Electronic Colloquium on Computational Complexity, Report No. 19 (2018)

Algebraic dependencies and PSPACE algorithms in approximative complexity

Zeyu Guo * Nitin Saxena † Amit Sinhababu ‡

Abstract

Testing whether a set $\mathbf{f}$ of polynomials has an algebraic dependence is a basic problem with several applications. The polynomials are given as algebraic circuits. Algebraic independence testing question is wide open over finite fields (Dvir, Gabizon, Wigderson, FOCS'07). The best complexity known is $\mathrm{NP}^{\#\mathsf{P}}$ (Mittmann, Saxena, Scheiblechner, Trans.AMS'14). In this work we put the problem in AM ∩ coAM. In particular, dependence testing is unlikely to be NP-hard and joins the league of problems of "intermediate" complexity, eg. graph isomorphism & integer factoring. Our proof method is algebro-geometric– estimating the size of the image/preimage of the polynomial map $\mathbf{f}$ over the finite field. A *gap* in this size is utilized in the AM protocols.

Next, we study the open question of testing whether every annihilator of $\mathbf{f}$ has zero constant term (Kayal, CCC'09). We give a geometric characterization using Zariski closure of the image of $\mathbf{f}$; introducing a new problem called *approximate* polynomials satisfiability (APS). We show that APS is NP-hard and, using projective algebraic-geometry ideas, we put APS in PSPACE (prior best was EXPSPACE via Gröbner basis computation). As an unexpected application of this to approximative complexity theory we get– Over *any* field, hitting-set for $\overline{\mathrm{VP}}$ can be designed 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).

1998 ACM Classification: I.1 Symbolic and Algebraic Manipulation, F.2.1 Numerical Algorithms and Problems, F.1.3 Complexity Measures and Classes, G.1.2 Approximation.
Keywords: algebraic dependence, Jacobian, Arthur-Merlin, approximate polynomial, satisfiability, hitting-set, border VP, finite field, PSPACE, EXPSPACE, GCT Chasm.

1 Introduction

Algebraic dependence is a generalization of linear dependence. Polynomials $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ are called *algebraically dependent* over field $\mathbb{F}$ if there exists a nonzero polynomial (called *annihilator*) $A(y_1, \ldots, y_m) \in \mathbb{F}[y_1, \ldots, y_m]$ such that $A(f_1, \ldots, f_m) = 0$. 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 maximal number of algebraically independent polynomials in the set. Both algebraic dependence and linear dependence share combinatorial properties of the matroid structure [ER93]. The algebraic matroid examples may not be linear (esp. over $\mathbb{F}_p$) [Ing71].

The simplest examples of algebraically independent polynomials are $x_1, \ldots, x_n \in \mathbb{F}[x_1, \ldots, x_n]$. 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, polynomials $x + y$ and $x^p + y^p$ are algebraically dependent over $\mathbb{F}_p$, but algebraically independent over $\mathbb{Q}$.

Thus, the following computational question *AD(𝔽)* is natural and it is the first problem we consider in this paper: Given algebraic circuits $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$, test if they are algebraically

*Department of Computer Science & Engineering, Indian Institute of Technology Kanpur, zguo@cse.iitk.ac.in
†CSE, IIT Kanpur, nitin@cse.iitk.ac.in
‡CSE, IIT Kanpur, amitks@cse.iitk.ac.in

ISSN 1433-8092

dependent. It can be solved in PSPACE using a classical result due to Perron [Per27, Pło05, Csa76]. Perron proved that given a set of algebraically dependent polynomials, there exists an annihilator whose degree is upper bounded by the product of the degrees of the polynomials in the set. This exponential degree bound on the annihilator is tight [Kay09].

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 [Jac41, BMS13]. The Jacobian efficiently reduces algebraic dependence testing of $f_1, \ldots, f_m$ over $\mathbb{F}$ to linear dependence testing of the differentials $df_1, \ldots, df_m$ over $\mathbb{F}(x_1, \ldots, x_n)$, where we view df_i as the vector $(\frac{\partial f_i}{\partial x_1}, \ldots, \frac{\partial f_i}{\partial x_n})$. Placing df_i as the i-th row gives us the Jacobian matrix J of $f_1, \ldots, f_m$. If the characteristic of the field is zero (or larger than the product of the degrees $\deg(f_i)$) then the trdeg equals $\text{rank}(J)$. It follows from [Sch80] that, with high probability, $\text{rank}(J)$ 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 AD($\mathbb{F}$) for certain $\mathbb{F}$.

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 Jacobian fails. The failure can be characterized by the notion of 'inseparable extension' [PSS16]. For example, x^p, y^p are algebraically independent over $\mathbb{F}_p$, yet their Jacobian determinant vanishes. Another example is, $\{x^{p-1}y, xy^{p-1}\}$ over $\mathbb{F}_p$ for prime $p > 2$. [MSS14] gave a criterion, called Witt-Jacobian, that works over fields of prime characteristic p; improving the complexity of independence testing problem from PSPACE to $\text{NP}^{\#\mathsf{P}}$. [PSS16] gave another generalization of Jacobian criterion that is efficient in special cases.

Given that an efficient algorithm to tackle prime characteristic is not in close sight, one could speculate the problem to be NP-hard or even outside the polynomial hierarchy PH. In this work we show that: *For finite fields, AD($\mathbb{F}$) is in AM $\cap$ coAM* (Theorem 1). This rules out the possibility of NP-hardness, under standard complexity theory assumptions [AB09].

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 the set of algebraic circuits $\mathbf{f} = \{f_1, \ldots, f_m\}$, is zero. Note that the annihilators of $\mathbf{f}$ constitute an ideal of the polynomial ring $\mathbb{F}[y_1, \ldots, y_m]$; this ideal is principal when trdeg of $\mathbf{f}$ is $m - 1$ [Kay09, Lem.7]. In this case, we can decide if the constant term of the minimal annihilator is zero in PSPACE, as the *unique* annihilator (up to scaling) can be computed in PSPACE.

