THEORY OF COMPUTING, Volume 15 (16), 2019, pp. 1–30
www.theoryofcomputing.org

SPECIAL ISSUE: CCC 2018

Algebraic Dependencies and PSPACE Algorithms in Approximative Complexity over Any Field

Zeyu Guo[*] Nitin Saxena[†] Amit Sinhababu[‡]

Received June 30, 2018; Revised June 16, 2019; Published December 14, 2019

Abstract: Testing whether a set **f** of polynomials has an algebraic dependence is a basic problem with several applications. The polynomials are given as algebraic circuits. The complexity of algebraic independence testing is wide open over finite fields (Dvir, Gabizon, Wigderson, FOCS'07). Previously, the best complexity bound known was $\mathsf{NP}^{\#\mathsf{P}}$ (Mittmann, Saxena, Scheiblechner, Trans. AMS 2014). In this article we put the problem in $\mathsf{AM} \cap \mathsf{coAM}$. In particular, dependence testing is unlikely to be NP-hard. Our proof uses methods of algebraic geometry. We estimate the size of the image and the sizes of the preimages of the polynomial map **f** over the finite field. A *gap* between the corresponding sizes for independent and for dependent sets of polynomials is utilized in the AM protocols.

A conference version of this paper appeared in the Proceedings of the 33rd Computational Complexity Conference (CCC'18) [24] and as a poster in STOC 2018: TheoryFest.

[*] Supported by DST and Research I Foundation of CSE, IITK.

[†] Supported by DST/SJF/MSA-01/2013-14.

[‡] Supported by DFG grant TH 472/5-1.

ACM Classification: I.1, F.2.1, F.1.3, G.1.2

AMS Classification: 03D15, 14Q20

Key words and phrases: algebraic dependence, Jacobian, Arthur-Merlin, approximate polynomial, satisfiability, hitting set, border VP, finite field, PSPACE, EXPSPACE, GCT Chasm, Polynomial Identity Lemma

DOI: 10.4086/toc.2019.v015a016

Next, we study the open question of testing whether every annihilator of $\mathbf{f}$ has zero constant term (Kayal, CCC'09). We introduce a new problem called *approximate polynomial satisfiability* (APS), which is equivalent to the preceding question by a classical characterization in terms of the Zariski closure of the image of $\mathbf{f}$. We show that APS is NP-hard and, using ideas from algebraic geometry, we put APS in PSPACE. (The best previous bound was EXPSPACE via Gröbner basis computation.) As an unexpected application of this to approximative complexity theory we obtain that, over *any* field, hitting sets for $\overline{\mathsf{VP}}$ can be constructed in PSPACE. This solves an open problem posed in (Mulmuley, FOCS'12, J. AMS 2017), greatly mitigating the GCT Chasm (exponentially in terms of space complexity).

1 Introduction

Algebraic dependence is a generalization of linear dependence. Polynomials $f_1,\dots,f_m \in \mathbb{F}[x_1,\dots,x_n]$ are called *algebraically dependent* over the field $\mathbb{F}$ if there exists a nonzero polynomial (called *annihilator*) $A(y_1,\dots,y_m) \in \mathbb{F}[y_1,\dots,y_m]$ such that $A(f_1,\dots,f_m) = 0$. If no A exists, then the given polynomials are called *algebraically independent* over $\mathbb{F}$. The *transcendence degree* (trdeg) of a set of polynomials is the analog of rank in linear algebra. It is defined as the maximum number of algebraically independent polynomials in the set. Both algebraic dependence and linear dependence define matroid structures [20]. There exist algebraic matroids over $\mathbb{F}_p$ that are not linear [28].

The simplest example of algebraically independent polynomials is $x_1,\dots,x_n \in \mathbb{F}[x_1,\dots,x_n]$. As an example of algebraically dependent polynomials, we can take $f_1 = x$, $f_2 = y$ and $f_3 = x^2+y^2$. Then, $y_1^2+y_2^2-y_3$ is an annihilator. The underlying field is crucial in this concept. For example, for a given prime number p, the polynomials $x+y$ and x^p+y^p are algebraically dependent over fields of characteristic p (as $(x+y)^p = x^p+y^p$ in characteristic p). But they are algebraically independent over fields of characteristic zero (e. g., $\mathbb{Q}$) and over fields of positive characteristic $\ell \neq p$.[1]

Thus, the following computational question, AD($\mathbb{F}$), is natural and it is the first problem we consider in this paper: Given polynomials $f_1,\dots,f_m \in \mathbb{F}[x_1,\dots,x_n]$, represented as algebraic circuits, test if they are algebraically dependent. It can be solved in PSPACE using a classical result due to Perron [48, 49]. We sketch the proof of this result here: Perron proved that given a set of algebraically dependent polynomials, there exists an annihilator whose degree is at most the product of the degrees of the polynomials in the set. (This exponential degree bound is tight [30].) It is not hard to see that testing the existence of such an annihilator reduces to solving a system of linear equations in exponentially many variables where the coefficients of the annihilator are regarded as the variables of the system. It is also known that solving a system of linear equations is in logspace-uniform NC [15, 9, 43], which is contained in PolyL (polylogarithmic space). Combining these results we see that testing algebraic dependence (and computing an annihilator polynomial) is in PSPACE.

Computing the annihilator may be quite hard, but it turns out that the decision version is easy over zero (or large) characteristic using a classical result known as the Jacobian criterion [29, 7]. The Jacobian efficiently reduces algebraic dependence testing of $f_1,\dots,f_m$ over $\mathbb{F}$ to linear dependence testing of the

[1] This can be seen using the Jacobian criterion [29, 7] as discussed below.

differentials $df_1, \dots, df_m$ over $\mathbb{F}(x_1, \dots, x_n)$, where we view df_i as the vector

$$\left(\frac{\partial f_i}{\partial x_1}, \dots, \frac{\partial f_i}{\partial x_n}\right).$$

Placing df_i as the i-th row gives us the Jacobian matrix J of $f_1, \dots, f_m$. If the characteristic of the field $\mathbb{F}$ is zero (or larger than the product of the degrees $\deg(f_i)$) then the transcendence degree of $f_1, \dots, f_m$ equals $\mathrm{rank}(J)$. It follows from the Polynomial Identity Lemma[2] that, with high probability, $\mathrm{rank}(J)$ is equal to the rank of J evaluated at a random point in $\mathbb{F}^n$. This gives a simple randomized polynomial-time algorithm solving $\mathsf{AD}(\mathbb{F})$, over the fields $\mathbb{F}$ satisfying the condition stated above.

For fields of positive characteristic, if the polynomials are algebraically dependent, then their Jacobian matrix is not full rank. But the converse is not true. There are infinitely many input instances (set of algebraically independent polynomials) for which the Jacobian criterion fails. The failure can be characterized by the notion of "inseparable extension" [47]. For example, x^p, y^p are algebraically independent over $\mathbb{F}_p$, yet their Jacobian determinant vanishes. Another example is, $\left\{x^{p-1}y, xy^{p-1}\right\}$ over $\mathbb{F}_p$ for prime $p > 2$. Mittmann, Saxena, and Scheiblechner [41] gave a criterion, called Witt-Jacobian, that works over fields of positive characteristic, improving the complexity of algebraic independence testing from PSPACE to $\mathsf{NP}^{\#\mathsf{P}}$. [47] gave another generalization of the Jacobian criterion that is efficient in special cases.

Given that an efficient algorithm to tackle positive characteristic is not in close sight, one could speculate the problem to be NP-hard or even outside the polynomial hierarchy PH. In the present article we show that *for finite fields,* $\mathsf{AD}(\mathbb{F})$ *is in* $\mathsf{AM} \cap \mathsf{coAM}$ (Theorem 1.1). This rules out the possibility of NP-hardness, unless the polynomial-time hierarchy collapses [4]. Thus, $\mathsf{AD}(\mathbb{F})$ joins the league of problems of "intermediate" complexity, such as graph isomorphism and integer factoring.

Constant term of the annihilators. We come to the second problem *AnnAtZero* that we discuss in this paper: Testing if the constant term of *every* annihilator of a set of polynomials (given as algebraic circuits), $\mathbf{f} = \{f_1, \dots, f_m\}$, is zero. The annihilators of $\mathbf{f}$ constitute a prime ideal of the polynomial ring $\mathbb{F}[y_1, \dots, y_m]$. This ideal is principal when the transcendence degree of $\mathbf{f}$ is $m-1$. This is a classical result in commutative algebra [39, Theorem 47]. See also [30, Lemma 7] for an exposition. In this case, we can decide in PSPACE if the constant term of the minimal annihilator is zero, as the *unique* annihilator (up to scaling) can be computed in PSPACE.

If the transcendence degree of $\mathbf{f}$ is less than $m-1$, the ideal of the annihilators of $\mathbf{f}$ is no longer principal. Although the ideal is finitely generated, finding the generators of this ideal is computationally very hard. (E. g., using Gröbner basis techniques, we can do it in $\mathsf{EXPSPACE}$ [17, Section 1.2.1].) In this case, can we decide if all the annihilators of $\mathbf{f}$ have constant term zero? *We give two equivalent characterizations of* AnnAtZero*—one geometric and the other algebraic—and we use them to devise a* PSPACE *algorithm to solve it in all cases* (Theorem 1.3).

Interestingly, there is an application of the above algorithm to algebraic complexity. *We give a* PSPACE*-explicit construction of a hitting set of the class* $\overline{\mathsf{VP}}_{\mathbb{F}_q}$ (Theorem 1.4). $\overline{\mathsf{VP}}_{\mathbb{F}_q}$ consists of n-variate

[2] Regarding the Polynomial Identity Lemma, the following footnote appears in [14]. "Variants of this lemma, often referred to as the Schwartz–Zippel Lemma, or the DeMillo–Lipton–Schwartz–Zippel Lemma, were discovered at least six times, starting with Øystein Ore in 1922 and David Muller in 1954 [46, 42, 56, 16, 60, 57]. For a brief history, see [5] where the term "Polynomial Identity Lemma" is attributed to L. Babai."

polynomials of degree $d = n^{O(1)}$ over the field $\overline{\mathbb{F}}_q$, that can be "infinitesimally approximated" by algebraic circuits of size $s = n^{O(1)}$. A polynomial $p(x_1, \ldots, x_n)$ over an algebraically closed field $\overline{\mathbb{F}}$ is said to be *infinitesimally approximated* by a circuit of size s, if the circuit computes a polynomial of the form $p + \varepsilon p_1 + \varepsilon^2 p_2 + \cdots + \varepsilon^m p_m$, where the circuit uses constants from $\overline{\mathbb{F}}(\varepsilon)$ (for example, $1/\varepsilon$ can be used as a constant) and $p_1, \ldots, p_m \in \overline{\mathbb{F}}[x_1, \ldots, x_n]$.

A set $\mathcal{H}$ of points is called a *hitting set* for a set C of polynomials, if any nonzero polynomial in C evaluates to a nonzero value in at least one point in $\mathcal{H}$. It was shown by Heintz and Schnorr [27] that hitting sets of size $\mathrm{poly}(n,s)$ and bit length $\mathrm{poly}(n,s,\log d)$ *exist* for the class of n-variate polynomials of degree at most d computed by size s arithmetic circuits. The same result extends to the class of n-variate polynomials of degree at most d *infinitesimally approximated* by size s arithmetic circuits. Now the problem of constructing explicit hitting sets for $\overline{\mathsf{VP}}$ asks to deterministically compute a set of points that is a hitting set for the class of n-variate polynomials of degree at most d, infinitesimally approximated by size s arithmetic circuits.

The above problem is interesting as natural questions like explicit construction of the normalization map (in Noether's Normalization Lemma NNL) reduce to the construction of a hitting set of $\overline{\mathsf{VP}}$ (Mulmuley [45]), which was previously known to be only in EXPSPACE [45, 44]. This was recently put in PSPACE, over the field $\mathbb{C}$, by Forbes and Shpilka [21]. Their proof uses real analysis and does not apply to finite fields. We need to develop purely algebraic concepts to solve the finite field case (namely through AnnAtZero), which apply to *any* field.

To further motivate the concept of algebraic dependence, we list a few recent problems in computer science. The first problem is about constructing an explicit randomness extractor for sources which are polynomial maps over finite fields. Using the Jacobian criterion, [19, 18] solved the problem for fields with large characteristic. The second application is to the famous polynomial identity testing (PIT) problem. To efficiently design hitting sets, for some interesting models, [7, 3, 34] constructed a family of trdeg-preserving maps. For more background and applications of algebraic dependence testing, see [47]. The annihilator has been a key concept to prove the connection between hitting sets and lower bounds [27], and in bootstrapping "weak" hitting sets [2].

Finally, we remark that a common thread among the problems we study in this paper is studying the closure of the polynomial map. Let $f : \mathbb{F}^n \to \mathbb{F}^n$ be a given polynomial map. Then, we study two computational questions: (1) (Algebraic Dependence Testing) whether the dimension of the Zariski closure of the image of f is $< n$? (2) (Origin in closure) whether the origin $\mathbf{0}$ is in the Zariski closure of the image of f?

1.1 Our results

In this paper, we give Arthur-Merlin protocols and algorithms, with proofs using basic tools from algebraic geometry. The first theorem we prove is about $\mathrm{AD}(\mathbb{F}_q)$.

Theorem 1.1. *Testing algebraic independence of multivariate polynomials over a finite field is in* $\mathsf{AM} \cap \mathsf{coAM}$.

This result vastly improves the current best upper bound known for $\mathrm{AD}(\mathbb{F}_q)$—from being "outside" the polynomial hierarchy (namely $\mathsf{NP}^{\#\mathsf{P}}$ [41]) to "lower" than the second level of the polynomial hierarchy (namely $\mathsf{AM} \cap \mathsf{coAM}$). This rules out the possibility of $\mathrm{AD}(\mathbb{F}_q)$ being NP-hard (unless the polynomial hierarchy collapses to the second level [4]). Recall that, for a field $\mathbb{F}$ of characteristic zero or of large characteristic, $\mathrm{AD}(\mathbb{F})$ is in coRP (Section 2). We conjecture such a result for $\mathrm{AD}(\mathbb{F}_q)$ too.

Our second result is about the problem AnnAtZero (i. e., testing whether all the annihilators of given $\mathbf{f}$ have constant term zero). A priori it is unclear why it should have complexity better than EXPSPACE. (Note: ideal membership is EXPSPACE-complete [40].)

First, we relate the problem AnnAtZero to a (new) version of polynomial system satisfiability, over the algebraic closure $\overline{\mathbb{F}}$.

Problem 1.2 (Approximate polynomials satisfiability (APS))**.** Given polynomials

$$f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]\,,$$

represented as algebraic circuits, does there exist $\beta \in \overline{\mathbb{F}}(\varepsilon)^n$ such that for all i, $f_i(\beta)$ is in the ideal $\varepsilon\overline{\mathbb{F}}[\varepsilon]$ of $\overline{\mathbb{F}}[\varepsilon]$? If yes, then we say that $\mathbf{f} := \{f_1, \ldots, f_m\}$ is in APS.

It is easy to show that the function field $\overline{\mathbb{F}}(\varepsilon)$ here can be equivalently replaced by the ring $\overline{\mathbb{F}}[\varepsilon, \varepsilon^{-1}]$ of *Laurent polynomials*, or, the field $\overline{\mathbb{F}}((\varepsilon))$ of *formal Laurent series* (use mod $\varepsilon\overline{\mathbb{F}}[\varepsilon]$). A reason why these objects appear in algebraic complexity can be found in [11, Section 5.2] and [37, Section 5]. They help algebrize the notion of "infinitesimal approximation" (in real analysis think of $\varepsilon \to 0$ & $1/\varepsilon \to \infty$). A notable computational issue involved is that the degree bound of ε required for β is exponential in the input size [37, Proposition 3]; this may again be a "justification" why APS may require that much space.

