3 lies in $\mathbb{F}[y_1, \ldots, y_{r+1}]$. Suppose $R_3 = R_4 R_5$, where R_4 is the product of those factors of R_3 that depend on y_{r+1}, and R_5 is the product of factors that do not. By Lemma 5.1, $\mathrm{V}(R_4)$ is the closure of the image of V under the projection to the $\mathbf{y}$ variables. Our assumptions also ensure that after rescaling R_4 and R_5, we can assume that the polynomial R_4 is monic in the variable y_{r+1}.

As described above, we will apply partial substitutions when carrying out the above computation. For this, it is important to study the factors of R_2 more closely. Let $S \in \mathbb{F}[y_1, \ldots, y_r, u_0, \ldots, u_{m-1}, v]$ be an irreducible factor of R_2. We can uniquely write S as $S = S_1 + (v-1)S_2 + S_4 S_5$, with the following properties. The polynomial S_1 lies in the ideal generated by $u_1, \ldots, u_{m-1}$, and none of S_2, S_4, S_5 depend on $u_1, \ldots, u_{m-1}$. The polynomial S_2 lies in $\mathbb{F}[u_0, y_1, \ldots, y_r, v]$, and none of S_4, S_5 depend on v. The polynomial S_5 lies in $\mathbb{F}[y_1, \ldots, y_r]$, and finally, every factor of $S_4 \in \mathbb{F}[y_1, \ldots, y_r, u_0]$ depends on the variable u_0. It is easy to see that the polynomial R_4 described above is exactly $\prod_S S_4$, with the variable u_0 renamed to y_{r+1}. Here, the product is over all the irreducible factors of R_2. Since R_4 is monic in y_{r+1}, each of the S_4 is monic in u_0. This will be crucial later on in the proof.

Pick $\alpha_1, \ldots, \alpha_{m-1}$ and $\beta_1, \ldots, \beta_r$ uniformly and independently from the set $B \subset \mathbb{F}$. Define P to be the specialization of R at $y_1 = \beta_1 p, \ldots, y_r = \beta_r p$ and $u_1 = \alpha_1 q, \ldots, u_{m-1} = \alpha_{m-1} q$, where

p, q are new variables. We have $P = R_1(p, q, v)R_2(u_0, p, q, v)$. We claim that the constant term of $\mathrm{TT}_p \mathrm{TT}_{v-1} \mathrm{TT}_q P$ is zero if and only if the constant term of R_4 is zero.

Since both substitutions and trailing term operations commute with products, we show the above claim by considering the factors of P. First consider $R_1(p, q, v)$. Since the α_i, β_i are picked at random, with high probability $R_1(p, q, v) \neq 0$. Therefore, $\mathrm{TT}_p \mathrm{TT}_{v-1} \mathrm{TT}_q R_1(p, q, v)$ is a nonzero constant, and does not affect our claim.

We now study $R_2(u_0, p, q, v)$. Fix a factor S of R_2. Writing $S = S_1 + (v-1)S_2 + S_4S_5$ as described above, the image of S under the substitution, denoted by S', is $S' \coloneqq q \cdot S_1'(u_0, p, q, v) + (v-1)S_2'(u_0, p, v) + S_4'(u_0, p)S_5'(p)$, where S_1', S_2', S_4', S_5' are obtained by specializing S_1, S_2, S_4, S_5 respectively. We thus see that $\mathrm{TT}_q S' = (v-1)S_2' + S_4'S_5'$, and consequently $\mathrm{TT}_{v-1} \mathrm{TT}_q S' = S_4'S_5'$. Finally, with high probability, S_4' and S_5' are nonzero, since S_4 and S_5 are always nonzero, and $\mathrm{TT}_p S_5'$ is always a nonzero constant. Therefore $\mathrm{TT}_p \mathrm{TT}_{v-1} \mathrm{TT}_q S'$ is a nonzero scalar multiple of $\mathrm{TT}_p S_4'$. Since S_4 is monic in u_0, every factor of S_4' is bivariate polynomial that is monic in u_0. Consequently, $\mathrm{TT}_p S_4'$ is the product of the constant terms of the factors of S_4' written as polynomials in p with coefficients in $\mathbb{F}[u_0]$. This is exactly the polynomial obtained by setting $y_1, \ldots, y_r$ to 0 in S_4. Therefore, the constant term of $\mathrm{TT}_p S_4'$ is zero if and only if the constant term of S_4 is zero. Taking a product over all the factors, we see that the constant term of $\mathrm{TT}_p \mathrm{TT}_{v-1} \mathrm{TT}_q R_2(u_0, p, q, v)$ is nonzero if and only if the constant term of R_4 is nonzero. By a union bound, all the above high probability events hold with probability at least $2/3$.