If trdeg 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. (Eg. using Gröbner basis techniques, we can do it in EXPSPACE [DK15, Sec.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 –using which we devise a PSPACE algorithm to solve it in all cases* (Theorem 2).

Interestingly, there is an algebraic-complexity application of the above algorithm. *We give a PSPACE-explicit construction of a hitting-set of the class* $\overline{\text{VP}}_{\overline{\mathbb{F}}_q}$ (Theorem 3). $\overline{\text{VP}}_{\overline{\mathbb{F}}_q}$ consists of n-variate degree $d = n^{O(1)}$ polynomials, over the field $\overline{\mathbb{F}}_q$, that can be 'infinitesimally approximated' by size $s = n^{O(1)}$ algebraic circuits. This 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 $\overline{\text{VP}}$ [Mul17]; which was previously known to be only in EXPSPACE [Mul17, Mul12]. This was recently improved greatly, over the field $\mathbb{C}$, by [FS17]. Their proof technique 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 then 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 Jacobian criterion, [DGW09, Dvi09] solved the problem for fields with large characteristic. The second application is in the famous polynomial identity testing (PIT) problem. To efficiently design hitting-sets, for some interesting models,

[BMS13, ASSS12, KS16] constructed a family of trdeg-preserving maps. For more background and applications of algebraic dependence testing, see [PSS16]. The annihilator has been a key concept to prove the connection between hitting-sets and lower bounds [HS80], and in bootstrapping 'weak' hitting-sets [AGS17].

1.1 Our results

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

Theorem 1. *Algebraic dependence testing of circuits in $\mathbb{F}_q[\mathbf{x}]$ is in AM $\cap$ coAM.*

This result vastly improves the current best upper bound known for $\mathrm{AD}(\mathbb{F}_q)$– from being 'outside' the polynomial hierarchy (namely $\mathrm{NP}^{\#\mathsf{P}}$ [MSS14]) to 'lower' than the second-level of polynomial hierarchy (namely AM $\cap$ coAM). This rules out the possibility of $\mathrm{AD}(\mathbb{F}_q)$ being NP-hard (unless polynomial hierarchy collapses to the second-level [AB09]). Recall that, for zero or large characteristic $\mathbb{F}$, $\mathrm{AD}(\mathbb{F})$ 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 [MM82]). Firstly, we relate to a (new) version of polynomial system satisfiability, over the algebraic closure $\overline{\mathbb{F}}$:

Problem 1 (Approximate polynomials satisfiability (APS))**.** *Given algebraic circuits $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$, does there exist $\beta \in \overline{\mathbb{F}}(\varepsilon)^n$ such that for all i, $f_i(\beta)$ is in the ideal $\varepsilon\overline{\mathbb{F}}[\varepsilon]$? If yes, then we say that $\mathbf{f} := \{f_1, \ldots, f_m\}$ is in APS.*

It is easy to show: Function field $\overline{\mathbb{F}}(\varepsilon)$ here can be equivalently replaced by *Laurent polynomials* $\overline{\mathbb{F}}[\varepsilon, \varepsilon^{-1}]$, 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 [Bür04, Sec.5.2] & [LL89, Sec.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 [LL89, Prop.3]; this may again be a "justification" for APS requiring that much space.

Classically, the *exact* version of APS has been extremely 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 and yields an impressive PSPACE algorithm [Koi96, Kol88]. 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 the former, assign $x = \varepsilon$ and $y = 1/\varepsilon$. Also, the instance $\{x, x + 1\}$ is neither in APS nor has 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 2. *APS is NP-hard and is in PSPACE.*

We apply this to design hitting-sets and solving NNL (refer [Mul17] for the background).

Theorem 3. *There is a PSPACE algorithm that (given input n, s, r in unary & suitably large $\mathbb{F}_q$) outputs a set, of points from $\mathbb{F}_q^n$ of size poly$(nsr, \log q)$, that hits all n-variate degree-r polynomials over $\overline{\mathbb{F}}_q$ that can be infinitesimally approximated by size s circuits.*

More applications? The exact polynomials satisfiability question HN (over $\overline{\mathbb{F}}$) is highly expressive and, naturally, most computer science problems get expressed that way. We claim that in a similar spirit, the APS question expresses those computer science problems that involve 'infinitesimal approximation'. One prominent example is the concept of *border rank* of tensor polynomials (used

in matrix multiplication algorithms and GCT, see [BCS13, Lan12, LG14]). 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 matches the complexity of tensor rank itself [SŠ17]. 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, $\text{HN}_{\mathbb{C}}$ is known to be in AM, conditionally under GRH [Koi96].)

The hitting-set result (Theorem 3) can be applied to compute, in PSPACE, the explicit system of parameters (esop) of the *invariant ring* of the variety $\Delta[\det, s]$, over $\overline{\mathbb{F}}_q$, with a given group action [Mul17, Thm.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 characteristic zero fields, see [FS17, Thms.1.1-1.4]. Bringing this complexity down to P is the longstanding problem of blackbox PIT (& lower bounds), see [Sax09, SY10, Sax13]. Mulmuley [Mul12] pointed out that small hitting-sets for $\overline{\text{VP}}$ 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 3 shows that small hitting-sets for $\overline{\text{VP}}_{\overline{\mathbb{F}}}$ can be designed in PSPACE (like those for VP) for *any* field $\mathbb{F}$.

1.2 Proof ideas

Proof idea of Theorem 1. Suppose we are given 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 $b = (b_1, \ldots, b_n) \in \mathbb{F}_{q'}^n$, 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 9] 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. Whereas, if the polynomials are algebraically dependent then $N_{f(a)}$ is much more.

Assume $\mathbf{f}$ are algebraically independent. Wlog (see the full version of [PSS16, Sec.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 the zeroset defined by the system of equations, for random $f(a)$, has dimension ≤ 0. 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 Bezout's theorem to upper bound $N_{f(a)}$. On the other hand, suppose $\mathbf{f}$ are algebraically dependent, say with annihilator Q. Let $\text{Im}(f) := f(\mathbb{F}_{q'}^n)$ be the image of f. Since Q vanishes on $\text{Im}(f)$, we know that $\text{Im}(f)$ is relatively small, whence we deduce that $N_{f(a)}$ is large for 'most' a's.

coAM gap. [Theorem 12] 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' b's. But in the independent case, we show that $N_b \geq 1$ for 'many' (may be not 'most'!) b's. The ideas are based on those sketched above.

