Electronic Colloquium on Computational Complexity, Report No. 299 (2026)

Approximate Polynomial Satisfiability and Integral Closure Membership in the Counting Hierarchy

Sanyam Agarwal* Archit Hari† Anurag Pandey‡ Himanshu Shukla§

Abstract

Andrews, Garg, and Schost (FOCS 2026) recently, in a breakthrough result, placed Hilbert's Nullstellensatz (HN) in the Counting Hierarchy (CH) using constant-depth circuits for multivariate resultants. While HN deals with exact polynomial satisfiability, Guo, Saxena, and Sinhababu (CCC 2018; Theory of Computing 2019) introduced approximate polynomial satisfiability (APS) as a natural approximative analogue of polynomial system satisfiability. They proved its NP-hardness and a PSPACE upper bound, and used APS to construct hitting sets for $\overline{\mathsf{VP}}$ in polynomial space, substantially narrowing the GCT chasm in geometric complexity theory.

We place APS in the Counting Hierarchy for rational polynomials given by arithmetic circuits. Our proof combines Noether normalization with a geometric restriction on how points in the image of a polynomial map approach the origin, reducing APS to a test on multivariate resultants which allows solvability in CH. It complements the independent and concurrent proofs of Balaji, Shirmohammadi, Tavenas, and Worrell, and Andrews, Garg, Oliveira, and Schost. Moreover, we also place integral closure membership testing in the Counting Hierarchy. Here, the question is whether a given polynomial f is integral over $\mathbb{C}[f_1, \ldots, f_m]$. Our approach uses a global annihilator criterion and an effective degree bound to reduce non-integrality to APS in polynomial time. In fact, we show that the reduction holds both ways, and Integral Closure Membership Testing is equivalent to APS under polynomial-time reductions.

*Universität des Saarlandes, Saarbrücken, Germany. agarwal@cs.uni-saarland.de
†Indian Institute of Technology Delhi, India. mt1240231@iitd.ac.in
‡Universität des Saarlandes, Saarbrücken, Germany. apandey@cs.uni-saarland.de
§Universität Regensburg, Germany. hshukla.math04@gmail.com

ISSN 1433-8092

1 Introduction

Deciding whether a system of polynomial equations has a complex solution is a central problem in algebraic complexity. This decision problem, usually called Hilbert's Nullstellensatz (HN), is NP-hard and has long been known to lie in PSPACE [Can88]. Koiran placed it in AM under the generalized Riemann hypothesis [Koi96]. The recent breakthrough of Andrews, Garg, and Schost gives an unconditional Counting Hierarchy upper bound [AGS26]. Their uniform constant-depth circuits for multivariate resultants extend the line of work on shallow algebraic computation developed by Andrews and Wigderson for univariate resultants and related linear-algebra problems [AW24].

Guo, Saxena, and Sinhababu [GSS18, GSS19] introduced *approximate polynomial satisfiability* (APS) as a natural approximative analogue of polynomial system satisfiability. They established algebraic and geometric characterizations of APS, proved its NP-hardness, and gave a PSPACE algorithm. Not only that, they also showed an equivalence of non-existence of APS to the system of polynomials having an annihilator with a non-zero constant term.

Intuitively, APS allows the input coordinates to vary, and even become unbounded, provided that all output values tend to zero. For example, the system

$$f_1(x, y) = x, \qquad f_2(x, y) = xy - 1 \tag{1.1}$$

has no exact solution, but the substitution $(x, y) = (t, t^{-1})$ makes its outputs $(t, 0)$ tend to the origin as t approaches 0. Formally, for a polynomial map $F = (f_1, \ldots, f_m) : \mathbb{C}^n \to \mathbb{C}^m$, the decision problem APS asks whether origin lies in the Zariski closure $Y := \overline{F(\mathbb{C}^n)}$ of the image of the polynomial map. In other words, APS asks whether $0 \in Y$. Note that over $\mathbb{C}$, the Euclidean and Zariski closures of this constructible image coincide [Mum95, Chapter 1].

Problem 1.1 (Approximate polynomial satisfiability)**.** Given arithmetic circuits over $\mathbb{Q}$ computing $F = (f_1, \ldots, f_m) \in \mathbb{Q}[x_1, \ldots, x_n]^m$, decide whether $0 \in \overline{F(\mathbb{C}^n)}$.

Moving from an image to its closure is fundamental in border complexity: it permits algebraic objects (eg: polynomials, tensors) to be represented as limits of "simpler" ones. Border rank of tensors is a basic example [BCS97, Lan12]; bounds on the order of such approximations go back to Lehmkuhl and Lickteig [LL89]. Guo, Saxena, and Sinhababu showed that APS also supplies an algorithmic route to problems in geometric complexity theory (GCT). In particular, they used it to construct polynomial-size hitting sets for $\overline{\mathsf{VP}}$ in polynomial space [GSS19]. Here $\overline{\mathsf{VP}}$ consists of polynomial families of polynomially bounded degree approximable by polynomial-size arithmetic circuits. A hitting set must detect every nonzero polynomial in this closure, including those obtained only by approximation. Through Mulmuley's connection between hitting sets and effective Noether normalization [Mul17], the construction narrows the GCT chasm: it replaces the EXPSPACE bound for these constructions by a PSPACE bound. With the recent improvement in the complexity of HN, it begs the question whether the complexity of APS can also be improved in the same way? Our first result gives an affirmative answer for polynomials input as arithmetic circuits with coefficients from $\mathbb{Q}$.

Our second result concerns integral closure, a basic construction in commutative algebra and algebraic geometry [AM69, Chapter 5]. Given a polynomial f and a finitely generated subalgebra $A \coloneqq \mathbb{C}[f_1, \ldots, f_m]$, we ask whether f satisfies a monic equation over A. Formally, we ask the following.

Problem 1.2 (Integral closure membership)**.** Given arithmetic circuits over $\mathbb{Q}$ computing polynomials $f, f_1, \ldots, f_m \in \mathbb{Q}[x_1, \ldots, x_n]$, decide whether f is integral over $A = \mathbb{C}[f_1, \ldots, f_m]$. In other words, we want to test whether there exists $r \in \mathbb{Z}_{>0}$ and $a_0, \ldots, a_{r-1} \in A$, such that $f^r + f^{r-1}a_{r-1} + \ldots + fa_1 + a_0 = 0$.

EXPSPACE upper bounds for the general integral closure testing are well-known through Gröbner Bases computations [DJ97]. However, we show that deciding integrality over polynomial subalgebras can be done much more efficiently than these worst-case exponential space bounds. In particular, we also put this problem in CH by reducing it to an instance of APS.

1.1 Our Contributions

The motivation for our work comes from two related recent results: the use of homogeneous multivariate resultants by Andrews, Garg, and Schost [AGS26] to put the decision problem of Hilbert's Nullstellensatz in the Counting Hierarchy, and the Strong Approximative Nullstellensatz by Agarwal, Dutta, Pandey, and Shukla [ADPS26] which showed that integral closure testing over a localized subring of a polynomial algebra is in PSPACE. Knowing HN $\in$ CH naturally leads to the question whether we can improve the PSPACE upper bound for APS in the same way, also posed as an open problem in [ADPS26]. Our first main result answers this question positively.

Theorem 1.3. *Approximate polynomial satisfiability (*APS*) belongs to the Counting Hierarchy.*

Input polynomials are represented by arithmetic circuits over $\mathbb{Q}$, with binary rational constants. Division gates are allowed, under the promise that every divisor is nonzero as a rational function and that every output represents a polynomial. Complexity statements use the ordinary Turing model and binary encodings of rational coefficients.

Remark 1.4 (Sparse representation)**.** Our results also apply to polynomials given in sparse representation, with exponents encoded in binary. Indeed, repeated squaring converts such inputs into division-free arithmetic circuits in time polynomial in the sparse input size.

Remark 1.5 (Division Gates)**.** Note that the proof also holds if circuits of input polynomials f_i have division gates. If degree of each f_i is polynomial in input length, then we can use [Str73] to remove these division gates with only a polynomial blowup. On the other hand, even if the degree of f_i were exponential in the input description, then writing each $f_i = \frac{P_i}{Q}$, it is easy to see that the system $F = (f_1(x), \ldots, f_m(x))$ has an APS if and only if the system $G = (uP_1(x), \ldots, uP_m(x), uQ(x) - 1)$ has an APS, where u is a new variable.

Remark 1.6 (Coefficients from other fields)**.** Theorem 1.3 also holds for arithmetic circuits over number fields and finite fields, with image closure taken over the algebraic closure of the coefficient field, see Remark 6.7. For simplicity of exposition, throughout this work, we assume that the input polynomials have rational coefficients.

Several standard applications of APS consequently inherit improved upper bounds. Below, k is any of the coefficient fields covered above, $K = \overline{k}$, and vectors and tensors are given by their full coordinate lists.

Corollary 1.7. *Theorem 1.3 has the following consequences.*

(i) ***Tensor border rank.*** *Given a tensor over k and an integer r encoded in binary, deciding whether its border rank over K is at most r belongs to* CH*.*

(ii) ***Orbit-closure problems.*** *For rational linear actions of products of general and special linear groups, given by arithmetic circuits in explicit matrix coordinates, deciding*

$$w \in \overline{G \cdot v}, \qquad \textit{equivalently,} \qquad \overline{G \cdot w} \subseteq \overline{G \cdot v},$$

belongs to CH*. This includes null-cone membership, obtained by taking $w = 0$.*

(iii) ***Hitting sets for*** $\overline{\mathsf{VP}}$***.*** *Given n, s, d in unary, a hitting set of size* $\mathrm{poly}(n, s, d)$ *for all nonzero n-variate polynomials over K of degree at most d and approximative circuit size at most s can be constructed in* $\mathsf{FP}^{\mathsf{CH}}$*. Thus these hitting sets are* CH*-explicit. Their coordinates have polynomial-length encoding; over finite fields, we allow a finite extension of polynomial degree.*

The first two consequences follow from the standard parametrizations of bounded-rank tensors and group orbits, using denominator clearing for rational parametrizations. For hitting sets, the certification criterion of Guo, Saxena, and Sinhababu [GSS19, Theorem 5.2 and Remark 5.3] reduces failure of a candidate hitting set for their universal circuit family to APS. Certification therefore belongs to CH, and bitwise search over polynomial-length candidate encodings gives the stated construction, improving their PSPACE upper bound.

For our second main result, we provide a solution to the question raised in Problem 1.2, bringing down the complexity of integral closure membership testing from $\mathsf{EXPSPACE}$ to CH.

Theorem 1.8. *Integral closure membership testing belongs to* CH*. More precisely, non-integrality has a deterministic polynomial-time many-one reduction to* APS*.*

Remark 1.9 (Other coefficient fields)**.** Theorem 1.8 also holds over the number fields and finite fields covered by our extension of Theorem 1.3, with integrality taken over $\overline{k}[f_1, \ldots, f_m]$, where k is the base field, see Remark 7.10.

Corollary 1.10. *Under the input and coefficient-field conventions above, the following problems belong to* CH*, where K denotes the algebraic closure of the coefficient field:*

(i) ***Integral closure of ideals.*** *Given polynomials $h, g_1, \ldots, g_m$, decide whether h belongs to the integral closure of the ideal $(g_1, \ldots, g_m) \subseteq K[x_1, \ldots, x_n]$.*

(ii) ***Finiteness of polynomial maps.*** *Given a polynomial map $F = (f_1, \ldots, f_m) : K^n \to K^m$, decide whether F is finite, or equivalently, proper.*

The first consequence follows from the standard equivalence between integrality of h over the ideal $(g_1, \ldots, g_m)$ and the integrality of th over $K[x_1, \ldots, x_n, tg_1, \ldots, tg_m]$, where t is a new variable. To see this consider the degree 1 graded part, i.e., $k = 1$ in the proof of [HS06, Proposition 5.2.1] with $R = K[x_1, \ldots, x_n]$, and $I = (g_1, \ldots, g_m)$. For the second, F is finite precisely when every coordinate x_j is integral over $K[f_1, \ldots, f_m]$; finiteness and properness are equivalent for affine morphisms [The26, Tag 01WN].

Moreover, we also show that Integral Closure Membership Testing is equivalent to APS under polynomial-time reductions.

Theorem 1.11. *Under polynomial time many-one reductions, non-existence of* APS *is equivalent to Integral Closure Membership Testing.*

Remark 1.12. The above equivalence works over all algebraically closed fields.

1.2 Related work

Independent and concurrent work. Independently and concurrently, Balaji, Shirmohammadi, Tavenas, and Worrell [BSTW26] obtained the Counting Hierarchy upper bound for APS established in Theorem 1.3. Both proofs use generalized characteristic polynomials and the resultant circuits of Andrews, Garg, and Schost [AGS26], but their geometric reductions differ. [BSTW26] first reduce to a minimally dependent tuple and prescribe generic scalar multiples of a single infinitesimal parameter

as the values of all but one coordinate. Their key argument uses the lowest-degree homogeneous part of an annihilating relation to show that, for a suitable choice of the remaining coordinate, a positive APS instance admits a solution on which that coordinate also tends to zero. They detect the existence of such a solution by comparing resultant valuations.

Our geometric reduction builds on ideas of Lehmkuhl and Lickteig [LL89] from their study of tensor border rank. We use finite Noether normalization of the image closure, reducing origin membership to membership in the finite fiber over zero. We then show that every point of this fiber is approached by image points whose projections lie on one generic line through zero. Crucially, finiteness of the normalization also ensures that the image coordinates of every solution branch have finite limits. Thus, the possible limits are exactly the points of this finite fiber. Applying a generic linear form allows us to represent these points by the roots of a univariate polynomial, with zero occurring as a root exactly when the original instance admits an approximate solution. We obtain this polynomial through the resultant construction of [AGS26, Section 4].

We also learned through personal communication that Andrews, Garg, Oliveira, and Schost [AGOS26] independently obtained the same upper bound. In concurrent work, Bhargav, Curticapean, Jindal, and Shukla [BCJS26] establish #P-hardness of computing a bit of the multivariate resultant.

Strong Approximative Nullstellensatz and its connection to integrality. Guo, Saxena, and Sinhababu characterize non-existence of APS by an annihilator with non-zero constant term and use bounded-degree relations and succinct linear algebra to obtain their PSPACE bound [GSS19]. This is very similar in spirit to the Weak Hilbert's Nullstellensatz. Inspired by this, Agarwal, Dutta, Pandey, and Shukla develop a strong approximative Nullstellensatz for containment of approximate vanishing sets [ADPS26]. Their criterion involves integral dependence over the maximal ideal of a *local* subalgebra of $\mathbb{C}(f_1, \ldots, f_m)$, thus, allowing the use of elements from $\mathbb{C}(f_1, \ldots, f_m)$. While similar in nature, the problem is distinct from checking integrality over $\mathbb{C}[f_1, \ldots, f_m]$. For example, given $f = x^2y$ and $g = xy - 1$, it can be checked that $h = x$ is not integral over $\mathbb{C}[f, g]$, but $h = \frac{f}{1+g}$, and hence lies in the localized subalgebra used in [ADPS26].

Polynomial Subalgebra Membership Testing. Kayser showed that Subalgebra Membership Testing is EXPSPACE-complete, and that its homogeneous restriction is PSPACE-complete [Kay25]. However similar, subalgebra membership is not the same as integral closure. For example, x is integral over $\mathbb{C}[x^2]$ but does not belong to it.

Resultants, ETR, and the Counting Hierarchy. Andrews and Wigderson gave constant-depth arithmetic algorithms for univariate resultants, greatest common divisors, and related problems [AW24]. This was later extended by Andrews, Garg, and Schost to multivariate resultants and they used it to place HN in the Counting Hierarchy [AGS26], using generalized characteristic polynomials originating with Ierardi and Canny [Ier89, Can90] to treat affine systems. Recently, [BCJS26, Ope26] have shown that the complexity class Existential Theory of Reals (ETR) also lies in the Counting Hierarchy, using the method of multivariate resultants. Additionally, [BCJS26] also show that computing a bit of this multivariate resultant is #P-Hard.