Finally, we show how the above short-circuited computation can be carried out in CH. Starting with the equations $g_1, \ldots, g_m$, we compute the polynomials $G_1, \ldots, G_m$ described above, and the polynomial $u_0 z + v y_{r+1} + \sum_{i=1}^{m-1} u_i x_i$, all in the dense representation. We replace every y_i by $\beta_i p$ for $1 \leq i \leq r$ and every u_i by $\alpha_i q$ for $1 \leq i \leq m-1$. This can be done in polynomial time in the dense representation. By [AGS26, Theorem 6.7], we can compute in CH the coefficients of the multivariate resultant of the above polynomials, treated as forms in the variables $x_1, \ldots, x_{m-1}, y_{r+1}$. This resultant is exactly the polynomial P described above. [4]

Next, we can nondeterministically guess the degree of the trailing term with respect to q in P and verify all smaller monomials in q have zero coefficient. This allows us to compute the coefficients of $\mathrm{TT}_q P$ in CH. To compute the coefficient of TT_{v-1}, we again nondeterministically guess the valuation of $\mathrm{TT}_q P$ with respect to $v-1$. To check that our guess is correct, for each smaller valuation, we use the circuits for polynomial division (Theorem 2.12) along with Lemma 2.22 to divide $\mathrm{TT}_q P$ by the appropriate power of $v-1$ and verify that the remainder is 0. This task can be carried out in CH. To compute $\mathrm{TT}_p \mathrm{TT}_{v-1} \mathrm{TT}_q P$, we simply repeat the above procedure. Finally, all that remains is to check if the constant term of the resulting polynomial is 0, which can be performed in CH. □

References

[ABKM09] Eric Allender, Peter Bürgisser, Johan Kjeldgaard-Pedersen, and Peter Bro Miltersen. "On the Complexity of Numerical Analysis". In: *SIAM Journal on Computing* 38.5 (2009), pp. 1987–2006. DOI: 10.1137/070697926 (cit. on pp. 19, 20).

[4] Note that the reduction to the dense representation is necessary to invoke the results of [AGS26] directly. The previous sections of this article discuss how the coefficients of the resultant of polynomials in the circuit representation can also be computed in CH, but those results are only presented in the characteristic zero case, and do not apply (as presented) in finite fields.

[AGS26] Robert Andrews, Abhibhav Garg, and Éric Schost. *Hilbert's Nullstellensatz is in the Counting Hierarchy*. 2026. arXiv: 2602.17904 [cs.CC] (cit. on pp. 1, 2, 5, 12–16, 18–21, 34, 44, 46, 47, 49, 50).

[AHPS26] Sanyam Agarwal, Archit Hari, Anurag Pandey, and Himanshu Shukla. *Approximate Polynomial Satisfiability and Integral Closure Membership in the Counting Hierarchy*. 2026. arXiv: 2610.42138 [cs.CC] (cit. on p. 8).

[AY83] L. A. Aizenberg and A. P. Yuzhakov. *Integral Representations and Residues in Multidimensional Complex Analysis*. Vol. 58. Translations of Mathematical Monographs. Providence, R.I.: American Mathematical Society, 1983. ISBN: 0821815504 (cit. on p. 17).

[BC06] Peter Bürgisser and Felipe Cucker. "Counting complexity classes for numeric computations II: Algebraic and semialgebraic sets". In: *Journal of Complexity* 22.2 (2006), pp. 147–191. ISSN: 0885-064X. DOI: https://doi.org/10.1016/j.jco.2005.11.001 (cit. on pp. 1, 2).