The two kinds of gaps shown above are based on the set $f^{-1}(f(\mathbf{x}))$ resp. $\text{Im}(f)$. 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 4 and devise the AM and coAM protocols for $\text{AD}(\mathbb{F}_{q'})$, which also apply to $\text{AD}(\mathbb{F}_q)$.

Remark– One advantage in our problem is that we could sample a random point in the set $\text{Im}(f)$. In contrast, it is not clear how to sample a random point in the zeroset $\text{Zer}(\mathbf{f}) := \{\mathbf{x} \in \mathbb{F}_{q'}^n \mid f(\mathbf{x}) = \mathbf{0}\}$. Thus, we manage to side-step the NP-hardness associated with most zeroset properties. Eg. computing the dimension of $\text{Zer}(\mathbf{f})$ is NP-hard.

Proof idea of Theorem 2. Let algebraic circuits $\mathbf{f} := \{f_1, \ldots, f_m\}$ in $\mathbb{F}[x_1, \ldots, x_n]$ be given over a field $\mathbb{F}$. 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 (resp. projective) space, write $\overline{S}$ for its *Zariski closure* in that space, i.e. it is the smallest subset that contains S and

equals the zeroset $\mathrm{Zer}(I)$ of some polynomial ideal I.

APS vs AnnAtZero. [Theorem 14] Now, we interpret the problem AnnAtZero in a geometric way through Lemma 13:

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 [Har92]. 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 [Koi96]. 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 [LL89]. We called this problem APS. As AnnAtZero problem is already known to be NP-hard [Kay09], APS is also NP-hard.

Upper bounding 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 trdeg k of $\mathbb{F}(\mathbf{f})/\mathbb{F}$ equals m or $m-1$, but the general case remained open (best being EXPSPACE).

In this work 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 f_i's. 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 trdeg. This gives a randomized poly-time reduction from the case $k < m-1$ to $k = m-1$ (Theorem 17). 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". Inspired by this 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 the construction of a projective subvariety– the *join* –to characterize $\pi^{-1}(V')$, and eventually rules out $W \subseteq \pi^{-1}(V')$ (Lemma 18).

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

Proof idea of Theorem 3. Define $\mathbb{A} := \overline{\mathbb{F}}_q$ and assume wlog $q \geq \Omega(sr^2)$ [AL86]. [HS80, Thm.4.4] showed that a hitting-set, of size $h := O(s^2 n^2 \log q)$ 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 $\overline{\mathrm{VP}}_{\mathbb{A}}$. Given a universal circuit Ψ, certification of a hitting-set $\mathcal{H}$ is based on the following observation, that follows from the definitions:

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: Candidate set $\mathcal{H} = \{\mathbf{v}_1, \ldots, \mathbf{v}_h\}$ is *not* a hitting-set iff $\exists \mathbf{y} \in \mathbb{A}(\varepsilon)^{s'},\ \Psi(\mathbf{y}, \mathbf{x}) \notin \varepsilon\mathbb{A}[\varepsilon][\mathbf{x}]$ and $\forall i \in [h], \Psi(\mathbf{y}, \mathbf{v}_i) \in \varepsilon\mathbb{A}[\varepsilon]$.

Note that this hitting-set certification 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 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 degree-r polynomial (and approximative complexity s'). Thus, by [Sch80], 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:

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

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

The idea is to rewrite it, instead using the $(r+1)$-th roots of unity $Z_{r+1} \subset \mathbb{A}$, 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 21). By Theorem 2 it can be done in PSPACE; finishing the proof. Moreover, this PSPACE algorithm idea is independent of the field characteristic. (Eg. it can be seen as an alternative to [FS17] over the complex field.)

2 Preliminaries

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

Jacobian criterion [Jac41, BMS13] states: 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 [Sch80]. For other fields, Jacobian criterion fails due to inseparability and AD($\mathbb{F}$) is open.

AM protocol. Arthur-Merlin class AM is a randomized version of the class NP (see [AB09]). Arthur-Merlin protocols, introduced by Babai [Bab85], 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 determining if 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 [KS06] for a few natural algebraic problems in AM $\cap$ coAM. If such a problem is NP-hard (even under random reductions) then polynomial hierarchy collapses to the second-level, i.e. PH$= \Sigma_2$.

In this work AM protocol will only be used to distinguish whether a set S is 'small' or 'large'. Formally, we refer to the Goldwasser-Sipser Set Lowerbound method:

Lemma 4. *[AB09, Chap.9] 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 $|S| \stackrel{?}{\geq} 2m$ is in AM.*

Geometry. Due to limited space we have moved the geometry preliminaries to Appendix A. One can also refer to a standard text, eg. [Har92, Har13]. Basically, we need terms about affine (resp. projective) zerosets and the underlying Zariski topology. The latter gives a way to 'impose' geometry even in very discrete situations, eg. finite fields in this work.

3 Algebraic dependence testing: Proof of Theorem 1

Given $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$, we want to decide if they are algebraically dependent. For this problem AD($\mathbb{F}_q$) we could assume, with some preprocessing, that $m = n$. For, $m > n$ means that

its a YES instance. If $m < n$ then we could apply a 'random' linear map on the variables to reduce them to m, preserving the YES/NO instances. Also, the trdeg does not change when we move to the algebraic closure $\overline{\mathbb{F}}_q$. The details can be found in [PSS16, Lem.2.7-2.9]. So, we assume the input instance to be $\mathbf{f} := \{f_1, \ldots, f_n\}$ 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 $a \mapsto (f_1(a), \ldots, f_n(a))$. For $b = (b_1, \ldots, b_n) \in \mathbb{F}_{q'}^n$, denote by N_b the size of the preimage $f^{-1}(b) = \{\mathbf{x} \in \mathbb{F}_{q'}^n \mid f(\mathbf{x}) = b\}$.