Annihilator degree bounds. Degree bounds for annihilating polynomials were first described by Perron [Per27], and this line of work was further extended in [Kay09, BMS13] that showed singly exponential bounds for the minimal annihilator. In particular, these bounds were used by Guo, Saxena, and Sinhababu [GSS19] to obtain an annihilator of singly exponential degree, which they

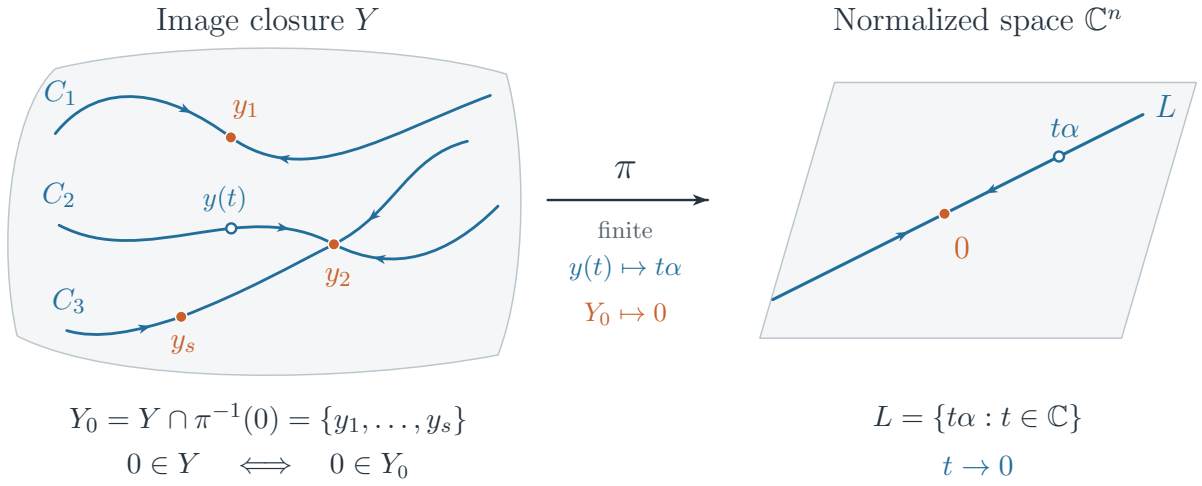


Figure 1: A finite Noether normalization $\pi : Y \to \mathbb{C}^n$ reduces testing $0 \in Y$ to testing membership in the finite set $Y_0 = Y \cap \pi^{-1}(0)$ (orange points). For a generic line $L = \{t\alpha : t \in \mathbb{C}\}$ through the origin, the irreducible components C_i of $Y \cap \pi^{-1}(L)$ are curves mapping onto L. Every point of Y_0 lies on at least one such curve. It can be approached along a branch with $\pi(y(t)) = t\alpha$, using actual image points away from the limit. The parameter may require a finite algebraic extension of $\mathbb{C}(t)$. Arrows indicate specialization as $t \to 0$.

then use to decide non-existence of APS in PSPACE. In the same vein, we also use these bounds to establish the singly exponential degree bound for our integral closure membership testing certificate.

2 Proof Ideas

We first describe our methods for proving Theorem 1.3.

2.1 Approximate Polynomial Satisfiability in Counting Hierarchy

Let

$$F = (f_1, \ldots, f_m) : \mathbb{C}^n \longrightarrow \mathbb{C}^m, \qquad Y = \overline{F(\mathbb{C}^n)}.$$

We want to decide whether $0 \in Y$. Write $r = \dim Y$, and first assume $r \geq 1$. Without loss of generality, we can assume that $m = r + 1$ and $n = r$ using the standard tricks which preserve existence of APS such as the random reduction theorem [GSS19] and the random hyperplane intersection lemma [AGS26], see Lemma 3.12 and Theorem 3.13 for precise statements. So for the rest of this section we assume $n = \dim(Y)$, and $m = n + 1$.

On a very high level, our proof has these main steps: (a) Initially, we need to check $0 \in Y = \overline{F(\mathbb{C}^n)}$, where Y might be an infinite set. However, we show that we can restrict ourselves to checking membership of origin in a *finite* subset of Y. We do this using the Noether normalization which gives a linear map π with the property that only a finite subset $Y_0 \subseteq Y$ maps to 0 in the normalized space, that is, $\pi(Y_0) = \{0\}$. (b) We then show that every point $y_0 \in Y_0$ can be approached by those points in the image $F(\mathbb{C}^n)$ which project to the same generic line L in the normalizing space under the map π (see Figure 1 for a visualization). Parameterizing the line L by t, we get that all solutions $x(t)$ of $(\pi \circ F)x(t) = t\alpha$ (where α is the direction of line L) satisfies $\lim_{t\to 0} F(x(t)) = y_0$

for some $y_0 \in Y_0$. Thus, our task of checking if origin is in the closure of the image is reduced to checking if $\lim_{t\to 0} F(x(t)) = 0$ for some $x(t)$ with $(\pi \circ F)x(t) = t\alpha$. Moreover, Noether normalization and fiber-dimension theorem guarantees that such $x(t)$ will only be finitely many. (c) Next, we show that in order to check if $\lim_{t\to 0} F(x(t)) = 0$ for some solution $x(t)$, it suffices to check if $\lim_{t\to 0}(\Sigma_i \lambda_i f_i(x(t))) = 0$ for some solution $x(t)$, for a generic choice of $\lambda \in \mathbb{C}^m$. (d) We then define a univariate polynomial with roots $\Sigma_i \lambda_i f_i(x(t))$ corresponding to the solutions $x(t)$, which has 0 as a limiting root $\Sigma_i \lambda_i f_i(x(t))$ if and only if $0 \in Y$. (e) This allows us to use the multivariate resultant method of [AGS26] - with slight modifications - to check if this affine root indeed exists.

We now describe each of these steps in more details.

1. Restricting to a finite subset of the image closure. Linear Noether normalization, is a standard tool in algebraic geometry which gives a linear map $\pi : \mathbb{C}^m \to \mathbb{C}^n$ such that

$$\pi(y) = \left(\sum_{i=1}^{m} a_{1i} y_i, \ldots, \sum_{i=1}^{m} a_{ni} y_i \right)$$

whose restriction to Y is finite and surjective, so $\pi|_Y$ takes Zariski closed sets to closed sets, see Lemma 3.15 for a precise statement. In particular, $Y_0 = \{y \in Y : \pi(y) = 0\}$ is finite. Since $\pi(0) = 0$,

$$0 \in Y \quad \iff \quad 0 \in Y_0.$$

2. Constructing a parametrized system of equations with finitely many solutions. Note that some of these points in Y_0 will originate from $\mathbb{C}^n$ under the polynomial map F, while the others will be points purely in $Y \setminus F(\mathbb{C}^n)$, and hence have no preimage. If 0 was indeed in $F(\mathbb{C}^n)$, then this corresponds to an actual root of the system, and the problem reduces to Hilbert's Nullstellensatz, which is known to be in CH [AGS26]. Hence, we assume that 0 has no preimage.

We then show that every point $y_0 \in Y_0$ can be approached by those points in the image $F(\mathbb{C}^n)$ which project to the same generic line $L \subset \mathbb{C}^n$ in the normalizing space under the map π. For this, choose a generic direction $\alpha \in \mathbb{C}^n$ corresponding to a line $L \subset \mathbb{C}^n$ through the origin. Identify the one dimensional space $\mathbb{C}$ with L via $t \mapsto \alpha t$. Then, $\pi^{-1}(L)$ can be split into irreducible curves, each of which is surjective on L, see Lemma 3.9. Since $0 \in L$, any point of Y_0 necessarily lies on one of these curves, see Figure 1.

By another standard consequence of linear Noether normalization (Lemma 3.15) the coordinates y_i of Y are integral elements over $\mathbb{C}[u_1, \ldots, u_n]$, where $\pi(y) = (u_1, \ldots, u_n)$, i.e., y_i satisfy monic polynomials equations over $\mathbb{C}[u_1, \ldots, u_n]$. Replacing u_i by $\alpha_i t$ makes $y_i(t)$ integral over $\mathbb{C}[t]$. Hence, no $y_i(t)$ can "diverge" at $t = 0$. In other words, the valuation of each $y_i(t) \geq 0$, see Section 3.2.

The connection to the approximate solutions can now be viewed as follows. Since the image of F and its domain have the same dimension, the fiber-dimension theorem (see Theorem 3.4) gives a Zariski open set $U \subset Y$ such that for each $y \in U$, the fiber set $\{x \in \mathbb{C}^n \ : \ F(x) = y\}$ is finite. Since π is surjective, there is a Zariski open set $V \subset \mathbb{C}^n$ such that $V = \mathbb{A}^n \setminus \pi(Y \setminus U)$, and $\pi^{-1}(V) \cap Y \subseteq U$. A general direction α will lie in V with high probability. Hence, for such an $\alpha \in V$, the line L is "almost" contained in V, i.e., $L \cap V$ misses only finitely many points of L. Thus every point $y_0 \in Y_0$ can be approached by actual outputs $F(x(t))$ satisfying

$$\sum_{i=1}^{m} a_{ji} f_i(x(t)) = t\alpha_j, \qquad j = 1, \ldots, n, \tag{2.1}$$

along an algebraic branch $x(t) \in \overline{\mathbb{C}(t)}^n$ such that $F(x(t)) \in U$. Hence, for every $y_0 \in Y_0$, there is an algebraic branch $x(t)$ with

$$F(x(t)) \longrightarrow y_0, \qquad \pi(F(x(t))) = t\alpha.$$

Note that the output paths $F(x(t))$ may differ for different points, and only their projections lie on the fixed line $t\alpha$. However, this allows us to search for the desired "limiting output" using the exact equations (2.1). Concretely, we work with the following system of polynomials:

$$\begin{cases} f_i(x) - y_i = 0 & 1 \leq i \leq m = n+1, \\ \sum_{i=1}^{m} a_{ji} y_i - t\alpha_j = 0 & 1 \leq j \leq n. \end{cases} \tag{2.2}$$

By the above discussion, this system has a finite nonempty set of solutions, and we have $2n+1$ equations in $2n+1$ variables $x_1, \ldots, x_n, y_1, \ldots, y_m$. Furthermore, every solution of (2.2) has a finite limit in the y-coordinates, (y coordinates are integral over $\mathbb{C}[t]$ as discussed) and that limit belongs to Y_0. Since Y_0 is covered exactly by these limits, the possible output limits are *exactly* the points of Y_0. Thus, we can restrict our attention to identifying if 0 occurs as a limit, see Section 4 for a detailed treatment. In particular, notice that we need to look at the algebraic solutions using Puiseux series and take the projective closure of a curve defined by Equation (2.2) on the graph associated to the polynomial system F to ensure that the ideas we describe extend to homogeneous systems required by the multivariate resultant.

3. Constructing the univariate polynomial associated to Y_0. Rename the x coordinates to $z_1, \ldots, z_n$ and y-coordinates as $z_{n+1}, \ldots, z_{n+m}$ in Equation (2.2). Since Y_0 is finite, we can always choose $\lambda \in \mathbb{C}^m$ such that $\lambda \cdot y \neq 0$ for every *non-zero* $y \in Y_0$, and define

$$\ell(z) = \sum_{i=1}^{m} \lambda_i z_{n+i} = \sum_{i=1}^{m} \lambda_i f_i(z_1, \ldots, z_n).$$

This gives us the following equivalence:

$$0 \in Y \quad \iff \quad \text{some solution of (2.2) satisfies } \lim_{t \to 0} \ell(z(t)) = 0. \tag{2.3}$$

Using the above defined linear form ℓ, construct the polynomial

$$Q_{Y_0,\ell}(T) \coloneqq \prod_{y \in Y_0} (T - \ell(y)).$$

So $0 \in Y_0$ exactly when $Q_{Y_0,\ell}(0) = 0$. Recall that each $y \in Y_0$ is obtained as a limit of some solution $z_y(t)$ of (2.2), and each solution $z(t)$ of (2.2) approaches a point in Y_0 in z_{n+i} coordinates. So the polynomial

$$P_\ell(T, t) = \prod_{z(t) \text{ a solution to (2.2)}} (T - \ell(z(t)))$$

has the same zeros at $t = 0$ as $Q_{\ell,Y_0}(T)$.

The observation that $P_\ell(T, t)$ is obtained as a product of evaluations of a linear polynomial on the solutions of a polynomial system (2.2) intuitively prompts us towards using resultants. Precisely, the *Poisson formula* [AGS26, Theorem 4.3] allows us to evaluate the new polynomial on roots of the rest of the polynomials.

4. Using the multivariate resultant. Let Z be the solutions to the system (2.2) over $\overline{\mathbb{C}(t)}$. Note that this system need not be homogeneous. On the other hand, the multivariate resultant is only defined for homogeneous systems as discussed in [AGS26]. Homogenizing the system (2.2) considered as polynomials over $\mathbb{C}(t)$ can introduce positive dimensional components at infinity that

are not closures of their affine solutions. In [AGS26] the authors tackle exactly this issue by using the generalized characteristic polynomials introduced by Canny-Ierardi [Can90, Ier89] which uses a perturbation of these polynomials. In general, let $G_1, \ldots, G_N$ be the homogenizations of (2.2), with $N = 2n + 1$ and d_i is the degree of G_i in $z_0, \ldots, z_N$ variables over $\mathbb{C}(t)$. Note that we are only homogenizing with respect to the z variables. Introduce ε and replace them by $\widehat{G}_i = G_i + \varepsilon z_i^{d_i}$. This removes the positive dimensional component but some finite set of points at infinity might still survive the Canny-Ierardi perturbation, for example $F = (x_1 + x_2, x_1 + x_2 - 1)$ has no APS, but the homogenized system $F = (x_1 + x_2, x_1 + x_2 - x_0)$ has a root $[0 : 1 : -1]$. Since we are concerned with the solutions to the affine system (2.2) over $\mathbb{C}(t)$, we introduce a new parameter w, that will track the points at infinity. So similarly to [AGS26] define

$$H_{T,w} = Tz_0^2 - z_0\ell(z) + \sum_{j=1}^{N} w^j z_j^2,$$

be a quadratic form over $\mathbb{C}(T, w)$. At an affine point z with $z_0 = 1$, and $w = 0$ $H_{T,0}(z) = T - \ell(z)$, which is exactly the form of the polynomial P_ℓ. So taking the multivariate resultant of G_i and $H_{w,T}$ should be connected to P_ℓ, and so to $Q_{Y_0,\ell}$. Let

$$\mathscr{R}(\varepsilon, t, w, T) = \mathrm{Res}_{z_0,\ldots,z_N}(\widehat{G}_1, \ldots, \widehat{G}_N, H_{T,w}). \tag{2.4}$$

We now use the finite limit set and factorization statements in [AGS26, Lemmas 4.6–4.7]. The limit set contains every isolated point of the original projective zero set, so every point of Z. Its affine points are precisely the set Z. Thus, we get

$$\widetilde{P_\ell}(T, t) := \mathrm{TC}_w \,\mathrm{TC}_\varepsilon \,\mathscr{R} = a(t) \prod_{z \in Z} (T - \ell(z(t)))^{\mu_z}, \qquad a(t) \in \mathbb{C}[t], \quad \mu_z > 0.$$

Here $\mathrm{TC}_v(\cdot)$ is the least degree coefficient of a polynomial in variable v. The polynomial P_ℓ and $\widetilde{P_\ell}$ differ by a non-zero factor $a(t)$. Thus, writing $a(t) = t^k v(t)$ such that $v(0) \neq 0$, we get $R_\ell(T) := \mathrm{TC}_t \,\widetilde{P_\ell}(T, t) = cP_\ell(T, 0)$ for some $c \in \mathbb{C}^\times$. Hence, by using multivariate resultants we construct a polyomial R_ℓ that has same zeros as $Q_{Y_0,\ell}$, see Section 5.1, and Section 5.2 for details.

5. Perform the resulting coefficient test in CH. The system of homogeneous polynomials $\widehat{G}_i, H_{T,w}$ has polynomial size. By [AGS26] we can access any specified coefficient bit of its resultant in CH, hence we do not need to write out the entire resultant.

After clearing denominators, the resultant has degree and integer coefficient bit lengths bounded by $2^{\mathrm{poly}(L)}$, where L is the input length. Thus both monomial exponents and positions within a coefficient's binary representation have polynomial-length encodings. Given CH access to individual coefficient bits, coefficient vanishing can be tested by quantifying over these bit positions. A fixed number of quantifier blocks over polynomial-length indices then suffices to identify the successive lowest nonzero powers and test the resulting constant coefficient in T. Hence the entire test lies in CH; see Section 6.

2.2 Integral Closure Membership Testing in Counting Hierarchy

In this section, we discuss the ideas we use to place the problem of deciding whether a polynomial f lies in the integral closure of the ring $A = \mathbb{C}[f_1, \ldots, f_m]$ in CH (see Problem 1.2), and the ideas needed to establish the computational equivalence of APS and Integral Closure Membership Testing.

In order to prove this we want to use the above $\mathsf{APS} \in \mathsf{CH}$ result. We do precisely that. We give a polynomial time reduction from integral closure membership testing to APS to get the

desired result. Apriori, it is not clear how integrality relates to APS. However, we observe that the Approximate Rabinowitsch's Trick [ADPS26, Lemma 2] exactly hints towards this connection. In fact, we can use the classical *valuative criterion* for integral dependence [AM69, Corollary 5.22] (see Corollary 7.6 for a precise statement) to make this connection precise. In particular, we can define a system of polynomials $\Psi_M = (uf_1^M, \ldots, uf_m^M, u, 1-uf)$ such that f is integral over $\mathbb{C}[f_1, \ldots, f_m]$ if and only if Ψ_M has no APS, where M is singly exponential in the degrees of the input polynomials. See Section 7 for a full proof. This also establishes that Integral Closure Membership Testing reduces to non-existence of APS. To show the reduction in the other direction, we observe that $f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$ have no APS if and only if z is integral over the polynomials $zf_1, \ldots, zf_m \in \mathbb{C}[z, x_1, \ldots, x_n]$, see Lemma 7.11.