[BKR+26] Somnath Bhattacharjee, Mrinal Kumar, Shanthanu S. Rai, Varun Ramanathan, Ramprasad Saptharishi, and Shubhangi Saraf. "Closure under Factorization from a Result of Furstenberg". In: *STOC*. ACM, 2026, pp. 174–185. DOI: 10.1145/3798129.3800738 (cit. on p. 17).

[BS09] Peter Bürgisser and Peter Scheiblechner. "On the complexity of counting components of algebraic varieties". In: *Journal of Symbolic Computation* 44.9 (2009), pp. 1114–1136 (cit. on pp. 2, 3).

[BSTW26] Nikhil Balaji, Mahsa Shirmohammadi, Sébastien Tavenas, and James Worrell. *Approximate Polynomial Satisfiability is in the Counting Hierarchy*. 2026. arXiv: 2610.00644 [cs.CC] (cit. on p. 7).

[Can90] John Canny. "Generalised characteristic polynomials". In: *Journal of Symbolic Computation* 9.3 (1990). Computational algebraic complexity editorial, pp. 241–250. ISSN: 0747-7171. DOI: https://doi.org/10.1016/S0747-7171(08)80012-0 (cit. on pp. 1, 5, 6).

[CG83] AL Chistov and D Yu Grigoriev. *Subexponential time solving systems of algebraic equations*. Tech. rep. LOMI preprint E-9-83, E-10-83, Steklov Institute, Leningrad, 1983 (cit. on p. 2).

[Chi86] AL Chistov. "Algorithm of polynomial complexity for factoring polynomials and finding the components of varieties in subexponential time". In: *Journal of Soviet Mathematics* 34.4 (1986), pp. 1838–1882 (cit. on p. 2).

[CLO05] David A. Cox, John Little, and Donal O'Shea. *Using Algebraic Geometry*. 2nd ed. Springer New York, NY, 2005. DOI: 10.1007/b138611 (cit. on p. 42).

[Csa76] L. Csanky. "Fast Parallel Matrix Inversion Algorithms". In: *SIAM Journal on Computing* 5.4 (1976), pp. 618–623. DOI: 10.1137/0205040 (cit. on p. 1).

[CT26] Dean Cureton and Jesse Thorner. *A quasi-Riemann hypothesis for Dedekind zeta functions*. Hexagon preprint hexagon:2610.00200v2. Contributors: Dean Cureton; Jesse Thorner. 2026 (cit. on p. 1).

[DGW09] Zeev Dvir, Ariel Gabizon, and Avi Wigderson. "Extractors And Rank Extractors For Polynomial Sources". In: *computational complexity* 18.1 (2009), pp. 1–58. DOI: 10.1007/s00037-009-0258-4 (cit. on p. 49).

[Ebe89] Wayne Eberly. "Very Fast Parallel Polynomial Arithmetic". In: *SIAM Journal on Computing* 18.5 (1989), pp. 955–976. DOI: 10.1137/0218066 (cit. on p. 14).

[Gao03] Shuhong Gao. "Factoring multivariate polynomials via partial differential equations". In: 72.242 (2003). ISSN: 0025-5718 (cit. on p. 16).

[GH91] Marc Giusti and Joos Heintz. "Algorithmes–disons rapides–pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles". In: *Effective Methods in Algebraic Geometry*. Springer. 1991, pp. 169–194 (cit. on pp. 2, 7).

[GHMMP98] M. Giusti, J. Heintz, J.-E. Morais, J. Morgenstern, and L.-M. Pardo. "Straight-line programs in geometric elimination theory". In: *Journal of Pure and Applied Algebra* 124 (1998), pp. 101–146 (cit. on pp. 7, 22).

[GHMP95] M. Giusti, J. Heintz, J.-E. Morais, and L.-M. Pardo. "When polynomial equation systems can be solved fast?" In: *AAECC-11*. Vol. 948. LNCS. Springer, 1995, pp. 205–231 (cit. on pp. 2, 7, 22).

