Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 26 (2026)

When Hilbert approximates: A Strong Nullstellensatz for Approximate Polynomial Satisfiability

Sanyam Agarwal
Universität des Saarlandes, Saarbrücken, Germany

Sagnik Dutta
Max-Planck-Institut für Informatik, Saarbrücken, Germany

Anurag Pandey
Universität des Saarlandes, Saarbrücken, Germany

Himanshu Shukla
Univeristät Bayreuth, Bayreuth, Germany

Abstract

Guo, Saxena, and Sinhababu (TOC'18, CCC'18) defined a natural, approximative analog of the polynomial system satisfiability problem, which they called approximate polynomial satisfiability (APS). They proved algebraic and geometric properties of it and showed an NP-hardness lower bound and a PSPACE upper bound for it. They further established how the problem naturally occurs in border complexity and Geometric complexity theory (GCT) and used the problem to construct hitting sets for $\overline{\mathsf{VP}}$ in PSPACE, hence greatly mitigating the GCT chasm.

The starting point of this work is the observation that Guo, Saxena, and Sinhababu's criterion for non-existence of approximative solution can be interpreted as an analog of Weak Hilbert's Nullstellensatz in the approximative setting. We extend their work by proving an analog of Strong Hilbert's Nullstellensatz in the approximative setting. Concretely, we give an algebraic criterion for containment between approximative solution sets defined by systems of polynomials. In fact, this characterization turns out to be equivalent to membership in the integral closure over a maximal ideal of a local subring of $\mathbb{C}(x_1, \ldots, x_n)$ determined by the given polynomials. In addition, we use our proof to provide a PSPACE algorithm for testing this containment, exponentially better than the EXPSPACE bounds for polynomial subalgebra mebership testing and the polynomial integral closure membership testing, hence matching the complexity bound of Guo, Saxena, and Sinhababu's Weak Approximative Nullstellensatz.

2012 ACM Subject Classification Theory of computation → Algebraic complexity theory

Keywords and phrases Approximate Polynomial Satisfiability, Algebraic Geometry, PSPACE

Digital Object Identifier 10.4230/LIPIcs...XX

Acknowledgements We would like to thank Bernd Sturmfels for pointing us towards Ganzstellensatz. AP would like to thank Nitin Saxena for initial discussions, and Karl Bringmann and Raimund Seidel for hosting him during this work. Finally, we would like to thank Markus Bläser for his unconditional support throughout.

1 Introduction

Deciding whether a multivariate polynomial system has a common zero is a central problem in mathematics, engineering, and computer science. Over an algebraically closed field, the classical *Weak Hilbert Nullstellensatz* characterizes *non-emptiness* of an affine algebraic set via the existence of an explicit polynomial certificate, while the *Strong Hilbert Nullstellensatz* characterizes *containment* of varieties by relating vanishing on a solution set to membership in a radical ideal (equivalently, by allowing powers) [9, 30]. From the algorithmic viewpoint,

Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

ISSN 1433-8092

the complexity of such feasibility and containment questions has been studied for decades, with PSPACE upper bounds appearing already in the context of algebraic decision problems and quantifier elimination [7, 25, 24]. In fact, over fields of characteristic zero, the feasibility/containment question can be decided in the low levels of the polynomial hierarchy [24], assuming the Generalized Reimann Hypothesis (GRH).

In many settings, exact satisfiability is often too strong an ask. Hence, one cares about *infinitesimal approximation* rather than equality. An example that clearly demonstrates this is the following.

▶ **Example 1.** Let $f_1, f_2 \in \mathbb{C}[x, y]$ such that $f_1 = xy - 1$ and $f_2 = x$. Clearly, these polynomials have no common root over $\mathbb{C}^2$. However, geometrically, the curves seem to converge on the y-axis. To capture such convergence we can allow the variables to take values in $\mathbb{C}(\varepsilon)$ where ε is an *infinitesimally* small parameter. In this case, the point $p = (\varepsilon, \frac{1}{\varepsilon}) \in \mathbb{C}(\varepsilon)^2$ is an approximative common root the system, as $\lim_{\varepsilon \to 0} f_1(p) = \lim_{\varepsilon \to 0} f_2(p) = 0$.

Guo, Saxena, and Sinhababu (GSS) formalized this perspective by introducing *approximate polynomial satisfiability* (APS) [17].

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

▶ **Example 2.** While this notion of approximation allows us to capture more solutions, it doesn't mean that every system of polynomials now has a solution. For example, take $f_1, f_2 \in \mathbb{C}[x, y]$ such that $f_1 = xy$ and $f_2 = xy + 1$. No assignment to x, y from $\mathbb{C}(\varepsilon)^2$ can make this satisfiable in the above approximative sense.

▶ Remark 1. As shown in Example 1, approximative solutions differ from affine solutions. Not only that, GSS showed that these approximative solutions *also* differed projective solutions. They showed that while every approximative solution is a projective solution, the converse is not true.

Informally, APS asks whether a polynomial system admits solutions that satisfy the constraints *to all orders* in an infinitesimal parameter (equivalently, whether a target point lies in the Zariski closure of a polynomial map's image, as made precise in [17]). This captures the "border" viewpoint pervasive in algebraic complexity, where one studies limits of efficiently computable objects. Further, they showed that APS captures canonical border phenomena such as tensor *border rank* (see [6, 26]).