Classically, the *exact* version of APS has been well-studied—Does there exist $\beta \in \overline{\mathbb{F}}^n$ such that for all i, $f_i(\beta) = 0$? This is what Hilbert's Nullstellensatz (HN) characterizes. HN also yields an impressive PSPACE algorithm [32, 33]. Note that if system $\mathbf{f}$ has an exact solution, then it is trivially in APS. But the converse is not true. For example, $\{x, xy-1\}$ is in APS, but there is no exact solution in $\overline{\mathbb{F}}$. To see that it is in APS, assign $x = \varepsilon$ and $y = 1/\varepsilon$. Also, the instance $\{x, x+1\}$ is neither in APS nor does it have an exact solution. Finally, note that if we restrict β to come from $\overline{\mathbb{F}}[\varepsilon]^n$ then APS becomes equivalent to exact satisfiability and HN applies. This can be seen by going modulo $\varepsilon\overline{\mathbb{F}}[\varepsilon]$, as the quotient $\overline{\mathbb{F}}[\varepsilon]/\varepsilon\overline{\mathbb{F}}[\varepsilon]$ is $\overline{\mathbb{F}}$.

Coming back to AnnAtZero, we show that it is equivalent both to a geometric question and to deciding APS. This gives us, with more work, the following surprising consequence.

Theorem 1.3. APS *is* NP*-hard and is in* PSPACE*.*

We apply this to designing hitting sets and solving NNL. (We refer to [45] for the background.)

Theorem 1.4. *There is a* PSPACE *algorithm that (given input n, s, r in unary and suitably large q in binary) computes a set of points from $\mathbb{F}_q^n$ of size* $\mathrm{poly}(n,s)$ *that hits all n-variate degree-r polynomials over $\overline{\mathbb{F}}_q$ that can be infinitesimally approximated by size-s circuits.*

To state the results on NNL, we need the following notation from [45]. Let m be a positive integer and $r = m^2$. Let V be the vector space of homogeneous degree-m polynomials in the variables $x_1, \ldots, x_r$ over an algebraically closed field $\mathbb{F}$. Each $f \in V$ determines a point $[f]$ in the projective space $\mathbb{P}V$. Let

$\Sigma[\det,m]$ be the set of points $[f]$ such that f is a symbolic determinant of a matrix $M \in \mathbb{F}^{m\times m}$ whose entries are linear forms in $x_1,\dots,x_r$. Finally, let $\Delta[\det,m] \subseteq \mathbb{P}V$ be the Zariski closure of $\Sigma[\det,m]$.

Mulmuley [45] considers the problem of constructing a homogeneous linear map that maps $\Sigma[\det,m] \subseteq \mathbb{P}V$ to a much smaller projective space $\mathbb{P}^k$ (a *normalizing map*). In particular, we want to compute a set $S = \{p_0,\dots,p_k\}$ in $\mathrm{poly}(m)$-time, where $k = \mathrm{poly}(m)$ and $p_i \in \mathbb{F}^r$ for $i \in [k]$, such that the map $f \mapsto (f(p_0),\dots,f(p_k))$ induces a well-defined map from $\Sigma[\det,m]$ to $\mathbb{P}^k$. Such a set S is called a (strict) *e.s.o.p.* (*explicit system of parameters*). In addition, an e.s.o.p. S is *separating* if for any distinct f,g satisfying $[f],[g] \in \Delta[\det,m]$, we have $f(p_i) \neq g(p_i)$ for some $p_i \in S$.

As shown in [45], the problem of constructing a separating e.s.o.p. reduces to that of constructing hitting sets for $\overline{\mathsf{VP}}$ [45, Theorem 4.5]. Combining this reduction with our PSPACE algorithm of constructing hitting sets for $\overline{\mathsf{VP}}$, we obtain the following result.

Theorem 1.5 (NNL for $\Delta[\det,m]$ in PSPACE)**.** *The problem of constructing a separating e.s.o.p. for* $\Delta[\det,m]$ *belongs to* PSPACE.

The results for $\Delta[\det,m]$ also hold for other varieties, as long as such varieties satisfy some explicitness condition. This is captured by the notion of an *explicit family* $\{W_n\}$ *of varieties* in [45]. See [45, Definition 5.1] for the formal definition. For such varieties W_n, constructing a separating e.s.o.p. also reduces to constructing hitting sets for $\overline{\mathsf{VP}}$ [45, Theorem 5.11]. So we have the following result.

Theorem 1.6 (NNL for explicit varieties in PSPACE)**.** *Let* $\{W_n\}$ *be an explicit family of varieties as in [45, Definition 5.1]. Then the problem of constructing a separating e.s.o.p. for* W_n *belongs to* PSPACE.

More applications? The exact polynomials satisfiability question HN (over $\overline{\mathbb{F}}$) is highly expressive and, naturally, many computational problems can be expressed that way. We claim that in a similar spirit, the APS question expresses those computer science problems that involve "infinitesimal approximation." Since finite fields do not have a topology allowing approximations, algebraic approximations over arbitrary fields are needed. The latter has been useful in fast matrix multiplication algorithms.

One prominent example of algebraic approximation is the concept of *border rank* of tensor polynomials (used in matrix multiplication algorithms and Geometric Complexity Theory (GCT), see [12, 35, 36]). Border rank computation of a given tensor (over $\overline{\mathbb{F}}$) can easily be reduced to an APS instance and, hence, now solved in PSPACE. This brings the complexity of border rank closer to the complexity of tensor rank [54]. From the point of view of Gröbner basis theory, APS is a problem that seems a priori much harder than HN. Now that both of them have a PSPACE algorithm, one may wonder whether it can be brought all the way down to NP or AM? (In fact, $\mathrm{HN}_{\mathbb{C}}$ is known to be in AM, conditionally under GRH [32].)

More generally, APS is naturally related to GCT as follows. The program of GCT aims to find an explicit hard polynomial g (e. g., the permanent) in a vector space $V \subseteq \mathbb{F}[x_1,\dots,x_n]$ and prove that its projective image $[g] \in \mathbb{P}V$ is not contained in a certain projective variety X that consists of the "easy" polynomials. The *affine cone* $\hat{X} \subseteq V$ of X is often specified as the Zariski closure of the image of some morphism $\mathbf{f}$ from an affine space (see, e. g., [50, Section 2] for the case that X is a higher secant variety of a Segre–Veronese variety). The problem then becomes proving $g \notin \hat{X} = \overline{\mathrm{Im}(\mathbf{f})}$, or equivalently, proving $\mathbf{0} \notin \overline{\mathrm{Im}(\mathbf{f}')}$, where $\mathbf{0}$ is the origin of V and $\mathbf{f}'$ is the translation of $\mathbf{f}$ by $-g$. As we will see in this paper, one equivalent formulation of APS is precisely the problem of deciding if $\mathbf{0}$ is in the Zariski closure of the image of a given morphism from an affine space.

Our methods in the proof of Theorem 1.3 also imply an interesting "degree bound" related to the (prime) ideal I of annihilators of the set $\mathbf{f}$ of polynomials. Namely, $I = \sqrt{I_{\leq d}}$, where $I_{\leq d}$ refers to the subideal generated by degree $\leq d$ polynomials in I, d is the Perron-like bound $(\max_{i\in[m]}\deg(f_i))^k$, and $k := \operatorname{trdeg}(\mathbf{f})$. This is equivalent to the geometric fact, which we prove, that the varieties defined by the two ideals I and $I_{\leq d}$ are equal (Theorem 4.6). This again is an exponential improvement over what one expects to get from the general Gröbner basis methods, because, the generators of I may well have doubly exponential degree.

The result on hitting set (Theorem 1.4) can be applied to compute, in PSPACE, the explicit system of parameters (e.s.o.p.) of the *invariant ring* of the variety $\Delta[\det, s]$, over $\overline{\mathbb{F}}_q$, with a given group action [45, Theorem 4.9]. Also, we can now construct, in PSPACE, polynomials in $\mathbb{F}_q[x_1,\ldots,x_n]$ that cannot even be approximated by "small" algebraic circuits. Such results were previously known only for fields of characteristic zero, see [21, Theorems 1.1–1.4]. Bringing this complexity down to P is the longstanding problem of blackbox PIT (and lower bounds), see [52, 58, 53]. Mulmuley [44] pointed out that small hitting sets for $\overline{\mathsf{VP}}$ can be designed in EXPSPACE which is a far worse complexity than that for VP. He called it the GCT Chasm. We bridge it somewhat, as the proof of Theorem 1.4 shows that small hitting sets for $\overline{\mathsf{VP}}_{\overline{\mathbb{F}}}$ can be designed in PSPACE (like those for VP) for *any* field $\mathbb{F}$.

In another application, the null-cone problem defined in [13] can be seen as a special case of APS and using our algorithm, it can be solved in PSPACE. Bürgisser et al. [13] gave an exponential-time algorithm for the above problem (bringing it down from EXPSPACE).

Finally, another motivation for AnnAtZero or APS comes from the study of the *geometric ideal proof system* in algebraic proof complexity, introduced in [23], where they essentially discuss AnnAtZero for systems of polynomial equations corresponding to Boolean tautologies. See [23, Appendix B] for more details.

Remark 1.7. Given a system of polynomial equations $f_1(x_1,\ldots,x_n) = 0,\ldots,f_m(x_1,\ldots,x_n) = 0$, we can always homogenize the f_i by introducing a new variable z. The question of *projective polynomials satisfiability* for a given system of equations is whether there is a nonzero solution (called a *projective solution*) to the homogenized system. We have seen that APS does not directly reduce to (affine) polynomials satisfiability, as there are unsatisfiable systems, e. g., $\{X = 0,\ XY = 1\}$, that have approximate solutions. We note that APS does not directly reduce to projective polynomials satisfiability either. Consider, for example, the system $\{X+Y = 0,\ X+Y = 1\}$, corresponding to two parallel affine lines. It has no approximate solution, but the homogenized system $\{X+Y = 0,\ X+Y = Z\}$ has a projective solution $(1,-1,0)$.

Nonetheless, it is true that if the equations $f_1 = 0,\ldots,f_m = 0$ have an approximate solution, then the homogenized equations $\hat{f}_1 = 0,\ldots,\hat{f}_m = 0$ have a projective solution (in $\mathbb{P}^n$). We sketch a proof of this fact. Suppose $a_1,\ldots,a_n \in \overline{\mathbb{F}}(\varepsilon) \subseteq \overline{\mathbb{F}}((\varepsilon))$ form an approximate solution of the original system. Let $a_{n+1} = 1$. Then $f_i(a_1,\ldots,a_n) = \hat{f}_i(a_1,\ldots,a_n,a_{n+1})$ for $i \in [m]$. Choose the smallest $k \in \mathbb{Z}$ such that $\varepsilon^k a_i$ is in the ring of formal power series $\overline{\mathbb{F}}[[\varepsilon]]$ for all $i \in [n+1]$. We have $k \geq 0$ as $a_{n+1} = 1$. For $i \in [n+1]$, let $\bar{a}_i \in \overline{\mathbb{F}}$ be the constant term of $\varepsilon^k a_i$. Minimality of k guarantees that $\bar{a}_i \neq 0$ for some $i \in [n+1]$. Assigning $\bar{a}_1,\ldots,\bar{a}_{n+1}$ to $x_1,\ldots,x_n,z$ then gives a projective solution to the equations $\hat{f}_1 = 0,\ldots,\hat{f}_m = 0$.

1.2 Proof ideas

Proof idea of Theorem 1.1. Suppose we are given polynomials (represented as algebraic circuits) $\mathbf{f} := \{f_1, \ldots, f_m\}$ computing in $\mathbb{F}_q[x_1, \ldots, x_n]$. For the AM and coAM protocols, we consider the following system of equations over a "small" extension $\mathbb{F}_{q'}$.

For $b = (b_1, \ldots, b_m) \in \mathbb{F}_{q'}^m$, define the system of equations $f_i(x_1, \ldots, x_n) = b_i$, for $i \in [m]$. We denote the number of solutions of the above system in $\mathbb{F}_{q'}^n$ as N_b. Let $f : \mathbb{F}_{q'}^n \to \mathbb{F}_{q'}^m$ be the polynomial map $a \mapsto (f_1(a), \ldots, f_m(a))$.

AM *gap.* [Theorem 3.5] We establish bounds for the number $N_{f(a)}$, where a is a random point in $\mathbb{F}_{q'}^n$. If $f_1, \ldots, f_m$ are independent, we show that $N_{f(a)}$ is relatively small. On the other hand, if the polynomials are algebraically dependent then $N_{f(a)}$ is much greater.

Assume $\mathbf{f}$ is algebraically independent. Without loss of generality [47, Section 2] we can assume that $m = n$ and for all $i \in [n]$, $x_i, f_1, \ldots, f_n$ are algebraically dependent. The first step is to show that with high probability, the zero set defined by the system of equations, for random $f(a)$, is finite (i. e., it has dimension ≤ 0 as a variety). This is proved using the Perron degree bound on the annihilator of $\{x_i, f_1, \ldots, f_n\}$. Next, one can apply an affine version of Bézout's theorem to obtain an upper bound on $N_{f(a)}$. On the other hand, suppose $\mathbf{f}$ is algebraically dependent, say with annihilator Q. Let $\mathrm{Im}(f) := f(\mathbb{F}_{q'}^n)$ be the image of f. Since Q vanishes on $\mathrm{Im}(f)$, we know that $\mathrm{Im}(f)$ is relatively small, whence we deduce that $N_{f(a)}$ is large for "most" values of a.

coAM *gap.* [Theorem 3.8] We pick a random point $b = (b_1, \ldots, b_m) \in \mathbb{F}_{q'}^m$ and bound N_b, which is the number of solutions of the system defined above. In the dependent case, we show that $N_b = 0$ for "most" values of b. But in the independent case, we show that $N_b \geq 1$ for "many" (maybe not "most"!) values of b. The ideas are based on those sketched above.

The two kinds of gaps shown above are based on the sets $f^{-1}(f(\mathbf{x}))$ and $\mathrm{Im}(f)$, resp.

Note that membership in either of these sets is testable in NP (the latter requires nondeterminism). Based on this and the gaps between the respective cardinalities, we can invoke Lemma 2.1 and devise the AM and coAM protocols for AD($\mathbb{F}_{q'}$), which also apply to AD($\mathbb{F}_q$).

Remark 1.8. Our proof of Theorem 1.1 employs the fact that we could efficiently sample a random point in the set $\mathrm{Im}(f)$. In contrast, it is not clear how to efficiently sample a random point in the zero set $\mathrm{Zer}(\mathbf{f}) := \{\mathbf{x} \in \mathbb{F}_{q'}^n \mid f(\mathbf{x}) = \mathbf{0}\}$. Thus, we manage to side-step the NP-hardness associated with most zero set properties. E. g., computing the dimension of $\mathrm{Zer}(\mathbf{f})$ is NP-hard.

Proof idea of Theorem 1.3. Let polynomials $\mathbf{f} := \{f_1, \ldots, f_m\}$ in $\mathbb{F}[x_1, \ldots, x_n]$ be given over a field $\mathbb{F}$, represented by algebraic circuits. We want to determine if the constant term of every annihilator for $\mathbf{f}$ is zero. Redefine the polynomial map $f : \overline{\mathbb{F}}^n \to \overline{\mathbb{F}}^m$; $a \mapsto (f_1(a), \ldots, f_m(a))$. For a subset S of an affine or projective space, write $\overline{S}$ for its *Zariski closure* in that space, i. e., for the smallest subset that contains S and equals the zero set $\mathrm{Zer}(I)$ of some polynomial ideal I (homogeneous ideal in the projective case).

APS *vs.* AnnAtZero. [Theorem 4.2] Now, we interpret the problem AnnAtZero in a geometric way through Lemma 4.1:

The constant term of every annihilator of $\mathbf{f}$ is zero iff the origin point $\mathbf{0} \in \overline{\mathrm{Im}(f)}$.

This has a simple proof using the ideal-variety correspondence [25]. Note that the stronger condition $\mathbf{0} \in \mathrm{Im}(f)$ is equivalent to the existence of a common solution to the equations $f_i(x_1, \ldots, x_n) = 0$,

$i = 1, \ldots, m$. The latter problem (call it HN for Hilbert's Nullstellensatz) is known to be in AM if $\mathbb{F} = \mathbb{Q}$ and GRH is assumed [32]. However, $\mathrm{Im}(f)$ is not necessarily Zariski closed; equivalently, it may be strictly smaller than $\overline{\mathrm{Im}(f)}$. So, we need new ideas to test $\mathbf{0} \in \overline{\mathrm{Im}(f)}$.