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

3.1 AM protocol

First, we study the independent case.

Lemma 5 (Dim=0 preimage)**.** *Suppose* $\mathbf{f}$ *are independent. Then* $N'_{f(a)}$ *is* finite *for all but at most* (nDD'/q')*-fraction of* $a \in \mathbb{F}_{q'}^n$*.*

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

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

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

Hence, each b_i is a root of G'_i. It follows that $N'_{f(a)} \le \prod_{i\in[n]} \deg(G'_i) < \infty$, 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 $G_{i,j} \in \mathbb{F}_q[y_1, \ldots, y_n]$, for $0 \le j \le d_i$. The leading coefficient G_{i,d_i} is nonzero. As $f_1, \ldots, f_n$ are algebraically independent, the polynomial $G_{i,d_i}(f_1, \ldots, f_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$ is also nonzero. Its degree is $\le D' \deg(G_{i,d_i}) \le D' \deg(G_i) \le DD'$. By [Sch80], for all but at most (DD'/q')-fraction of $a \in \mathbb{F}_{q'}^n$, we have $G_{i,d_i}(f_1(a), \ldots, f_n(a)) \neq 0$ which implies

$$G'_i(z) = G_i(z, f_1(a), \ldots, f_n(a)) = \sum_{j=0}^{d_i} G_{i,j}(f_1(a), \ldots, f_n(a)) z^j \neq 0\,.$$

The claim now follows from the union bound. □

We need the following affine version of Bézout's Theorem. Its proof can be found in [Sch95, Thm.3.1].

Theorem 6 (Bézout's)**.** *Let* $g_1, \ldots, g_n \in \mathbb{A}[x_1, \ldots, x_n]$*. Then the number of common zeros of* $g_1, \ldots, g_n$ *in* $\mathbb{A}^n$ *is either infinite, or at most* $\prod_{i\in[n]} \deg(g_i)$*.*

Combining Lemma 5 with Bézout's Theorem, we obtain

Lemma 7 (Small preimage)**.** *Suppose* $\mathbf{f}$ *are 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 8 (Large preimage)**.** *Suppose* $\mathbf{f}$ *are 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, $|\mathrm{Im}(f)| \leq Dq'^{n-1}$ by [Sch80].

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

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

which proves the lemma. □

Theorem 9 (AM)**.** *Testing algebraic dependence of* $\mathbf{f}$ *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 Lemmas 7 & 8: When Arthur picks a randomly, with high probability, $|f^{-1}(f(a))| = N_{f(a)}$ is more than $2D$ in the dependent case while $\leq D$ 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 f_i's; thus, we know D. Moreover, containment in $f^{-1}(f(a))$ can be tested in P. Thus, by Lemma 4, $\mathrm{AD}(\mathbb{F}_q)$ is in AM. □

3.2 coAM protocol

We again study the independent case wrt a different point in the range of f.

Lemma 10 (Large image)**.** *Suppose* $\mathbf{f}$ *are 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 7. 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 11 (Small image)**.** *Suppose* $\mathbf{f}$ *are 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 8 that $|\mathrm{Im}(f)| \leq Dq'^{n-1}$. The lemma follows. □

Theorem 12 (coAM)**.** *Testing algebraic dependence of* $\mathbf{f}$ *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: $b \in \mathbb{F}_{q'}^n$ has $N_b > 0$ iff $b \in S$. Thus, by Lemma 10 (resp. Lemma 11), $|S| \geq (D^{-1} - nD'q'^{-1})q'^n > 2Dq'^{n-1}$ (resp. $|S| \leq Dq'^{n-1}$) when $\mathbf{f}$ are independent (resp. 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 f_i's; thus, we know Dq'^{n-1}. Moreover, containment in S can be tested in NP. Thus, by Lemma 4, $\mathrm{AD}(\mathbb{F}_q)$ is in coAM. □

Proof of Theorem 1. The statement immediately follows from Theorems 9 & 12. □

4 Approximate polynomials satisfiability: Proof of Theorem 2

Theorem 2 is proved in two parts. First, we show that APS is equivalent to AnnAtZero problem; which means that it is NP-hard [Kay09]. Next, we utilize the beautiful underlying geometry to devise a PSPACE algorithm.

4.1 APS is equivalent to AnnAtZero

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 nonzero constant term iff there is an annihilator over $\mathbb{A}$ with nonzero constant term. This is because if Q is an annihilator over $\mathbb{A}$ with nonzero constant term, wlog 1, then (by basic linear algebra) the linear system 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 $x = (x_1, \ldots, x_n) \in \mathbb{A}^n$ to $(f_1(x), \ldots, f_m(x)) \in \mathbb{A}^m$. 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 APS in a geometric way.

Lemma 13 (O in the closure)**.** *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 an interesting corner case, the above lemma proves that whenever $\mathbf{f}$ are algebraically *independent*, we have $\mathbb{A}^m = \overline{\mathrm{Im}(f)}$. Eg. $f_1 = X_1$ and $f_2 = X_1X_2 - 1$. Even in the dependent cases, $\mathrm{Im}(f)$ is not necessarily closed in the Zariski topology.

Example 1. *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 13 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. Wlog we assume $\mathbf{f}$ to be m nonconstant polynomials.

Theorem 14 (Approx. wrt ε)**.** $O \in \overline{\mathrm{Im}(f)}$ *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*

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

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

The proof of Theorem 14 is almost the same as that in [LL89]. First, we recall a tool to reduce the domain from a variety to a curve, proven in [LL89].

Lemma 15. [LL89, Prop.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 $\deg(C) \leq \deg(\Gamma_\varphi)$, where Γ_φ denotes the graph of φ embedded in $\mathbb{A}^n \times \mathbb{A}^m$.*

Next, [LL89] 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 $\mathbb{A}(\varepsilon)$.

Lemma 16. [LL89, Cor. of Prop.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 can use the above two lemmas to prove the connection of APS with $O \in \overline{\mathrm{Im}(f)}$, and hence with AnnAtZero (by Lemma 13).