Along with this, GSS also showed that computationally this problem is NP-Hard and, in fact, lies in PSPACE when the input polynomials are given as algebraic circuits. They do this by showing that existence of an approximative solution to a set of polynomials is equivalent to testing whether all the *annihilators* of the input polynomials have constant term 0 (Note that given a field k and polynomials $\mathbf{f} \coloneqq \{f_1, \ldots, f_m\} \in k[x_1, \ldots, x_n]$, an annihilator of $\mathbf{f}$ is a polynomial $A(y_1, \ldots, y_m) \in k[y_1, \ldots, y_m]$ such that $A(f_1, \ldots, f_m) = 0$).

We observe that this can be reformulated as a weak "approximative" Nullstellensatz. Intuitively, the non-existence of an approximate solution is equivalent to the existence of an annihilator having a non-zero constant (equivalently, constant term being 1) which is analogous to a variety defined by polynomials being empty if 1 lies in their ideal. Hence, we call their characterization the *Weak Approximative Nullstellensatz* (WAN), and formally define it below. Before that, we need to define the approximative vanishing set of a given system of polynomials.

▶ **Definition 1** (Approximative Vanishing Set (AV)). *Given polynomials* $\mathbf{f} \coloneqq f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$ *the approximative vanishing set* $\mathsf{AV}(\mathbf{f})$ *is defined as:*

$$\mathsf{AV}(\mathbf{f}) \coloneqq \{\beta \in \mathbb{C}(\varepsilon)^n \mid \forall i,\ f_i(\beta) = \varepsilon \frac{p_{i,\beta}(\varepsilon)}{q_{i,\beta}(\varepsilon)} \text{ with } p_{i,\beta}, q_{i,\beta} \in \mathbb{C}[z], \text{and } q_{i,\beta}(0) \neq 0\}.$$

▶ **Example 3.** Using Example 1, $\mathsf{AV}(f_1, f_2)$ contains the point $(\varepsilon, \frac{1}{\varepsilon})$. But it also contains many other points like $(\varepsilon^2, \frac{1}{\varepsilon^2}), (\frac{\varepsilon}{1+\varepsilon}, \frac{1+\varepsilon}{\varepsilon})$, and so on.

▶ Remark 2. In [17], APS is defined as containing those $\beta \in \mathbb{C}(\varepsilon)^n$ such that $f_i(\beta)$ is in the ideal $\varepsilon\mathbb{C}[\varepsilon]$ of $\mathbb{C}[\varepsilon]$, while in our case $f_i(\beta)$ has numerators in the same ideal, but denominators are polynomials in ε with non-zero constant terms. These two conditions are equivalent when talking about non-emptiness of approximate vanishing sets. To see this assume for some $\beta \in \mathbb{C}(\varepsilon)^n$, for all i, $f_i(\beta) = \varepsilon \frac{p_{i,\beta}(\varepsilon)}{q_{i,\beta}(\varepsilon)}$. Then, we can scale β to get $\beta' = \beta \prod_{i=1}^{m} q_{i,\beta}(\varepsilon)$ such that $f_i(\beta')$ lies in the ideal $\varepsilon\mathbb{C}[\varepsilon]$ of $\mathbb{C}[\varepsilon]$.

▶ Remark 3. We choose all such $\beta \in \mathbb{C}(\varepsilon)^n$ as geometrically all these points also ensure that $f_i(\beta)$ converges to 0 in the limit. Further, this is more aligned with the literature on valued fields (see [13] for more details on valued fields and Ganzstellensatz in §1.2).

▶ **Theorem 1.1** (Weak Approximative Nullstellensatz (WAN), [17]). *Given polynomials* $\mathbf{f} = f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$, $\mathsf{AV}(\mathbf{f})$ *is empty* if and only if *there exists an annihilator of* $\mathbf{f}$ *with constant-term* 1*.*

Thus, GSS showed that computationally testing WAN is in PSPACE. Not only that, they showed that this enables the construction of hitting sets for $\overline{\mathsf{VP}}$ in PSPACE (over any field), thereby substantially narrowing the "GCT chasm" studied before in [32, 14]. For complex numbers, PSPACE-constructible hitting sets for the closure of small algebraic circuits already appear in the work of Forbes and Shpilka [15].

1.1 Our Contributions

The starting point of this work is the observation that the GSS algebraic criterion for *non-existence* of approximative solutions can be viewed as an analog of the *Weak Hilbert's Nullstellensatz* (WHN) in the approximative setting. In classical algebraic geometry, the next structural step is the *Strong Hilbert's Nullstellensatz* (SHN), which answers questions about containment of solutions. Formally, it asks whether polynomial constraints defining one variety *force* another polynomial to vanish? Motivated by this, we study the following natural problem about containment of approximative vanishing sets.