Next, we observe that although $\mathbf{0} \in \overline{\mathrm{Im}(f)}$ is not equivalent to the existence of a solution $\mathbf{x} \in \overline{\mathbb{F}}^n$ to $f(\mathbf{x}) = \mathbf{0}$, it *is* equivalent to the existence of an "approximate solution" $\mathbf{x} \in \overline{\mathbb{F}}(\varepsilon)^n$, which is an n-tuple of rational functions in a formal variable ε. The proof idea of this uses a degree bound on ε due to [37]. We called this problem APS. As AnnAtZero problem is already known to be NP-hard [30], APS is also NP-hard.

Upper bound on APS. We now know that solving APS for $\mathbf{f}$ is equivalent to solving AnnAtZero for $\mathbf{f}$. AnnAtZero was previously known to be in PSPACE in the special case when the transcendence degree k of $\mathbb{F}(\mathbf{f})/\mathbb{F}$ equals m or $m-1$, but the general case remained open (best being EXPSPACE).

In this article we prove that AnnAtZero is in PSPACE even when $k < m-1$. Our simple idea is to reduce the input to a smaller $m = k+1$ instance, by choosing new polynomials $g_1, \ldots, g_{k+1}$ that are random linear combinations of the polynomials f_i. We show that with high probability, replacing $\{f_1, \ldots, f_m\}$ by $\{g_1, \ldots, g_{k+1}\}$ preserves YES/NO instances as well as the transcendence degree. This gives a randomized poly-time reduction from the case $k < m-1$ to $k = m-1$ (Theorem 4.6). The latter has a standard PSPACE algorithm.

For notational convenience view $\overline{\mathbb{F}}$ as the *affine line* $\mathbb{A}$. Define $V := \overline{\mathrm{Im}(f)} \subseteq \mathbb{A}^m$. Proving that the above reduction (of m) does preserve YES/NO instances amounts to proving the following geometric statement: If V does not contain the origin $O \in \mathbb{A}^m$, then with high probability, the variety $V' := \overline{\pi(V)}$ does not contain the origin $O' \in \mathbb{A}^{k+1}$ either, where $\pi : \mathbb{A}^m \to \mathbb{A}^{k+1}$ is a random linear map.

As π is picked at random, the kernel W of π is a random linear subspace of $\mathbb{A}^m$. We have $O' \notin \pi(V)$ whenever $V \cap W = \emptyset$, but this is not sufficient for proving $O' \notin \overline{\pi(V)}$, since V may "get arbitrarily close to W" in $\mathbb{A}^m$ and meet W "at infinity."

Example 1. The hyperbola $V := V(X_1X_2 - 1)$ and the line $W := V(X_1)$ do not meet in the affine space $\mathbb{A}^2$, even though they get closer and closer as we increase the absolute value of the coordinate X_2. However, note that the projective closures of these two varieties $V_c := V(X_1X_2 - X_0^2)$ and $W_c := V(X_1)$ do meet at the point $(0,0,1)$ of the projective space $\mathbb{P}^2$, which is thought of as one of the "points at infinity."

Inspired by the above observation, we consider projective geometry instead of affine geometry, and prove that $O' \notin V'$ holds as long as the projective closure of V and that of W are disjoint. The proof uses a construction of a projective subvariety—the *join*—to characterize $\pi^{-1}(V')$, and eventually rules out $W \subseteq \pi^{-1}(V')$ (Lemma 4.8).

Moreover, we show that this holds with high probability if $O \notin V$, by (repeatedly) using the fact that a general (=random) hyperplane section reduces the dimension of a variety by one.

Proof idea of Theorem 1.4. Define $\mathbb{A} := \overline{\mathbb{F}}_q$ and assume w.l.o.g. $q \geq \Omega(sr^2)$ [1]. [27, Theorem 4.4] showed that a hitting set, of size $h := O(s^2n^2)$ in $\mathbb{F}_q^n$, *exists* for the class of degree-r polynomials, in $\mathbb{A}[x_1, \ldots, x_n]$, that can be infinitesimally approximated by size-s algebraic circuits. So, we can search over all possible subsets of size h from $\mathbb{F}_q^n$ and "most" of them are hitting sets.

How do we certify that a candidate set $\mathcal{H}$ is a hitting set? The idea is to use universal circuits. A *universal circuit* has n essential variables $\mathbf{x} = \{x_1, \ldots, x_n\}$ and $s' := O(sr^4)$ auxiliary variables $\mathbf{y} = \{y_1, \ldots, y_{s'}\}$. We can fix the auxiliary variables, from $\mathbb{A}(\varepsilon)$, in such a way so that it can output any homogeneous circuit of size-s, approximating a degree-r polynomial in $\overline{\mathsf{VP}}_{\mathbb{A}}$. Given a universal circuit Ψ, certification of a hitting set $\mathcal{H}$ is based on the following observation, that follows from the definitions:

A candidate set $\mathcal{H} =: \{\mathbf{v}_1, \ldots, \mathbf{v}_h\}$ is a hitting set iff

$$\forall \mathbf{y} \in \mathbb{A}(\varepsilon)^{s'}, \Psi(\mathbf{y}, \mathbf{x}) \notin \varepsilon\mathbb{A}[\varepsilon][\mathbf{x}] \Rightarrow \exists i \in [h], \Psi(\mathbf{y}, \mathbf{v}_i) \notin \varepsilon\mathbb{A}[\varepsilon].$$

Equivalently, a candidate set $\mathcal{H} = \{\mathbf{v}_1, \ldots, \mathbf{v}_h\}$ is *not* a hitting set iff

$$\exists \mathbf{y} \in \mathbb{A}(\varepsilon)^{s'}, \Psi(\mathbf{y}, \mathbf{x}) \notin \varepsilon\mathbb{A}[\varepsilon][\mathbf{x}] \qquad \text{and} \qquad \forall i \in [h], \Psi(\mathbf{y}, \mathbf{v}_i) \in \varepsilon\mathbb{A}[\varepsilon]\,.$$

Note that certification of hitting set is more challenging than the one against polynomials in VP, because the degree bounds for ε are exponentially high and moreover, we do not know how to frame the first "non-containment" condition as an APS instance. To translate it to an APS instance, our key idea is the following.

Pick $q \geq \Omega(s'r^2)$ so that a hitting set exists, in $\mathbb{F}_q^n$, that works against polynomials infinitesimally approximated by the specializations of Ψ. Suppose $\Psi(\alpha, \mathbf{x})$ is not in $\varepsilon\mathbb{A}[\varepsilon][\mathbf{x}]$, for some $\alpha \in \mathbb{A}(\varepsilon)^{s'}$. This means that we can write it as $\sum_{-m \leq i \leq m'} \varepsilon^i g_i(\mathbf{x})$ with $g_{-m} \neq 0$ and $m \geq 0$. Clearly, $\varepsilon^m \cdot \Psi(\alpha, \mathbf{x})$ infinitesimally approximates the nonzero polynomial $g_{-m} \in \mathbb{A}[\mathbf{x}]$. By the conditions on Ψ, we know that g_{-m} is a homogeneous polynomial of degree r (and approximative complexity s'). Thus, by Lemma 2.2, there exists a $\beta \in \mathbb{F}_q^n$ such that $g_{-m}(\beta) =: a$ is a nonzero element in $\mathbb{A}$. We can normalize by this and consider $a^{-1}\varepsilon^m \cdot \Psi(\mathbf{y}, \mathbf{x})$, which evaluates to $1 + \varepsilon\mathbb{A}[\varepsilon]$ at (α, β). Since this normalization factor only affects the auxiliary variables $\mathbf{y}$, we get another equivalent criterion:

A candidate set $\mathcal{H} = \{\mathbf{v}_1, \ldots, \mathbf{v}_h\}$ is *not* a hitting set iff $\exists \mathbf{y} \in \mathbb{A}(\varepsilon)^{s'}$ and $\exists \mathbf{x} \in \mathbb{F}_q^n$ such that,

$$\Psi(\mathbf{y}, \mathbf{x}) - 1 \in \varepsilon\mathbb{A}[\varepsilon] \quad \text{and} \quad \forall i \in [h], \Psi(\mathbf{y}, \mathbf{v}_i) \in \varepsilon\mathbb{A}[\varepsilon].$$

We reach closer to APS, but how do we implement $\exists ?\mathbf{x} \in \mathbb{F}_q^n$ (it takes exponential space)?

The idea is to rewrite it, instead using the $(r+1)$-th roots of unity $Z_{r+1} \subseteq \mathbb{A}$, as $\exists \mathbf{x} \in \mathbb{A}(\varepsilon)^n$, $\forall i \in [n]$, $x_i^{r+1} - 1 \in \varepsilon\mathbb{A}[\varepsilon]$. This gives us a criterion that is an instance of APS with $n + h + 1$ input polynomials (Theorem 5.2). By Theorem 1.3 it can be done in PSPACE, finishing the proof. Moreover, this PSPACE algorithm is independent of the characteristic of the underlying field. (E. g., it can be seen as an alternative to [21] over the complex field.)

2 Preliminaries

Jacobian. Although this work would not need it, we define the classical Jacobian: Given polynomials $\mathbf{f} = \{f_1, \cdots, f_m\}$ in $\mathbb{F}[x_1, \cdots, x_n]$, the *Jacobian* of $\mathbf{f}$ is the matrix $\mathcal{J}_{\mathbf{x}}(\mathbf{f}) := (\partial_{x_j} f_i)_{m \times n}$, where $\partial_{x_j} f_i := \partial f_i / \partial x_j$.

The Jacobian criterion [29, 7] states that for degree $\leq d$ and trdeg $\leq r$ polynomials $\mathbf{f}$, if $\mathrm{char}(\mathbb{F}) = 0$ or $\mathrm{char}(\mathbb{F}) > d^r$, then $\mathrm{trdeg}(\mathbf{f}) = \mathrm{rank}_{\mathbb{F}(\mathbf{x})} \mathcal{J}_{\mathbf{x}}(\mathbf{f})$. This yields a randomized poly-time algorithm by Lemma 2.2. For other fields, the Jacobian criterion fails due to inseparability and $\mathrm{AD}(\mathbb{F})$ is open.

AM **protocol.** The Arthur-Merlin class AM is a randomized version of the class NP [4]. Arthur-Merlin protocols, introduced by Babai [6], can be considered as a special type of interactive proof system in which the randomized poly-time verifier (Arthur) and the all-powerful prover (Merlin) have only constantly many rounds of exchange. AM contains interesting problems like verifying that two graphs are non-isomorphic. AM $\cap$ coAM is the class of decision problems for which both YES and NO answers can be verified by an AM protocol. It can be thought of as the randomized version of NP $\cap$ coNP. See [31] for a few natural algebraic problems in AM $\cap$ coAM. If such a problem is NP-hard (even under random reductions) then the polynomial hierarchy collapses to the second level, i. e., $\mathsf{PH} = \Sigma_2$.

In this article, AM protocols will only be used to distinguish whether a set S is "small" or "large." Formally, we refer to the Goldwasser-Sipser [22] Set Lowerbound method.

Lemma 2.1 (Goldwasser-Sipser [22])**.** *Let $m \in \mathbb{N}$ be given in binary. Suppose S is a set whose membership can be tested in nondeterministic polynomial time and its size is promised to be either $\leq m$ or $\geq 2m$. Then, the problem of deciding whether $|S| \geq 2m$ is in* AM.

See, e. g., [4, Chapter 8] for a proof. We also use the Polynomial Identity Lemma several times. The version we use is stated below.

Lemma 2.2 (Polynomial Identity Lemma [57, 60, 16])**.** *Let $f(x_1,\dots,x_n)$ be a nonzero polynomial of total degree d over a field $\mathbb{F}$. Let S be a finite subset of $\mathbb{F}$. Then the total number of roots of $f(x_1,\dots,x_n)$ in S^n is bounded by $d|S|^{n-1}$.*

For a proof, see [4, Lemma A.36].

Geometry. Our proof requires some basic facts and definitions from classical algebraic geometry, which are listed below. One can also refer to a standard text, e. g., [25, 26].

Let $\mathbb{A} := \overline{\mathbb{F}}$ be the algebraic closure of a field $\mathbb{F}$. For $d \in \mathbb{N}^+$, write $\mathbb{A}^d$ for the *d-dimensional affine space* over $\mathbb{A}$. It is defined to be the set $\mathbb{A}^d$, equipped with the *Zariski topology*, defined as

Definition 2.3 (Zariski topology)**.** A subset S of $\mathbb{A}^d$ is *closed* if it is the set of common zeros of some set of polynomials in $\mathbb{A}[X_1,\dots,X_d]$. For a set S of polynomials, the *closure* $\overline{S}$ is defined as the smallest closed set containing S. A set S is *dense* in $\mathbb{A}^d$ if $\overline{S} = \mathbb{A}^d$. The complement of a closed set is called an *open* set.

A closed set is called a *hypersurface* if it is definable by a single polynomial. A hypersurface is a *hyperplane* if its defining polynomial is linear.

Define $\mathbb{A}^\times := \mathbb{A} \setminus \{0\}$. Write $\mathbb{P}^d$ for the d-dimensional projective space over $\mathbb{A}$, defined to be the quotient set $(\mathbb{A}^{d+1} \setminus \{(0,\dots,0)\})/\sim$ where $(x_0,\dots,x_d) \sim (y_0,\dots,y_d)$ iff there exists $c \in \mathbb{A}^\times$ such that $y_i = cx_i$ for $0 \leq i \leq d$. We use $(d+1)$-tuples $(x_0,\dots,x_d)$ to represent points in $\mathbb{P}^d$. Such a $(d+1)$-tuple is called a list of *homogeneous coordinates* of the point it represents.

The set $\mathbb{P}^d$ is again equipped with the *Zariski topology*.

Definition 2.4 (Zariski topology on a projective space)**.** A subset S of $\mathbb{P}^d$ is closed if it is the set of common zeros of some set of *homogeneous* polynomials in $\mathbb{A}[X_0,\dots,X_d]$.

Definition 2.5 (Variety)**.** Closed subsets of $\mathbb{A}^d$ or $\mathbb{P}^d$ are also called *algebraic sets* or *zero sets*. An algebraic set is *irreducible* if it cannot be written as the union of finitely many proper algebraic sets. An irreducible algebraic subset of an affine (or projective) space is also called an *affine variety* (*projective variety*, resp.).

(In some references, varieties are not required to be irreducible, but in this paper we always assume they are.) An algebraic set V can be uniquely represented as the union of finitely many varieties, and these varieties are called the *irreducible components* of V.

Affine zero sets are in 1-1 correspondence with *radical* ideals; varieties correspond to *prime* ideals.

Irreducible decomposition of an affine variety mirrors the factoring of an ideal into primary ideals. Finally, note that the affine points are in 1-1 correspondence with *maximal* ideals; this is a simple reformulation of Hilbert's Nullstellensatz.

The affine space $\mathbb{A}^d$ may be regarded as a subset of $\mathbb{P}^d$ via the map $(x_1,\ldots,x_d) \mapsto (1,x_1,\ldots,x_d)$. Then the subspace topology of $\mathbb{A}^d$ induced from the Zariski topology of $\mathbb{P}^d$ is just the Zariski topology of $\mathbb{A}^d$. The set $\mathbb{P}^d \setminus \mathbb{A}^d$ is the projective subspace of $\mathbb{P}^d$ defined by $X_0 = 0$, called the *hyperplane at infinity*.