Proof of Theorem 14. First assume that an x, satisfying the conditions in Theorem 14, exists. Pick such an x. If $\mathbf{f}$ are algebraically independent then by Lemma 13 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 13, 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 $\deg(\Gamma_f) \leq \prod_{i=1}^m \deg(f_i) = D$ by Bézout's Theorem.

By Lemma 15, there exists a curve $C \subseteq \mathbb{A}^n$ such that $O \in \overline{f(C)}$ and $\deg(C) \leq \deg(\Gamma_f) \leq D$. Pick such a curve C. Apply Lemma 16 to C, $f|_C$ and O, and let $p_1, \ldots, p_n \in \varepsilon^{-\deg(C)}\mathbb{A}[[\varepsilon]] \subseteq \varepsilon^{-D}\mathbb{A}[[\varepsilon]]$ 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 D'. When evaluating $f_1, \ldots, f_m$, at $(p_1, \ldots, p_n)$, such truncation does not affect the coefficient of ε^k for $k \leq 0$ by the choice of D'. So $f_i(x_1, \ldots, x_n) \in \varepsilon\mathbb{A}[\varepsilon]$, for all $i \in [m]$. □

Remark– The lower bound $-D = -\prod_{i=1}^m \deg(f_i)$ 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 $-D = -d^{n-1}$.

4.2 Putting APS in PSPACE

Owing to the exponential upper bound on the precision (= degree wrt ε) shown in Theorem 14, 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 trdeg of $\mathbb{F}(f_1, \ldots, f_m)/\mathbb{F}$. Computing k can be done in PSPACE using linear algebra [Pło05, Csa76]. We assume $k < m - 1$, since the cases $k = m - 1$ and $k = m$ are again easy to solve in PSPACE using linear algebra.

We reduce the number of polynomials from m to $k+1$ as follows: Fix a finite subset $S \subseteq \mathbb{F}$, 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 17 (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 17 in a geometric way, and later we will analyze the error probability.

For $d \in \mathbb{N}$, denote by $\mathbb{A}^d$ (resp. $\mathbb{P}^d$) the d-dimensional affine space (resp. projective space) 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 $V' = \overline{\pi(V)}$.[1] Now (1) of Theorem 17 is equivalent to $\dim V' = k$, and (2) is equivalent to $O' \in V'$ iff $O \in V$.

$$\begin{array}{ccccc} \mathbb{A}^n & \xrightarrow{f} & V = \overline{\mathrm{Im}(f)} & \xrightarrow{\subseteq} & \mathbb{A}^m \\ & \searrow^{g} & \downarrow{\scriptstyle \pi|_V} & & \downarrow{\scriptstyle \pi} \\ & & V' = \overline{\mathrm{Im}(g)} & \xrightarrow{\subseteq} & \mathbb{A}^{k+1} \end{array}$$

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 $O' \in \overline{\pi(V)} = V'$. See Example 2 in the appendix.

To overcome this 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 (resp. W_c) the *projective closure* of V (resp. W) 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.

Lemma 18 (Sufficient condns)**.** *We have:*
(1) dim $V' = k$, if $V_c \cap W_H = \emptyset$, and
(2) $O' \notin V'$, if $V_c \cap W_c = \emptyset$.

Proof. (1): Assume $\dim V' < k$. Choose $P \in \pi(V)$. The dimension of $\pi^{-1}(P) \cap V$ is at least $\dim V - \dim V' \geq 1$ [Har92, Thm.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 $Z \cap H \neq \emptyset$ [Har92, Prop.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.[2] So, $Y \cap H = W_c \cap H = W_H$. Therefore, $V_c \cap W_H = V_c \cap Y \cap H \supseteq Z \cap H \neq \emptyset$.

(2): 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 (1).

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 $\mathbb{P}^m$ [Har92, Example 6.17]. 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 $\overline{OQ} \cap \mathbb{A}^m \subseteq W_c \cap \mathbb{A}^m = W$.

Conversely, let $P \in V$. Let W_P denote the unique translate of W containing P. 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

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

[2] 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.

intersect H at the same point Q. We have $Q \in \ell \cap H \subseteq W_H$. So $\ell_P = \overline{PQ} \cap \mathbb{A}^m \subseteq J(V_c, W_H) \cap \mathbb{A}^m$. We conclude that

$$J(V_c, W_H) \cap \mathbb{A}^m = \bigcup_{P \in V} W_P \,. \tag{1}$$

We claim that $J(V_c, W_H) \cap \mathbb{A}^m = \pi^{-1}(V')$. As π is a linear map, Equation (1) 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, $\dim J(V_1, V_2) = \dim V_1 + \dim V_2 + 1$ [Har92, Prop.11.37-Ex.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.

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– The converse of Lemma 18 (Condition 2) is false; see Example 3 in the appendix.

Error probability. It remains to bound the probability of failure of the conditions $V_c \cap W_H = \emptyset$ and (in the case $O \notin V$) $V_c \cap W_c = \emptyset$ in Lemma 18. We need the following lemma.

Lemma 19 (Cut by hyperplanes)**.** *Let $V \subseteq \mathbb{P}^m$ be a projective subvariety 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 by 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} [Har92, 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 $1/|S|$ (eg. 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 17. As mentioned above, Theorem 17 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 $\deg(V_c \cap H) \leq \deg(V_c) \leq (\max_{i \in [m]} \deg(f_i))^k$ (see, e.g., [BCS13, Thm.8.48]).

Assume $O \in V$. Then $O' \in V'$ since $\pi(O) = O'$. Applying Lemma 19 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 $1 - k \deg(V_c \cap H)/|S| \geq 1 - \delta$. So by Lemma 18, $\dim V' = k$ 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 [Har92, Thm.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 $\deg(\pi_{O,H}(V_c)) \leq \deg(V_c)$ [Har92, Eg.18.16]. Applying Lemma 19 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 $1 - (k+1)\deg(\pi_{O,H}(V_c))/|S| \geq 1 - \delta$.