▶ **Problem 2.** *Given two systems of polynomials* $\mathbf{f} = (f_1, \ldots, f_m)$ *and* $\mathbf{g} = (g_1, \ldots, g_t)$ *over* $\mathbb{C}$*, decide whether the* approximative solution set *of* $\mathbf{f}$ *is contained in that of* $\mathbf{g}$*, i.e., whether every infinitesimal solution to* $\mathbf{f}$ *necessarily satisfies* $\mathbf{g}$ *(in the same approximative sense).*

The containment condition mentioned above is not always obvious to check, as demonstrated in the following example.

▶ **Example 4.** Given $f_1, f_2, g, h \in \mathbb{C}[x, y]$ where $f_1 = x, f_2 = xy - 1, g = x^2y, h = xy^2 - 1$.

- *Containment of* AV*:* It can be verified that $\mathsf{AV}(f_1, f_2) \supseteq \mathsf{AV}(g, f_2)$.
- *Non-containment of* AV*:* It is easy to see that $\mathsf{AV}(f_1, h) \supsetneq \mathsf{AV}(f_1, f_2)$ as $(\varepsilon, \frac{1}{\varepsilon})$ lies in $\mathsf{AV}(f_1, f_2)$ but not $\mathsf{AV}(f_1, h)$, and similarly $\mathsf{AV}(f_1, h) \subsetneq \mathsf{AV}(f_1, f_2)$ as $(\varepsilon^2, \frac{1}{\varepsilon})$ lies in $\mathsf{AV}(f_1, h)$ but not $\mathsf{AV}(f_1, f_2)$.

▶ Remark 4. We do not need to always check the containment for the whole system of polynomials together. Instead, we can check containment for each individual polynomial. This is because $\mathsf{AV}(g_1, \ldots, g_t) = \cap_{i=1}^{t} \mathsf{AV}(g_i)$. Hence, checking $\mathsf{AV}(g_1, \ldots, g_t) \supseteq \mathsf{AV}(f_1, \ldots, f_m)$ is equivalent to checking $\mathsf{AV}(g_i) \supseteq \mathsf{AV}(f_1, \ldots, f_m)$ for each $i \in [t]$.

In the approximative setting, this is the natural strengthening of WAN. To resolve this question, we prove our main result.

▶ **Theorem 1.2** (Strong Approximative Nullstellensatz (SAN)). *Given a set of polynomials* $f_1, \ldots, f_m, g \in \mathbb{C}[x_1, \ldots, x_n]$,

$$\mathsf{AV}(g) \supseteq \mathsf{AV}(f_1, \ldots, f_m) \quad \text{if and only if} \quad g^r = \sum_{i=0}^{r-1} \frac{F_i(f_1, \ldots, f_m)}{1 + G_i(f_1, \ldots, f_m)} g^i,$$

for some $r \in \mathbb{N}$*, and constant free polynomials* $F_i, G_i \in \mathbb{C}[y_1, \ldots, y_m]$*, for* $0 \leq i \leq r-1$.

▶ **Example 5.** Consider polynomials $f_1, f_2 \in \mathbb{C}[x, y]$ where $f_1 = xy^2 - y + x^2 y$ and $f_2 = xy - 1$. Then, it can be verified that $g = x$ such that $\mathsf{AV}(g) \supseteq \mathsf{AV}(f_1, f_2)$. On first look, its hard to see why this is true. But if we use our algebraic criterion, then $g^2 = \frac{f_1}{1+f_2} g - f_2$ certifies this containment.

Clearly, SAN implies WAN: if $\mathsf{AV}(f_1, \ldots, f_m)$ was empty then 1 would lie in their integral closure. Using the characetrization above, we can rearrange to get $1 = A(f_1, \ldots, f_m)$ where $A(y_1, \ldots, y_m)$ was constant-free in $\mathbb{C}[y_1, \ldots, y_m]$. But this simply means that there exists an annihilator with constant-term 1. Further, our containment criterion can be reformulated as a membership condition in the *integral closure* over a maximal ideal of a local subring of $\mathbb{C}(x_1, \ldots, x_n)$ determined by $\mathbf{f}$, see Section 2 for more details. This connects approximative containment to classical commutative-algebraic notions surrounding integral dependence and closure [19, 37]. We informally state our correspondence theorem here. For a formal statement, see Theorem 2.1.

▶ **Theorem 1.3** (Approximate Vanishing to Integral Closure correspondence (Informal)). *For* $f_1, \ldots, f_m, g \in \mathbb{C}[x_1, \ldots, x_n]$, $\mathsf{AV}(g) \supseteq \mathsf{AV}(f_1, \ldots, f_m)$ if and only if g *lies in the integral closure of a local subring of* $\mathbb{C}(x_1, \ldots, x_n)$ *determined by* $f_1, \ldots, f_m$.

As discussed before, GSS also gave a PSPACE algorithm for testing WAN. In the same spirit, we also look at the computational problem defined by SAN. We assume the polynomials are given as algebraic circuits. Formally, we define the computational problem of testing SAN as the following:

▶ **Problem 3** (Computational Problem of testing SAN). *Given polynomials* $f_1, \ldots, f_m, g \in \mathbb{C}[x_1, \ldots, x_n]$, SAN *is the decision problem asking whether* $\mathsf{AV}(g) \supseteq \mathsf{AV}(f_1, \ldots, f_m)$.