For an algebraic subset V of $\mathbb{A}^d \subseteq \mathbb{P}^d$, the smallest algebraic subset V' of $\mathbb{P}^d$ containing V (i. e., the intersection of all algebraic subsets containing V) is the *projective closure* of V, and we have $V' \cap \mathbb{A}^d = V$. To see this, note that for $P = (x_1,\ldots,x_d) \in \mathbb{A}^d \setminus V$, there exists a polynomial $Q \in \mathbb{A}[X_1,\ldots,X_d]$ of degree $D \in \mathbb{N}$ not vanishing on P (but vanishing on V). Then its homogenization $Q' \in \mathbb{A}[X_0,\ldots,X_d]$, defined by replacing each monomial

$$M = \prod_{i=1}^{d} X_i^{d_i} \qquad \text{by} \qquad X_0^{D-\deg(M)} \prod_{i=1}^{d} X_i^{d_i},$$

does not vanish on $(1,x_1,\ldots,x_d)$. So, $(1,\mathbf{x}) \notin V'$.

For distinct points $P = (x_0,\ldots,x_d), Q = (y_0,\ldots,y_d) \in \mathbb{P}^d$, write $\overline{PQ}$ for the *projective line* passing through them, i. e., $\overline{PQ}$ consists of the points $(ux_0 + vy_0,\ldots,ux_d + vy_d)$, where $(u,v) \in \mathbb{A}^2 \setminus \{(0,0)\}$.

Definition 2.6 (Dimension and degree)**.** The *dimension* of a variety V is defined to be the largest integer m such that there exists a chain of varieties $\emptyset \subsetneq V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_m = V$. More generally, the dimension of an algebraic set V, denoted by $\dim V$, is the maximal dimension of its irreducible components. E. g., we have $\dim \mathbb{A}^d = \dim \mathbb{P}^d = d$. The dimension of the empty set is -1 by convention. One-dimensional varieties are called *curves*.

The *degree* of a variety V in $\mathbb{A}^d$ (or in $\mathbb{P}^d$) is the number of intersections of V with a general[3] affine subspace (projective subspace, resp.) of dimension $d - \dim V$. More generally, we define the degree of an algebraic set V, denoted by $\deg(V)$, to be the sum of the degrees of its irreducible components. The degree of an algebraic subset of $\mathbb{A}^d$ coincides with the degree of its projective closure in $\mathbb{P}^d$.

Suppose $V \subseteq \mathbb{A}^d$ is an algebraic set, defined by polynomials $f_1,\ldots,f_k$. Let $(a_1,\ldots,a_d) \in \mathbb{A}^d$. Then the set $\{(x_1 + a_1,\ldots,x_d + a_d) : (x_1,\ldots,x_d) \in V\}$ is called a *translate* of V. It is also an algebraic set, defined by $f_i(X_1 - a_1,\ldots,X_d - a_d)$, $i = 1,\ldots,k$.

Definition 2.7 (Morphism)**.** Let $V \subseteq \mathbb{A}^n$, $W \subseteq \mathbb{A}^m$ be affine varieties. A *morphism* from V to W is a function $f : V \to W$ that is a restriction of a polynomial map $\mathbb{A}^n \to \mathbb{A}^m$.

A morphism $f : V \to W$ is called *dominant* if $\overline{\mathrm{Im}(f)} = W$. The preimage of a closed subset under a morphism is closed (i. e., morphisms are *continuous* in the Zariski topology).

[3] We do not rigorously define the word *general* here, but just remark that it essentially means "random" in algebraic geometry. In fact, as long as we work over a large enough field, replacing "general" by "random" would not cause any problem.

For a polynomial map $f : \mathbb{A}^n \to \mathbb{A}^m$ and an affine variety $V \subseteq \mathbb{A}^n$, $W := \overline{f(V)}$ is also an affine variety (i. e., it is irreducible). To see this, assume to the contrary that W is the union of two proper closed subsets W_1 and W_2. By the definition of closure, $f(V)$ is not contained in either W_1 or W_2, i. e., it intersects both. Then $f^{-1}(W_1) \cap V$ and $f^{-1}(W_2) \cap V$ are two proper closed subsets of V, and their union is V. This contradicts the irreducibility of V.

The *graph* Γ_f of a morphism f is the set $\{(x, f(x)) : x \in V\} \subseteq V \times W \subseteq \mathbb{A}^n \times \mathbb{A}^m$. Here $V \times W = \{(x,y) : x \in V, y \in W\}$ denotes the *product* of V and W, which is a subvariety of the $(n+m)$-dimensional affine space $\mathbb{A}^n \times \mathbb{A}^m \cong \mathbb{A}^{n+m}$. Note the graph Γ_f is closed in $\mathbb{A}^n \times \mathbb{A}^m$: Suppose f sends $x \in V$ to $(f_1(x), \dots, f_m(x)) \in \mathbb{A}^m$, where $f_i \in \mathbb{A}[X_1, \dots, X_n]$ for $i \in [m]$. And suppose V is defined by an ideal $I \subseteq \mathbb{A}[X_1, \dots, X_n]$. Then Γ_f is defined by the ideal of $\mathbb{A}[X_1, \dots, X_n, Y_1, \dots, Y_m]$ generated by I and the polynomials $Y_i - f_i(X_1, \dots, X_n)$, $i = 1, \dots, m$.

3 Algebraic dependence testing: Proof of Theorem 1.1

Given $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$, we want to decide if they are algebraically dependent. For this problem, $\mathrm{AD}(\mathbb{F}_q)$, we could assume, with some preprocessing, that $m = n$. For, $m > n$ means that it is a YES instance. If $m < n$ then we could apply a "random" linear map on the variables to reduce n to m, preserving the YES/NO instances. Also, the transcendence degree does not change when we move to the algebraic closure $\overline{\mathbb{F}}_q$. The details can be found in [47, Lemmas 2.7–2.9]. So, we assume the input instance to be $\mathbf{f} := \{f_1, \dots, f_n\}$ with nonconstant polynomials.

In the following, let $D := \prod_{i \in [n]} \deg(f_i) > 0$ and $D' := \max_{i \in [n]} \deg(f_i) > 0$. Let $d \in \mathbb{N}^+$ and $q' = q^d$. The value of d will be determined later. Let $f : \mathbb{F}_{q'}^n \to \mathbb{F}_{q'}^n$ be the polynomial map $a \mapsto (f_1(a), \dots, f_n(a))$. For $b = (b_1, \dots, b_n) \in \mathbb{F}_{q'}^n$, denote by N_b the size of the preimage

$$f^{-1}(b) = \left\{ \mathbf{x} \in \mathbb{F}_{q'}^n \;\middle|\; f(\mathbf{x}) = b \right\}.$$

Define $\mathbb{A} := \overline{\mathbb{F}}_q$ and $\overline{N}_b := \#\{\mathbf{x} \in \mathbb{A}^n \mid f_i(\mathbf{x}) = b_i, \text{ for all } i \in [n]\}$ which might be ∞. Let $Q \in \mathbb{F}_q[y_1, \dots, y_n]$ be a nonzero annihilator, of minimal degree, of $f_1, \dots, f_n$. If it exists then $\deg(Q) \le D$ by Perron's bound.

3.1 AM protocol

First, we study the independent case.

Lemma 3.1 (Dimension-zero preimage). *Suppose* $\mathbf{f}$ *is independent. Then* $\overline{N}_{f(a)}$ *is* finite *for all but at most* (nDD'/q')*-fraction of* $a \in \mathbb{F}_{q'}^n$.

Proof. For $i \in [n]$, let $G_i \in \mathbb{F}_q[z, y_1, \dots, y_n]$ be the annihilator of $\{x_i, f_1, \dots, f_n\}$. We have $\deg(G_i) \le D$ by Perron's bound. Consider $a \in \mathbb{F}_{q'}^n$ such that $G_i'(z) := G_i(z, f_1(a), \dots, f_n(a)) \in \mathbb{F}_q[z]$ is a nonzero polynomial for every $i \in [n]$. We claim that $\overline{N}_{f(a)}$ is finite for such a.

To see this, note that for any $b = (b_1, \dots, b_n) \in \mathbb{A}^n$ satisfying the equations $f_i(b) = f_i(a)$, $i \in [n]$, we have

$$0 = G_i(b_i, f_1(b), \dots, f_n(b)) = G_i(b_i, f_1(a), \dots, f_n(a)) = G_i'(b_i), \quad \forall i \in [n].$$

Hence, each b_i is a root of G_i'. It follows that $\overline{N}_{f(a)} \le \prod_{i\in[n]} \deg(G_i') < \infty$, as claimed.

It remains to prove that the number of $a \in \mathbb{F}_{q'}^n$ satisfying $G_i' = 0$, for some index $i \in [n]$, is bounded by $nDD'q'^{-1} \cdot q'^n$. Fix $i \in [n]$. Suppose $G_i = \sum_{j=0}^{d_i} G_{i,j} z^j$, where $d_i := \deg_z(G_i)$ and $G_{i,j} \in \mathbb{F}_q[y_1,\dots,y_n]$, for $0 \le j \le d_i$. The leading coefficient G_{i,d_i} is a nonzero polynomial. As $f_1,\dots,f_n$ are algebraically independent, the polynomial $G_{i,d_i}(f_1,\dots,f_n) \in \mathbb{F}_q[x_1,\dots,x_n]$ is also nonzero. Its degree is $\le D' \deg(G_{i,d_i}) \le D' \deg(G_i) \le DD'$. By Lemma 2.2, for all but at most (DD'/q')-fraction of $a \in \mathbb{F}_{q'}^n$, we have

$$G_{i,d_i}(f_1(a),\dots,f_n(a)) \ne 0,$$

which implies

$$G_i'(z) \,=\, G_i(z, f_1(a),\dots,f_n(a)) \,=\, \sum_{j=0}^{d_i} G_{i,j}(f_1(a),\dots,f_n(a)) z^j \ne 0\,.$$

The claim now follows from the union bound. □

We need the following affine version of Bézout's Theorem. Its proof can be found in [55, Theorem 3.1].

Theorem 3.2 (Bézout's). *Let $g_1,\dots,g_n \in \mathbb{A}[x_1,\dots,x_n]$. Then the number of common zeros of $g_1,\dots,g_n$ in $\mathbb{A}^n$ is either infinite, or at most $\prod_{i\in[n]} \deg(g_i)$.*

Combining Lemma 3.1 with Bézout's Theorem, we obtain

Lemma 3.3 (Small preimage). *Suppose* **f** *is independent. Then $N_{f(a)} \le D$ for all but at most (nDD'/q')-fraction of $a \in \mathbb{F}_{q'}^n$.*

Next, we study the dependent case (with an annihilator Q).

Lemma 3.4 (Large preimage). *Suppose* **f** *is dependent. Then for $k > 0$, we have $N_{f(a)} > k$ for all but at most (kD/q')-fraction of $a \in \mathbb{F}_{q'}^n$.*

Proof. Let $\mathrm{Im}(f) := f(\mathbb{F}_{q'}^n)$ be the image of the map. Note that Q vanishes on all the points in $\mathrm{Im}(f)$. So, $|\mathrm{Im}(f)| \le Dq'^{n-1}$ by Lemma 2.2.

Let $B := \{b \in \mathrm{Im}(f) : N_b \le k\}$ be the "bad" images. We can estimate the bad domain points as,

$$\#\{a \in \mathbb{F}_{q'}^n : N_{f(a)} \le k\} \,=\, \#\{a \in \mathbb{F}_{q'}^n : f(a) \in B\} \,\le\, k|B| \le k|\mathrm{Im}(f)| \,\le\, kDq'^{n-1}\,.$$

which proves the lemma. □

Theorem 3.5 (AM). *Testing algebraic dependence of* **f** *is in* AM.

Proof. Fix $q' = q^d > 4nDD' + 4kD$ and $k := 2D$. Note that d will be polynomial in the input size. For an $a \in \mathbb{F}_{q'}^n$, consider the set $f^{-1}(f(a)) := \{\mathbf{x} \in \mathbb{F}_{q'}^n \mid f(\mathbf{x}) = f(a)\}$.

By Lemma 3.3 and Lemma 3.4, when Arthur picks a randomly, with high probability, $|f^{-1}(f(a))| = N_{f(a)}$ is more than $2D$ in the dependent case while $\le D$ in the independent case. Note that an upper bound on $\prod_{i\in[n]} \deg(f_i)$ can be deduced from the size of the input circuits for the polynomials f_i; thus, we know D. Moreover, containment in $f^{-1}(f(a))$ can be tested in P. Thus, by Lemma 2.1, $\mathrm{AD}(\mathbb{F}_q)$ is in AM. □

3.2 coAM protocol

We first study the independent case.

Lemma 3.6 (Large image)**.** *Suppose* **f** *is independent. Then $N_b > 0$ for at least $(D^{-1} - nD'q'^{-1})$-fraction of $b \in \mathbb{F}_{q'}^n$.*

Proof. Let $S := \{a \in \mathbb{F}_{q'}^n : N_{f(a)} \leq D\}$. Then $|S| \geq (1 - nDD'q'^{-1}) \cdot q'^n$ by Lemma 3.3. As every $b \in f(S)$ has at most D preimages in S under f, we have $|f(S)| \geq |S|/D \geq (D^{-1} - nD'q'^{-1}) \cdot q'^n$. This proves the lemma since $N_b > 0$ for all $b \in f(S)$. □

Next, we study the dependent case.

Lemma 3.7 (Small image)**.** *Suppose* **f** *is dependent. Then $N_b = 0$ for all but at most (D/q')-fraction of $b \in \mathbb{F}_{q'}^n$.*

Proof. By definition, $N_b > 0$ iff $b \in \mathrm{Im}(f) := f(\mathbb{F}_{q'}^n)$. It was shown in the proof of Lemma 3.4 that $|\mathrm{Im}(f)| \leq Dq'^{n-1}$. The lemma follows. □

Theorem 3.8 (coAM)**.** *Testing algebraic dependence of* **f** *is in* coAM.

Proof. Fix $q' = q^d > D(2D + nD')$. Note that d will be polynomial in the input size. For $b \in \mathbb{F}_{q'}^n$, consider the set $f^{-1}(b) := \{\mathbf{x} \in \mathbb{F}_{q'}^n \mid f(\mathbf{x}) = b\}$ of size N_b.

Define $S := \mathrm{Im}(f)$. Note that $b \in \mathbb{F}_{q'}^n$ satisfies $N_b > 0$ iff $b \in S$. Thus, by Lemma 3.6, $|S| \geq (D^{-1} - nD'q'^{-1})q'^n > 2Dq'^{n-1}$ when **f** is independent, and by Lemma 3.7, $|S| \leq Dq'^{n-1}$ when **f** is dependent.

Note that an upper bound on $\prod_{i\in[n]} \deg(f_i)$ can be deduced from the size of the input circuits for the polynomials f_i; thus, we know Dq'^{n-1}. Moreover, containment in S can be tested in NP. Thus, by Lemma 2.1, $\mathrm{AD}(\mathbb{F}_q)$ is in coAM. □

Proof of Theorem 1.1. The statement immediately follows from Theorem 3.5 and Theorem 3.8. □

4 Approximate polynomials satisfiability: Proof of Theorem 1.3

Theorem 1.3 is proved in two parts. First, we show that APS is equivalent to AnnAtZero problem, which means that it is NP-hard [30]. Next, we utilize the beautiful underlying geometry to devise a PSPACE algorithm.

4.1 APS is equivalent to AnnAtZero

The proof that APS is equivalent to AnnAtZero is classical and follows from two statements in algebraic geometry and commutative algebra, which we state as Lemma 4.1 and Theorem 4.2. The first statement (Lemma 4.1) gives a geometric reinterpretation of AnnAtZero. This can be seen as a direct application of the ideal-variety correspondence. The second statement (Theorem 4.2) is also classical. It was essentially proved in [37] and was also discussed in [12, Lemma 20.28] and [23, Page 37:53].

Let $\mathbb{A}$ be the algebraic closure of $\mathbb{F}$. Note that for the given polynomials $\mathbf{f} := \{f_1, \ldots, f_m\}$ in $\mathbb{F}[\mathbf{x}]$, there is an annihilator over $\mathbb{F}$ with a nonzero constant term iff there is an annihilator over $\mathbb{A}$ with a nonzero constant term. This is because if Q is an annihilator over $\mathbb{A}$ with a nonzero constant term, w.l.o.g. 1, then by basic linear algebra, the linear system defined by the equation $Q(\mathbf{f}) = 0$, in terms of the unknown coefficients of Q, would also have a solution in $\mathbb{F}$. Thus, there is an annihilator over $\mathbb{F}$ with constant term 1. This proves that it suffices to solve AnnAtZero over the algebraically closed field $\mathbb{A}$. This provides us with a better geometry.