We now describe the proof idea for Theorem 1.8 in more details. For the proof we need some concepts from valuation theory of rings [AM69]. In particular, for $\beta_i \in \mathbb{C}(t)$, we say that the valuation of a polynomial $g \in \mathbb{C}[x_1, ..., x_n]$ (denoted $\mathsf{val}_t(g(x))$) is the exponent of the least power of t in $g(\beta_1(t), \ldots, \beta_n(t))$. If $g(\beta) = 0$, then valuation is defined to be infinity. For a precise definition, see Section 3.2.

Example 2.1 (Valuations)**.** Let $g = x_1x_2 - 1$.

(i) If $\beta_1 = \beta_2 = t$, then $g(\beta) = t^2 - 1$, and $\mathsf{val}_t(g(\beta)) = 0$.

(ii) If $\beta_1 = t; \beta_2 = t + \frac{1}{t}$, then $g(\beta) = t^2$, and $\mathsf{val}_t(g(\beta)) = 2$.

(iii) If $\beta_1 = t; \beta_2 = \frac{1}{t}$, then $g(\beta) = 0$, and $\mathsf{val}_t(g(\beta)) = \infty$.

By definition, f is integral if and only if there is a monic polynomial in f with coefficients from A. Observe that this monic polynomial guarantees that if valuation of each f_i is non-negative then valuation of f will also be non-negative. At this point, it is not so clear if the converse also holds. But the valuative criterion for integral dependence says exactly this, see Corollary 7.6. In other words, it means that if f is not integral, then there is an assignment β such that all the f_i are bounded (i.e., $\mathsf{val}_t(f_i(\beta)) \geq 0$), but f diverges (i.e., $\mathsf{val}_t(f(\beta)) < 0$). We observe that this is very similar to the approximate Rabinowitsch's trick relating to non-divergence used in [ADPS26, Lemma 2] which gives a criterion for this non-divergence in terms of APS. Since we have shown that APS is in CH, this gives an approach towards also putting integral closure membership testing in CH. However, at this point there is still a computational roadblock as this requires deciding APS for $f_i - c_i$, for each $c_i \in \mathbb{C}$. Precisely, it requires deciding whether for each $c \in \mathbb{C}^m$, $f_1 - c_1, \ldots, f_m - c_m, u, 1 - uf$ have no APS.

In terms of annihilators, using [GSS19] criteria, the system $f_1 - c_1, \ldots, f_m - c_m, u, 1 - uf$ might give different annihilators for different $c \in \mathbb{C}^m$. We show in Theorem 7.3 that in fact the "local" annihilators for each $c \in \mathbb{C}^m$ can be used to get a single *global* polynomial certificate Q of degree D which is singly exponential in the input parameters, see Theorem 7.7 for a full statement. At this point, since linear algebra over a singly exponential system is in PSPACE [Csa76, Ber84], we can check for integrality in PSPACE. Still, we cannot reduce the complexity to CH yet, as this global polynomial doesn't directly correspond to an APS instance.

To achieve this, we again use Corollary 7.6. We claim that setting $M > D$, we can define a system of polynomials $\Psi_M = (uf_1^M, \ldots, uf_m^M, u, 1 - uf)$ such that f is integral over $\mathbb{C}[f_1, \ldots, f_m]$ if and only if Ψ_M has no APS, see Theorem 7.8 for a full proof. For the easy direction, f not being integral implies that there is an algebraic branch $x(t)$ such that each f_i had a non-negative valuation but f had a negative valuation. Then, select $u = \frac{1}{f}$, and so u has a positive valuation. Thus each of the polynomials in Ψ_M has a positive valuation, and hence there is an APS. The converse is where

the choice of M becomes crucial. Intuitively, it ensures that the valuation of u doesn't dominate the valuation of any f_i and we don't get false witnesses of non-integrality.

Example 2.2. Let $f_1 = x$ and $f = x^2$. Clearly, f is integral over $\mathbb{C}[f_1]$, yet if we set $M = 1$, $(u, 1 - ux^2, ux)$ has the approximate zero $(x, u) = (t^{-1}, t^2)$. Here, the generator f_1 is also diverging, just more slowly than f along $x = 1/t$.

Suppose f is integral and there is an APS of Ψ_M, and let $x(t), u(t)$ be an approximate solution witnessing APS. Thus, $a = \mathsf{val}_t(u(t))$ and each $u(t)f_i^M(x(t))$ is positive. Hence, valuation of each $f_i(x(t))$ is greater than $-\frac{a}{M}$. Now using the global degree D certificate Q obtained above we get the identity

$$1 + \sum_{j=1}^{r} b_j(f_1, \ldots, f_m) f^{-j} = 0.$$

At an approximate zero of Ψ_M, the choice $M > D$ makes every summand after 1 have positive valuation. They therefore cannot cancel the constant term, giving a contradiction.

Since M is singly exponential, we can compute each uf_i^M in polynomial depth and get a polynomial sized APS criterion for the integral closure test putting integral closure testing in CH.

3 Preliminaries

Let K be an algebraically closed field. We write $x = (x_1, \ldots, x_n) \in \mathbb{A}^n_K$, for a general point in the affine n-space $\mathbb{A}^n_K$ over K, and also for coordinates on $\mathbb{A}^n_K$. The distinction will be clear from the context. We use dimension in the sense of [Vak25, Definition 12.1.1]. The degree of an affine variety is the degree of its projective closure, with projective degree defined in [Vak25, Section 18.6, p. 520]

3.1 Dominant and finite morphisms, and integral dependence

Throughout this paper, an affine algebraic set will be the same as an algebraic variety, and when an algebraic variety it irreducible we will explicitly state this. We first recall the definition of coordinate ring associated to an affine algebraic set over K. Let $X \subset \mathbb{A}^n_K \simeq K^n$ (the last isomorphism is as a set) be an algebraic set, and $I_X \subset K[x_1, \ldots, x_n]$ be its assoicated ideal, then the cooridinate ring is given by $K[X] \simeq K[x_1, \ldots, x_n]/I_X$. A morphism of affine algebraic sets $f : X \to Y$ given by polynomials induces a ring homomorphism of associated coordinate rings $f^* : K[Y] \to K[X]$ in the opposite direction.

Definition 3.1 ([Vak25, Section 3.6.4])**.** Let K be an algebraically closed field. An *irreducible affine variety over k* is a nonempty Zariski-closed subset $X \subseteq \mathbb{A}^n_K$ that cannot be written as the union of two proper Zariski-closed subsets of X. Equivalently, the associated ideal I_X is a prime ideal.

For an irreducible affine variety X over K, since I_X is a prime ideal its coordinate ring $K[X]$ is an integral domain. Hence, its *function field* is $K(X) = \mathrm{Frac}(K[X])$, where $\mathrm{Frac}(K[X])$ is the field of fractions of $K[X]$.

Example 3.2. Any affine space $\mathbb{A}^n_K$ is by definition irreducible. If X and Y are irreducible, then so is $X \times Y$. Furthremore, if $f : X \to Y$ is map affine algebraic sets, and X is irreducible, then the image $f(X)$ is irreducible. In particular, for $X = \mathbb{A}^n_K$, $f(\mathbb{A}^n_K)$ is always irreducible.

Definition 3.3 ([The26, Tag 01RI])**.** Let X and Y be irreducible affine varieties over an algebraically closed field K. A morphism $f : X \to Y$ is *dominant* if its image is Zariski dense in Y, that is,

$$\overline{f(X)} = Y,$$

where the closure is taken in Y. Equivalently, $f^{-1}(U) \neq \varnothing$ for every nonempty Zariski-open subset $U \subseteq Y$.

We recall the following properties of dominant morphisms [Vak25, Exercise 7.5.C and Theorem 12.2.1].

Theorem 3.4 ([Vak25, Theorem 8.4.2,Corollary 12.4.2])**.** *Let X and Y be irreducible affine varieties over an algebraically closed field K, and let $f : X \to Y$ be a dominant morphism. Then f induces a field embedding $f^* : K(Y) \hookrightarrow K(X)$. Identifying $K(Y)$ with its image, we have*

$$\operatorname{trdeg}_{K(Y)} K(X) = \dim X - \dim Y.$$

Moreover, there is a nonempty Zariski-open subset $U \subseteq Y$ such that, for every $y \in U$, the fiber $f^{-1}(y)$ is nonempty, and each of its irreducible components has dimension $\dim X - \dim Y$.

Example 3.5. In Theorem 3.4, if $\dim X = \dim Y$, then $K(X)/K(Y)$ is finite algebraic, since it is a finitely generated field extension of transcendence degree zero. Thus a dominant morphism from an irreducible curve D to $\mathbb{A}^1_K$ gives a finite extension $K(D)/K(t)$, with the function field of $\mathbb{A}^1_K$ as $K(t)$.

Now we recall the notions of integrality and integral closures, and state some geometric consequences.

Definition 3.6. For a ring extension of commutative rings with 1 $A \subseteq B$, an element $b \in B$ is *integral over* A if

$$b^d + a_{d-1}b^{d-1} + \cdots + a_0 = 0 \quad \text{for some } d \geq 1 \text{ and } a_i \in A.$$

The extension is *integral* if every element of B is integral over A. The elements integral over A form its *integral closure* in B. An integral domain A is *integrally closed* if its integral closure in $\operatorname{Frac}(A)$ equals A; see [AM69, Chapter 5, pp. 59–63].

A morphism $f : X \to Y$ of affine varieties is *finite* when its coordinate ring $\mathbb{C}[X]$ is a finite $\mathbb{C}[Y]$-module via f^*.

Remark 3.7 ([AM69, Proposition 5.1 and Corollary 5.2])**.** Every finite ring extension $A \subseteq B$ is integral. Furthermore, if B is generated by adjoining finitely many integral elements over A, then B is finite as an A-module.

We recall the following standard geometric properties of finite morphisms.

Theorem 3.8 ([The26, Tags 01WM,02LS,0ECG,0F32,0BQ3])**.** *Let $f : X \to Y$ be a finite morphism of affine varieties over K. Then the map f is closed (maps closed subspaces to closed subspaces) and every fiber is finite. So* $\dim(f(Z)) = \dim(Z)$ *for each closed $Z \subset X$. In particular, if f is dominant, then it is surjective.*

Furthermore, if X and Y are irreducible, with $K[Y]$ integrally closed in $K(Y)$, and f is dominant, then f is open, i.e., f maps open subsets to open subsets.

The following useful consequence is an application of the above theorem to $Y = \mathbb{A}^d_K$.

Lemma 3.9. *Let X be an irreducible affine variety of dimension $d \geq 1$ and let $\pi : X \to \mathbb{A}^d_K$ be finite and dominant. For any affine line $\mathbb{A}^1_K \simeq L \subseteq \mathbb{A}^d_K$, let $C := \pi^{-1}(L)$, and let $W_1, \ldots, W_k$ be the irreducible components of C. Then π maps each W_i surjectively onto L. In particular, for $b \in L$, every point of $\pi^{-1}(b)$ is in one of W_i.*

Proof. The closed space C is a curve because π is finite and dominant, hence surjective, and $\dim(C) = \dim(\pi(C)) = \dim(L) = 1$.

Since $K[\mathbb{A}^d] \simeq K[x_1, \ldots, x_d]$ is just the polynomial ring in d-variables, and so is integrally closed in $K(x_1, \ldots, x_d)$, the map π is also open, and so is its restriction to C. We show without loss of generality that π restricted to W_1 is surjective. Let U be the open set obtained after removing the irreducible closed sets $W_2, \ldots, W_k$ from X. Then $\pi(W_1) \supseteq \pi(U \cap C) = \pi(U) \cap L \neq \emptyset$ is open in L. Also, $\pi(W_1)$ is closed, as W_1 is a closed set. Since L is irreducible and $\pi(U) \cap L$ is a non-empty open set, its closure is L. Hence $\pi(W_1) = L$. □

3.2 Image closures and approximate vanishing

From now on we assume $K = \mathbb{C}$, however one may as well take K to be any algebraically closed field. Recall from Theorem 3.4 and Example 3.2 that for a polynomial map $F = (f_1, \ldots, f_m) : \mathbb{A}^n_{\mathbb{C}} \to \mathbb{A}^m_{\mathbb{C}}$ and $Y = \overline{F(\mathbb{A}^n_{\mathbb{C}})}$, Y is irreducible of dimension $\dim(Y) = \mathrm{trdeg}(f_1, \ldots, f_m)$ with I_Y being the annihilator ideal $\mathrm{Ann}(F)$ of $f_1, \ldots, f_m$.

Let

$$\mathcal{K} = \bigcup_{e \geq 1} \mathbb{C}((t^{1/e})), \qquad \mathcal{O}_{\mathcal{K}} = \{a \in K : \mathsf{val}_t(a) \geq 0\}, \qquad \mathfrak{m}_{\mathcal{K}} = \{a \in K : \mathsf{val}_t(a) > 0\}.$$

Here $\mathcal{K}$ is the field of formal Puiseux series that is algebraically closed, and $\mathsf{val}_t = \mathrm{ord}_t : K \to \mathbb{Q}$, is the valuation map, defined as follows: for an element $\alpha = t^e(c_0 + c_1 t^{e_1} + \ldots)$ with $c_0 \neq 0$, we define $\mathsf{val}_t(\alpha) = e \in \mathbb{Q}$, and set $\mathsf{val}_t(0) = +\infty$.

Definition 3.10 (Approximate vanishing and APS)**.** For a tuple $F = (f_1, \ldots, f_m)$ of polynomials in $\mathbb{C}[x_1, \ldots, x_n]$, let

$$\mathrm{AV}(F) = \{\beta \in \mathcal{K}^n : \mathsf{val}_t(f_i(\beta)) > 0 \text{ for every } i\}.$$

We say that the system (equivalently the map) F has APS if $\mathrm{AV}(F) \neq \emptyset$.

The following is the statement of weak approximative nullstellensatz (in the sense of [ADPS26]).

Theorem 3.11 ([GSS19, Lemma 4.1 and Theorem 4.2])**.** *Let F be as above. Then*

$$\mathrm{AV}(F) \neq \varnothing \iff 0 \in \overline{F(\mathbb{A}^n_{\mathbb{C}})} \iff P(0) = 0 \text{ for all } P \in \mathrm{Ann}(F). \tag{3.1}$$

The definition of $\mathrm{AV}(F)$ in [GSS19] is given in terms of $\beta \in \mathbb{C}((t))^n$, however it is enough to assume $\beta \in (\mathcal{K})^n$. Indeed, a Puiseux witness $\beta(t) \in \mathcal{K}^n$ of AV will belong to $\mathbb{C}((t^{1/e}))^n$, for some large enough e, and so $\beta(t^e) \in \mathbb{C}((t))^n$ gives a witness in the sense of [GSS19].

In the following section we recall the standard results that reduce the general setting to the case when $\mathrm{trdeg}(f_1, \ldots, f_m) = n$ and $m = n + 1$.

3.3 Random hyperplane sections and random projections

Set $r = \dim Y$ and $d = \max(1, \deg f_1, \ldots, \deg f_m)$. We assume that f_i are non-constant, otherwise there is nothing to prove. If $r = m$, then $Y = \mathbb{A}^m$ and APS trivially holds. Hence we assume from now on that $1 \leq r < m$.

We state the random hyperplane-section and projection results in the forms used in this paper. In each statement, coefficients are sampled independently and uniformly from a finite set $B \subset \mathbb{Q}$. We recall the following standard result mentioned in [AGS26]. It estimates the probability with which a random hyperplane intersection drops the dimension of a given affine algebraic set W. This is in some ways, explicitization of the classical result of Bertini on hyperplane intersections. Successively intersecting with $\dim(W)$ many random hyperplanes, one can reduce the dimension of W to 0.

Lemma 3.12 ([AGS26, Lemma 4.9])**.** *Let $W \subseteq \mathbb{A}^a_{\mathbb{C}}$ be an affine algebraic set of degree Δ. A random affine linear equation reduces its dimension to $\dim(W) - 1$ with probability at least $1 - 2\Delta/|B|$. Consequently, $\dim(W)$ successive random affine linear equations have a finite nonempty intersection with W with probability at least $1 - 2\Delta \cdot \dim(W)/|B|$.*

Degree does not increase under hyperplane sections. The following result reduces the number of outputs to $r + 1$ by a random linear projection, preserving both the image dimension and APS.

Theorem 3.13 (Geometric form of [GSS19, Theorem 4.6])**.** *Let $F = (f_1, \ldots, f_m)$ be polynomials of degree at most d and transcendence degree $r < m - 1$. Choose $c_{ij} \in B$ and put $\widetilde{f}_i = \sum_{j=1}^{m} c_{ij} f_j$, $1 \leq i \leq r + 1$. With probability at least $1 - (r + 1)d^r/|B|$,*

$$\operatorname{trdeg}_{\mathbb{C}}(\widetilde{f}_1, \ldots, \widetilde{f}_{r+1}) = r, \qquad 0 \in \overline{F(\mathbb{A}^n_{\mathbb{C}})} \iff 0 \in \overline{\widetilde{F}(\mathbb{A}^n_{\mathbb{C}})}.$$

Combining these two results reduces deciding APS to $m = n + 1$ and transcendence degree n case, which we record as the following proposition.