Depending on the context, we will use SAN interchangeably for both the decision problem and the containment criteria. We show that testing containment of approximate vanishing sets can also be done in PSPACE, thus matching the upper bound of WAN.

▶ **Theorem 1.4.** SAN *is in* PSPACE.

This beautifully coincides with the known matching upper bounds of the WHN and SHN in conventional algebraic geometry, where it is typically achieved through the use of "Rabinowitsch's trick" [36].

1.2 Related works

In this section, we survey the known related works and their implications in our setting.

Hilbert's Nullstellensatz: It is well-known that the Weak Hilbert's Nullstellensatz (WHN) and the Strong Hilbert's Nullstellensatz (SHN) are equivalent [9]. Typically, this equivalence is achieved using "Rabinowitsch's trick" [36]. The trick works like this: given polynomials $f_1, .., f_m, g \in \mathbb{C}[x_1, .., x_n]$, checking whether the zeroset of g contains the zeroset of $f_1, \ldots, f_m$ is equivalent to checking if the zeroset of the polynomials $f_1, \ldots, f_m, 1 - yg \in \mathbb{C}[x_1, .., x_n, y]$ is empty or not. Further, this also ensures that WHN and SHN are computationally equivalent. Hence, a natural starting point is to see if this correspondence also holds in the approximative setting. However, this is not the case and "Rabinowitsch's trick" can't be directly used to get equivalence between WAN and SAN. This can be intuitively seen as follows: Suppose at a point $p \in \mathbb{C}^n$, $f_i(p) = g(p) = 0$ for all i. Then, clearly the polynomial $1 - yg$ is non-zero. However, in the approximative setting this does not hold. Since we are now looking at approximative vanishing instead of exact vanishing, it might be the case that at $p \in \mathbb{C}(\varepsilon)^n$, $g(p) = \varepsilon \frac{p(\varepsilon)}{q(\varepsilon)}$ where $q(0) \neq 0$ and $p(\varepsilon) \neq 0$. Then setting $y = \frac{1}{\varepsilon} \frac{q(\varepsilon)}{p(\varepsilon)} \in \mathbb{C}(\varepsilon)$ ensures that the polynomial $1 - yg$ approximatively vanishes. Thus, this extra polynomial doesn't fully capture the notion of approximative vanishing. hence, the conventional Rabinowitsch trick can't be used to show equivalence of WAN and SAN. At the same time, this also makes the path to obtain efficient runtime for the decision problem SAN unclear.

ε-approximate Nullstellensatz: In an interesting parallel direction, Göös et al. [16] defined the notion of *ε-approximate Nullstellensatz*. In particular, they used a robust version of the WHN to show separations in proof complexity where they show that *Resolution proofs* cannot be efficiently simulated by *Sherali-Adams proofs* when the coefficients are written in unary.

Subalgebra Membership: Looking at the geometric containment $\mathsf{AV}(g) \supseteq \mathsf{AV}(f_1, \ldots, f_m)$, it is natural to ask whether the notion of subalgebra membership can be used to capture this algebraically. Given polynomials $g, f_1, \ldots, f_m \in \mathbb{C}[x_1, .., x_n]$, the *subalgebra membership* problem asks if g can be written as $g = \sum a_k f_1^{k_1} \ldots f_m^{k_m}$, where the sum is finite. Recently, it was shown that, in the general case, this problem is EXPSPACE-complete, see [22] for definitions and more details. However, while subalgebra membership implies containment of approximative vanishing sets, the converse is not true. This can be seen by the following example.

▶ **Example 6.** Given $f_1, f_2 \in \mathbb{C}[x, y]$, such that $f_1 = x^2$ and $f_2 = x^2y - 1$. Let $g = x$. It is easy to verify that $\mathsf{AV}(g) = \mathsf{AV}(f_1)$, and hence $\mathsf{AV}(g) \supseteq \mathsf{AV}(f_1, f_2)$. However, g doesn't lie in the subalgebra formed bsy $\mathbb{C}[f_1, f_2]$.

Ganzstellensatz: The closest related notions to SAN in literature comes from the work on *Ganzstellensatz*, see [23, 35, 18, 27] for more details. These works approach this question through the point of view of valuations. Let $K := \mathbb{C}\{\{\varepsilon\}\}$, i.e., field of *Puiseux series* over $\mathbb{C}$ with the ε-adic valuation val_ε of ε normalized to 1, and let $g, f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$. Consider the set $S \subset K^n$ such that for all $s \in S$ and for all $i \in [m]$, $\mathrm{val}_\varepsilon(f_i(s)) \geq 0$. Then they give an algebraic criterion on g such that for all $s \in S$, $\mathrm{val}_\varepsilon(g(s)) \geq 0$. Restricting to our setting, i.e., when $g, f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$, the criterion of Haskell and Yaffe [18] gives that g is integral over $\mathbb{C}[f_1, \ldots, f_m]$, i.e., $g^r = \sum_{i=0}^{r-1} F_i g^i$ for some $r \in \mathbb{N}$ and $F_i \in \mathbb{C}[f_1, \ldots, f_m]$. Clearly, if g is integral over $\mathbb{C}[f_1, \ldots, f_m]$, then $\mathrm{val}_\varepsilon(g(s)) \geq 0$, for all $s \in K^n$ such that for all $i \in [m]$, $\mathrm{val}_\varepsilon(f_i(s)) \geq 0$. .
Another way to interpret this is the following: they look at all points such that when $f_1, \ldots, f_m$