[Gri86] Dima Grigoriev. "Factorization of polynomials over a finite field and the solution of systems of algebraic equations". In: *Journal of Soviet Mathematics* (1986) (cit. on p. 2).

[Gri87] D. Yu. Grigoriev. "Computational complexity in polynomial algebra". In: *Proceedings of the International Congress of Mathematicians (Berkeley, 1986)*. Vol. 2. Providence, RI: American Mathematical Society, 1987, pp. 1452–1460 (cit. on p. 22).

[GSS19] Zeyu Guo, Nitin Saxena, and Amit Sinhababu. "Algebraic Dependencies and PSPACE Algorithms in Approximative Complexity over Any Field". In: *Theory of Computing* 15.16 (2019), pp. 1–30. DOI: 10.4086/toc.2019.v015a016 (cit. on pp. 4, 47, 49).

[GTZ88] Patrizia Gianni, Barry Trager, and Gail Zacharias. "Gröbner bases and primary decomposition of polynomial ideals". In: *Journal of Symbolic Computation* 6.2-3 (1988), pp. 149–167 (cit. on p. 1).

[HAM02] William Hesse, Eric Allender, and David A. Mix Barrington. "Uniform constant-depth threshold circuits for division and iterated multiplication". In: *Journal of Computer and System Sciences* 65.4 (2002). Special Issue on Complexity 2001, pp. 695–716. ISSN: 0022-0000. DOI: https://doi.org/10.1016/S0022-0000(02)00025-9 (cit. on p. 14).

[Hei83] J. Heintz. "Definability and fast quantifier elimination in algebraically closed fields". In: *Theor. Comput. Sci.* 24 (1983), pp. 239–277. DOI: 10.1016/0304-3975(83)90002-6 (cit. on pp. 9, 10, 23, 24).

[Her26] Grete Hermann. "Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. (Unter Benutzung nachgelassener Sätze von K. Hentzelt)". In: *Mathematische Annalen* 95 (1926), pp. 736–788. DOI: 10.1007/BF01206635 (cit. on p. 1).

[Ier89] Doug Ierardi. "Quantifier Elimination in the Theory of an Algebraically-closed Field". In: *Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC 1989)*. Ed. by David S. Johnson. ACM, 1989, pp. 138–147. DOI: 10.1145/73007.73020 (cit. on pp. 1, 5, 6, 28, 49).

[IM83] Oscar H. Ibarra and Shlomo Moran. "Probabilistic Algorithms for Deciding Equivalence of Straight-Line Programs". In: *J. ACM* 30.1 (1983), pp. 217–228 (cit. on p. 40).

[Jel05] Zbigniew Jelonek. "On the effective Nullstellensatz". In: *Invent. Math.* 162.1 (2005), pp. 1–17. DOI: 10.1007/s00222-004-0434-8 (cit. on pp. 1, 46).

[JKSS04] Gabriela Jeronimo, Teresa Krick, Juan Sabia, and Martin Sombra. "The Computational Complexity of the Chow Form". In: *Foundations of Computational Mathematics* 4.1 (2004), pp. 41–117 (cit. on pp. 2, 7, 27, 33).

[Jou91] Jean-Pierre Jouanolou. "Le formalisme du résultant". In: *Adv. Math.* 90.2 (1991), pp. 117–263. ISSN: 0001-8708,1090-2082. DOI: 10.1016/0001-8708(91)90031-2 (cit. on p. 10).

[Kal95] E. Kaltofen. "Effective Noether Irreducibility Forms and Applications". In: *Journal of Computer and System Sciences* 50.2 (1995), pp. 274–295. ISSN: 0022-0000. DOI: https://doi.org/10.1006/jcss.1995.1023 (cit. on p. 16).

[Koi96] Pascal Koiran. "Hilbert's Nullstellensatz is in the polynomial hierarchy". In: *Journal of complexity* 12.4 (1996), pp. 273–286. DOI: https://doi.org/10.1006/jcom.1996.0019 (cit. on pp. 1, 44).