Proposition 3.14. *With the notation above, impose $n - r$ random affine linear equations on the variables and parametrize their intersection. If $m > r+1$, then take $r+1$ random linear combinations of the outputs. With probability at least*

$$1 - \frac{2(n - r)d^m + (r + 1)d^r}{|B|},$$

this construction produces a map $\widetilde{F} : \mathbb{A}^r_{\mathbb{C}} \to \mathbb{A}^{r+1}_{\mathbb{C}}$ of transcendence degree r such that F has APS if and only if $\widetilde{F}$ has APS.

Proof. Let $Y = \overline{F(\mathbb{A}^n_{\mathbb{C}})}$, and $E = \overline{\mathbb{C}(Y)}$, the algebraic closure of function field of Y. Recall that the map F is a map of irreducible algebraic sets and is dominant on its image $F(\mathbb{A}^n_{\mathbb{C}})$, Theorem 3.4 gives that a general fiber has dimension $n - r$, and degree at most d^m by Bézout's inequality. This corresponds to saying that in $\mathbb{A}^n_E$ the system of equations $f_i - y_i$, for all $1 \leq i \leq m$ define an affine algebraic set of dimension $n - r$ over E. Since $\mathbb{C}^n \subset \mathbb{A}^n_E$ is Zariski dense we can as well sample the coefficients of our random hyperplanes from $\mathbb{Q}$. Applying Lemma 3.12 to this affine algebraic set over E gives that $n - r$ random hyperplanes cut it to a finite nonempty set with failure probability at most $2(n - r)d^m/|B|$. So the map F restricted to the r-plane given by the intersection of $n - r$ random hyperplanes is still dominant onto $F(\mathbb{A}^n_{\mathbb{C}})$. So we obtain a map $\mathbb{A}^r_{\mathbb{C}} \to \mathbb{A}^m_{\mathbb{C}}$, that preserves APS.

Theorem 3.13, then gives $r + 1$ outputs while preserving APS and transcendence degree. The sum of the failure probabilities, then give the claimed bound. □

Both operations preserve polynomial circuit size. If the input circuit length is L, then $\log d$ and the logarithms of the displayed degree bounds are polynomial in L. Hence an integer grid B of polynomial coefficient bit length makes the failure probability a fixed small constant. The image dimension can be found as in Lemma 6.1. Thus the geometric construction may be carried out with the reduced map, renamed F, and dimensions n, m satisfying

$$m = n + 1, \qquad \dim Y = \mathrm{trdeg}_{\mathbb{C}}(f_1, \ldots, f_m) = n \geq 1. \tag{3.2}$$

In this reduced case, we use the following standard form of linear Noether normalization.

Lemma 3.15 ([Mil24, Proposition 2.42 and Lemma 2.43])**.** *Let $Y \subseteq \mathbb{A}^{n+1}_{\mathbb{C}}$ be an irreducible affine variety of dimension $n \geq 1$. For a linear map $\pi : \mathbb{A}^{n+1}_{\mathbb{C}} \to \mathbb{A}^{n}_{\mathbb{C}}$ given by $\pi(y_1, \ldots, y_{n+1}) = (y_1 - c_1 y_{n+1}, \ldots, y_n - c_n y_{n+1})$, for general $(c_1, \ldots, c_n) \in \mathbb{A}^{n}_{\mathbb{C}}$ the restriction $\pi : Y \to \mathbb{A}^{n}_{\mathbb{C}}$ is finite and surjective.*

By Remark 3.7, the restriction $\pi : Y \to \mathbb{A}^{n}_{\mathbb{C}}$ induces an injective ring homomorphism

$$\pi^* : \mathbb{C}[u_1, \ldots, u_n] \longrightarrow \mathbb{C}[Y] = \mathbb{C}[y_1, \ldots, y_{n+1}]/I_Y, \qquad u_i \longmapsto (y_i - c_i y_{n+1}) \bmod I_Y.$$

Moreover, $\mathbb{C}[Y]$ is a finite module over the image of π^*. Consequently, each coordinate function $y_j|_Y$, for $1 \leq j \leq n+1$, is integral over this image.

The following gives the failure probability of a random choice of $c \in \mathbb{A}^{n}_{\mathbb{C}}$ in Lemma 3.15.

Remark 3.16. Since Y is an irreducible affine hypersurface, it is given by the vanishing of a single irreducible polynomial P. Let $\delta = \deg P$, and P_δ be the highest-degree homogeneous part of P. By the proof of [Mil24, Lemma 2.43] the linear map $\pi : \mathbb{A}^{n+1}_{\mathbb{C}} \to \mathbb{A}^{n}_{\mathbb{C}}$ fails to give a Noether normalization if the chosen $(c_1, \ldots, c_n) \in \mathbb{A}^{n}_{\mathbb{C}}$ satisifes $P_\delta(c_1, \ldots, c_n, 1) = 0$. If c_i are drawn independently and uniformly from a set $B \subset \mathbb{Q}$, then Schwartz-Zippel lemma gives the failure probability of π being a Noether normalization being at most $\delta/|B|$.

3.4 Complexity theoretic inputs

Input size. For both problems, L denotes the total size of the input circuits, including binary rational constants. Gates perform addition, subtraction, and binary multiplication. Formal degrees are computed by taking the maximum at addition gates and the sum at multiplication gates; they have polynomial-length binary representations. Output degrees and coefficient bit lengths are at most $2^{\mathrm{poly}(L)}$. We never expand these outputs. After clearing rational denominators gate by gate, Kronecker substitution reduces coefficient-bit access to $\mathsf{BitSLP} \in \mathsf{CH}$ [ABKPM09, Theorem 4.1]. The implicit coefficient table has size $2^{\mathrm{poly}(L)}$; hence [AGS26, Corollaries 5.13 and 6.4, Lemma 6.5] give resultant-coefficient access in CH for polynomially many such forms, without a degree-two assumption. A sparse polynomial with binary exponents converts to a circuit in polynomial time by repeated squaring. An input rational target is handled by subtracting its coordinates at the output gates. Dummy variables and a zero generator allow us to assume $n, m \geq 1$ without changing either problem.

The Counting Hierarchy. Set $C_0\mathsf{P} = \mathsf{P}$ and $C_{i+1}\mathsf{P} = \mathsf{PP}^{C_i\mathsf{P}}$. Then $\mathsf{CH} = \bigcup_{i \geq 0} C_i\mathsf{P}$ [KP11]. A fixed number of polynomially bounded existential or universal quantifiers over a language at a fixed level stays in CH. The hierarchy is closed under complement and polynomial-time Turing reductions to a language at a fixed level. A randomized polynomial-time computation with such an oracle also stays in CH, since $\mathsf{BPP}^A \subseteq \mathsf{PP}^A$. A fixed finite collection of these oracles can be combined at one fixed level.

Trailing coefficients. For a nonzero polynomial $R(t,z) = \sum_{i\geq 0} t^i R_i(z)$ over a domain, let

$$\mathrm{TC}_t\, R = R_e(z), \qquad e = \min\{i : R_i \neq 0\}.$$

Thus TC extracts a coefficient, not the coefficient times t^e. Trailing coefficients are multiplicative, and nested operations are read from right to left. The coefficients are polynomials in all the remaining variables. Consequently, evaluation at $s = 0$ generally does not commute with a trailing-coefficient operation.

4 The geometry of APS

In this section, we discuss the geometric construction behind reducing the problem to multivariate resultants. We follow the discussion in Section 2.1. Let 0_m, 0_n, and 0 be the origins of $\mathbb{A}^m_{\mathbb{C}}$, $\mathbb{A}^n_{\mathbb{C}}$, and $\mathbb{A}^1_{\mathbb{C}}$, respectively, and let $Y = \overline{F(\mathbb{A}^n_{\mathbb{C}})}$. Then Proposition 3.14 reduces the problem to

$$F = (f_1, \ldots, f_m) : \mathbb{A}^n_{\mathbb{C}} \longrightarrow \mathbb{A}^m_{\mathbb{C}}, \qquad m = n+1, \qquad \dim Y = n, \qquad .$$

Let $x_1, \ldots, x_n$ be the input coordinates (variables) of F and $y_1, \ldots, y_m$ be the coordinates on $\mathbb{A}^m_{\mathbb{C}}$, i.e., the output variables of F. For notational simplicity we will refer to $x_1, \ldots, x_m$ and $y_1, \ldots, y_m$ by x and y coordinates, respectively. Let $d \geq \max(2, \deg f_1, \ldots, \deg f_m)$ be the formal-degree bound from the input-size discussion; thus $d \leq 2^{\mathrm{poly}(L)}$. Recall the field of Puiseux series $\mathcal{K}$ of Section 3.2. The aim is to construct a system of $m+n$ homogeneous polynomials in $m+n+1$ variables over $\mathcal{K}$ such that affine solutions of this system over $\mathcal{K}$ exactly capture if $0_m \in Y$.

4.1 The graph and a finite family along a line

Let $\Gamma_F \subset \mathbb{A}^n_{\mathbb{C}} \times \mathbb{A}^m_{\mathbb{C}}$ be the graph of the polynomial map F, and let $p : \Gamma_F \to Y$ given by $(x, y) \mapsto y$ be the projection map to the second component. Then

$$\Gamma_F = V(y_1 - f_1(x), \ldots, y_m - f_m(x)).$$

Recall that $\Gamma_F \cong \mathbb{A}^n_{\mathbb{C}}$, and p is a dominant morphism of irreducible affine algebraic spaces by the definition of Y. Theorem 3.4 gives a nonempty open $U \subseteq Y$ over which the fibers of p are finite and nonempty. Choose a finite surjective linear projection $\pi : Y \to \mathbb{A}^n_{\mathbb{C}}$ using Lemma 3.15 (π gives a Noether normalization of Y). Let $u_1, \ldots, u_n$ be the coordinates on the image of π, denoted by u.

It will be important to choose U as a complement of a closed set of singly exponential degree. The composition $\pi \circ F : \mathbb{A}^n_{\mathbb{C}} \to \mathbb{A}^n_{\mathbb{C}}$ is dominant, so Theorem 3.4 shows that x_i is algebraic over the field generated by the polynomials $\pi \circ F$, equivalently over $\mathbb{C}(u_1, \ldots, u_n)$. Indeed, Perron's bound [GSS19, Section 1, p. 2] gives relations $Q_i(\pi(F), x_i) = 0$ with $\deg Q_i \leq d^n$. Let b be the product of the leading coefficients of $Q_i(u, T)$ in T, which are nonzero. Outside the algebraic set $b = 0$, the map p is finite and surjective by Section 3.1. So we can choose U as the complement of the closed set defined by $b = 0$ of degree nd^n. Bézout along with $\deg(Y) = \deg(\mathrm{Ann}(F)) \leq d^n$ gives $\deg(Y \setminus U) \leq nd^{2n}$. We summarize this in the following proposition.

Proposition 4.1. *Let $U \subset Y$ be as above. Then U can be chosen as a complement of a closed set of degree at most nd^{2n}.*

By Theorem 3.8, π is closed, so $\pi(Y \setminus U)$ is closed of dimension $\dim(Y \setminus U) < n$. Hence let V be the open set

$$V = \mathbb{A}^n_{\mathbb{C}} \setminus \pi(Y \setminus U).$$

Thus every point of Y above V belongs to U.

Choose a nonzero $\alpha \in \mathbb{A}^n_{\mathbb{C}}$ such that $L = \{t\alpha : t \in \mathbb{C}\}$ meets V, and identify L with $\mathbb{A}^1_{\mathbb{C}}$, whose coordinate ring is given by $\mathbb{C}[t]$. Let

$$C \coloneqq Y \cap \pi^{-1}(L), \qquad D \coloneqq \overline{(\pi \circ p)^{-1}(L \cap V)} \subseteq \Gamma_F.$$

Let $\beta \coloneqq \pi \circ p$. Then β is finite and surjective over V. Since V is an open subset of $\mathbb{A}^n_{\mathbb{C}}$, so it is integrally closed in its field of fractions which is the same as $\mathbb{C}(u_1, \ldots, u_n)$. Hence by Theorem 3.8 β is open. The following proposition shows that the map β is dominant on each component of D.

Proposition 4.2. *Let D, β, L and V be as above, and let D' be an irreducible component of D. Then $\beta|_{D'} : D' \to L$ is dominant, and $K(D')/K(L)$ is a finite extension.*

Proof. The proof is similar to Lemma 3.9. Recall that β is open. We apply the component argument as in the proof of Lemma 3.9, over $L \cap V$. Each component of $\beta^{-1}(L \cap V)$ maps onto $L \cap V$ and has dimension one. On taking closures, one obtains that each irreducible component D' of D is a curve that dominates L, and so the function field of D', $\mathbb{C}(D')$ is a finite extension of fields over $\mathbb{C}(t) \simeq \mathbb{C}(L)$ by Theorem 3.4. □

Over $\mathbb{C}(t)$ the required equations of D are simply

$$\begin{cases} g_i = y_i - f_i(x) = 0 & (1 \le i \le m), \\ g_{m+j} = \pi_j(y) - \alpha_j t = 0 & (1 \le j \le n). \end{cases} \tag{4.1}$$

There are $n + m$ equations in $n + m$ variables. Their solution set is finite and nonempty for $\alpha t \in V$. When viewed over $\mathbb{C}(t)$, the Proposition 4.2 says that each coordinate x_i or y_i is algebraic over $\mathbb{C}(t)$, and so a solution to the system 4.1 over $\mathbb{C}(t)$ has coordinates that are algebraic over $\mathbb{C}(t)$. In the next section, we see that the y-coordinates are in fact integral, and how one can view them as elements of $\mathcal{K}$. The following example illustrates the above discussion.

Example 4.3. For $F(x_1, x_2) = (x_1, x_1x_2 - 1, x_1^2x_2 - 1)$, the image closure is $Y = V(y_3 - y_1(y_2+1)+1)$. Take the y_1, y_2-plane $H = \{y_3 = 0\}$, identified with $\mathbb{A}^2$, and project by $\pi(y) = (y_1, y_2)$. This is an isomorphism on Y, hence a finite Noether normalization. The line $L \subset H$ given by $y_1 = y_2 = t$ imposes $x_1 = t$ and $x_1x_2 = t + 1$. The projection and line restriction therefore give a finite generic fiber whose coordinates lie in $\mathbb{C}(t)$. We can choose our open set V to be $\mathbb{A}^2_{\mathbb{C}} \setminus \{y_1 = 0\}$. The generators g_i of I_D are given by

$$g_1 = y_1 - x_1,\ g_2 = y_2 - x_1x_2 + 1,\ g_3 = y_3 - x_1^2x_2 + 1,\ g_4 = y_1 - t,\ g_5 = y_2 - t. \tag{4.2}$$

Above V, the solution set over $\mathbb{C}(t)$ of the system (4.2) is finite.

4.2 Specializing the finite generic fiber

Put $Y_0 = Y \cap \pi^{-1}(0_n)$. This set is finite and nonempty by Theorem 3.8. Lemma 3.9 already ensures that every $y_0 \in Y_0$ lies on a component of C dominating L. First we recall the following standard fact about algebraic embeddings and integral elements.

Lemma 4.4 ([The26, Tags 09GU, 00IC])**.** *The natural inclusion $\mathbb{C}(t) \hookrightarrow \mathbb{C}((t))$ extends to an embedding $M \hookrightarrow \mathcal{K} = \overline{\mathbb{C}((t))}$, for each Galois extension M of $\mathbb{C}(t)$. Every such embedding maps the integral closure of $\mathbb{C}[t]$ in M into $\mathcal{O}_{\mathcal{K}}$, and $\mathcal{O}_{\mathcal{K}}$ is integrally closed.*

Recall from Proposition 4.2 that for each irreducible component D' of D, $\mathbb{C}(D')$ is a finite extension of $\mathbb{C}(t)$. In fact, the coordinates $(x(t), y(t))$ of a point on $\mathbb{C}(D')$ are algebraic over $\mathbb{C}(t)$. By Lemma 4.4 we consider them as elements of $\mathcal{K}$. The following proposition gives the valuation theoretic properties of the y-coordinates.

Proposition 4.5. *Every solution $(x(t), y(t)) \in \mathcal{K}^{n+m}$ of (4.1) satisfies $\mathsf{val}_t(y_i(t)) \geq 0$, i.e., $y_i(t) \in \mathcal{O}_\mathcal{K}$, and $y(0) \in Y_0$. Conversely, every point of Y_0 occurs as such a residue.*

Proof. Since π is finite, Remark 3.7 shows that each y_i is integral over $\mathbb{C}[u_1, \ldots, u_n]$ via π^*. Substituting $u_j = \pi_j(y) = \alpha_j t$ gives monic equations over $\mathbb{C}[t]$, so $\mathsf{val}_t(y_i(t)) \geq 0$. Taking constant terms in the equations of Y and in $\pi(y) = t\alpha$ gives $y(0) \in Y_0$.