is "well-behaved", then so is g. That is, for all points s in $S = \{\beta \in K^n \mid \lim_{\varepsilon\to 0} f_i(\beta) = a,\ a \in \mathbb{C}\}$, they want $\lim_{\varepsilon\to 0} g(s) = b$ for some $b \in \mathbb{C}$. In particular, they don't enforce the condition of "vanishing". While close to our setting, it is a different characterization. The following example demonstrates this.

▶ **Example 7.** Using Example 6, we know that for $f_1 = x^2y$ and $f_2 = xy - 1$, $g = x$ contains their approximative vanishing set. However, for $s = (\frac{1}{\epsilon}, \epsilon^3)$, we have $\lim_{\varepsilon\to 0} f_1(s) = 0, \lim_{\varepsilon\to 0} f_2(s) = -1$, but $\lim_{\varepsilon\to 0} g(s)$ does not exist. Hence, g does not lie in the *Ganzstellensatz* criterion for f_1, f_2 defined above.

1.3 Our methods

In this section, our aim is to convey the fundamental ideas behind the proofs of our main results. Hence, we occasionally gloss over the finer technical arguments needed to formally prove the claims.

Proof ideas for Theorem 1.2 (SAN)**:** One direction is easy to show, that is if g lies in the defined integral closure, then it will contain the approximative vanishing set of $f_1, \ldots, f_m$. Intuitively, when all the f_i vanish approximatively, so will F_i, G_i in Theorem 1.2, hence so will g, see Proof 2 for details. For the converse direction, as discussed above, the conventional Rabinowitsch's trick doesn't work in the approximative setting. However, when geometrically looking at the containment of approximative vanishing sets, simultaneous approximative vanishing of $f_1, \ldots, f_m$ forces g to also approximatively vanish, which is equivalent to saying that g neither diverges nor converges to a non-zero constant $c \in \mathbb{C}$ (see Lemma 1 for more details). We call these two conditions the "*approximative* Rabinowitsch tricks". Using these two conditions along with GSS criterion (Theorem 1.1) we can obtain the desired formulation as follows. Using the first trick (the non-divergence condition), we first obtain a univariate polynomial P of degree r with coefficients from $\mathbb{C}[f_1, ..., f_m]$, such that g satisfies P (see Lemma 2). Using the obtained polynomial recursively along with the second approximative Rabinowitsch trick (non-convergence to any non-zero constant), we can get the claimed characterization (refer to Lemma 3 and subsequent discussion).

Proof ideas for Theorem 1.4 (SAN **in** PSPACE)**:** Apriori, it is not clear how to put the decision problem of SAN in PSPACE using the geometric conditions obtained in Lemma 1. This is because the second approximative Rabinowitsch's condition (non-convergence to any non-zero constant) requires the elimination of a *universal* quantifier. Quantifier elimination for algebraically closed fields and its complexity has a long history, with foundational algorithms due to Chistov and Grigor'ev [8]. Ierardi developed an exponential-space decision procedure for the first-order theory of algebraically closed fields and showed improved space bounds under bounded alternations [20]. Hence, a naive elimination-based approach to SAN would suggest an EXPSPACE upper bound. Even if we use the algebraic criterion devised in Theroem 1.2, it is not clear how to put the decision problem in PSPACE. de Jong [11] gave an algorithm for computing the integral closure which requires computation of ideals in the intermediate steps. Typically this involves the use of Gröbner Basis methods, for which doubly-exponential degree bounds are known in the worst case [29, 12, 1]. Consequently, one should expect an EXPSPACE algorithm.

However, we are looking for polynomials in a specific integral closure defined by a local subring determined by the input polynomials. This additional structure, along with known annihilator bounds (see Theorem 3.1) help us in attaining a PSPACE algorithm. We can interpret our algebraic characterization in Theorem 1.2 as a univariate polynomial P of

degree r with coefficients from $\mathbb{C}[f_1, ..., f_m]$, such that g satisfies P. Hence, this means that the polynomials $g, f_1, \ldots, f_m$ have a non-zero annihilator. However, currently, we cannot say anything about the degree bounds of this annihilator, as Theorem 3.1 does not guarantee an exponential degree bound for *all* the annihilators, but the minimal one, and the annihilator obtained through P might not be the minimal annihilator of $g, f_1, \ldots, f_m$. To overcome this, we now use the random reduction trick introduced by GSS (see Theorem 3.2), where they show that given a system of polynomials $f_1, \ldots, f_m$ of transcendence degree ρ, we can reduce to $\rho + 1$ random linear combinations of these f_i such that the non-emptiness of AV is preserved. The advantage of doing this is the following: the annihilator ideal of ℓ polynomials is principal if the transcendence degree is $\ell - 1$ (see [17, 21]). Once we have this, we can now degree bound all the annihilators appearing in the proofs of Lemma 2 and Lemma 3, both of which only deal with *non-emptiness* of approximative vanishing set, thanks to our *approximative* Rabinowitsch tricks, and hence, GSS' random reduction lemma can indeed be invoked. Repeated application of this helps us to finally upper bound, in Theorem 1.2, the exponent r and the degrees of F_i's and G_i's to at most singly exponential in the input parameters using the degree bound on the minimal annihilating polynomial [33, 21]. Finally, we only need to solve a system of exponentially many linear equations in exponentially many variables, which is known to be in PSPACE [4, 10, 31], see Section 3 for details.