By Lemma 18 and the previous paragraphs, it holds with probability at least $1-\delta$ that $\dim V' = k$ and $O' \notin V'$. □

Proof of Theorem 2. AnnAtZero is known to be NP-hard [Kay09]. The NP-hardness of APS follows from Lemma 13 and Theorem 14.

Given an instance $\mathbf{f}$ of APS, we can first find the trdeg k. Fix a subset $S \subset \mathbb{A}$ 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 $\mathbf{g} := \{g_i := \sum_{j=1}^{m} c_{i,j} f_j \mid i \in [k+1]\}$. Compute the trdeg 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 $\mathbf{g}$ [Kay09, Lem.7], Perron's degree bound [Pło05] and linear algebra [Csa76]. □

5 Hitting-set for $\overline{\text{VP}}$: Proof of Theorem 3

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 $q \geq \Omega(sr^6)$, for the given parameters s, r. Assume that $p \nmid (r+1)$. Also, fix a model for the finite field $\mathbb{F}_q$ [AL86]. We now define the notion of 'infinitesimally approximating' a polynomial by a small circuit.

Approximative closure of VP. [BIZ17] A family $(f_n|n)$ of polynomials from $\mathbb{A}[\mathbf{x}]$ is in the *class* $\overline{\text{VP}}_{\mathbb{A}}$ if there are polynomials $f_{n,i}$ and a function $t : \mathbb{N} \mapsto \mathbb{N}$ such that g_n has a poly(n)-size poly(n)-degree algebraic circuit, over the field $\mathbb{A}(\varepsilon)$, computing $g_n(\mathbf{x}) = f_n(\mathbf{x}) + \varepsilon f_{n,1}(\mathbf{x}) + \varepsilon^2 f_{n,2}(\mathbf{x}) + \ldots + \varepsilon^{t(n)} f_{n,t(n)}(\mathbf{x})$. 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 $\overline{\text{VP}}_{\mathbb{A}}$. Given functions $s = s(n)$ and $r = r(n)$, a finite subset $\mathcal{H} \subset \mathbb{A}^n$ 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. We are interested in computing such a hitting-set in poly$(s, \log r, \log q)$-time.

Before our work, the best result known was EXPSPACE [Mul12, Mul17]. Heintz and Schnorr [HS80] proved that poly$(s, \log qr)$-sized hitting-sets exist aplenty (for degree-r $\overline{\text{size}}$-s polynomials).

Lemma 20. [HS80, Thm.4.4] *There exists a hitting-set $\mathcal{H} \subset \mathbb{F}_q^n$ 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.*

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 (see [SY10]).

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 (see [FS17, Thm.2.2]).

Note that by [HS80] 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 of polynomials $\mathcal{P}$ approximated by the specializations of $\Psi(\mathbf{y}, \mathbf{x})$. A universal circuit construction can be found in [Raz08, SY10]. Using the above notation, we give a criterion to decide whether a candidate set is a hitting-set.

Theorem 21 (hs criterion)**.** *Set $\mathcal{H} =: \{\mathbf{v}_1, \ldots, \mathbf{v}_m\} \subset \mathbb{F}_q^n$ is* not *a hitting-set for the family of polynomials $\mathcal{P}$ iff there is a satisfying assignment $(\alpha, \beta) \in \mathbb{A}(\varepsilon)^{s'} \times \mathbb{A}(\varepsilon)^n$ such that:*
(1) $\forall i \in [n]$, ${\beta_i}^{r+1} - 1 \in \varepsilon\mathbb{A}[\varepsilon]$, and
(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– The above criterion holds for algebraically closed fields $\mathbb{A}$ of *any* characteristic. Thus, it reduces those hitting-set design problems 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 $\varepsilon = 0$).

Recall the formal power series $\mathbb{A}[[\varepsilon]]$ and its group of units $\mathbb{A}[[\varepsilon]]^*$. Note that for any polynomial $a = (\sum_{i_0 \leq i \leq d} a_i\varepsilon^i)$ with $a_{i_0} \neq 0$, the inverse $a^{-1} = \varepsilon^{-i_0} \cdot (\sum_{i_0 \leq i \leq d} a_i\varepsilon^{i-i_0})^{-1}$ is in $\varepsilon^{-i_0} \cdot \mathbb{A}[[\varepsilon]]^*$. This is just a consequence of the identity $(1-\varepsilon)^{-1} = \sum_{i \geq 0} \varepsilon^i$. 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 $i \geq 0$. Thus, write x as $\varepsilon^{-i} \cdot (b_0 + b_1\varepsilon + \cdots)$ for $i \geq 0$ 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 $Z_{r+1} \subset \mathbb{A}$ (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 show is that conditions (1) and (2) can be satisfied too.

Consider the polynomial $g(\mathbf{x}) := \Psi(\alpha, \mathbf{x})|_{\varepsilon=0}$. It is a nonzero polynomial, in $\mathbb{A}[\mathbf{x}]$ of degree-r, that 'fools' $\mathcal{H}$. By [Sch80], 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 (eg. 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 before, condition (1) implies: $\beta_i' \in Z_{r+1} + \varepsilon\mathbb{A}[[\varepsilon]]$ for all $i \in [n]$. Let us define $\beta_i := \beta_i'|_{\varepsilon=0}$, for all $i \in [n]$; they are in $Z_{r+1} \subset \mathbb{A}$. By Condition (3): $\forall i \in [m]$, $\Psi(\alpha, \mathbf{v}_i) \in \varepsilon\mathbb{A}[\varepsilon]$.

Previous calculations suggest that $\Psi(\alpha, \mathbf{x})$ is in $\varepsilon^{-j}\mathbb{A}[[\varepsilon]][\mathbf{x}]$, for some $j \geq 0$. Expand the polynomial $\Psi(\alpha, \mathbf{x})$, wrt ε, as:

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

Let us study Condition (2). If for each $0 \leq \ell \leq j$, polynomial $g_{-\ell}(\mathbf{x})$ is zero, then $\Psi(\alpha, \beta')|_{\varepsilon=0} = 0$ contradicting the condition. Thus, we can pick the largest $0 \leq \ell \leq j$ 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 3. Given a prime p and parameters n, r, s in unary (wlog $p \nmid (r+1)$), 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 $\mathcal{H} =: \{\mathbf{v}_1, \ldots, \mathbf{v}_m\} \subset \mathbb{F}_q^n$ solve the APS instance described by Conditions (1)-(3) in Theorem 21. These are $(n+m+1)$ algebraic circuits of degree $\mathrm{poly}(srn, \log p)$ and a similar bitsize. Using the algorithm from Theorem 2 it can be solved in $\mathrm{poly}(srn, \log p)$-space.