Conversely, fix $y_0 \in Y_0$ and choose an irreducible component W of C through y_0 dominating L, by Lemma 3.9. Since $p(D)$ contains the part of C above $L \cap V$, some irreducible component D' of D dominates W. Let $E = \mathbb{C}(D')$ and take a finite Galois extension $M/\mathbb{C}(t)$ containing E. Since $W \to L$ is finite, the coordinate ring $\mathbb{C}[W]$ is contained in the integral closure B of $\mathbb{C}[t]$ in M.

Recall from the classical geometric points and maximal ideals correspondence that there is a maximal ideal $\mathfrak{m}_{y_0}$ of $\mathbb{C}[W]$ whose vanishing set is exactly the point y_0. The ideal $\mathfrak{m}_{y_0}$ is generated by image of $y_i - y_{0,i}$ in $\mathbb{C}[W]$ by Hilbert Nullstellensatz. By the lying-over theorem [AM69, Theorem 5.10], there exists a maximal ideal $\mathfrak{n}$ of B lying above $\mathfrak{m}_{y_0}$.

By Lemma 4.4, choose an embedding $\rho : M \hookrightarrow \mathcal{K}$ over $\mathbb{C}(t)$. Since B is integral over $\mathbb{C}[t]$, we have $\rho(B) \subseteq \mathcal{O}_\mathcal{K}$. The embedding ρ therefore determines a maximal ideal of B above (t) because $\mathfrak{m}_{y_0}$ maps to an ideal above (t) in $\rho(\mathbb{C}[W])$. Since the maximal ideals in a finite Galois extension are Galois conjugates [The26, Tag 09EA], we may compose ρ with a Galois automorphism so that the resulting embedding satisfies

$$\mathsf{val}_t(\rho(y_i) - y_{0,i}) > 0 \qquad (1 \leq i \leq m).$$

Applying this embedding to the coordinate functions of D' gives a solution $(x(t), y(t)) \in \mathcal{K}^{n+m}$ of (4.1) satisfying $y(0) = y_0$. □

In Example 4.3, the curve C is itself irreducible, and for $t \in V = \mathbb{A}^1_\mathbb{C} \setminus \{0\}$, the coordinates of solutions over $\mathbb{C}(t)$ of the system 4.2 are

$$(x_1(t), x_2(t), y_1(t), y_2(t), y_3(t)) = \left(t, \frac{t+1}{t}, t, t, t^2 + t - 1\right) \in D,$$

of whom the y-coordinates t, t, $t^2 + t - 1$ are integral over $\mathbb{C}[t]$. Furthermore, $Y_0 = \{(0, 0, -1)\}$, and one can directly see that $y_i - y_{0,i}$ is $t, t, t^2 + t$, for $i = 1,\ 2,\ 3$, respectively. So for all i $\mathsf{val}_t(y_i - y_{0,i}) = 1$.

4.3 Relative closure and homogenization of all coordinates

Take the closure $\overline{D} \subseteq \mathbb{P}^n_\mathbb{C} \times C$ via the natural embedding $\mathbb{A}^n_\mathbb{C} \times C \to \mathbb{P}^n_\mathbb{C} \times C$. The closure $\overline{D}$ is the union of the closures $\overline{D'}$ of the irreducible components D' of D. By Proposition 4.2, each D' is an irreducible curve. Since D' is locally closed, it is open and dense in $\overline{D'}$. Thus $\overline{D'} \setminus D'$ is a proper closed subset of an irreducible curve and hence consists of finitely many points (see [Har77, Chapter I, §8, p. 56]). Moreover, the irreducible components of $\overline{D}$ are precisely the closures of the irreducible components of D.

Since $\mathbb{P}^n_\mathbb{C}$ is complete, the projection $\mathbb{P}^n_\mathbb{C} \times C \to C$ is closed [Mil24, Definition 7.1 and Theorem 7.22]. Extend the map p to $\overline{D}$, and call it again p. Thus $p(\overline{D})$ is closed and contains the dense part of C

above $L \cap V$, so $p(\overline{D}) = C$. Since $C \to L$ is finite and surjective, the composition $\overline{\beta} = \pi \circ p : \overline{D} \to L$ is surjective with finite fibers.

Moreover, recall by Proposition 4.2, every irreducible component of D' of D is a curve dominating L, and we obtain $\overline{D}$ by closing each irreducible component of D. Hence for each irreducible component D' of D, the map $\overline{\beta}|_{\overline{D'}} : \overline{D'} \to L$ is surjective with finite fiber.

For $t\alpha \in L$, define the finite set

$$\overline{S_t} \coloneqq \overline{\beta}^{-1}(t\alpha).$$

Then

$$p(\overline{S_0}) = Y_0, \qquad 0_m \in Y \iff 0_m \in p(\overline{S_0}). \tag{4.3}$$

By Proposition 4.5, the points of D over $\mathcal{K}$ are represented by solutions $(x(t), y(t))$ of (4.1), with $y(t) \in \mathcal{O}_{\mathcal{K}}^m$. Clearing denominators in the projective x-coordinates gives

$$[1 : x_1(t) : \cdots : x_n(t)] = [t^a : t^a x_1(t) : \cdots : t^a x_n(t)],$$

where $a \in \mathbb{Q}_{\geq 0}$ is chosen so that all coordinates have nonnegative valuation and at least one has valuation zero. Taking constant terms gives a point of $\overline{D}$ above $t = 0$.

Conversely, let $q \in \overline{S_0}$, and choose an irreducible component $\overline{D'}$ of $\overline{D}$ containing q. By Proposition 4.2, $\overline{D'}$ dominates L.

By the local Newton–Puiseux parametrization theorem for algebraic curves [The26, Tags 0C45, 0C0S] (see also [Abh90, Lecture 14, p. 104]), there is a Puiseux branch $\tilde{q}(s)$ of $\overline{D'}$ through q, parametrized by $s = t^{1/e}$ for some $e \geq 1$, such that the projective x-coordinates of $\tilde{q}(s)$ are

$$[x_0(s) : x_1(s) : \cdots : x_n(s)], \qquad x_i(s) \in \mathbb{C}[[s]],$$

with $\tilde{q}(0) = q$. Since the component intersects D in an open set of D, we have $x_0(s) \not\equiv 0$. Consequently, $x_i(s)/x_0(s) \in \mathcal{K}$, and together with the corresponding y-coordinates these give a solution of (4.1). Clearing denominators in its projective x-coordinates recovers $\tilde{q}$. We summarize this discussion as the following proposition.

Proposition 4.6. *Every point $q \in \overline{S_0}$ is the specialization of a Puiseux family $\tilde{q}(t) \in \overline{S_t}$ with homogeneous coordinates $[x_0(t) : \cdots : x_n(t)]$, where for all i, $x_i(t) \in \mathcal{O}_{\mathcal{K}}$, and $x_0(t) \not\equiv 0$. Therefore, $\overline{S_t} \subseteq \{x_0 \neq 0\} \simeq \mathbb{A}^n_{\mathcal{K}}$, so $\overline{S_t}$, viewed as a projective algebraic set over $\mathcal{K}$, is affine.*

Returning back to the Example 4.3, one sees that the curve D is given by $(t, (t+1)/t, t, t, t^2+t-1)$. The x coordinates are defined over $\mathbb{C}(t)$. Viewing it in projective coordinates, we obtain that $\overline{D}$ is given by

$$\left(\left(1 : t : \frac{t+1}{t}\right), (t, t, t^2 + t - 1)\right) = \left((t : t^2 : t+1), (t, t, t^2 + t - 1)\right) \subset \mathbb{P}^2_{\mathbb{C}} \times C.$$

Furthermore, $x_0 \neq 0 \in \mathcal{O}_{\mathcal{K}}$.

This relative closure explains the geometry, but does not provide a homogeneous system with the same number of homogeneous equations as the number of homogenized variables, which is needed for a resultant. Homogenizing only in x would still require the equations of C, which we do not know.

In Example 4.3, the homogenized graph equations in just the x-coordinates allow $[x_0 : x_1 : x_2] = [0 : 0 : 1]$ with arbitrary y_3, whereas C requires $y_3 = t^2 + t - 1$. In particular, at $t = 0$ just homogenizing in x-coordinates will not be able to distinguish if $0 \in Y$ unless the equations defining C are known, which is something we want to avoid.

We observe, that if we could homogenize the system 4.1 with respect to all x and y variables, then we will get a homogeneous system amenable to the resultant method of [AGS26]. So we use the map

$$\iota : \mathbb{P}^n_{\mathcal{K}} \times \mathbb{A}^m_{\mathcal{K}} \longrightarrow \mathbb{P}^{n+m}_{\mathcal{K}}, \qquad ([x_0 : \cdots : x_n], y) \longmapsto [x_0 : \cdots : x_n : x_0y_1 : \cdots : x_0y_m],$$

and show that we do not lose the information we were looking for. Observe that on $x_0 \neq 0$, division by x_0 recovers both x and y. Thus the Puiseux branches in Proposition 4.6 retain their output coordinates over $\mathcal{K}$; information is lost only when x_0 is identically zero.

Once again for the case of Example 4.3, the relative to L branch and its image under ι are

$$\Big([t : t^2 : t+1], (t, t, t^2+t-1))\Big) \longmapsto v(t) = [t : t^2 : t+1 : t^2 : t^2 : t(t^2+t-1)].$$

Its first coordinate is nonzero over $\mathcal{K}$, so we can extract y-coordinates by factoring out $x_0(t) = t$, which is not identically 0, from the last three coordinates $t^2, t^2, t(t^2+t-1)$. If we specialize to $t = 0$, then the last three y-coordinates become $(0, 0, 0)$, and so the projection to the y-coordinates will contain $(0, 0, 0)$, but as noted earlier it is not a point in Y_0. This also shows why it is important to first work over $\mathbb{C}[t]$, and then specialize later to $t = 0$, instead of specializing first to $t = 0$.

We set $N = n + m$, $z = (x, y)$, and homogenize using the formal degree bounds over $\mathbb{C}[t]$. Let

$$G_i(z_0, z, t) = z_0^{d_i} g_i(z/z_0, t), \qquad \max(1, \deg_z g_i) \leq d_i \leq d, \quad 1 \leq i \leq N. \tag{4.4}$$

These are N homogeneous equations in $N + 1$-variables over $\mathbb{C}[t]$. On the chart $z_0 \neq 0$ over $\mathcal{K}$, they give exactly the finite solution set of (4.1).

Theorem 4.7. *The map F has APS if and only if there are $z_0(t), \ldots, z_N(t) \in \mathcal{K}$ satisfying*

$$\begin{aligned} z_0(t) \neq 0, \qquad & \min_{0 \leq j \leq N} \mathsf{val}_t(z_j(t)) = 0, \\ G_i(z_0(t), \ldots, z_N(t)) = 0 \quad & (1 \leq i \leq N), \\ \mathsf{val}_t\left(\frac{z_{n+i}(t)}{z_0(t)}\right) > 0 \quad & (1 \leq i \leq m). \end{aligned} \tag{4.5}$$

Proof. If $0 \in Y$, Proposition 4.5 supplies an affine solution with $y(0) = 0$, so $\mathsf{val}_t(y_i(t)) > 0$. Clearing the denominators in homogeneous coordinates $(1 : x_1(t) : \ldots : y_m(t))$ with a power of t such that the minimum of $\mathsf{val}_t(x_i)$ or $\mathsf{val}_t(y_i)$ is zero, one obtains z_0 with required properties. Conversely, dehomogenizing a tuple in (4.5) gives $y_i(t) = f_i(x(t)) = z_{n+i}(t)/z_0(t)$, so $\mathsf{val}_t(y_i(t)) > 0$ and $y(0) = 0$ and $0 \in Y$. □

5 An approximative characteristic polynomial

We now construct the polynomial $R_\ell(T)$ from the proof idea in Section 2.1. Keep the reduced map and the square system (4.1), i.e., the number of variables are the same as the number of equations, and homogeneous system (4.4) from Section 4. In Section 4.3, Proposition 4.6 and Theorem 4.7 we saw that the Puiseaux branches in $\overline{S_t}$ on $\overline{D}$ that specialize to the points on $\overline{S_0}$ and project to a point in Y_0 under p correspond to the affine $(z_0 \neq 0 \in \mathcal{K})$ solutions of the homogeneous system (4.4) over $\mathcal{K}$. As noted before, this is exactly the kind of problem studied in [AGS26, Section 4].

So we let $Z \subseteq \mathcal{K}^N$ be finite nonempty solution set of the system (4.1) viewed over $\mathcal{K}$, and let $y(z)$ denote the tuple $(z_{n+1}, \ldots, z_{n+m})$ in the $n + m$-tuple $z = (z_1, \ldots, z_{n+m})$. Proposition 4.5 says that the set of $y(z)(0)$, as z ranges over Z, are exactly Y_0. Choose a linear form ℓ injective on $Y_0 \cup \{0\}$.

Such forms exist because the excluded coefficient tuples lie in finitely many proper hyperplanes. Then

$$Q_{Y_0,\ell}(T) = \prod_{y\in Y_0}(T-\ell(y)), \qquad Q_{Y_0,\ell}(0) = 0 \iff 0 \in Y. \tag{5.1}$$

We compute a polynomial with the same set of roots as $Q_{Y_0,\ell}$, allowing positive multiplicities, using only the explicit homogeneous equations G_i.

5.1 The perturbation of Ierardi and $H_{T,w}$

Let $d_i = \deg(G_i)$, and d be a degree bound on d_i, and let

$$\widehat{G}_i \coloneqq G_i + \varepsilon z_i^{d_i}, \qquad B \coloneqq \prod_{i=1}^{N} d_i \le d^N.$$

Here ε is independent of the line parameter t. Let

$$H_{T,w} \coloneqq Tz_0^2 - z_0\ell(y(z)) + \sum_{j=1}^{N} w^j z_j^2, \tag{5.2}$$

and define

$$\mathscr{R}(T,t,w,\varepsilon) \coloneqq \mathrm{Res}_{z_0,\ldots,z_N}(\widehat{G}_1,\ldots,\widehat{G}_N,H_{T,w}). \tag{5.3}$$

The quadratic form $H_{T,w}$ over $\mathbb{C}(T,w)$ is chosen to output the factors of the polynomial $Q_{Y_0,\ell}(T)$. Similar to [AGS26, Lemma 4.8], we note that if $z = (z_0 : \ldots : z_N) \in Z$, then $\mathrm{TC}_w(H_{T,w}(z)) = T - \ell(y(z))$ when $z_0 = 1$, and $H_{T,w}(z) = \sum_{j=1}^{N} w^j z_j^2$ when $z_0 = 0$. Here recall from Section 3.2 that $\mathrm{TC}_v(P)$ is the trailing coefficient of P with respect to a variable v. So $H_{T,w}(z)$ is a constant free polynomial in w exactly when $z_0 = 0 \in \mathcal{K}$. This is what we use to single out the affine solutions of the homogeneous system (4.4). Let $Z_0^* \subset \mathbb{P}^N_{\mathcal{K}}$ be a finite set of limit points in the sense of [AGS26, Definition 4.5 and Lemma 4.6] for the system defined by polynomials $\widehat{G}_i$ over $\mathbb{C}(t,\varepsilon)$. Then Z_0^* contains all the isolated projective points over $\mathcal{K}$ of the system (4.4) and is finite.

Remark 5.1. The set Z_0^* contains may contain a finite set of points from the positive dimensional components of $V(G_1,\ldots,G_N)$ over $\mathcal{K}$ at $z_0 = 0$. However, the affine points in Z_0^* are exactly the ones in Z, i.e., the solutions to the affine system (4.1) over $\mathcal{K}$, as the system (4.1) defines the 0-dimensional Z over $\mathcal{K}$.

We now state the standard factorization lemma of [Ier89, Lemma 2.6] applied to our polynomials $\widehat{G_i}$ and $H_{T,w}$.

Lemma 5.2 ([Ier89, Lemma 2.6] or [AGS26, Lemma 4.7])**.** *Let G_i, $\widehat{G_i}$, $H_{T,w}$, and Z_0^* be as above. For each $z \in Z_0^*$, there are positive integers $\mu_z > 0$ such that*

$$(\mathrm{TC}_\varepsilon \mathscr{R})(T,t,w) = \prod_{z\in Z_0^*} H_{T,w}(z)^{\mu_z}.$$

Recall that each $z \in Z$, corresponds to the projective solution $[1 : z]$ to the system (4.4), so we choose $z_0 = 1$. As a consequence of the above lemma we obtain that

$$\mathrm{TC}_w\left(\prod_{z\in Z_0^*} H_{T,w}(z)^{\mu_z}\right) = c(t)\prod_{z\in Z} H_{T,w}(z)^{\mu_z} = c(t)\prod_{z\in Z}(T-\ell(y(z)))^{\mu_z}, \tag{5.4}$$

for some $c(t) \in \mathcal{O}_{\mathcal{K}}$. Here $c(t)$ turns out to be an element in $\mathcal{O}_{\mathcal{K}}$ precisely because it is coming from the points $z \in Z^*$ with $z_0 = 0$, and for such points we can clear the denominators and assume that $z_1,\ldots,z_N \in \mathcal{O}_{\mathcal{K}}$. Futhermore, at least one of $z_1,\ldots,z_N$ is non-zero, so $c(t) \neq 0$.