2 Proof of Strong Approximative Nullstellensatz

In this section we prove our main characterization theorem, the Strong Approximative Nullstellensatz, where analogous to the ideal-variety correspondence in algebraic geometry, we have the correspondence between the integral closure (over a maximal ideal of a local/fractional/natural subring of $\mathbb{C}(x_1, \ldots, x_n)$ determined by $f_1, \ldots, f_m$) and the approximative vanishing set (recall Definition 1).

It is easy to see the correspondence with WHN in the classical setting: the vanishing set $V(f_1, \ldots, f_m)$ of $f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$ is empty $\iff 1 \in \langle f_1, \ldots, f_m \rangle$. Similarly, in the classical setting SHN says that the ideal generated by all functions vanishing on $V(f_1, \ldots, f_m)$ is exactly the radicle ideal $\sqrt{\langle f_1, \ldots, f_m \rangle}$, or in other words, if $f \in \mathbb{C}[x_1, \ldots, x_n]$, then $f^r \in \langle f_1, \ldots, f_m \rangle \iff V(f_1, \ldots, f_m) \subseteq V(f)$. We now present the natural analogue of SHN in the approximative setting.

▶ **Theorem** (Strong Approximative Nullstellensatz (SAN)). *Given $f_1, \ldots, f_m, g \in \mathbb{C}[x_1, \ldots, x_n]$,*

$$\mathsf{AV}(g) \supseteq \mathsf{AV}(f_1, \ldots, f_m) \quad \text{if and only if} \quad g^r = \sum_{i=0}^{r-1} \frac{F_i}{1 + G_i} g^i,$$

for some $r \in \mathbb{N}$, where F_i, G_i are constant free polynomials in $\mathbb{C}[f_1, \ldots, f_m]$.

We first prove the easier direction of the theorem, that the algebraic condition implies the geometric condition: g being in the integral closure implies that the approximative vanishing set of g contains the common approximative vanishing set of $f_1, \ldots, f_m$. Before moving forward, we give some definitions. For a nonzero $h(\varepsilon) \in \mathbb{C}(\varepsilon)$, define $\mathrm{ord}_\varepsilon(h)$ to be the *highest power of ε dividing h*, i.e., the unique integer $t \in \mathbb{Z}$ such that

$$h(\varepsilon) = \varepsilon^t \cdot \frac{p(\varepsilon)}{q(\varepsilon)} \quad \text{with } p, q \in \mathbb{C}[\varepsilon],\ p(0) \neq 0,\ q(0) \neq 0.$$

Set $\mathrm{ord}_\varepsilon(0) = +\infty$. Then $\mathrm{ord}_\varepsilon(h_1 + h_2) \geq \min\{\mathrm{ord}_\varepsilon(h_1), \mathrm{ord}_\varepsilon(h_2)\}$, where equality holds if $\mathrm{ord}_\varepsilon(h_1) \neq \mathrm{ord}_\varepsilon(h_2)$, and $\mathrm{ord}_\varepsilon(h_1 h_2) = \mathrm{ord}_\varepsilon(h_1) + \mathrm{ord}_\varepsilon(h_2)$. We say $h \equiv 0 \mod \varepsilon \iff \mathrm{ord}_\varepsilon(h) \geq 1$, and $h \equiv c \mod \varepsilon$, for some $c \in \mathbb{C} \setminus \{0\} \iff \mathrm{ord}_\varepsilon(h) = 0$ and $c = h(0)$.

Proof. ($\Leftarrow$) Assume that for some $r \in \mathbb{N}$ and $F_i, G_i \in \mathbb{C}[f_1, \ldots, f_m]$ constant free polynomials, for $0 \leq i \leq r-1$, the identity

$$g^r \;=\; \sum_{i=0}^{r-1} \frac{F_i}{1+G_i}\, g^i$$

holds. Let $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{C}(\varepsilon)^n$ be such that for all $1 \leq j \leq m$, $f_j(\mathbf{x}) \equiv 0 \mod \varepsilon$. We show that $f(\mathbf{x}) \equiv 0 \mod \varepsilon$. Since each F_i and G_i is constant-free in $\mathbb{C}[f_1, \ldots, f_m]$, every monomial in F_i (resp. G_i) contains at least one f_j. Therefore, for $0 \leq i \leq r-1$, substituting $\mathbf{x}$ gives $\mathrm{ord}_\varepsilon(F_i) \geq 1$ and $\mathrm{ord}_\varepsilon(G_i) \geq 1$. In particular, $\mathrm{ord}_\varepsilon(1 + G_i(\mathbf{x})) = \min\{\mathrm{ord}_\varepsilon(1), \mathrm{ord}_\varepsilon(G_i(\mathbf{x}))\}$. Let $u := g(\mathbf{x}) \in \mathbb{C}(\varepsilon)$ and define

$$c_i := \frac{F_i(\mathbf{x})}{1+G_i(\mathbf{x})} \in \mathbb{C}(\varepsilon).$$