Write $f : \mathbb{A}^n \to \mathbb{A}^m$ for the polynomial map sending a point

$$x = (x_1, \ldots, x_n) \in \mathbb{A}^n \quad \text{to} \quad (f_1(x), \ldots, f_m(x)) \in \mathbb{A}^m .$$

For a subset S of an affine or projective space, write $\overline{S}$ for its Zariski closure in that space. We will use O to denote the origin $\mathbf{0}$ of an affine space.

The following lemma reinterprets AnnAtZero in a geometric way.

Lemma 4.1 (classical). *The constant term of every annihilator for* $\mathbf{f}$ *is zero iff* $O \in \overline{\mathrm{Im}(f)}$.

Proof. Note that $Q \in \mathbb{A}[Y_1, \ldots, Y_m]$ vanishes on $\mathrm{Im}(f)$ iff $Q(\mathbf{f})$ vanishes on $\mathbb{A}^n$, which holds iff $Q(\mathbf{f}) = 0$, i. e., Q is an annihilator for $\mathbf{f}$. So $\overline{\mathrm{Im}(f)} = V(I)$, where the ideal $I \subseteq \mathbb{A}[Y_1, \ldots, Y_m]$ consists of the annihilators for $\mathbf{f}$. Also note that $\{O\} = V(\mathfrak{m})$, where $\mathfrak{m}$ is the maximal ideal $\langle Y_1, \ldots, Y_m \rangle$.

Let us study the condition $O \in \overline{\mathrm{Im}(f)}$. By the ideal-variety correspondence, $\{O\} = V(\mathfrak{m}) \subseteq \overline{\mathrm{Im}(f)} = V(I)$ is equivalent to $I \subseteq \mathfrak{m}$, i. e., $Q \bmod \mathfrak{m} = 0$ for $Q \in I$. But $Q \bmod \mathfrak{m}$ is just the constant term of the annihilator Q. Hence, we have the equivalence. □

As a special case, the above lemma proves that whenever $\mathbf{f}$ is algebraically *independent*, we have $\mathbb{A}^m = \overline{\mathrm{Im}(f)}$. E. g., $f_1 = X_1$ and $f_2 = X_1X_2 - 1$.

In general, $\mathrm{Im}(f)$ is not necessarily closed in the Zariski topology.

Example 2. Let $n = 2$, $m = 3$. Consider $f_1 = f_2 = X_1$ and $f_3 = X_1X_2 - 1$. The annihilators are multiples of $(Y_1 - Y_2)$, which means by Lemma 4.1 that $O \in \overline{\mathrm{Im}(f)}$. But there is no solution to $f_1 = f_2 = f_3 = 0$, i. e., $O \notin \mathrm{Im}(f)$.

Approximation. Although $O \in \overline{\mathrm{Im}(f)}$ is not equivalent to the existence of a solution $x \in \mathbb{A}^n$ to $f_i = 0$, $i \in [m]$, it is equivalent to the existence of an "approximate solution" $x \in \mathbb{A}[\varepsilon, \varepsilon^{-1}]^n$, which is a tuple of Laurent polynomials in a formal variable ε. The formal statement is as follows. W.l.o.g. we assume $\mathbf{f}$ to be m nonconstant polynomials.

Theorem 4.2 (classical). $O \in \overline{\mathrm{Im}(f)}$ *iff there exists* $x = (x_1, \ldots, x_n) \in \mathbb{A}(\varepsilon)^n$ *such that* $f_i(x) \in \varepsilon\mathbb{A}[\varepsilon]$, *for all* $i \in [m]$. *Moreover, when such* x *exists, it may be chosen such that*

$$x_i \in \varepsilon^{-\Delta}\mathbb{A}[\varepsilon] \cap \varepsilon^{\Delta'}\mathbb{A}[\varepsilon^{-1}] = \left\{ \sum_{j=-\Delta}^{\Delta'} c_j \varepsilon^j : c_j \in \mathbb{A} \right\}, \quad i \in [n],$$

where $\Delta := \prod_{i \in [m]} \deg(f_i) > 0$ *and* $\Delta' := (\max_{i \in [m]} \deg(f_i)) \cdot \Delta > 0$.

For example, choosing $x = (x_1, x_2) := (\varepsilon, 1/\varepsilon)$ in Example 2, we have $f_1(x) = f_2(x) = \varepsilon$ and $f_3(x) = 0$. Thus Theorem 4.2 gives another way of seeing $O \in \overline{\mathrm{Im}(f)}$ in Example 2.

As mentioned previously, Theorem 4.2 was essentially proved in [37]. We include a proof here for the sake of completeness.

First, we recall a tool to reduce the domain from a variety to a curve, proven in [37].

Lemma 4.3 ([37, Proposition 1])**.** *Let $V \subseteq \mathbb{A}^n$, $W \subseteq \mathbb{A}^m$ be affine varieties, $\varphi : V \to W$ dominant, and $t \in W \setminus \varphi(V)$. Then there exists a curve $C \subseteq \mathbb{A}^n$ such that $t \in \overline{\varphi(C)}$ and $\deg(C) \le \deg(\Gamma_\varphi)$, where Γ_φ denotes the graph of φ embedded in $\mathbb{A}^n \times \mathbb{A}^m$.*

Next, [37] essentially shows that in the case of a curve one can approximate the preimage of f by using a *single* formal variable ε and working in $\mathbb{A}(\varepsilon)$. Here $\mathbb{A}[[\varepsilon]]$ denotes a formal power series in ε with coefficients from $\mathbb{A}$.

Lemma 4.4 ([37, Corollary of Proposition 3])**.** *Let $C \subseteq \mathbb{A}^n$ be an affine curve. Let $f : C \to \mathbb{A}^m$ be a morphism sending $x \in C$ to $(f_1(x), \ldots, f_m(x)) \in \mathbb{A}^m$, where $f_1, \ldots, f_m \in \mathbb{A}[X_1, \ldots, X_n]$. Let $t = (t_1, \ldots, t_m) \in \overline{f(C)}$. Then there exists $p_1, \ldots, p_n \in \varepsilon^{-\deg(C)}\mathbb{A}[[\varepsilon]]$ such that $f_i(p_1, \ldots, p_n) - t_i \in \varepsilon\mathbb{A}[[\varepsilon]]$, for all $i \in [m]$.*

Finally, we use the above two lemmas to prove the connection of APS with $O \in \overline{\mathrm{Im}(f)}$, and hence with AnnAtZero (by Lemma 4.1).

Proof of Theorem 4.2. First assume that an x, satisfying the conditions in Theorem 4.2, exists. Pick such an x. If $\mathbf{f}$ is algebraically independent then by Lemma 4.1 we have that $\mathbb{A}^m = \overline{\mathrm{Im}(f)}$ and we are done. So, assume that there is a nonzero annihilator Q for $\mathbf{f}$. We have $Q(f_1(x), \ldots, f_m(x)) = 0 \in \varepsilon\mathbb{A}[\varepsilon]$. On the other hand, as $f_i(x) \in \varepsilon\mathbb{A}[\varepsilon]$, for all $i \in [m]$; we deduce that $Q(f_1(x), \ldots, f_m(x)) \bmod \varepsilon\mathbb{A}[\varepsilon]$ is $Q(\mathbf{0})$, which is the constant term of Q. So it equals zero. By Lemma 4.1, we have $O \in \overline{\mathrm{Im}(f)}$ and again we are done.

Conversely, assume $O \in \overline{\mathrm{Im}(f)}$ and we will prove that x exists. If $O \in \mathrm{Im}(f)$, then we can choose $x \in \mathbb{A}^n$ and we are done. So assume $O \in \overline{\mathrm{Im}(f)} \setminus \mathrm{Im}(f)$. Regard f as a dominant morphism from $\mathbb{A}^n$ to $\overline{\mathrm{Im}(f)}$. Its graph Γ_f is cut out in $\mathbb{A}^n \times \mathbb{A}^m$ by $Y_i - f_i(X_1, \ldots, X_n)$, $i \in [m]$. So $\deg(\Gamma_f) \le \prod_{i=1}^m \deg(f_i) = \Delta$ by Bézout's Theorem.

By Lemma 4.3, there exists a curve $C \subseteq \mathbb{A}^n$ such that $O \in \overline{f(C)}$ and $\deg(C) \le \deg(\Gamma_f) \le \Delta$. Pick such a curve C. Apply Lemma 4.4 to C, $f|_C$ and O, and let $p_1, \ldots, p_n \in \varepsilon^{-\deg(C)}\mathbb{A}[[\varepsilon]] \subseteq \varepsilon^{-\Delta}\mathbb{A}[[\varepsilon]]$ be as given by the lemma. Then $f_i(p_1, \ldots, p_n) \in \varepsilon\mathbb{A}[[\varepsilon]]$, for all $i \in [m]$.

For $i \in [n]$, let x_i be the Laurent polynomial obtained from p_i by truncating the terms of degree greater than Δ'. When evaluating $f_1, \ldots, f_m$, at $(p_1, \ldots, p_n)$, such truncation does not affect the coefficient of ε^k for $k \le 0$ by the choice of Δ'. So $f_i(x_1, \ldots, x_n) \in \varepsilon\mathbb{A}[\varepsilon]$, for all $i \in [m]$. □

Remark 4.5. The lower bound $-\Delta = -\prod_{i=1}^m \deg(f_i)$ for the least degree of x_i in ε can be achieved up to a factor of $1 + o(1)$. Consider the polynomials $f_1 = f_2 = X_1$, $f_3 = X_1^{d-1}X_2 - 1$, and $f_i = X_{i-2}^d - X_{i-1}$ for $i = 4, \ldots, m$, where $m = n+1$. Then we are forced to choose $x_1 \in \varepsilon\mathbb{A}[\varepsilon]$ and $x_i \in \varepsilon^{-(d-1)d^{i-2}} \cdot \mathbb{A}[\varepsilon^{-1}]$, for $i = 2, \ldots, n$. So the least degree of x_n in ε is at most $-(d-1)d^{n-2}$, while $-\Delta = -d^{n-1}$.

4.2 Putting APS in PSPACE

Owing to the exponential upper bound on the precision (= degree w.r.t. ε) shown in Theorem 4.2, one expects to solve APS in EXPSPACE only. Surprisingly, in this section, we give a PSPACE algorithm. This we do by reducing the general AnnAtZero instance to a very special instance, that is easy to solve.

Let $\mathbb{A}$ be the algebraic closure of the field $\mathbb{F}$. Let $f_1,\ldots,f_m \in \mathbb{F}[X_1,\ldots,X_n]$ be given. Denote by k the transcendence degree of $\mathbb{F}(f_1,\ldots,f_m)/\mathbb{F}$. Computing k can be done in PSPACE using linear algebra [49, 15, 9, 43]. We assume $k < m-1$, since the cases $k = m-1$ and $k = m$ are again easy. In the case $k = m$, the input instances are always in APS since $\overline{\mathrm{Im}(f)} = \mathbb{A}^m$. And in the case $k = m-1$, the ideal of the annihilators is a principal ideal, and hence has a unique generator (up to scaling). The degree of this generator is at most $\prod_{i=1}^m \deg(f_i)$. Thus checking whether it has a nonzero constant term can be solved in PSPACE by solving an exponential sized linear system of equations using [15, 9, 43].

We reduce the number of polynomials from m to $k+1$ as follows: Fix a finite set $S \subseteq \mathbb{F}$, and choose $c_{i,j} \in S$ at random for $i \in [k+1]$ and $j \in [m]$. For this to work, we need a large enough S and $\mathbb{F}$. For $i \in [k+1]$, let $g_i := \sum_{j=1}^m c_{i,j} f_j$.

Let $\delta := (k+1)(\max_{i\in[m]} \deg(f_i))^k/|S|$. Our algorithm is immediate once we prove the following claim.

Theorem 4.6 (Random reduction)**.** *It holds, with probability* $\geq (1-\delta)$*, that*

(1) the transcendence degree of $\mathbb{F}(g_1,\ldots,g_{k+1})/\mathbb{F}$ *equals k, and*

(2) the constant term of every annihilator for $g_1,\ldots,g_{k+1}$ *is zero iff the constant term of every annihilator for* $f_1,\ldots,f_m$ *is zero.*

First, we reformulate the two items of Theorem 4.6 in a geometric way, and later we will analyze the error probability.

For $d \in \mathbb{N}$, denote by $\mathbb{A}^d$ (and by $\mathbb{P}^d$) the d-dimensional affine space (projective space, resp.) over $\mathbb{A} := \overline{\mathbb{F}}$. Let $f : \mathbb{A}^n \to \mathbb{A}^m$ (resp. $g : \mathbb{A}^n \to \mathbb{A}^{k+1}$) be the polynomial map sending x to $(f_1(x),\ldots,f_m(x))$ (resp. $(g_1(x),\ldots,g_{k+1}(x))$). Let O and O' be the origin of $\mathbb{A}^m$ and that of $\mathbb{A}^{k+1}$ respectively. Define the affine varieties $V := \overline{\mathrm{Im}(f)} \subseteq \mathbb{A}^m$ and $V' := \overline{\mathrm{Im}(g)} \subseteq \mathbb{A}^{k+1}$. Then $\dim V = \mathrm{trdeg}(\mathbf{f}) = k$.

Let $\pi : \mathbb{A}^m \to \mathbb{A}^{k+1}$ be the linear map sending $(x_1,\ldots,x_m)$ to $(y_1,\ldots,y_{k+1})$ where $y_i = \sum_{j=1}^m c_{i,j} x_j$. Then $g = \pi \circ f$ and $V' = \overline{\pi(V)}$.[4] Now (1) of Theorem 4.6 is equivalent to $\dim V' = k$, and (2) is equivalent to $O' \in V'$ iff $O \in V$.

$$\begin{tikzcd}
\mathbb{A}^n \arrow[r, "f"] \arrow[dr, "g"'] & V = \overline{\mathrm{Im}(f)} \arrow[r, "\subseteq"] \arrow[d, "\pi|_V"] & \mathbb{A}^m \arrow[d, "\pi"] \\
& V' = \overline{\mathrm{Im}(g)} \arrow[r, "\subseteq"] & \mathbb{A}^{k+1}
\end{tikzcd}$$

We will give sufficient conditions of (1) and (2) in terms of incidence properties. Note that $O \in V$ implies $O' \in V'$, since $\pi(O) = O'$. Now suppose $O \notin V$. Let $W := \pi^{-1}(O')$, which is a linear subspace of $\mathbb{A}^m$. Then $O' \notin \pi(V)$ iff $V \cap W = \emptyset$. However, $V \cap W = \emptyset$ does not imply $O' \notin V'$, as V may "get infinitesimally close to W" without actually meeting W, so that $O' \in \overline{\pi(V)} = V'$. This is shown by the following example.

[4] To see $V' \supseteq \overline{\pi(V)}$, note that $\pi^{-1}(V')$ contains $\mathrm{Im}(f)$ and is closed, and hence contains $V = \overline{\mathrm{Im}(f)}$.

Example 3. Let $m = 4$ and $(f_1, f_2, f_3, f_4) = (X_1, X_2, X_1X_2 - 1, X_1 + X_2)$. Then $k := \operatorname{trdeg}(\mathbf{f}) = 2$. Let $(g_1, g_2, g_3) = (f_1, f_3, f_1 + f_2 - f_4) = (X_1, X_1X_2 - 1, 0)$. Suppose $\mathbb{A}^m$ has coordinates $Y_1, \ldots, Y_4$ and $\mathbb{A}^{k+1}$ has coordinates $Z_1, \ldots, Z_3$.