5.2 R_ℓ and $Q_{Y_0,\ell}$ have same roots

In this section we finally show that the univariate polynomials R_ℓ and $Q_{Y_0,\ell}$ have same roots as claimed.

Theorem 5.3. *Let R_ℓ, and $\mathscr{R}$ be as above. Then there is a $c \in \mathbb{C}^\times$ such that*

$$R_\ell(T) := \mathrm{TC}_t \,\mathrm{TC}_w \,\mathrm{TC}_\varepsilon \,\mathscr{R} = c \prod_{y \in Y_0} (T - \ell(y))^{M_y}, \quad M_y > 0. \tag{5.5}$$

Therefore,

$$F \text{ has APS} \iff R_\ell(0) = 0. \tag{5.6}$$

Proof. By Proposition 4.5, for $z \in Z$ the coordinates of $y(z)$ are elements of $\mathcal{O}_\mathcal{K}$, and so have non-negative valuation with respect to val_t. Therefore, $\mathsf{val}_t(\ell(y(z))) \geq 0$, for $z \in Z$. By Lemma 5.2 and equation (5.4), we obtain

$$R_\ell(T) = \mathrm{TC}_t \left(c(t) \prod_{z \in Z} (T - \ell(y(z)))^{\mu_z} \right) = \mathrm{TC}_t(c(t)) \prod_{z \in Z} (T - \ell(y(z)(0)))^{\mu_z}.$$

The last equality above follows because at the factors $\mathrm{TC}_t(T - \ell(y(z))) = T - \ell(y(z)(0))$, and the trailing coefficient operation distributes over a product. Once again by Proposition 4.5, the set $\{y(z)(0) \mid z \in Z\}$ is the same as Y_0, so we obtain

$$R_\ell(T) = c \prod_{y \in Y_0} (T - \ell(y))^{M_y},$$

where $c \in \mathbb{C}^\times$ and $M_y > 0$. Note that for $y(z)(0) = y$, M_y may not be equal to μ_z, since we only have a equality of sets $\{y(z)(0) \mid z \in Z\} = Y_0$. This finishes the proof. □

In Example 4.3, the polynomials $G_i = x_0^{\deg(g_i)} g_i(x_1/x_0, \ldots, y_3/x_0)$, where g_i polynomials over $\mathbb{C}[t]$ given in (4.2). The solution set over K consists of $p(t) = (t : t^2 : t+1 : t^2 : t^2 : t(t^2+t-1))$ and $[0:0:a:0:0:b] \simeq \mathbb{P}^1_\mathcal{K}$. The operation TC_ε will get rid of all but finitely many points of the component $\mathbb{P}^1_\mathcal{K}$ at $x_0 = 0$, and the only isolated affine point is $p(t) \in \mathbb{P}^5_\mathcal{K}$. Choose $\ell(y) = y_3$. Over $\mathbb{C}(t)$, the affine system has the unique solution

$$(x_1, x_2, y_1, y_2, y_3) = \left(t, \frac{t+1}{t}, t, t, t^2 + t - 1 \right).$$

This solution is simple: the equations determine y_1, y_2, x_1, x_2, y_3 successively, with the coefficient of x_2 equal to $-t \neq 0$.

For the projective representative $p(t)$ displayed above,

$$H_{T,w}(p(t))|_{w=0} = t^2(T - (t^2 + t - 1)).$$

Every point of Z_0^* at infinity contributes a factor whose trailing coefficient in w is nonzero and independent of T. Since the unique affine solution is simple, the resultant factorization therefore gives

$$\mathrm{TC}_w \,\mathrm{TC}_\varepsilon \,\mathscr{R} = c(t)(T - (t^2 + t - 1))$$

for some nonzero $c(t) \in \mathbb{C}[t]$. Here $c(t)$ is a polynomial because it is the coefficient of T on the left-hand side.

Taking the trailing coefficient in t, we obtain

$$R_\ell(T) = c(T+1), \qquad c = \mathrm{TC}_t(c(t)) \neq 0.$$

Thus R_ℓ has the same roots as $Q_{Y_0,\ell}(T) = T + 1$. In particular, $R_\ell(0) \neq 0$, so Theorem 5.3 confirms that the original system has no APS.

5.3 The test in the Counting Hierarchy

Theorem 5.3 reduces APS, for generic choices of the auxiliary parameters, to the test

$$(\mathrm{TC}_t\,\mathrm{TC}_w\,\mathrm{TC}_\varepsilon\,\mathscr{R})\,(0) = 0.$$

To obtain a Counting Hierarchy algorithm, we must implement this test from the given arithmetic circuits. This requires choosing the auxiliary parameters with polynomial bit length and bounded failure probability, and accessing the required coefficients without expanding the resultant.

Section 6 supplies these details. In particular, the resultant degrees and coefficient bit lengths are at most singly exponential in the input length, so monomial exponents and bit positions have polynomial-length encodings. Access to individual coefficient bits, together with a fixed number of quantifier blocks over these indices, suffices to perform the three trailing-coefficient operations and the final vanishing test.

6 Effective construction in the Counting Hierarchy

We now implement the criterion in Equation (5.6) from the given arithmetic circuits. Throughout this section, L denotes the original input length, including the binary encodings of rational constants. All circuits constructed below have size polynomial in L. Their formal degrees, and the bit lengths of their expanded coefficients, may be singly exponential.

6.1 Dimension and reduction of the input

We first determine the image dimension needed for Proposition 3.14.

Lemma 6.1 (Image dimension from exact feasibility)**.** *For a polynomial map given by rational circuits, the dimension of its image closure is computable in deterministic polynomial time with an oracle at a fixed level of* CH.

Proof. Let $F = (f_1, \dots, f_m)$ be a map in n variables, and let J_F be its Jacobian matrix. In characteristic zero, the transcendence degree of $\mathbb{Q}(f_1, \dots, f_m)$ equals the rank of J_F over $\mathbb{Q}(x_1, \dots, x_n)$.

For $1 \le k \le \min\{m, n\}$, introduce matrices of variables $B \in \mathbb{A}^{k\times m}$ and $C \in \mathbb{A}^{n\times k}$, and a variable v. Then

$$\operatorname{rank}_{\mathbb{Q}(x)} J_F \ge k \quad\Longleftrightarrow\quad v\det(BJ_F(x)C) - 1 = 0 \text{ has a complex solution.} \tag{6.1}$$

Indeed, a nonzero k-minor can be made nonzero at some point x, and B, C can select that minor. Conversely, an invertible $BJ_F(x)C$ certifies rank at least k.

Differentiation and the determinant construction of [Ber84] give a polynomial-size circuit for the polynomial in (6.1). Introduce one variable for each gate value, impose its defining equation, and set the output to zero. This gives a polynomial-size quadratic HN instance with the same feasibility status. By [AGS26, Theorem 6.9], its feasibility is decidable at a fixed level of CH. Testing the polynomially many values of k determines the image dimension. □

Write r for this dimension. If $r = 0$, the image consists of one point, so APS is equivalent to exact feasibility of the original system. We decide this using HN. If $r = m$, the image closure is $\mathbb{A}^m$, so APS holds.

For $1 \le r < m$, apply Proposition 3.14, choosing its sampling grid so that the failure probability is at most $1/12$. The logarithms of the degree bounds in that proposition are polynomial in L, so the

sampled integers have polynomial bit length. The affine subspace can be parametrized by rational linear algebra, and substitution preserves polynomial circuit size. If the sampled equations do not define an r-dimensional affine subspace, we return an arbitrary answer; this is included among the unsuccessful reduction choices.

Without loss of generality, we have the polynomial map $F = (f_1, \dots, f_m)$ such that $m = n + 1$, and $\dim \overline{F(\mathbb{A}^n)} = n \geq 1$ for which we need to check the existence of APS. Let $d \geq 2$ bound its formal degrees. Then $d \leq 2^{\mathrm{poly}(L)}$. Use the equations and homogenizations from Equations (4.1) and (4.4), with

$$N = n + m, \qquad 1 \leq d_i \leq d, \qquad B = \prod_{i=1}^{N} d_i \leq d^N.$$

Here the d_i are fixed homogenizing degrees, chosen before sampling the remaining parameters. Homogenization can be performed gate by gate using formal degrees; powers of the homogenizing variable are computed by repeated squaring. Consequently, the homogeneous equations and their perturbations still have polynomial-size circuit descriptions.

6.2 Choosing the auxiliary parameters

Let Θ collect the coefficients of the projection π, the direction α, and the linear form ℓ. There are polynomially many such parameters. For the fixed reduced input, regard them first as independent indeterminates, and form the resultant from (5.3):

$$\mathscr{R}_\Theta \in \mathbb{Q}[\Theta, \varepsilon, t, w, T].$$

The geometric argument of Theorem 5.3 applies over an algebraic closure of $\mathbb{Q}(\Theta)$. Hence, defining

$$Q_\Theta(T) := \mathrm{TC}_t \, \mathrm{TC}_w \, \mathrm{TC}_\varepsilon \, \mathscr{R}_\Theta, \qquad F \text{ has APS} \iff Q_\Theta(0) = 0 \text{ in } \mathbb{Q}[\Theta], \tag{6.2}$$

we obtain a polynomial identity on yes-instances and a nonzero polynomial on no-instances. We use this symbolic construction only to analyze the random choices; the algorithm does not construct Q_Θ.

We next bound the degree of $\mathscr{R}_\Theta$. The resultant is homogeneous of degree $2B/d_i$ in the coefficients of the ith perturbed equation and degree B in the coefficients of $H_{T,w}$. Its total degree in these coefficient groups is therefore at most $(2N + 1)B$. Each substituted coefficient has total degree at most $N + 1$ in $\Theta, \varepsilon, t, w, T$. Thus

$$\deg \mathscr{R}_\Theta \leq D_* := (N + 1)(2N + 1)d^N = 2^{\mathrm{poly}(L)}. \tag{6.3}$$

In particular, D_* has a polynomial-length binary encoding.

The following lemma controls the effect of substituting numerical values for Θ.

Lemma 6.2 (Stability of nested trailing coefficients)**.** *Let*

$$R(\Theta, t_1, \dots, t_k, T) \in \mathbb{Q}[\Theta, t_1, \dots, t_k, T]$$

be nonzero and have total degree at most D. There are nonzero polynomials $A_1, \dots, A_k \in \mathbb{Q}[\Theta]$, each of degree at most D, such that, whenever $A_i(\theta) \neq 0$ for all i,

$$(\mathrm{TC}_{t_k} \cdots \mathrm{TC}_{t_1} R)(\theta, T) = \mathrm{TC}_{t_k} \cdots \mathrm{TC}_{t_1} \big(R(\theta, t_1, \dots, t_k, T)\big).$$

Proof. Take the first nonzero coefficient of R in t_1. Choose a nonzero coefficient $A_1(\Theta)$ of one of its monomials in the remaining variables. If $A_1(\theta) \neq 0$, this coefficient polynomial remains nonzero after substitution. All lower coefficients were identically zero, so the first trailing exponent is unchanged.

Repeat this argument on the selected coefficient polynomial, successively for $t_2, \ldots, t_k$. Extracting coefficients never increases total degree, so each A_i has degree at most D. □

Let $M = 2^k$ for some k such that $M \geq 48D_*$, and sample each coordinate of θ independently and uniformly from $\{1, \ldots, M\}$. Apply Lemma 6.2 with

$$(t_1, t_2, t_3) = (\varepsilon, w, t).$$

If none of its three exceptional polynomials vanishes, then

$$\mathrm{TC}_t \, \mathrm{TC}_w \, \mathrm{TC}_\varepsilon \, \mathscr{R}_\theta = Q_\Theta(\theta, T).$$

On a yes-instance, the constant coefficient on the right is zero by (6.2). On a no-instance, $Q_\Theta(0)$ is a nonzero polynomial in Θ of degree at most D_*, and its specialization can vanish only on one additional exceptional set. Schwartz–Zippel therefore gives

$$\Pr_\theta[(\mathrm{TC}_t \, \mathrm{TC}_w \, \mathrm{TC}_\varepsilon \, \mathscr{R}_\theta)\,(0) = 0 \text{ gives the wrong answer}] \leq \frac{4D_*}{M} \leq \frac{1}{12}. \tag{6.4}$$

Every sampled integer has polynomial bit length. Neither the exceptional polynomials nor Q_Θ need to be computed.

Remark 6.3 (Nonzero resultant for every sample)**.** The polynomial $\mathscr{R}_\theta$ is nonzero for every specialization θ, including unsuccessful choices. Indeed, its coefficient of the highest possible power of ε is

$$\mathrm{Res}_{z_0,\ldots,z_N}(z_1^{d_1}, \ldots, z_N^{d_N}, H_{T,w}) = \pm T^B.$$

Thus all three trailing-coefficient operations are defined for every sample.

6.3 Coefficient access and the final test

We now fix a sampled tuple θ of polynomial bit length. The remaining auxiliary variables are ε, t, w, T.

Since the input coefficients are rational, we allow a coefficient to be represented as a/b, where $a \in \mathbb{Z}$ and $b \in \mathbb{Z}_{>0}$; this representation need not be reduced. Access to its bits means access to the sign and binary magnitude bits of a and to the bits of b. A coefficient vanishes exactly when its numerator vanishes.

Theorem 6.4 (Resultant coefficient access)**.** *For the resultant $\mathscr{R}_\theta$, a specified bit of the numerator or denominator representing a specified coefficient is computable at a fixed level of* CH*. Its degrees and the bit lengths of these representations are bounded by $2^{\mathrm{poly}(L)}$. These statements hold uniformly over all sampled tuples θ of polynomial bit length.*

Proof. The coefficient-access argument in Section 3 provides a CH oracle for the coefficients of the input forms. Their implicit dense descriptions have singly exponential length.

By [AGS26, Corollary 5.13], the resultant coefficients are computed by uniform constant-depth arithmetic circuits of size

$$\big(P(N+1)\big)^{\mathrm{poly}(N)} = 2^{\mathrm{poly}(L)}, \qquad P = B + \sum_{i=1}^{N} \frac{2B}{d_i}.$$

Here there are four auxiliary variables, and their degrees in the input coefficients are at most $N+1$. The arithmetic-to-threshold simulation of [AGS26, Lemma 6.1] preserves constant depth and gives singly exponential size and output bit-length bounds.

The gate-evaluation argument of [AGS26, Lemma 6.3] applies with the input bits supplied by the coefficient oracle: gate indices have polynomial length, input gates are evaluated in CH, and each further threshold layer adds one majority quantifier. Since the depth is constant, output bits remain at a fixed level of CH. The degree bound follows from (6.3). □

In particular, exponentially long coefficients cause no difficulty: a position within such a coefficient still has a polynomial-length binary encoding. The next lemma makes the resulting vanishing test explicit.

Lemma 6.5 (Trailing-coefficient test)**.** *Let $R(t_1,\dots,t_k,T)$ be a nonzero rational polynomial, where k is fixed. Suppose its degrees and the numerator and denominator bit lengths in its coefficient representations are bounded by $2^{\mathrm{poly}(L)}$, and that individual coefficient bits are accessible at a fixed level of CH. Then the predicate*

$$(\mathrm{TC}_{t_k}\cdots\mathrm{TC}_{t_1}\,R)\,(0)=0$$

also belongs to a fixed level of CH.

Proof. Write

$$R=\sum_{e,j} c_{e,j}t_1^{e_1}\cdots t_k^{e_k}T^j.$$

Choose a bound $U=2^{p(L)}$ large enough to cover all exponents and coefficient bit lengths. Each exponent and bit position then has a polynomial-length encoding.

If $c_{e,j}=a_{e,j}/b_{e,j}$ with $b_{e,j}>0$, then

$$c_{e,j}\neq 0 \quad\Longleftrightarrow\quad \exists\, q<U : \text{the } q\text{th magnitude bit of } a_{e,j} \text{ is } 1.$$

Thus coefficient vanishing and nonvanishing are decidable in CH.

The successive trailing operations select the lexicographically least tuple e for which some $c_{e,j}$ is nonzero, with e_1 compared first. Guess this tuple and require

$$\exists j\ c_{e,j}\neq 0, \qquad \forall e' <_{\mathrm{lex}} e\ \forall j\ c_{e',j}=0.$$

Finally, require $c_{e,0}=0$. All indices are bounded by U, and all quantified strings have polynomial length. Expanding the coefficient tests introduces only a fixed number of additional quantifier blocks over the coefficient-bit oracle. Hence the whole predicate lies at a fixed level of CH. □

Proof of Theorem 1.3. Compute the image dimension using Lemma 6.1. Handle the cases $r=0$ and $r=m$ as described above. Otherwise, perform the reduction of Proposition 3.14, with failure probability at most $1/12$.