Therefore, $\mathrm{ord}_\varepsilon(c_i) = \mathrm{ord}_\varepsilon(F_i(\mathbf{x}) - \mathrm{ord}_\varepsilon(1 + G_i(\mathbf{x})) \geq 1$, and $u^r = \sum_{i=0}^{r-1} c_i\, u^i$. Comparing the orders one obtains

$$r\,\mathrm{ord}_\varepsilon(u) \geq \min_{0\leq i\leq r-1}\big(\mathrm{ord}_\varepsilon(c_i u^i)\big) = \min_{0\leq i\leq r-1}\big(\mathrm{ord}_\varepsilon(c_i)+i\,\mathrm{ord}_\varepsilon(u)\big) \geq \min_{0\leq i\leq r-1}(1+i\,\mathrm{ord}_\varepsilon(u)) \geq 1.$$

Since $\mathrm{ord}_\varepsilon(u) \in \mathbb{Z}$, so $\mathrm{ord}_\varepsilon(u) \geq 1$, or equivalently $g(\mathbf{x}) \equiv 0 \mod \varepsilon$. ◀

The converse direction — showing that the geometric condition implies the algebraic condition — is significantly more involved. The first step towards this is to reduce the containment problem for approximative vanishing sets to the problem of emptiness of approximative vanishing set, taking inspiration from the classical *Rabinowitsch trick*. In contrast to the classical Rabinowitsch trick, we do not obtain a single augmented system whose WAN-infeasibility is equivalent to containment. Instead, we obtain one fixed APS-infeasibility instance (see Condition 2) together with a *family* of APS-infeasibility instances indexed by all nonzero scalars $c \in \mathbb{C}$ (see Condition 1). A key additional step is a finiteness reduction: although, Condition 1 is stated universally over all $c \neq 0$, we show that it suffices to check it for only *finitely many* values of c, given by bounded-degree algebraic dependencies arising in our proof. This finiteness reduction is essential for turning the apparent "for-all" obstacle into an efficient (ultimately PSPACE) decision procedure.

The following lemma shows that the geometric condition $\mathsf{AV}(f_1, \ldots, f_m) \subseteq \mathsf{AV}(g)$ can be intuitively rephrased as follows: *Whenever $f_1, \ldots, f_m$ simultaneously approximatively vanish, the value of g can neither diverge nor converge to a non-zero constant $c \in \mathbb{C}$, consequently, it must converge to 0.*

▶ **Lemma 1.** $\mathsf{AV}(f_1, \ldots, f_m) \subseteq \mathsf{AV}(g)$ if and only if *both the following conditions hold.*

1. *For all $c \in \mathbb{C}^\times$, $f_1, \ldots, f_m, g - c$ have no common* APS*, and*
2. *$f_1, \ldots, f_m, y, 1 - yg$ have no common* APS*.*

Proof. We assume $\mathsf{AV}(f_1, \ldots, f_m) \neq \emptyset$ as otherwise $\mathsf{AV}(g)$ always contains $\mathsf{AV}(f_1, ..., f_m)$. Recall that for $g \in \mathbb{C}[x_1, \ldots, x_n]$, $\mathbf{x} \in \mathsf{AV}(g) \iff g(\mathbf{x}) \equiv 0 \mod \varepsilon \iff \mathrm{ord}_\varepsilon(g(\mathbf{x})) \geq 1$. ($\Rightarrow$) Assume, first, that $\mathsf{AV}(f_1, \ldots, f_m) \subseteq \mathsf{AV}(g)$.

- *Proof of condition 1*: Let $c \in \mathbb{C}$. If $f_1, \ldots, f_m, g-c$ had a common APS at some $\mathbf{x} \in \mathbb{C}(\varepsilon)^n$, then for all $1 \leq i \leq m$, $f_i(\mathbf{x}) \equiv 0 \mod \varepsilon$, and $(g-c)(\mathbf{x}) \equiv 0 \mod \varepsilon$. Therefore, $g(\mathbf{x}) \equiv c \mod \varepsilon$. Therefore, $c = 0$, and $f_1, \ldots, f_m$ and $g - c$ have no common APS, for $c \neq 0$.
- *Proof of condition 2.* If $f_1, \ldots, f_m, y, 1 - yg$ had a common APS $(\mathbf{x}, h) \in \mathbb{C}(\varepsilon)^{n+1}$. Then $h \equiv 0 \mod \varepsilon$, and for all $1 \leq i \leq m$, $f_i(\mathbf{x}) \equiv 0 \mod \varepsilon$, and $hg(\mathbf{x}) \equiv 1 \mod \varepsilon$. Since $\mathsf{AV}(f_1, \ldots, f_m) \subseteq \mathsf{AV}(g)$, $\mathrm{ord}_\varepsilon(g(\mathbf{x})) \geq 1$, which contradicts $hg(\mathbf{x}) \equiv 1 \mod \varepsilon$.