Then $V \subseteq \mathbb{A}^m$ is defined by $Y_1Y_2 - Y_3 - 1 = 0$ and $Y_1 + Y_2 - Y_4 = 0$, and W is defined by $Y_1 = 0$, $Y_3 = 0$, and $Y_2 - Y_4 = 0$. So $V \cap W = \emptyset$. But $V' \subseteq \mathbb{A}^{k+1}$ is the plane $Z_3 = 0$, which contains the origin.

To overcome the above problem, we consider projective geometry instead of affine geometry. Suppose $\mathbb{A}^m$ have coordinates $X_1, \ldots, X_m$ and $\mathbb{P}^m$ have homogeneous coordinates $X_0, \ldots, X_m$. Regard $\mathbb{A}^m$ as a dense open subset of $\mathbb{P}^m$ via $(x_1, \ldots, x_m) \mapsto (1, x_1, \ldots, x_m)$. Then $H := \mathbb{P}^m \setminus \mathbb{A}^m \cong \mathbb{P}^{m-1}$ is the *hyperplane at infinity*, defined by $X_0 = 0$. Denote by V_c (and W_c) the *projective closure* of V (W, resp.) in $\mathbb{P}^m$. Then $V = V_c \cap \mathbb{A}^m$. Let $W_H := W_c \cap H$, which is a projective subspace of H.

For distinct points $P, Q \in \mathbb{P}^m$, write $\overline{PQ}$ for the projective line passing through them. The following two lemmas provide sufficient conditions for $\dim V' = k$ and $O' \notin V'$, respectively.

Lemma 4.7. *If $V_c \cap W_H = \emptyset$, then $\dim V' = k$.*

Proof. Assume $\dim V' < k$. Choose $P \in \pi(V)$. The dimension of $\pi^{-1}(P) \cap V$ is at least $\dim V - \dim V' \geq 1$ [25, Theorem 11.12]. Denote by Y and Z the projective closure of $\pi^{-1}(P)$ and that of $\pi^{-1}(P) \cap V$ in $\mathbb{P}^m$, respectively. Then $Z \subseteq Y \cap V_c$. As $\dim Z = \dim \pi^{-1}(P) \cap V \geq 1$ and $\dim H = m - 1$, we have $Z \cap H \neq \emptyset$ [25, Proposition 11.4].

As π is a linear map, $\pi^{-1}(P) = Y \cap \mathbb{A}^m$ is a translate of $\pi^{-1}(O') = W = W_c \cap \mathbb{A}^m$. It is well known that two projective subspaces $W_1, W_2 \not\subseteq H$ have the same intersection with H iff $W_1 \cap \mathbb{A}^m$ and $W_2 \cap \mathbb{A}^m$ are translates of each other.[5] So, $Y \cap H = W_c \cap H = W_H$. Therefore, $V_c \cap W_H = V_c \cap Y \cap H \supseteq Z \cap H \neq \emptyset$. □

Lemma 4.8. *If $V_c \cap W_c = \emptyset$, then $O' \notin V'$.*

Proof. Assume to the contrary that $V_c \cap W_c = \emptyset$ but $O' \in V'$. We will derive a contradiction. As $W_H \subseteq W_c$, we have $V_c \cap W_H = \emptyset$ and hence $\dim V' = k$ by Lemma 4.7.

Denote by $J(V_c, W_H)$ the *join* of V_c and W_H, which is defined to be the union of the projective lines $\overline{PQ}$, where $P \in V_c$ and $Q \in W_H$. It is known that $J(V_c, W_H)$, as the join of two *disjoint* projective subvarieties, is again a projective subvariety of $\mathbb{P}^m$ [25, Example 6.17].

For $P \in V$, denote by W_P the unique translate of W containing P. We need the following two claims.

Claim 4.9. $J(V_c, W_H) \cap \mathbb{A}^m = \bigcup_{P \in V} W_P$.

Proof of Claim 4.9. Consider $P \in V_c$ and $Q \in W_H$. If $P \in H$, the line $\overline{PQ}$ lies in H and does not meet $\mathbb{A}^m$. Now suppose $P \in V_c \setminus H = V$. Then $\overline{PQ}$ meets $\overline{OQ}$ at the point Q. So $\overline{PQ} \cap \mathbb{A}^m$ is a translate of $\overline{OQ} \cap \mathbb{A}^m \subseteq W_c \cap \mathbb{A}^m = W$. It follows that $\overline{PQ} \cap \mathbb{A}^m \subseteq W_P$. This proves $J(V_c, W_H) \cap \mathbb{A}^m \subseteq \bigcup_{P \in V} W_P$.

Conversely, let $P \in V$. Let ℓ_P be an affine line contained in W_P and passing through P (note that W_P is the union of such lines). Then ℓ_P is a translate of an affine line $\ell \subseteq W$. As ℓ_P and ℓ are translates of each other, their projective closures intersect H at the same point Q. We have $Q \in \ell \cap H \subseteq W_H$. So $\ell_P = \overline{PQ} \cap \mathbb{A}^m \subseteq J(V_c, W_H) \cap \mathbb{A}^m$. □

[5] Indeed, $W_i \cap \mathbb{A}^m$ is defined by linear equations $\sum_{j=1}^m a_{j,t} X_j + a_{0,t} = 0$ iff $W_i \cap H$ is defined by homogeneous linear equations $X_0 = 0$ and $\sum_{j=1}^m a_{j,t} X_j = 0$. So the constant terms $a_{0,t}$ do not matter.

Claim 4.10. $J(V_c, W_H) \cap \mathbb{A}^m = \pi^{-1}(V')$.

Proof of Claim 4.10. As π is a linear map, Claim 4.9 implies $J(V_c, W_H) \cap \mathbb{A}^m \subseteq \pi^{-1}(V')$. We prove the other direction by comparing dimensions. It is known that for two *disjoint* projective subvarieties V_1 and V_2, $\dim J(V_1, V_2) = \dim V_1 + \dim V_2 + 1$ [25, Proposition 11.37 and Exercise 11.38]. Therefore,

$$\dim J(V_c, W_H) = \dim V_c + \dim W_H + 1 = \dim V + \dim W = k + \dim W\,.$$

So, $\dim J(V_c, W_H) \cap \mathbb{A}^m = k + \dim W$. On the other hand, we have $\pi^{-1}(V') \cong V' \times W$. So $\dim \pi^{-1}(V') = \dim V' + \dim W = k + \dim W$. Now $J(V_c, W_H) \cap \mathbb{A}^m$ and $\pi^{-1}(V')$ are (irreducible) affine varieties of the same dimension, and one is contained in the other. So they must be equal. This proves the claim. □

So $\pi^{-1}(V') = \bigcup_{P \in V} W_P$ by Claim 4.9 and Claim 4.10. As $O' \in V'$, we have $W = \pi^{-1}(O') \subseteq \pi^{-1}(V') = \bigcup_{P \in V} W_P$. So $W_P = W$ for some $P \in V$, since W is a linear space. But then $P \in V \cap W_P = V \cap W \subseteq V_c \cap W_c$, contradicting the assumption $V_c \cap W_c = \emptyset$. □

Remark 4.11. The converse of Lemma 4.8 is false, as shown by the following example.

Example 4. Consider Example 3 but choose f_4 to be $X_1 + X_2 + 1$ instead of $X_1 + X_2$. Now we have $g_3 = 1$, V is defined by $Y_1Y_2 - Y_3 - 1 = 0$ and $Y_1 + Y_2 - Y_4 + 1 = 0$, and V' is the plane $Z_3 = 1$. So $O' \notin V'$.

On the other hand, suppose $\mathbb{P}^m$ has coordinates $Y_0, \ldots, Y_4$. Then $V_c \cap H$ is defined by $Y_0 = Y_1Y_2 = Y_1 + Y_2 - Y_4 = 0$, and W_H is defined by $Y_0 = Y_1 = Y_2 - Y_4 = Y_3 = 0$. So $(0,0,1,0,1) \in V_c \cap W_H \subseteq V_c \cap W_c$.

Error probability. It remains to bound the probability of failure of the conditions $V_c \cap W_H = \emptyset$ and (in the case $O \notin V$) $V_c \cap W_c = \emptyset$. We need the following lemma.

Lemma 4.12 (Cut by hyperplanes)**.** *Let $V \subseteq \mathbb{P}^m$ be a projective variety of dimension r and degree d. Let $r' \geq r+1$. Choose $c_{i,j} \in S$ at random, for $i \in [r']$ and $0 \leq j \leq m$. Let $W \subseteq \mathbb{P}^m$ be the projective subspace cut out by the equations $\sum_{j=0}^m c_{i,j} X_j = 0$, $i = 1, \ldots, r'$, where $X_0, \ldots, X_m$ are homogeneous coordinates of $\mathbb{P}^m$. Then $V \cap W = \emptyset$ holds with probability at least $1 - (r+1)d/|S|$.*

Proof. For $i \in [r']$, let $H_i \subseteq \mathbb{P}^m$ be the hyperplane defined by $\sum_{j=0}^m c_{i,j} X_j = 0$. By ignoring H_i for $i > r+1$, we may assume $r' = r+1$. Let $V_0 := V$ and $V_i := V_{i-1} \cap H_i$ for $i \in [r']$. It suffices to show that $\dim V_i = \dim V_{i-1} - 1$ holds with probability at least $1 - d/|S|$, for each $i \in [r']$ (the dimension of the empty set is -1 by convention).

Fix $i \in [r']$ and $c_{i',j}$, for $i' \in [i-1]$ and $0 \leq j \leq m$. So V_{i-1} is also fixed. Note that $V_{i-1} \neq \emptyset$ since taking a hyperplane section reduces the dimension by at most one. If $\dim V_i \neq \dim V_{i-1} - 1$, then $\dim V_i = \dim V_{i-1}$, and H_i contains some irreducible component of V_{i-1} [25, Exercise 11.6]. Let Y be an irreducible component of V_{i-1}, and fix a point $P \in Y$. Then $Y \subseteq H_i$ only if $P \in H_i$, which holds only if $c_{i,0}, \ldots, c_{i,m}$ satisfy a nonzero linear equation determined by P. This occurs with probability at most $1/|S|$ (e. g., by fixing all but one $c_{i,j}$). We also have $\deg(V_{i-1}) \leq \deg(V) \leq d$, and hence the number of irreducible components of V_{i-1} is bounded by d. By the union bound, H_i contains an irreducible component of V_{i-1} with probability at most $d/|S|$. □

Proof of Theorem 4.6. As mentioned above, Theorem 4.6 is equivalent to showing that, with probability at least $1-\delta$: (1) $\dim V' = k$, and (2) $O' \in V'$ iff $O \in V$. Note that W_c is cut out in $\mathbb{P}^m$ by the linear equations $\sum_{j=1}^m c_{i,j}X_j = 0$, $i = 1,\ldots,k+1$. So W_H is cut out in $H \cong \mathbb{P}^{m-1}$ (corresponding to $X_0 = 0$) by the linear equations $\sum_{j=1}^m c_{i,j}X_j = 0$, $i = 1,\ldots,k+1$. We also have $\deg(V_c \cap H) \le \deg(V_c) \le (\max_{i\in[m]} \deg(f_i))^k$ (see, e. g., [12, Theorem 8.48]).

Assume $O \in V$. Then $O' \in V'$ since $\pi(O) = O'$. Applying Lemma 4.12 to each of the irreducible components of $V_c \cap H$ and W_H, as subvarieties of $H \cong \mathbb{P}^{m-1}$, we see $V_c \cap W_H = (V_c \cap H) \cap W_H = \emptyset$ holds with probability at least $1 - k\deg(V_c \cap H)/|S| \ge 1-\delta$. So by Lemma 4.7, $\dim V' = k$ holds with probability at least $1-\delta$.

Now assume $O \notin V$. Let $\pi_{O,H} : V_c \to H$ be the *projection of V_c from O to H*, defined by $P \mapsto \overline{OP} \cap H$ for $P \in V_c$. It is well defined since $O \notin V_c$. The image $\pi_{O,H}(V_c)$ is a projective subvariety of H [25, Theorem 3.5]. If $V_c \cap W_c$ contains a point P, then $\pi_{O,H}(V_c) \cap W_H$ contains $\pi_{O,H}(P)$. Conversely, if $\pi_{O,H}(V_c) \cap W_H$ contains a point Q, then there exists $P \in V_c$ such that $Q = \pi_{O,H}(P)$, and we have $P \in \overline{OQ} \subseteq W_c$. We conclude that $\pi_{O,H}(V_c) \cap W_H = \emptyset$ iff $V_c \cap W_c = \emptyset$, which implies $V_c \cap W_H = \emptyset$.

Note that $\dim \pi_{O,H}(V_c) = \dim V_c = k$, since

$$\pi_{O,H}(V_c) = J(\{O\}, V_c) \cap H\,.$$

We also have $\deg(\pi_{O,H}(V_c)) \le \deg(V_c)$ [25, Example 18.16]. Applying Lemma 4.12 to $\pi_{O,H}(V_c)$ and W_H, as subvarieties of $H \cong \mathbb{P}^{m-1}$, we see $\pi_{O,H}(V_c) \cap W_H = \emptyset$ holds with probability at least

$$1 - \frac{(k+1)\deg(\pi_{O,H}(V_c))}{|S|} \ge 1-\delta\,.$$

We have shown above that $\pi_{O,H}(V_c) \cap W_H = \emptyset$ imply $V_c \cap W_H = \emptyset$ and $V_c \cap W_c = \emptyset$. By Lemma 4.7 and Lemma 4.8, $V_c \cap W_H = \emptyset$ and $V_c \cap W_c = \emptyset$ imply $\dim V' = k$ and $O' \notin V'$, respectively. Therefore, it holds with probability at least $1-\delta$ that $\dim V' = k$ and $O' \notin V'$. □

Proof of Theorem 1.3. AnnAtZero is known to be NP-hard [30]. The NP-hardness of APS follows from Lemma 4.1 and Theorem 4.2.

Given an instance $\mathbf{f}$ of APS, we can first find $k = \operatorname{trdeg}(\mathbf{f})$. Fix a set $S \subseteq \mathbb{A}$ to be larger than $2(k+1)(\max_{i\in[m]} \deg(f_i))^k$ (which can be scanned using only polynomial space). Consider the points $((c_{i,j} \mid i \in [k+1], j \in [m])) \in S^{(k+1)\times m}$; for each such point define $\mathbf{g} := \left\{g_i := \sum_{j=1}^m c_{i,j}f_j \mid i \in [k+1]\right\}$. Compute the transcendence degree of $\mathbf{g}$, and if it is k then solve AnnAtZero for the instance $\mathbf{g}$. Output NO iff some $\mathbf{g}$ failed the AnnAtZero test.

All these steps can be achieved in space polynomial in the input size, using the uniqueness of the annihilator for $\mathbf{g}$ [39, Theorem 47], Perron's degree bound [49] and linear algebra [15, 9, 43]. □

5 Hitting set for $\overline{\mathsf{VP}}$: Proof of Theorem 1.4

Suppose p is a prime. Define $\mathbb{A} := \overline{\mathbb{F}}_p$. We want to find hitting sets for certain polynomials in $\mathbb{A}[x_1,\ldots,x_n]$. Fix a p-power $q \ge \Omega(sr^6)$, for the given parameters s, r. Assume that $p \nmid (r+1)$. Also, fix a model for the finite field $\mathbb{F}_q$ [1]. We now define the notion of "infinitesimally approximating" a polynomial by a small circuit.

Approximative closure of VP**.** [10] A family $(f_n|n)$ of polynomials from $\mathbb{A}[\mathbf{x}]$ is in the *class* $\overline{\mathsf{VP}}_{\mathbb{A}}$ if there are polynomials $f_{n,i}$ and a function $t : \mathbb{N} \mapsto \mathbb{N}$ such that g_n has a algebraic circuit of size $\text{poly}(n)$ and degree $\text{poly}(n)$, over the field $\mathbb{A}(\varepsilon)$, computing $g_n(\mathbf{x}) = f_n(\mathbf{x}) + \varepsilon f_{n,1}(\mathbf{x}) + \varepsilon^2 f_{n,2}(\mathbf{x}) + \cdots + \varepsilon^{t(n)} f_{n,t(n)}(\mathbf{x})$. That is, $g_n \equiv f_n \bmod \varepsilon\mathbb{A}[\varepsilon][\mathbf{x}]$.