For the reduced map, choose the auxiliary parameters from the grid specified above and form the circuit descriptions of the homogeneous equations and their perturbations. By Theorem 6.4 and Lemma 6.5, we can test

$$(\mathrm{TC}_t\,\mathrm{TC}_w\,\mathrm{TC}_\varepsilon\,\mathscr{R}_\theta)\,(0)=0$$

using an oracle at a fixed level of CH. This test is defined for every sample by Remark 6.3.

Conditional on a successful input reduction, Theorem 5.3 and (6.4) show that the test is correct with probability at least $11/12$. Including the input reduction, the total error probability is at most $1/6$.

All random choices use polynomially many bits, and all remaining computations take polynomial time with the stated oracles. Choose a fixed b large enough to include these oracles in $C_b\mathsf{P}$. The resulting algorithm belongs to

$$\mathsf{BPP}^{C_b\mathsf{P}} \subseteq \mathsf{PP}^{C_b\mathsf{P}} = C_{b+1}\mathsf{P} \subseteq \mathsf{CH}.$$

This proves the theorem for rational circuit input. Sparse input with binary exponents converts to this representation in polynomial time by repeated squaring. □

Corollary 6.6. *For rational circuit input, and hence for sparse input with binary rational coefficients and binary exponents, deciding whether a system has an approximate zero but no exact zero belongs to* CH.

Proof. Combine Theorem 1.3 with HN in CH and closure of CH under complement and finite Boolean combinations. □

Remark 6.7 (Other coefficient fields)**.** Theorem 1.3 also holds for arithmetic circuits over number fields and finite fields, with image closure taken over the algebraic closure of the coefficient field. We use the standard representation by an irreducible defining polynomial and power-basis coordinates; for finite fields, the characteristic is given in binary. We need the following modifications to accommodate positive characteristic

- The image dimension cannot, in general, be computed by Jacobian rank. Instead, for a tuple of algebraically independent indeterminates z, we compute the dimension of the generic fiber $F(x) = F(z)$ over $k(z)$ and subtract it from the number of input variables. This computation is in CH by [AGS26, Corollary 7.2], using auxiliary variables for the arithmetic circuit gates.
- Writing $K = \overline{k}$, we replace Puiseux series by elements of $\overline{K((t))}$ equipped with the extended t-adic valuation, and interpret limits as residues of elements of nonnegative valuation. The lifting argument uses normalization of curves and extension of valuations, allowing inseparable extensions as well; see [The26, Tag 0ASF]. Noether normalization and the resulting integrality argument remain valid. Products over solutions retain their algebraic multiplicities, which do not affect whether the specialized constant coefficient vanishes.
- Finally, generic parameters are sampled from a sufficiently large finite extension of k. An extension of polynomial degree suffices for our degree bounds and can be constructed using [AGS26, Lemma 2.13]. The resultant coefficient tests use the finite-field version of [AGS26, Theorem 6.7], preserving the CH upper bound. No lower bound on the characteristic relative to the input degrees is required. For number fields, the characteristic-zero geometric argument applies, with arithmetic performed in the given number-field representation.

7 Integral closure membership in the Counting Hierarchy

Here, we prove Theorem 1.8. We do it by reducing integral closure membership testing to APS.

The well-known valuative criterion for integral dependence [AM69, Corollary 5.22] establishes a connection between integrality and valuation theory, see Corollary 7.6 for an equivalent version useful for our purposes. Meanwhile there also exists a connection between valuation theory and APS, see Theorem 3.11. This suggests an underlying connection between integrality and APS, which was also made somewhat explicit in the approximate Rabinowitsch's trick in [ADPS26, Lemma 2]. In the rest of this section, we formalize this intuition to get the desired criterion.

Fix $f, f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$, and let $A = \mathbb{C}[f_1, \ldots, f_m]$. Without loss of generality, we can assume $f \neq 0$, otherwise it is always integral. Using Theorem 3.11, it is easy to see the following connection between APS of a locally defined system of polynomials and their valuations.

Lemma 7.1. *Given $c = (c_1, \ldots, c_m) \in \mathbb{C}^m$ consider the system of polynomials $\Phi_c := (f_1 - c_1, \ldots, f_m - c_m, u, 1 - uf)$ where each polynomial lies in $\mathbb{C}[x_1, \ldots, x_n, u]$. Then, Φ_c has an APS if and only if there exists some $\beta \in \mathbb{C}(t)^{n+1}$, such that for each polynomial $h \in \Phi_c$, $\mathsf{val}_t(h(\beta)) > 0$.*

We can now use the connection of APS to annihilators to get an equivalent local "annihilator" for this locally defined system of polynomials.

Lemma 7.2. *Fix $c = (c_1, \ldots, c_m) \in \mathbb{C}^m$. Then, the system of polynomials $\Phi_c = (f_1 - c_1, \ldots, f_m - c_m, u, 1 - uf)$ has no APS if and only if there exists*

$$Q_c(Y_1, \ldots, Y_m, U, V) \in \mathbb{C}[Y_1, \ldots, Y_m, U, V]$$

such that

(i) $Q_c(f_1, \ldots, f_m, u, 1 - uf) = 0$, *and*

(ii) $Q_c(c_1, \ldots, c_m, 0, 0) = 1$

Proof. By the criterion of [GSS19, ADPS26], non-existence of APS for Φ_c is equivalent to existence of a polynomial $B_c(Z_1, \ldots, Z_m, U, V)$ with constant term equal to 1 after rescaling, such that $B_c(f_1 - c_1, \ldots, f_m - c_m, u, 1 - uf) = 0$. Now define

$$Q_c(Y_1, \ldots, Y_m, U, V) := B_c(Y_1 - c_1, \ldots, Y_m - c_m, U, V).$$

Then $Q_c(f_1, \ldots, f_m, u, 1 - uf) = 0$, and $Q_c(c_1, \ldots, c_m, 0, 0) = B_c(0, \ldots, 0, 0, 0) = 1$.

For the converse, if a Q_c satisfying (i) and (ii) exists, then define

$$B_c(Y_1, \ldots, Y_m, U, V) := Q_c(Y_1 + c_1, \ldots, Y_m + c_m, U, V).$$

Clearly, $B_c(0, \ldots, 0) = Q_c(c_1, \ldots, c_m, 0, 0) = 1$, and $B_c(f_1 - c_1, \ldots, f_m - c_m, u, 1 - uf) = Q_c(f_1, \ldots, f_m, u, 1 - uf) = 0$. Hence, B_c is the annihilator for Φ_c with non-zero constant term, and hence Φ_c has no APS. □

We now come to our main observation: these "local" annihilator certificates Q_c can in fact be converted into a global certificate Q. This is essential as we have infinitely many local certificates which makes any computational strategy impossible to execute. Let Φ denote the system of polynomials $f_1, \ldots, f_m, u, 1-uf$, i.e., $\Phi := (f_1, \ldots, f_m, u, 1-uf)$, and $\mathrm{Ann}(\Phi)$ denote the annihilator ideal of polynomials in Φ.

Theorem 7.3 (Equivalence of the pointwise and global criteria)**.** *With the above notation, the following are equivalent:*

(1) For every $c = (c_1, \ldots, c_m) \in \mathbb{C}^m$, there exists a polynomial $Q_c(Y_1, \ldots, Y_m, U, V) \in \mathrm{Ann}(\Phi)$ such that $Q_c(c_1, \ldots, c_m, 0, 0) = 1$.

(2) There exists a single polynomial $Q(Y_1, \ldots, Y_m, U, V) \in \mathrm{Ann}(\Phi)$ such that $Q(Y_1, \ldots, Y_m, 0, 0) = 1$.

Proof. Let $J := (\mathrm{Ann}(\Phi) + (U, V)) \cap \mathbb{C}[Y_1, \ldots, Y_m]$. Thus, the ideal J may be viewed as the ideal of all Y-polynomials that arise from annihilator relations in $\mathrm{Ann}(\Phi)$ after forgetting all terms divisible by U or by V. Assume first that (1) holds. Fix $c \in \mathbb{C}^m$. By hypothesis there exists $Q_c \in \mathrm{Ann}(\Phi)$ with $Q_c(c, 0, 0) = 1$. Passing to the quotient modulo (U, V), the image $q_c(Y) := Q_c(Y, 0, 0)$ lies in J, and satisfies $q_c(c) = 1 \neq 0$. Hence c is not a common zero of J. Since this is true for every $c \in \mathbb{C}^m$, the variety $V(J)$ is empty. By Hilbert's Nullstellensatz, $J = \mathbb{C}[Y_1, \ldots, Y_m]$, and $1 \in J$. By definition of J, $1 \in J$ means that there exists an annihilator $Q \in \mathrm{Ann}(\Phi)$ whose restriction to the slice $U = V = 0$ is the constant polynomial 1. That is, there exists $Q \in \mathrm{Ann}(\Phi)$ and $R, S \in \mathbb{C}[Y_1, \ldots, Y_m, U, V]$ such that $1 = Q + UR + VS$. Setting $U = V = 0$ gives $Q(Y, 0, 0) = 1$. Thus (2) holds.

Conversely, assume (2). Then for every $c \in \mathbb{C}^m$, evaluating the identity $Q(Y, 0, 0) = 1$ at $Y = c$ yields $Q(c, 0, 0) = 1$. Since $Q \in \mathrm{Ann}(\Phi)$, the same polynomial Q serves as a witness in (1) for every c. Thus (1) holds. □

Remark 7.4. From an algebraic geometric viewpoint one can also see Theorem 7.3 as an explicit version of a classical result: finitely generated locally trivial modules of rank 1 over a unique factorization domain are globally trivial. Indeed $\mathrm{Ann}(\Phi_0)$ is a locally finitely generated module of $R := \mathbb{C}[Y_1, \ldots, Y_m, U, V]$. Our local conditions (1) corresponds in Theorem 7.3 mean that at each $c \in \mathbb{A}^m$ the localized module

$$\left(\mathrm{Ann}(\Phi_0) \otimes \frac{R}{(U, V)}\right)_c \simeq Q_c \cdot \left(\frac{R}{(U, V)}\right)_c \simeq \left(\frac{R}{(U, V)}\right)_c,$$

i.e., locally trivial of rank 1 over $(R/(U, V))_c$ via the witness Q_c. Hence, there exists a $Q \in R$ such that

$$\mathrm{Ann}(\Phi_0) \otimes \frac{R}{(U, V)} \simeq Q \cdot \frac{R}{(U, V)} \simeq \frac{R}{(U, V)}$$

as $R/(U, V)$-modules.

Thus, the above discussion relates non-existence of APS for all local systems to a global polynomial certificate. But, we still don't have an explicit connection to integrality. This is provided in the following theorem.

Theorem 7.5. *A polynomial f is integral over $A = \mathbb{C}[f_1, \ldots, f_m]$ if and only if there exists $Q(Y_1, \ldots, Y_m, U, V) \in \mathbb{C}[Y_1, \ldots, Y_m, U, V]$ such that $Q(f_1, \ldots, f_m, u, 1 - uf) = 0$ and $Q(Y_1, \ldots, Y_m, 0, 0) = 1$.*

Proof. Suppose f is integral over A. Then, there exists a monic relation $f^r + a_{r-1}(f_1, \ldots, f_m) f^{r-1} + \cdots + a_1(f_1, \ldots, f_m) f + a_0(f_1, \ldots, f_m) = 0$ for some $r \in \mathbb{Z}_{>0}$ and some $a_i(Y_1, \ldots, Y_m) \in \mathbb{C}[Y_1, \ldots, Y_m]$. Define

$$Q(Y_1, \ldots, Y_m, U, V) := (1 - V)^r + a_{r-1}(Y)\, U(1 - V)^{r-1} + \cdots + a_1(Y)\, U^{r-1}(1 - V) + a_0(Y)\, U^r.$$

Clearly, $Q(Y_1, \ldots, Y_m, 0, 0) = (1 - 0)^r = 1$. Further, on substituting $Y_i = f_i, U = u, V = 1 - uf$. Since $1 - V = uf$, we obtain

$$\begin{aligned} Q(f_1, \ldots, f_m, u, 1 - uf) &= (uf)^r + a_{r-1}(f)\, u(uf)^{r-1} + \cdots + a_0(f)\, u^r \\ &= u^r \Big(f^r + a_{r-1}(f) f^{r-1} + \cdots + a_0(f) \Big) \\ &= 0. \end{aligned}$$

For the converse, let $Q(Y, U, 0) = 1 + b_1(Y)U + b_2(Y)U^2 + \cdots + b_r(Y)U^r$ for some $r \geq 0$ and some polynomials $b_i(Y) \in \mathbb{C}[Y_1, \ldots, Y_m]$. Since $Q(f_1, \ldots, f_m, u, 1 - uf) = 0$ in $\mathbb{C}[x_1, \ldots, x_n, u]$, the same identity holds in the localization $\mathbb{C}(x_1, \ldots, x_n)[u]$. Now substitute $u = \frac{1}{f}$ in the fraction field $\mathbb{C}(x_1, \ldots, x_n)$. Then $1 - uf = 0$. Hence,

$$0 = Q\left(f_1, \ldots, f_m, \frac{1}{f}, 0\right) = 1 + \frac{b_1(f_1, \ldots, f_m)}{f} + \cdots + \frac{b_r(f_1, \ldots, f_m)}{f^r}.$$

Multiplying by f^r gives a monic polynomial relation for f over A. □

In fact, this can also be extended to an equivalence with valuations.

Corollary 7.6 (Boundedness criterion)**.** *The polynomial f is integral over A if and only if, for every $\beta \in \mathbb{C}(t)^n$,*

$$(\mathsf{val}_t f_i(\beta) \geq 0 \text{ for all } i) \quad \Longrightarrow \quad \mathsf{val}_t f(\beta) \geq 0.$$

Proof. For a monic relation, a negative valuation of $f(\beta)$ makes its highest power the unique term of least valuation, a contradiction. Conversely, if f is not integral, then Lemma 7.2 and Theorems 7.3 and 7.5 imply that there is an approximate zero $(\beta, u(t))$ of a Φ_c for some $c \in \mathbb{C}^m$. All $f_i(\beta)$ are nonnegative valuations, whereas u has positive valuation and $\mathsf{val}_t(1 - u(t))f(\beta) > 0$. Hence $\mathsf{val}_t(f(\beta)) = -\mathsf{val}_t(u(t)) < 0$. □

Hence, we can now check for integrality by checking for this global annihilator certificate. However, computationally the issue is that we currently have no handle on the degree of this polynomial Q, which could make computation very expensive. But as we now show, we can establish a singly exponential bound on this polynomial using Noether normalization.

7.1 A singly exponential certificate

First note that we can always compute the transcendence degree of the input polynomials with rational coefficients in CH by just creating a minimally independent set by sequentially adding elements and checking for algebraic independence using the Jacobian criterion [CKW11]. Now, look at the system $\Phi = (f_1, \ldots, f_m, u, 1 - uf)$. If f is integral over A, then $\operatorname{trdeg} \Phi = \rho + 1$, if $\operatorname{trdeg}(f_1, ..., f_m) = \rho$. We use Noether normalization to project these f_i to a space defined by their linear combinations $\{g_i\}_{1 \leq i \leq \rho}$ such that f is integral over this new system. Along with the polynomials $u, 1 - uf$, this makes a new system of $\rho + 2$ polynomials whose transcendence degree is $\rho + 1$. Hence, the annihilating ideal of the new system is a principal ideal [Kay09]. This helps us to establish the singly exponential degree bound on the annihilator.

Theorem 7.7. *Assume f is integral over $A = \mathbb{C}[f_1, \ldots, f_m]$. Let $\rho := \operatorname{trdeg}_{\mathbb{C}} \mathbb{C}(f_1, \ldots, f_m)$, and $\Delta := \max\{\deg(f_1), \ldots, \deg(f_m), \deg(f) + 1\}$. Then there exists Q satisfying conditions in Theorem 7.5, and $\deg(Q) \leq D := (\rho + 2)\Delta^{\rho+1}$. For rational input polynomials, Q may be chosen over $\mathbb{Q}$.*

Proof. Let f be integral over A. Since $\operatorname{trdeg} f_1, \ldots, f_m = \rho$, by applying first random linear projections Theorem 3.13 and then linear Noether normalization Lemma 3.15, there exists $g_1, \ldots, g_\rho$ such that $g_i = \sum_{j=1}^m c_{ij} f_j$ for $i = 1, \ldots, \rho$. Let $\widetilde{\Phi} := (g_1, \ldots, g_\rho, u, 1 - uf)$. For generic choices of c_{ij}, the above procedure gives a Noether normalization of closure of the image of $(f_1, \ldots, f_m) : \mathbb{A}^n_{\mathbb{C}} \to \mathbb{A}^m_{\mathbb{C}}$, so g_i are algebraically independent. Hence the ring A is integral over $B := \mathbb{C}[g_1, \ldots, g_\rho]$. Since, f is integral over A, so f is integral over B, and the transcendence degree of the system $\widetilde{\Phi}$ is $\rho + 1$. Thus,

$\mathrm{Ann}(\widetilde{\Phi})$ is a principal ideal. Then, using Theorem 7.5 we have $P \in \mathrm{Ann}(\widetilde{\Phi})$ such that $P(Z,0,0) = 1$ and by [Kay09, Theorem 11], we have that $\deg(P) \leq (\rho+2)\Delta^{\rho+1} = D_0$. Now define

$$Q(Y,U,V) = P\left(\sum_j c_{1j}Y_j, \ldots, \sum_j c_{\rho j}Y_j, U, V\right).$$

Clearly, $Q(Y,0,0) = P(Z,0,0) = 1$. Further, $Q(f_1,\ldots,f_m,U,V) = P(g_1,\ldots,g_\rho,U,V) = 0$. hence, $Q \in \mathrm{Ann}(\Phi)$. Since, Q only uses linear combinations of variables of P, $\deg Q = \deg P \leq D_0$.