The number of subsets $\mathcal{H}$ is q^{nm}. So, in $\mathrm{poly}(nm \log q)$-space we can go over all of them. 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. □

6 Conclusion

Our result on algebraic dependence testing in AM ∩ coAM gives further indication that a randomized polynomial time algorithm for the problem exists. 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 [PSS16].

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 characteristic zero fields, assuming GRH [Koi96]. Can we solve AnnAtZero (or APS) in AM for characteristic zero fields assuming GRH?) [Kay09]? This would also imply better hitting-set construction for $\overline{\text{VP}}$.

Acknowledgements. We thank Anurag Pandey and Sumanta Ghosh for insightful discussions on the approximate polynomials satisfiability and the hitting-set construction problems. N.S. thanks the funding support from DST (DST/SJF/MSA-01/2013-14). Z.G. is funded by DST and Research I Foundation of CSE, IITK.

References

[AB09] S. Arora and B. Barak. *Computational Complexity – A Modern Approach*. Cambridge University Press, 2009. 2, 3, 6

[AGS17] Manindra Agrawal, Sumanta Ghosh, and Nitin Saxena. Bootstrapping variables in algebraic circuits. Technical report, https://www.cse.iitk.ac.in/users/nitin/research.html, 2017. 3

[AL86] L. M. Adleman and H. W. Lenstra. Finding irreducible polynomials over finite fields. In *STOC*, pages 350–355, 1986. 5, 13

[ASSS12] M. Agrawal, C. Saha, R. Saptharishi, and N. Saxena. Jacobian hits circuits: Hitting-sets, lower bounds for depth-D occur-k formulas & depth-3 transcendence degree-k circuits. In *Proceedings of the 44th ACM Symposium on Theory of Computing (STOC)*, pages 599–614, 2012. (In SICOMP special issue). 3

[Bab85] László Babai. Trading group theory for randomness. In *Proceedings of the seventeenth annual ACM symposium on Theory of computing*, pages 421–429. ACM, 1985. 6

[BCS13] Peter Bürgisser, Michael Clausen, and Amin Shokrollahi. *Algebraic complexity theory*, volume 315. Springer Science & Business Media, 2013. 4, 12

[BIZ17] Karl Bringmann, Christian Ikenmeyer, and Jeroen Zuiddam. On algebraic branching programs of small width. In *32nd Computational Complexity Conference, CCC 2017, July 6-9, 2017, Riga, Latvia*, pages 20:1–20:31, 2017. 13

[BMS13] M. Beecken, J. Mittmann, and N. Saxena. Algebraic Independence and Blackbox Identity Testing. *Inf. Comput.*, 222:2–19, 2013. (Conference version in ICALP 2011). 2, 3, 6

[Bür04] Peter Bürgisser. The complexity of factors of multivariate polynomials. *Foundations of Computational Mathematics*, 4(4):369–396, 2004. (Preliminary version in FOCS 2001). 3

[Csa76] Laszlo Csanky. Fast parallel matrix inversion algorithms. *SIAM Journal on Computing*, 5(4):618–623, 1976. (Conference version in FOCS 1975). 2, 10, 13

[DGW09] Z. Dvir, A. Gabizon, and A. Wigderson. Extractors and rank extractors for polynomial sources. *Comput. Complex.*, 18(1):1–58, 2009. (Conference version in FOCS 2007). 2

[DK15] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Springer, 2015. 2

[Dvi09] Zeev Dvir. Extractors for varieties. In *Proceedings of the 24th IEEE Conference on Computational Complexity (CCC)*, pages 102–113, 2009. 2

[ER93] Richard Ehrenborg and Gian-Carlo Rota. Apolarity and canonical forms for homogeneous polynomials. *European Journal of Combinatorics*, 14(3):157–181, 1993. 1

[FS17] Michael A Forbes and Amir Shpilka. A PSPACE construction of a hitting set for the closure of small algebraic circuits. *arXiv preprint arXiv:1712.09967*, 2017. 2, 4, 6, 14

[Har92] Joe Harris. *Algebraic Geometry: A First Course*. Springer, 1992. 5, 6, 11, 12, 13

[Har13] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013. 6

[HS80] Joos Heintz and Claus-Peter Schnorr. Testing polynomials which are easy to compute. In *Proceedings of the twelfth annual ACM symposium on Theory of computing*, pages 262–272. ACM, 1980. 3, 5, 13, 14

[Ing71] Aubrey W Ingleton. Representation of matroids. *Combinatorial mathematics and its applications*, 23, 1971. 1

[Jac41] C. G. J. Jacobi. De determinantibus functionalibus. *J. Reine Angew. Math.*, 22(4):319–359, 1841. 2, 6

[Kay09] N. Kayal. The Complexity of the Annihilating Polynomial. In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity (CCC)*, pages 184–193, 2009. 2, 5, 8, 13, 15

[Koi96] Pascal Koiran. Hilbert's Nullstellensatz is in the polynomial hierarchy. *Journal of complexity*, 12(4):273–286, 1996. 3, 4, 5, 15

[Kol88] János Kollár. Sharp effective Nullstellensatz. *Journal of the American Mathematical Society*, 1(4):963–975, 1988. 3

[KS06] Neeraj Kayal and Nitin Saxena. Complexity of ring morphism problems. *computational complexity*, 15(4):342–390, 2006. 6

[KS16] Mrinal Kumar and Shubhangi Saraf. Arithmetic circuits with locally low algebraic rank. In *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*, pages 34:1–34:27, 2016. 3

[Lan12] Joseph M Landsberg. *Tensors: geometry and applications*, volume 128. American Mathematical Society Providence, RI, 2012. 4