The smallest possible circuit size of g_n is called the *approximative complexity* of f_n, namely $\overline{\text{size}}(f_n)$.

It may happen that g_n is much easier than f_n in terms of traditional circuit complexity. That possibility makes the definition interesting and opens up a long line of research.

Hitting set for $\overline{\mathsf{VP}}_{\mathbb{A}}$ Given functions $s = s(n)$ and $r = r(n)$, a finite set $\mathcal{H} \subseteq \mathbb{A}^n$ is called a *hitting set* for degree-r polynomials of approximative complexity s, if for every such nonzero polynomial f: $\exists \mathbf{v} \in \mathcal{H}$, $f(\mathbf{v}) \neq 0$.

Explicitness. Heintz and Schnorr [27] proved that $\text{poly}(n,s)$-sized hitting sets exist aplenty (for degree-r $\overline{\text{size}}$-s polynomials) as follows.

Lemma 5.1 ([27, Theorem 4.4])**.** *There exists a hitting set $\mathcal{H} \subseteq \mathbb{F}_q^n$ of size $O(s^2n^2)$ (assuming $q \geq \Omega(sr^2)$) that hits all nonzero degree-r n-variate polynomials in $\mathbb{A}[\mathbf{x}]$ that can be infinitesimally approximated by size-s algebraic circuits.*

The ultimate goal is computing such a hitting set in time $\text{poly}(n,s,\log qr)$. Before our work, the best result known was $\mathsf{EXPSPACE}$ [44, 45].

Note that for the hitting-set design problem it suffices to focus only on homogeneous polynomials. They are known to be computable by homogeneous circuits, where each gate computes a homogeneous polynomial [58].

Universal circuit. It can simulate any circuit of size s computing a degree-r homogeneous polynomial in $\mathbb{A}(\varepsilon)[x_1,\ldots,x_n]$. We define the *universal circuit* $\Psi(\mathbf{y},\mathbf{x})$ as a circuit in n essential variables $\mathbf{x}$ and $s' := O(sr^4)$ auxiliary variables $\mathbf{y}$. The variables $\mathbf{y}$ are the ones that one can specialize in $\mathbb{A}(\varepsilon)$, to compute a specific polynomial in $\mathbb{A}(\varepsilon)[x_1,\ldots,x_n]$. Every specialization gives a homogeneous degree-r $\overline{\text{size}}$-s' polynomial. Moreover, the set of these polynomials is closed under constant multiples [21, Theorem 2.2].

Note that by [27] there is a hitting set, with $m := O(s'^2n^2)$ points in $\mathbb{F}_q^n$ ($\because q \geq \Omega(s'r^2)$), for the set $\mathcal{P}$ of the polynomials infinitesimally approximated by the specializations of $\Psi(\mathbf{y},\mathbf{x})$. A universal circuit construction can be found in [51, 58]. Using the above notation, we give a criterion to decide whether a candidate set is a hitting set.

Theorem 5.2 (hitting-set criterion)**.** *Set $\mathcal{H} =: \{\mathbf{v}_1,\ldots,\mathbf{v}_m\} \subseteq \mathbb{F}_q^n$ is* not *a hitting set for the family $\mathcal{P}$ of the polynomials infinitesimally approximated by the specializations of $\Psi(\mathbf{y},\mathbf{x})$ iff there is a satisfying assignment $(\alpha,\beta) \in \mathbb{A}(\varepsilon)^{s'} \times \mathbb{A}(\varepsilon)^n$ such that:*

(1) $\forall i \in [n]$, $\beta_i^{r+1} - 1 \in \varepsilon\mathbb{A}[\varepsilon]$, where r is the degree of the specializations of $\Psi(\mathbf{y},\mathbf{x})$,
(2) $\Psi(\alpha,\beta) - 1 \in \varepsilon\mathbb{A}[\varepsilon]$, and
(3) $\forall i \in [m]$, $\Psi(\alpha,\mathbf{v}_i) \in \varepsilon\mathbb{A}[\varepsilon]$.

Remark 5.3. The above criterion holds for algebraically closed fields $\mathbb{A}$ of *any* characteristic. Thus, it reduces the hitting set verification problems for the family $\mathcal{P}$ over these fields to APS as well.

Proof. First we show that $\exists x \in \mathbb{A}(\varepsilon)$, $x^{r+1} - 1 \in \varepsilon\mathbb{A}[\varepsilon]$ implies $x \in \mathbb{A}[[\varepsilon]] \cap \mathbb{A}(\varepsilon)$ (= rational functions defined at $\varepsilon = 0$).

Claim 5.4. *$\exists x \in \mathbb{A}(\varepsilon)$, $x^{r+1} - 1 \in \varepsilon\mathbb{A}[\varepsilon]$ implies $x \in Z_{r+1} + \varepsilon\mathbb{A}[[\varepsilon]]$, where Z_{r+1} is the set of $(r+1)$-th roots of unity in $\mathbb{A}$.*

Proof. Recall the formal power series $\mathbb{A}[[\varepsilon]]$ and its group of units $\mathbb{A}[[\varepsilon]]^*$. Note that for any polynomial

$$a = \left(\sum_{i_0 \le i \le d} a_i \varepsilon^i \right)$$

with $a_{i_0} \neq 0$, the inverse

$$a^{-1} = \varepsilon^{-i_0} \cdot \left(\sum_{i_0 \le i \le d} a_i \varepsilon^{i-i_0} \right)^{-1}$$

is in $\varepsilon^{-i_0} \cdot \mathbb{A}[[\varepsilon]]^*$. This is just a consequence of the identity $(1-\varepsilon)^{-1} = \sum_{i \ge 0} \varepsilon^i$. In other words, any rational function $a \in \mathbb{A}(\varepsilon)$ can be written as an element in $\varepsilon^{-i}\mathbb{A}[[\varepsilon]]^*$, for some $i \ge 0$. Thus, write x as $\varepsilon^{-i} \cdot (b_0 + b_1\varepsilon + \cdots)$ for $i \ge 0$ and $b_0 \in \mathbb{A}^*$. This gives

$$x^{r+1} - 1 \; = \; \varepsilon^{-i(r+1)} (b_0 + b_1\varepsilon + b_2\varepsilon^2 + \cdots)^{r+1} \; - \; 1 \, .$$

For this to be in $\varepsilon\mathbb{A}[\varepsilon]$, clearly i has to be 0 (otherwise, $\varepsilon^{-i(r+1)}$ remains uncancelled), implying that $x \in \mathbb{A}[[\varepsilon]]$.

Moreover, we deduce that $b_0^{r+1} - 1 = 0$. Thus, Condition (1) implies that b_0 is one of the $(r+1)$-th roots of unity $Z_{r+1} \subseteq \mathbb{A}$ (recall that, since $p \nmid (r+1)$, $|Z_{r+1}| = r+1$). Thus, $x \in Z_{r+1} + \varepsilon\mathbb{A}[[\varepsilon]]$. □

[⇒]: Suppose $\mathcal{H}$ is not a hitting set for $\mathcal{P}$. Then, there is a specialization $\alpha \in \mathbb{A}(\varepsilon)^{s'}$ of the universal circuit such that $\Psi(\alpha, \mathbf{x})$ computes a polynomial in $\mathbb{A}[\varepsilon][\mathbf{x}] \setminus \varepsilon\mathbb{A}[\varepsilon][\mathbf{x}]$, but still "fools" $\mathcal{H}$, i. e., $\forall i \in [m]$, $\Psi(\alpha, \mathbf{v}_i) \in \varepsilon\mathbb{A}[\varepsilon]$. What remains to be shown is that Conditions (1) and (2) can be satisfied too.

Consider the polynomial $g(\mathbf{x}) := \Psi(\alpha, \mathbf{x})\big|_{\varepsilon=0}$. It is a nonzero polynomial, in $\mathbb{A}[\mathbf{x}]$ of degree r, that "fools" $\mathcal{H}$. By Lemma 2.2, there is a $\beta \in Z_{r+1}^n$ such that $a := g(\beta)$ is in $\mathbb{A}^*$. Clearly, $\beta_i^{r+1} - 1 = 0$, for all i. Consider $\psi' := a^{-1} \cdot \Psi(\alpha, \mathbf{x})$. Note that $\psi'(\beta) - 1 \in \varepsilon\mathbb{A}[\varepsilon]$, and $\psi'(\mathbf{v}_i) \in \varepsilon\mathbb{A}[\varepsilon]$ for all i. Moreover, the normalized polynomial $\psi'(\mathbf{x})$ can easily be obtained from the universal circuit Ψ by changing one of the coordinates of α (e. g., the incoming wires of the root of the circuit). This means that the three conditions (1) – (3) can be simultaneously satisfied by (some) $(\alpha', \beta) \in \mathbb{A}(\varepsilon)^{s'} \times Z_{r+1}^n$.

[⇐]: Suppose the satisfying assignment is $(\alpha, \beta') \in \mathbb{A}(\varepsilon)^{s'} \times \mathbb{A}(\varepsilon)^n$. As shown in Claim 5.4, Condition (1) implies $\beta'_i \in Z_{r+1} + \varepsilon\mathbb{A}[[\varepsilon]]$ for all $i \in [n]$. Let us define $\beta_i := \beta'_i\big|_{\varepsilon=0}$, for all $i \in [n]$; they are in $Z_{r+1} \subseteq \mathbb{A}$. By Condition (3), $\forall i \in [m]$, $\Psi(\alpha, \mathbf{v}_i) \in \varepsilon\mathbb{A}[\varepsilon]$.

Since any rational function $a \in \mathbb{A}(\varepsilon)$ can be written as an element in $\varepsilon^{-i}\mathbb{A}[[\varepsilon]]^*$, for some $i \ge 0$, we get that $\Psi(\alpha, \mathbf{x})$ is in $\varepsilon^{-j}\mathbb{A}[[\varepsilon]][\mathbf{x}]$, for some $j \ge 0$. Expand the polynomial $\Psi(\alpha, \mathbf{x})$, w.r.t. ε, as

$$g_{-j}(\mathbf{x})\varepsilon^{-j} + \cdots + \varepsilon^{-2} g_{-2}(\mathbf{x}) + g_{-1}(\mathbf{x})\varepsilon^{-1} + g_0(\mathbf{x}) + \varepsilon g_1(\mathbf{x}) + \varepsilon^2 g_2(\mathbf{x}) + \dots .$$

Let us study Condition (2). If for each $0 \le \ell \le j$, polynomial $g_{-\ell}(\mathbf{x})$ is zero, then $\Psi(\alpha, \beta')\big|_{\varepsilon=0} = 0$ contradicting the condition. Thus, we can pick the largest $0 \le \ell \le j$ such that the polynomial $g_{-\ell}(\mathbf{x}) \neq 0$.

Note that the normalized circuit $\varepsilon^\ell \cdot \Psi(\alpha, \mathbf{x})$ equals $g_{-\ell}$ at $\varepsilon = 0$. This means that $g_{-\ell} \in \mathcal{P}$, and it is a nonzero polynomial fooling $\mathcal{H}$. Thus, $\mathcal{H}$ cannot be a hitting set for $\mathcal{P}$ and we are done. □

Proof of Theorem 1.4. Given a prime p and parameters n, r, s in unary (w.l.o.g. $p \nmid (r+1)$), fix a field $\mathbb{F}_q$ with $q \geq \Omega(sr^6)$. Fix the universal circuit $\Psi(\mathbf{y}, \mathbf{x})$ with n essential variables $\mathbf{x}$ and $s' := \Omega(sr^4)$ auxiliary variables $\mathbf{y}$. Fix $m := \Omega(s'^2 n^2)$.

For every subset $\mathcal{H} =: \{\mathbf{v}_1, \ldots, \mathbf{v}_m\} \subseteq \mathbb{F}_q^n$ solve the APS instance described by Conditions (1) – (3) in Theorem 5.2. These are $(n+m+1)$ algebraic circuits of degree $\text{poly}(srn, \log p)$ and a similar bit size. Using the algorithm from Theorem 1.3 it can be solved in space $\text{poly}(srn, \log p)$.

The number of subsets $\mathcal{H}$ is at most q^{nm}. So we can go over all of them in space $\text{poly}(nm \log q)$. If APS fails on one of them (say $\mathcal{H}$) then we know that $\mathcal{H}$ is a hitting set for $\mathcal{P}$. Since Ψ is universal, for homogeneous degree-r $\overline{\text{size}}$-s polynomials in $\mathbb{A}[\mathbf{x}]$, we output $\mathcal{H}$ as the desired hitting set. □

Remark 5.5. One advantage of our method compared to the one in [21] is that in our construction, the bit complexity of the coordinates of the points in the hitting set is $O(\log rs)$, whereas the bit complexity of those in [21] is $\text{poly}(n, s, r)$.

6 Conclusion

Our result that algebraic dependence testing is in $\mathsf{AM} \cap \mathsf{coAM}$ gives some hope that a randomized polynomial-time algorithm for the problem might exist. Studying the following special case might be helpful to get an idea for designing better algorithms.

Given quadratic polynomials $f_1, \ldots, f_n \in \mathbb{F}_2[x_1, \ldots, x_n]$, test if they are algebraically dependent in randomized polynomial time [47].

In addition, Ilya Volkovich [59] asked whether $\text{AD}(\mathbb{F}) \in \mathsf{SBP} \cap \mathsf{coSBP}$ is true, and whether our method can be used to prove this stronger result. Here SBP, introduced in [8], stands for "small bounded-error probability" and is a subclass of AM.

As indicated in this paper, approximate polynomials satisfiability, or equivalently testing zero-membership in the Zariski closure of the image, may have further applications to problems in computational algebraic geometry and algebraic complexity.

We know that HN is in AM over fields of characteristic zero, assuming GRH [32]. Can we prove that AnnAtZero (or APS) is also in AM over fields of characteristic zero assuming GRH [30]? This would also imply a better hitting set construction for $\overline{\mathsf{VP}}$.

Acknowledgements. We thank Anurag Pandey and Sumanta Ghosh for insightful discussions on the approximate polynomials satisfiability and explicit construction of hitting set for the closure of VP. We are also grateful to the anonymous reviewers for their careful reading of the manuscript and for their many helpful comments. We thank the editor-in-chief Laci Babai for his meticulous suggestions regarding grammar and style. Finally, N.S. thanks the funding support from DST (DST/SJF/MSA-01/2013-14), and Z.G. thanks the funding support from DST and Research I Foundation of CSE, IITK.