[Koi97] Pascal Koiran. "Randomized and deterministic algorithms for the dimension of algebraic varieties". In: *Proceedings of the 38th Annual IEEE Symposium on Foundations of Computer Science (FOCS 1997)*. IEEE Computer Society, 1997, pp. 36–45. ISBN: 0818681977. DOI: 10.1109/SFCS.1997.646091 (cit. on pp. 1, 44).

[KP96] T. Krick and L. M. Pardo. "A computational method for diophantine approximation". In: *Algorithms in Algebraic Geometry and Applications*. Ed. by Laureano González-Vega and Tomás Recio. Basel: Birkhäuser Basel, 1996, pp. 193–253. ISBN: 978-3-0348-9104-2 (cit. on p. 9).

[KPS01] Teresa Krick, Luis Miguel Pardo, and Martín Sombra. "Sharp estimates for the arithmetic Nullstellensatz". In: *Duke Mathematical Journal* 109.3 (2001), pp. 521–598. DOI: 10.1215/S0012-7094-01-10934-4 (cit. on p. 21).

[Las05] Emanuel Lasker. "Zur Theorie der moduln und Ideale". In: *Mathematische Annalen* 60.1 (1905), pp. 20–116 (cit. on p. 1).

[Lec00] Grégoire Lecerf. "Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions". In: *Proceedings of the 2000 international symposium on Symbolic and algebraic computation*. 2000, pp. 209–216 (cit. on pp. 2, 7).

[MV05] Peter Bro Miltersen and N. V. Vinodchandran. "Derandomizing Arthur-Merlin Games using Hitting Sets". In: *Comput. Complex.* 14.3 (2005), pp. 256–279. DOI: 10.1007/S00037-005-0197-7 (cit. on p. 1).

[Ope26] OpenAI. *The Quasi-Riemann Hypothesis: A Zero-Free Half-Plane* $\mathrm{Re}(s) > 7/8$. OpenAI Math Release preprint OAI:The-Quasi-Riemann-Hypothesis-September-30-2026. 2026 (cit. on p. 1).

[Phi86] Patrice Philippon. "Critères pour l'indépendance algébrique". In: *Inst. Hautes Études Sci. Publ. Math.* 64 (1986), pp. 5–52. ISSN: 0073-8301,1618-1913. DOI: 10.1007/BF02699191 (cit. on p. 21).

[RT92] John H. Reif and Stephen R. Tate. "On threshold circuits and polynomial computation". In: *SIAM J. Comput.* 21.5 (1992), pp. 896–908. ISSN: 0097-5397. DOI: 10.1137/0221053 (cit. on p. 14).

[Sch03] Éric Schost. "Computing parametric geometric resolutions". In: *Applicable Algebra in Engineering, Communication and Computing* 13.5 (2003), pp. 349–393. DOI: https://doi.org/10.1007/s00200-002-0109-x (cit. on p. 42).

[Sch07] Peter Scheiblechner. "On the complexity of deciding connectedness and computing Betti numbers of a complex algebraic variety". In: *Journal of Complexity* 23.3 (2007), pp. 359–379 (cit. on p. 3).

[Sch10] Peter Scheiblechner. "On a generalization of Stickelberger's theorem". In: *Journal of Symbolic Computation* 45.12 (2010), pp. 1459–1470 (cit. on pp. 2–4).

[Sei74] A. Seidenberg. "Constructions in algebra". In: *Trans. Amer. Math. Soc.* 197 (1974), pp. 273–313. ISSN: 0002-9947,1088-6850. DOI: 10.2307/1996938 (cit. on p. 1).

[Sha94] Igor Rostislavovich Shafarevich. *Basic algebraic geometry 2*. Springer, 1994. DOI: 10.1007/978-3-642-38010-5 (cit. on pp. 23, 29–31).

[Sta26] The Stacks project authors. *The Stacks project*. https://stacks.math.columbia.edu. 2026 (cit. on p. 10).

[Vol99] Heribert Vollmer. *Introduction to circuit complexity: a uniform approach*. Springer Science & Business Media, 1999. DOI: doi.org/10.1007/978-3-662-03927-4 (cit. on p. 11).

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il