□

At this point, we can use this singly exponential degree bound to put integral closure testing in PSPACE by solving an exponential-sized system of linear equations in the same way as for computing annihilator using Perron's bound [Per27, GSS19], which can be solved in PSPACE [Csa76, Ber84, Mul86]. However, this still does not give a CH upper bound, because while similar, this global annihilator certificate does not exactly correspond to any APS instance.

7.2 A polynomial-time reduction to APS

In this section, we show how we can get an equivalent APS instance for integral closure membership testing, which will finally put Problem 1.2 in CH.

Theorem 7.8 (From non-integrality to APS)**.** *Let D be the bound from Theorem 7.7, or any larger integer, and let $M = D+1$. Define a system of polynomials Ψ_M by $\Psi_M = (uf_1^M \ldots, uf_m^M, u, 1-uf)$. Then f is integral over A if and only if Ψ_M does not have APS.*

Proof. If f is not integral over A, Corollary 7.6 supplies $\beta \in \mathbb{C}(t)^n$ with $\mathsf{val}_t f_i(\beta) \geq 0$ for all i, and $\mathsf{val}_t f(\beta) < 0$. Substituting $u = 1/f(\beta)$ we obtain $\mathsf{val}_t u(\beta) > 0$, so $\mathsf{val}_t(u(\beta)f_i(\beta)^M) > 0$ for all i. Thus $(\beta, u(\beta)) \in \mathbb{C}(t)^{n+1}$ is an approximate zero of Ψ_M by [ADPS26, Definition 1].

Conversely, suppose f is integral and (β, u) is an approximate zero of Ψ_M. Set $a = \mathsf{val}_t(u) > 0$. Since $\mathsf{val}_t(1-uf(\beta)) > 0$, we obtain $\mathsf{val}_t(f(\beta)) = -a$, and $\mathsf{val}_t(f_i(\beta)) > -a/M$ for all i. The case $f = 0$ is already excluded, since then $1 - uf = 1$. By Theorem 7.7, there is a certificate Q with $\deg Q \leq D$. Write

$$Q(Y,U,0) = 1 + \sum_{j=1}^{r} b_j(Y)U^j, \qquad r \leq D, \quad \deg b_j \leq D - j.$$

Substituting $u = 1/f$ in its annihilating identity gives the rational-function identity

$$1 + \sum_{j=1}^{r} b_j(f_1,\ldots,f_m)f^{-j} = 0. \tag{7.1}$$

It can be evaluated at β because $f(\beta) \neq 0$. Each monomial $c_\alpha Y^\alpha$ in b_j with nonzero evaluation contributes a term with valuation

$$ja + \sum_{i:\alpha_i>0} \alpha_i \mathsf{val}_t(f_i(\beta)) \;\geq\; a\left(j - \frac{|\alpha|}{M}\right) \;\geq\; a\left(1 - \frac{D}{M}\right) > 0.$$

A monomial evaluating to zero has infinite valuation and causes no exception. The coefficients $c_\alpha \in \mathbb{C}^\times$ have valuation zero. Hence every summand after 1 in Equation (7.1) has positive valuation and cannot cancel the constant term. This contradiction proves the first equivalence. □

Proof of Theorem 1.8. Let L be the circuit input length. Compute formal-degree upper bounds and choose an integer $\Delta \geq \max\{1, \deg f_1, \ldots, \deg f_m, 1 + \deg f\}$ from them. Define D as in Theorem 7.7 with $\rho = n$ (as trdeg $\leq n$ always) and $M = D + 1$. These integers have polynomial binary length and can be computed in polynomial time. The proof of Theorem 7.7 applies to these upper bounds as well as to the actual degrees. Repeated squaring computes each f_i^M using $O(\log M)$ additional multiplication gates. Sharing the given circuits therefore yields a rational circuit for Ψ_M of size polynomial in L. By Theorem 7.8, this is a deterministic polynomial-time many-one reduction from non-integrality to APS. Our APS algorithm from Theorem 1.3 decides the resulting instance in CH. Closure under complement of CH proves the claimed upper bound for integral closure membership. □

Thus, we have established a CH procedure of integral closure membership testing. The idea behind introducing Ψ_M was to ensure that the valuation of f_i dominate the valuation of u and don't allow false witnesses of non-integrality by providing a uniform exponent without knowing a monic equation in advance. This can also be seen in the following example.

Example 7.9 (Why the power is needed)**.** Let $A = \mathbb{C}[x]$ and $f = x^k$ for $k \geq 2$. The element f belongs to A and is therefore integral. Yet the tuple $(u, 1 - ux^k, ux)$ has an approximate zero: take $x = t^{-1}$ and $u = t^k$, giving $(t^k, 0, t^{k-1})$. For the powered tuple $(u, 1 - ux^k, ux^M)$, approximate vanishing of its first two coordinates forces $\mathsf{val}_t(x) = -\mathsf{val}_t(u)/k$. Hence, if $M \geq k$, then

$$\mathsf{val}_t(ux^M) = \mathsf{val}_t(u)(1 - M/k) \leq 0,$$

so this false witness is excluded.

Remark 7.10. The global annihilator criterion and the reduction from non-integrality to APS are valid in arbitrary characteristic. For the certificate degree bound, we use the arbitrary-characteristic annihilator bound of [BMS13, Corollary 6]. Using trdeg $\leq n$ in this bound avoids any Jacobian computation. The same polynomial-time reduction therefore applies, and the claimed upper bound follows from the corresponding result for APS.

Lemma 7.11 (From APS to non-integrality)**.** *Let K be an algebraically closed field, let $F = (f_1, \ldots, f_m) \in K[x_1, \ldots, x_n]^m$, and let z be a fresh variable. Then*

$$0 \in \overline{F(K^n)} \quad \Longleftrightarrow \quad z \text{ is not integral over } K[zf_1, \ldots, zf_m].$$

This gives a deterministic polynomial-time many-one reduction from APS to non-integrality.

Proof. If F has no APS, the annihilator criterion gives a relation

$$H(Y) = 1 + \sum_{0<|\alpha|\leq D} h_\alpha Y^\alpha, \qquad H(F) = 0.$$

Multiplying this identity by z^D gives

$$z^D + \sum_{0<|\alpha|\leq D} h_\alpha (zf_1)^{\alpha_1} \cdots (zf_m)^{\alpha_m} z^{D-|\alpha|} = 0,$$

a monic relation for z over $K[zf_1, \ldots, zf_m]$.

Conversely, suppose that z is integral over this algebra. Write a monic relation as

$$z^d + \sum_{j=0}^{d-1} A_j(zf_1, \ldots, zf_m) z^j = 0.$$

Taking the coefficient of z^d in the above monic relation produces an annihilator of F with constant term 1: every contribution from A_j has positive total degree $d - j$ in the f_i. Thus F has no APS.

The reduction simply introduces z and multiplies each input polynomial by it, so its circuit size is polynomial. □

Proof of Theorem 1.11. Lemma 7.11 along with Theorem 7.8 proves the claim. □

8 Conclusion and open questions

We place approximate polynomial satisfiability and integral closure membership over polynomial subalgebras in the Counting Hierarchy. Our APS algorithm uses finite Noether normalization to restrict attention to finitely many points of the image closure. These points arise as limits of solutions to a one-parameter polynomial system, and their membership can be tested through coefficients of a multivariate resultant. For integral closure membership, a global annihilator criterion and an effective degree bound give a deterministic polynomial-time reduction from non-integrality to APS.

These results yield Counting Hierarchy upper bounds for tensor border rank, the orbit-closure problems specified in Corollary 1.7, integral closure membership for ideals, and finiteness of polynomial maps. They also give $\mathsf{FP}^{\mathsf{CH}}$ constructions of polynomial-size hitting sets for $\overline{\mathsf{VP}}$. The results apply to the coefficient fields and input representations discussed above.

The connection between APS and integral dependence also works in the reverse direction. For a fresh variable z, a tuple $(f_1, \ldots, f_m)$ has an approximate zero precisely when z is not integral over $K[zf_1, \ldots, zf_m]$ (Lemma 7.11). Consequently, APS and non-integrality are equivalent under deterministic polynomial-time many-one reductions.

Exact versus approximate satisfiability. Can APS be reduced to Hilbert's Nullstellensatz by a polynomial-time many-one reduction? The reverse reduction is known [BSTW26]. Such a reduction would transfer further upper bounds for exact satisfiability to APS and, through the equivalence above, to non-integrality. More broadly, can APS be placed in the polynomial hierarchy?

From decision to certificates. Our integral closure algorithm decides whether a polynomial is integral without constructing a monic relation or a global annihilator certificate. Can the Counting Hierarchy upper bound be extended to accessing the coefficients of such certificates? Since a degree-bounded certificate may have exponentially many coefficients, a natural formulation asks whether one can select a valid certificate and compute a specified coefficient bit within CH.

Acknowledgements

AP and SA would like to thank the *SiMul Research group @ CRAN* for hosting the *Geometry of Neural Networks and Tensors in Nancy* workshop. They would also like to thank Alex Massarenti who they met there and a discussion with whom resulted in the idea about formalizing the intuition about "approaching" the approximate solution. HS would like to thank Cornelius Brand for pointing us to the reference [LL89], that was very helpful in completing the geometric picture. AH would like to thank Markus Bläser for hosting him for an internship in his group. AP would also like to thank Raimund Seidel for hosting him during this work. Finally, we would like to thank Markus Bläser for his guidance throughout.

Funding

HS was supported by the European Union (ERC, CountHom, 101077083). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

AI Disclosure

OpenAI Codex assisted with organizing and drafting the manuscript from the authors' supplied notes, checking references, and reviewing the arguments. It contributed to the global certificate and degree-bound proofs, the reduction from non-integrality to APS in Section 7, and the circuit-input and dimension arguments. Its assistance also affected the exposition and verification of the APS in Counting Hierarchy construction.

References

[Abh90] Shreeram S. Abhyankar. *Algebraic Geometry for Scientists and Engineers*, volume 35 of *Mathematical Surveys and Monographs*. American Mathematical Society, 1990.

[ABKPM09] Eric Allender, Peter Bürgisser, Johan Kjeldgaard-Pedersen, and Peter Bro Miltersen. On the complexity of numerical analysis. *SIAM Journal on Computing*, 38(5):1987–2006, 2009. `https://people.cs.rutgers.edu/~allender/papers/slp.pdf`.

[ADPS26] Sanyam Agarwal, Sagnik Dutta, Anurag Pandey, and Himanshu Shukla. When Hilbert approximates: A strong Nullstellensatz for approximate polynomial satisfiability. In Dana Moshkovitz, editor, *41st Computational Complexity Conference (CCC 2026)*, volume 383 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 19:1–19:18. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2026. `https://doi.org/10.4230/LIPIcs.CCC.2026.19`.

[AGOS26] Robert Andrews, Abhibhav Garg, Rafael Oliveira, and Éric Schost, 2026.

[AGS26] Robert Andrews, Abhibhav Garg, and Éric Schost. Hilbert's Nullstellensatz is in the counting hierarchy, 2026. arXiv:2602.17904. `https://arxiv.org/abs/2602.17904`.

[AM69] Michael F. Atiyah and Ian G. Macdonald. *Introduction to Commutative Algebra*. Addison–Wesley, 1969.

[AW24] Robert Andrews and Avi Wigderson. Constant-depth arithmetic circuits for linear algebra problems. In *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 2367–2386. IEEE, 2024.

[BCJS26] C. S. Bhargav, Radu Curticapean, Gorav Jindal, and Himanshu Shukla. Multivariate resultants: Complexity and applications for ETR, 2026.

[BCS97] Peter Bürgisser, Michael Clausen, and Mohammad Amin Shokrollahi. *Algebraic Complexity Theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1997.

[Ber84] Stuart J. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Information Processing Letters*, 18(3):147–150, 1984.

[BMS13] Malte Beecken, Johannes Mittmann, and Nitin Saxena. Algebraic independence and blackbox identity testing. *Inf. Comput.*, 222:2–19, 2013.

[BSTW26] Nikhil Balaji, Mahsa Shirmohammadi, Sébastien Tavenas, and James Worrell. Approximate polynomial satisfiability is in the counting hierarchy, 2026. arXiv:2610.00644, version 1, September 30, 2026. `https://arxiv.org/abs/2610.00644`.

[Can88] John F. Canny. Some algebraic and geometric computations in PSPACE. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 460–467. ACM, 1988.

[Can90] John Canny. Generalised characteristic polynomials. *Journal of Symbolic Computation*, 9(3):241–250, 1990.

[CKW11] Xi Chen, Neeraj Kayal, and Avi Wigderson. Partial derivatives in arithmetic complexity and beyond. *Foundations and Trends® in Theoretical Computer Science*, 6(1-2):1–138, 2011.

[Csa76] Laszlo Csanky. Fast parallel matrix inversion algorithms. *SIAM Journal on Computing*, 5(4):618–623, 1976.

[DJ97] Theo De Jong. An algorithm for computing the integral closure. *arXiv preprint alg-geom/9704017*, 1997.

[GSS18] Zeyu Guo, Nitin Saxena, and Amit Sinhababu. Algebraic dependencies and PSPACE algorithms in approximative complexity. In Rocco A. Servedio, editor, *33rd Computational Complexity Conference (CCC 2018)*, volume 102 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 10:1–10:21. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2018.

[GSS19] Zeyu Guo, Nitin Saxena, and Amit Sinhababu. Algebraic dependencies and PSPACE algorithms in approximative complexity over any field. *Theory of Computing*, 15(16):1–30, 2019. `https://theoryofcomputing.org/articles/v015a016/`.

[Har77] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, 1977.

[HS06] Craig Huneke and Irena Swanson. *Integral Closure of Ideals, Rings, and Modules*, volume 336 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 2006.

[Ier89] Douglas Ierardi. Quantifier elimination in the theory of an algebraically-closed field. In *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing*, pages 138–147. ACM, 1989.

[Kay09] Neeraj Kayal. The complexity of the annihilating polynomial. In *2009 24th Annual IEEE Conference on Computational Complexity*, pages 184–193. IEEE, 2009.

[Kay25] Leonie Kayser. Computational complexity of polynomial subalgebras. In *Proceedings of the 2025 International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 337–344. ACM, 2025. Full version: `https://arxiv.org/abs/2502.05278`.

[Koi96] Pascal Koiran. Hilbert's Nullstellensatz is in the polynomial hierarchy. *Journal of Complexity*, 12(4):273–286, 1996.

[KP11] Pascal Koiran and Sylvain Perifel. Interpolation in valiant's theory. *Computational Complexity*, 20(1):1–20, 2011.

[Lan12] J. M. Landsberg. *Tensors: Geometry and Applications*, volume 128 of *Graduate Studies in Mathematics*. American Mathematical Society, 2012.

[LL89] Thomas Lehmkuhl and Thomas Lickteig. On the order of approximation in approximative triadic decompositions of tensors. *Theoretical Computer Science*, 66(1):1–14, 1989.

[Mil24] James S. Milne. Algebraic geometry, 2024. Version 6.10, November 11, 2024. `https://www.jmilne.org/math/CourseNotes/AG.pdf`.

[Mul86] Ketan Mulmuley. A fast parallel algorithm to compute the rank of a matrix over an arbitrary field. In *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, pages 338–339, 1986.

[Mul17] Ketan D. Mulmuley. Geometric complexity theory V: Efficient algorithms for Noether normalization. *Journal of the American Mathematical Society*, 30(1):225–309, 2017.

[Mum95] David Mumford. *Algebraic geometry I: complex projective varieties*. Springer Science & Business Media, 1995.

[Ope26] OpenAI. Existential universal real sentences in the counting hierarchy, 2026.

[Per27] Oskar Perron. Algebraische abhängigkeit und ihre anwendung in der algebra. *Mathematische Annalen*, 1927.

[Str73] Volker Strassen. Vermeidung von divisionen. *Journal für die reine und angewandte Mathematik*, 264:184–202, 1973.

[The26] The Stacks project authors. The Stacks project, 2026. `https://stacks.math.columbia.edu`.

[Vak25] Ravi Vakil. The Rising Sea: Foundations of Algebraic Geometry, 2025. Notes, October 21, 2025 version. `https://math.stanford.edu/~vakil/216blog/FOAGoct2125public.pdf`.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il