[LG14] François Le Gall. Powers of tensors and fast matrix multiplication. In *Proceedings of the 39th international symposium on symbolic and algebraic computation*, pages 296–303. ACM, 2014. 4

[LL89] Thomas Lehmkuhl and Thomas Lickteig. On the order of approximation in approximative triadic decompositions of tensors. *Theoretical Computer Science*, 66(1):1–14, 1989. 3, 5, 9, 10

[MM82] Ernst W Mayr and Albert R Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Advances in mathematics*, 46(3):305–329, 1982. 3

[MSS14] Johannes Mittmann, Nitin Saxena, and Peter Scheiblechner. Algebraic independence in positive characteristic: A p-adic calculus. *Transactions of the American Mathematical Society*, 366(7):3425–3450, 2014. 2, 3

[Mul12] Ketan D. Mulmuley. Geometric complexity theory V: Equivalence between blackbox derandomization of polynomial identity testing and derandomization of Noether's normalization lemma. In *FOCS*, pages 629–638, 2012. 2, 4, 13

[Mul17] Ketan Mulmuley. Geometric complexity theory V: Efficient algorithms for Noether normalization. *Journal of the American Mathematical Society*, 30(1):225–309, 2017. 2, 3, 4, 13

[Per27] O. Perron. *Algebra I (Die Grundlagen)*. W. de Gruyter, Berlin, 1927. 2

[Pło05] Arkadiusz Płoski. Algebraic dependence of polynomials after o. perron and some applications. *Computational Commutative and Non-Commutative Algebraic Geometry*, pages 167–173, 2005. 2, 10, 13

[PSS16] Anurag Pandey, Nitin Saxena, and Amit Sinhababu. Algebraic independence over positive characteristic: New criterion and applications to locally low algebraic rank circuits. In *LIPIcs-Leibniz International Proceedings in Informatics*, volume 58. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016. 2, 3, 4, 7, 15

[Raz08] Ran Raz. Elusive functions and lower bounds for arithmetic circuits. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 711–720. ACM, 2008. 14

[Sax09] Nitin Saxena. Progress on polynomial identity testing. *Bulletin of the EATCS*, 99:49–79, 2009. 4

[Sax13] Nitin Saxena. Progress on polynomial identity testing - II. *Electronic Colloquium on Computational Complexity (ECCC)*, 20:186, 2013. 4

[Sch80] J.T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, 1980. 2, 6, 7, 8, 14

[Sch95] Joachim Schmid. On the affine Bezout inequality. *manuscripta mathematica*, 88(1):225–232, 1995. 7

[SŠ17] Marcus Schaefer and Daniel Štefankovič. The complexity of tensor rank. *Theory of Computing Systems*, Aug 2017. 4

[SY10] 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, 2010. 4, 13, 14

A From Section 2: Algebraic-Geometry

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 follows: A subset S of $\mathbb{A}^d$ is *closed* iff it is the set of common zeros of some subset of polynomials in $\mathbb{A}[X_1, \ldots, X_d]$. For other subsets S it makes sense to consider the *closure* $\overline{S}$– the smallest closed set containing S. Set S is *dense* if $\overline{S} = \mathbb{A}^d$. Complement of closed sets are called *open*.

A closed set is called a *hypersurface* (resp. *hyperplane*) if it is definable by a single polynomial (resp. single linear polynomial).

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 $(\mathbb{A}^{d+1} \setminus \{(0, \ldots, 0)\})/\sim$. Where $(x_0, \ldots, x_d) \sim (y_0, \ldots, y_d)$ iff there exists $c \in \mathbb{A}^\times$ such that $y_i = cx_i$ for $0 \leq i \leq d$. The set $\mathbb{P}^d$ is again equipped with the *Zariski topology*, where a subset is closed iff it is the set of common zeros of some subset of *homogeneous* polynomials in $\mathbb{A}[X_0, \ldots, X_d]$. We use $(d+1)$-tuples $(x_0, \ldots, x_d)$ to represent points in $\mathbb{P}^d$.

Closed subsets of $\mathbb{A}^d$ or $\mathbb{P}^d$ are also called *algebraic sets* or *zerosets*. 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 (resp. projective) space is also called an *affine variety* (resp. *projective variety*). (In some references, varieties are not required to be irreducible, but in this work we always assume it.) 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 zerosets (resp. varieties) are in 1-1 correspondence with *radical* (resp. *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; it 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 $M = \prod_{i=1}^d X_i^{d_i}$ by $X_0^{D-\deg(M)} \prod_{i=1}^d X_i^{d_i}$, 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 $(u, v) \in \mathbb{A}^2 \setminus \{(0, 0)\}$.

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. Eg. 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 $\mathbb{A}^d$ (resp. $\mathbb{P}^d$) is the number of intersections of V with a general affine subspace (resp. projective subspace) of dimension $d - \dim V$. More generally, the degree of an algebraic set V, denoted by $\deg(V)$, is 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 $f_i(X_1 - a_1, \ldots, X_d - a_d)$, $i = 1, \ldots, k$.

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).

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 $(f_1(x), \ldots, f_m(x)) \in \mathbb{A}^m$, where $f_i \in \mathbb{A}[X_1, \ldots, X_n]$ for $i \in [m]$. And suppose V and W are defined by ideals $I \subseteq \mathbb{A}[X_1, \ldots, X_n]$ and $I' \subseteq \mathbb{A}[Y_1, \ldots, Y_m]$ respectively. Then Γ_f is defined by I, I', and the polynomials $Y_i - f_i(X_1, \ldots, X_n) \in \mathbb{A}[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$, $i = 1, \ldots, m$.

B From Section 4

Example 2. *Let $m = 4$, $(f_1, f_2, f_3, f_4) = (X_1, X_2, X_1X_2 - 1, X_1 + X_2)$. Then $k := trdeg\mathbf{f} = 2$. 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.

Example 3. *Consider Example 2 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 $(0, 0, 1, 0, 1) \in V_c \cap W_H \subseteq V_c \cap W_c$.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il