References

[1] LEONARD M. ADLEMAN AND HENDRIK W. LENSTRA: Finding irreducible polynomials over finite fields. In *Proc. 18th STOC*, pp. 350–355. ACM Press, 1986. [doi:10.1145/12130.12166] 9, 21

[2] MANINDRA AGRAWAL, SUMANTA GHOSH, AND NITIN SAXENA: Bootstrapping variables in algebraic circuits. *Proc. Nat. Acad. of Sciences (USA)*, 116(17):8107–8118, 2019. Preliminary version in STOC'18. [doi:10.1073/pnas.1901272116] 4

[3] MANINDRA AGRAWAL, CHANDAN SAHA, RAMPRASAD SAPTHARISHI, AND NITIN SAXENA: Jacobian hits circuits: Hitting sets, lower bounds for depth-D occur-k formulas and depth-3 transcendence degree-k circuits. *SIAM J. Comput.*, 45(4):1533–1562, 2016. Preliminary version in STOC'12. [doi:10.1137/130910725, arXiv:1111.0582] 4

[4] SANJEEV ARORA AND BOAZ BARAK: *Computational Complexity: A Modern Approach*. Cambridge Univ. Press, 2009. [doi:10.1017/CBO9780511804090] 3, 5, 10, 11

[5] VIKRAMAN ARVIND, PUSHKAR S. JOGLEKAR, PARTHA MUKHOPADHYAY, AND S. RAJA: Randomized polynomial-time identity testing for noncommutative circuits. *Theory of Computing*, 15(7):1–36, 2019. Preliminary version in STOC'17. [doi:10.4086/toc.2019.v015a007] 3

[6] LÁSZLÓ BABAI: Trading group theory for randomness. In *Proc. 17th STOC*, pp. 421–429. ACM Press, 1985. [doi:10.1145/22145.22192] 10

[7] MALTE BEECKEN, JOHANNES MITTMANN, AND NITIN SAXENA: Algebraic independence and blackbox identity testing. *Inform. and Comput.*, 222:2–19, 2013. Preliminary version in ICALP'11. [doi:10.1016/j.ic.2012.10.004, arXiv:1102.2789] 2, 4, 10

[8] ELMAR BÖHLER, CHRISTIAN GLASSER, AND DANIEL MEISTER: Error-bounded probabilistic computations between MA and AM. *J. Comput. System Sci.*, 72(6):1043–1076, 2006. Preliminary version in MFCS'03. [doi:10.1016/j.jcss.2006.05.001] 24

[9] ALLAN BORODIN, JOACHIM VON ZUR GATHEM, AND JOHN HOPCROFT: Fast parallel matrix and GCD computations. *Inf. Control*, 52(3):241–256, 1982. Preliminary version in FOCS'82. [doi:10.1016/S0019-9958(82)90766-5] 2, 18, 21

[10] KARL BRINGMANN, CHRISTIAN IKENMEYER, AND JEROEN ZUIDDAM: On algebraic branching programs of small width. *J. ACM*, 65(5):32:1–32:29, 2018. Preliminary version in CCC'17. [doi:10.1145/3209663, arXiv:1702.05328] 22

[11] PETER BÜRGISSER: The complexity of factors of multivariate polynomials. *Foundations of Computational Mathematics*, 4(4):369–396, 2004. Preliminary version in FOCS'01. [doi:10.1007/s10208-002-0059-5] 5

[12] PETER BÜRGISSER, MICHAEL CLAUSEN, AND AMIN SHOKROLLAHI: *Algebraic Complexity Theory*. Springer, 1997. [doi:10.1007/978-3-662-03338-8] 6, 15, 21

[13] PETER BÜRGISSER, ANKIT GARG, RAFAEL OLIVEIRA, MICHAEL WALTER, AND AVI WIGDERSON: Alternating minimization, scaling algorithms, and the null-cone problem from invariant theory. In *Proc. 9th Innovations in Theoretical Computer Science Conf. (ITCS'18)*, pp. 24:1–24:20. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2018. [doi:10.4230/LIPIcs.ITCS.2018.24, arXiv:1711.08039] 7

[14] CHI-NING CHOU, MRINAL KUMAR, AND NOAM SOLOMON: Closure results for polynomial factorization. *Theory of Computing*, 15(13):1–34, 2019. Preliminary version in CCC'18. [doi:10.4086/toc.2019.v015a013] 3

[15] LASZLO CSANKY: Fast parallel matrix inversion algorithms. *SIAM J. Comput.*, 5(4):618–623, 1976. [doi:10.1137/0205040] 2, 18, 21

[16] RICHARD A. DEMILLO AND RICHARD J. LIPTON: A probabilistic remark on algebraic program testing. *Inform. Process. Lett.*, 7(4):193–195, 1978. [doi:10.1016/0020-0190(78)90067-4] 3, 11

[17] HARM DERKSEN AND GREGOR KEMPER: *Computational Invariant Theory*. Springer, 2015. [doi:10.1007/978-3-662-48422-7] 3

[18] ZEEV DVIR: Extractors for varieties. *Comput. Complexity*, 21(4):515–572, 2012. Preliminary version in CCC'09. [doi:10.1007/s00037-011-0023-3] 4

[19] ZEEV DVIR, ARIEL GABIZON, AND AVI WIGDERSON: Extractors and rank extractors for polynomial sources. *Comput. Complexity*, 18(1):1–58, 2009. Preliminary version in FOCS'07. [doi:10.1007/s00037-009-0258-4] 4

[20] RICHARD EHRENBORG AND GIAN-CARLO ROTA: Apolarity and canonical forms for homogeneous polynomials. *Eur. J. Combinatorics*, 14(3):157–181, 1993. [doi:10.1006/eujc.1993.1022] 2

[21] MICHAEL A. FORBES AND AMIR SHPILKA: A PSPACE construction of a hitting set for the closure of small algebraic circuits. In *Proc. 50th STOC*, pp. 1180–1192. ACM Press, 2018. [doi:10.1145/3188745.3188792] 4, 7, 10, 22, 24

[22] SHAFI GOLDWASSER AND MICHAEL SIPSER: Private coins versus public coins in interactive proof systems. In SILVIO MICALI, editor, *Randomness in Computation*, volume 5 of *Advances in Computing Research*, pp. 73–90. JAI Press, 1989. Preliminary version in STOC'86. 11

[23] JOSHUA A. GROCHOW AND TONIANN PITASSI: Circuit complexity, proof complexity, and polynomial identity testing: The ideal proof system. *J. ACM*, 65(6):37:1–37:59, 2018. Preliminary version in FOCS'14. [doi:10.1145/3230742] 7, 15

[24] ZEYU GUO, NITIN SAXENA, AND AMIT SINHABABU: Algebraic dependencies and PSPACE algorithms in approximative complexity. In *Proc. 33rd Computational Complexity Conf. (CCC'18)*, pp. 10:1–10:21. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2018. [doi:10.4230/LIPIcs.CCC.2018.10, arXiv:1801.09275] 1

[25] JOE HARRIS: *Algebraic Geometry: A First Course*. Springer, 1992. [doi:10.1007/978-1-4757-2189-8] 8, 11, 19, 20, 21

[26] ROBIN HARTSHORNE: *Algebraic Geometry*. Springer, 1977. [doi:10.1007/978-1-4757-3849-0] 11

[27] JOOS HEINTZ AND CLAUS-PETER SCHNORR: Testing polynomials which are easy to compute. In *Proc. 12th STOC*, pp. 262–272. ACM Press, 1980. [doi:10.1145/800141.804674] 4, 9, 22

[28] AUBREY W. INGLETON: Representation of matroids. *Combinatorial Mathematics and its applications*, pp. 149–167, 1971. 2

[29] CARL GUSTAV JACOB JACOBI: De Determinantibus functionalibus. *Journal für die reine und angewandte Mathematik (Crelles J.)*, 1841(22):319–359, 1841. [doi:10.1515/crll.1841.22.319] 2, 10

[30] NEERAJ KAYAL: The complexity of the annihilating polynomial. In *Proc. 24th IEEE Conf. on Computational Complexity (CCC'09)*, pp. 184–193. IEEE Comp. Soc. Press, 2009. [doi:10.1109/CCC.2009.37] 2, 3, 9, 15, 21, 24

[31] NEERAJ KAYAL AND NITIN SAXENA: Complexity of ring morphism problems. *Comput. Complexity*, 15(4):342–390, 2006. [doi:10.1007/s00037-007-0219-8] 11

[32] PASCAL KOIRAN: Hilbert's Nullstellensatz is in the polynomial hierarchy. *J. Complexity*, 12(4):273–286, 1996. [doi:10.1006/jcom.1996.0019] 5, 6, 9, 24

[33] JÁNOS KOLLÁR: Sharp effective Nullstellensatz. *J. Amer. Math. Soc.*, 1(4):963–975, 1988. [doi:10.2307/1990996] 5

[34] MRINAL KUMAR AND SHUBHANGI SARAF: Arithmetic circuits with locally low algebraic rank. *Theory of Computing*, 13(6):1–33, 2017. Preliminary version in CCC'16. [doi:10.4086/toc.2017.v013a006, arXiv:1806.06097] 4

[35] JOSEPH M. LANDSBERG: *Tensors: Geometry and Applications*. Amer. Math. Soc., 2012. [doi:10.1090/gsm/128] 6

[36] FRANÇOIS LE GALL: Powers of tensors and fast matrix multiplication. In *Proc. 39th Internat. Symp. Symbolic and Algebraic Computation (ISSAC'14)*, pp. 296–303. ACM Press, 2014. [doi:10.1145/2608628.2608664, arXiv:1401.7714] 6

[37] THOMAS LEHMKUHL AND THOMAS LICKTEIG: On the order of approximation in approximative triadic decompositions of tensors. *Theoret. Comput. Sci.*, 66(1):1–14, 1989. [doi:10.1016/0304-3975(89)90141-2] 5, 9, 15, 17

[38] RUDOLF LIDL AND HARALD NIEDERREITER: *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge Univ. Press, 2nd edition, 1996. [doi:10.1017/CBO9780511525926] 28

[39] HIDEYUKI MATSUMURA: *Commutative Algebra*. Benjamin-Cummings Pub Co, 1980. 3, 21

[40] ERNST W. MAYR AND ALBERT R. MEYER: The complexity of the word problems for commutative semigroups and polynomial ideals. *Adv. Math.*, 46(3):305–329, 1982. [doi:10.1016/0001-8708(82)90048-2] 5

[41] JOHANNES MITTMANN, NITIN SAXENA, AND PETER SCHEIBLECHNER: Algebraic independence in positive characteristic: A p-adic calculus. *Trans. Amer. Math. Soc.*, 366(7):3425–3450, 2014. [doi:10.1090/S0002-9947-2014-06268-5, arXiv:1202.4301] 3, 4

[42] DAVID E. MULLER: Application of boolean algebra to switching circuit design and to error detection. *Trans. Inst. Radio Engineers Professional Group on Electronic Computers*, EC-3(3):6–12, 1954. [doi:10.1109/IREPGELC.1954.6499441] 3

[43] KETAN D. MULMULEY: A fast parallel algorithm to compute the rank of a matrix over an arbitrary field. *Combinatorica*, 7(1):101–104, 1987. Preliminary version in STOC'86. [doi:10.1007/BF02579205] 2, 18, 21

[44] KETAN D. MULMULEY: Geometric complexity theory V: Equivalence between blackbox derandomization of polynomial identity testing and derandomization of Noether's normalization lemma. In *Proc. 53rd FOCS*, pp. 629–638. IEEE Comp. Soc. Press, 2012. [doi:10.1109/FOCS.2012.15] 4, 7, 22

[45] KETAN D. MULMULEY: Geometric complexity theory V: Efficient algorithms for Noether normalization. *J. Amer. Math. Soc.*, 30(1):225–309, 2017. Preliminary version in FOCS'12. [doi:10.1090/jams/864, arXiv:1209.5993] 4, 5, 6, 7, 22

[46] ØYSTEIN ORE: Über höhere Kongruenzen. *Norsk Mat. Forenings Skrifter Ser. I*, 7(15):27, 1922. Polynomial Identity Lemma cited with full proof in [38, Theorem 6.13]. 3

[47] ANURAG PANDEY, NITIN SAXENA, AND AMIT SINHABABU: Algebraic independence over positive characteristic: New criterion and applications to locally low-algebraic-rank circuits. *Comput. Complexity*, 27(4):617–670, 2018. Preliminary version in MFCS'16. [doi:10.1007/s00037-018-0167-5] 3, 4, 8, 13, 24

[48] OSKAR PERRON: *Algebra. I: Die Grundlagen*. Walter de Gruyter, 1927. 2

[49] ARKADIUSZ PŁOSKI: Algebraic dependence of polynomials after O. Perron and some applications. In *Computational Commutative and Non-Commutative Algebraic Geometry*, pp. 167–173. IOS Press, 2005. 2, 18, 21

[50] CLAUDIU RAICU: Secant varieties of Segre–Veronese varieties. *Algebra & Number Theory*, 6(8):1817–1868, 2012. [doi:10.2140/ant.2012.6.1817] 6

[51] RAN RAZ: Elusive functions and lower bounds for arithmetic circuits. *Theory of Computing*, 6(7):135–177, 2010. Preliminary version in STOC'08. [doi:10.4086/toc.2010.v006a007] 22

[52] NITIN SAXENA: Progress on polynomial identity testing. *Bulletin of the EATCS*, 99:49–79, 2009. Online version ECCC TR09-101. 7

[53] NITIN SAXENA: Progress on polynomial identity testing - II. In *Perspectives in Computational Complexity*, pp. 131–146. Springer, 2014. [doi:10.1007/978-3-319-05446-9_7, arXiv:1401.0976] 7

[54] MARCUS SCHAEFER AND DANIEL ŠTEFANKOVIČ: The complexity of tensor rank. *Theory of Computing Systems*, 62(5):1161–1174, 2018. [doi:10.1007/s00224-017-9800-y, arXiv:1612.04338] 6

[55] JOACHIM SCHMID: On the affine Bezout inequality. *manuscripta mathematica*, 88(1):225–232, 1995. [doi:10.1007/BF02567819] 14

[56] WOLFGANG M. SCHMIDT: *Equations over Finite Fields: An Elementary Approach*. Volume 536 of *Lecture Notes in Math.* Springer, 1st edition, 1976. [doi:10.1007/BFb0080437] 3

[57] JACOB T. SCHWARTZ: Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, 1980. Preliminary version in EUROSAM'79. [doi:10.1145/322217.322225] 3, 11

[58] AMIR SHPILKA AND AMIR YEHUDAYOFF: Arithmetic circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5(3–4):207–388, Now Publ., 2009. [doi:10.1561/0400000039] 7, 22

[59] ILYA VOLKOVICH: Private Communication, 2018. 24

[60] RICHARD E. ZIPPEL: Probabilistic algorithms for sparse polynomials. In *Proc. Internat. Symp. Symbolic and Algebraic Manipulation (EUROSAM'79)*, pp. 216–226. Springer, 1979. [doi:10.1007/3-540-09519-5_73] 3, 11

AUTHORS

Zeyu Guo
Postdoctoral researcher
University of Haifa
Haifa, Israel
zguotcs@gmail.com
http://zeyuguo.bitbucket.io

Nitin Saxena
Professor of CSE
Indian Institute of Technology Kanpur
Kanpur, India
nitin@cse.iitk.ac.edu
http://www.cse.iitk.ac.in/users/nitin

Amit Sinhababu
Ph. D. student
Indian Institute of Technology Kanpur
Kanpur, India
amitks@cse.iitk.ac.edu
http://www.cse.iitk.ac.in/users/amitks

ABOUT THE AUTHORS

ZEYU GUO is a postdoctoral researcher at the University of Haifa. Previously, he was a postdoc at the Indian Institute of Technology Kanpur. He grew up in northern China and completed his Bachelor's degree at Fudan University, Shanghai. He earned his Ph. D. at Caltech in 2017, where his advisor was Chris Umans. His Ph. D. thesis studies the problem of deterministic univariate polynomial factoring over finite fields. His research interests include algebraic methods in theoretical computer science, pseudorandomness and its connections with coding theory, algorithms in number theory and algebra.

NITIN SAXENA received his Ph. D. from the Indian Institute of Technology Kanpur in 2006. His advisor was Manindra Agrawal. He also spent stints at Princeton University (2003-04) and at the National University of Singapore (2004-05). He was a postdoc at the Centrum voor Wiskunde en Informatica in Amsterdam (2006-08) and a faculty at the Hausdorff Center for Mathematics in Bonn (2008-13). Nitin's long-term interests are in algebra-flavored computational complexity problems.

He has contributed to primality testing, polynomial identity testing, algebraic dependence testing, polynomial factoring and polynomial equivalence problems. Some of these works have been awarded the Gödel prize, Fulkerson prize, CCC best paper (2006), and ICALP best paper (2011). He enjoys interacting with, and mentoring, enthusiastic young researchers. In his spare (and non-spare) time he enjoys listening to music, watching movies, reading non-fiction, swimming and travelling.

AMIT SINHABABU is a Ph. D. student at the Indian Institute of Technology Kanpur. His advisor is Nitin Saxena. Currently he is visiting Ulm University, Ulm, Germany and is affiliated with HTW Aalen, where his mentor is Thomas Thierauf. Amit grew up in West Bengal, India. He completed his Bachelor's degree at Bengal Engineering and Science University Shibpur, now known as IIEST Shibpur, and his Masters at IIT Kanpur. His current research interests are in algebraic complexity and computational complexity. He likes reading fiction and listening to Indian classical music.