($\Leftarrow$) Assume both conditions 1 and 2 hold, and let $\mathbf{x} \in \mathsf{AV}(f_1, \ldots, f_m) \setminus \mathsf{AV}(g)$. Then $\mathrm{ord}_\varepsilon(g(\mathbf{x})) \leq 0$. If $\mathrm{ord}_\varepsilon(g(\mathbf{x})) = 0$, then there is a $c \in \mathbb{C}^\times$ such that $g(\mathbf{x}) \equiv c \mod \varepsilon$. Therefore, $(g-c)(\mathbf{x}) \equiv 0 \mod \varepsilon$, which contradicts the condition 1. On the other hand, if $\mathrm{ord}_\varepsilon(g(\mathbf{x})) = t \leq -1$. Then $(\mathbf{x}, h)$, where $h = \frac{\varepsilon^{-t}}{(\varepsilon^{-t} g(\mathbf{x}))(0)} \equiv 0 \mod \varepsilon$, is in $\mathsf{AV}(f_1, \ldots, f_m, y, 1-yg)$, thus contradicting the condition 2. ◀

While Lemma 1 gives us geometric connection in relation to common solutions, it still doesn't give any insight algebraically into the problem. We now show how we can use the two conditions defined in the lemma to get an algebraic relation between the polynomials $f_1, \ldots, f_m, f$.

▶ **Lemma 2.** *Suppose $f_1, \ldots, f_m, y, 1-yg$ have no common* APS*. Then for some $r \geq 1$,*

$$g^r = \sum_{i=0}^{r} g^i Q_i(f_1, \ldots, f_m),$$

where $Q_r \in \mathbb{C}[y_1, \ldots, y_m]$ is a constant free polynomial.

Proof. Using Theorem 1.1, if $f_1, \ldots, f_m, y, 1-yg$ have no common APS, then there exists a constant free polynomial A in $\mathbb{C}[y_1, \ldots, y_{m+2}]$ such that $A(f_1, \ldots, f_m, y, 1-yg) = 1$, (the polynomial $A(y_1, \ldots, y_{m+2}) - 1$ is an annihilator of $f_1, \ldots, f_m, y, 1-yg$). Now the polynomial $A(f_1, \ldots, f_m, y, 1-yg) - 1 \in \mathbb{C}[x_1, \ldots, x_n, y]$ is the 0 polynomial and remains so in $\mathbb{C}(x_1, \ldots, x_n)[y]$. We can set $y = \frac{1}{g}$, to get

$$A(f_1, \ldots, f_m, \frac{1}{g}, 0) = 1 \tag{1}$$

Therefore, $A(y_1, \ldots, y_{m+2}) \neq 0 \mod y_{m+2}$, otherwise Equation 1 gives us $0 = 1$. Consequently, there is an $r \geq 1$ and $G_i \in C[f_1, \ldots, f_m]$ with G_0 constant free (since A was constant free)such that

$$\sum_{i=0}^{r} \frac{1}{g^i} G_i(f_1, \ldots, f_m) = 1$$

Rearranging, we get $g^r = \sum_{i=0}^{r} g^i Q_i(f_1, \ldots, f_m)$, where Q_r is constant free. ◀

Thus, we have shown how we can use condition (2) to get a polynomial relation. Using this result along with ondition (1), we can show the following.

▶ **Lemma 3.** *Assume that for all $c \in \mathbb{C}^\times$, $f_1, \ldots, f_m, g-c$ have no common* APS*. Let $r \geq 1$, and for $1 \leq i \leq r$ let $Q_i \in \mathbb{C}[y_1, \ldots, y_m]$ be polynomials with Q_r constant free such that*

$$g^r = \sum_{i=0}^{r} g^i Q_i(f_1, \ldots, f_m).$$

Then there are $1 \leq k \leq r$, $l \geq 1$, and constant free polynomials $F_i \in \mathbb{C}[y_1, \ldots, y_m]$, for $1 \leq i \leq l$, such that

$$g^k = \sum_{i=0}^{l} g^i F_i(f_1, \ldots, f_m).$$

Proof. If Q_i is constant free for all i, then we set $k = l = r$ and $F_i = Q_i$ and we are done. Otherwise, there is atleast some Q_i with non-zero constant term. Consider the polynomial $A \in \mathbb{C}[y_1, \ldots, y_m, z]$ given by $z^{r+1}(1 - Q_r) - \left(\sum_{i=1}^{r} Q_{i-1} z^i\right)$. Clearly A is constant free and $A(f_1, \ldots, f_m, g) = 0$. We rewrite each $Q_i = Q'_i + c_i$ such that Q'_i is constant free for each i. We know that $c_r = 0$ and for some $i < r$, $c_i \neq 0$. Then $A = h(z) - \left(\sum_{i=1}^{r+1} Q'_{r-1} z^i\right)$, where $h(z) = z^{r+1} - c_{r-1} z^r - \ldots - c_0 z$ is a polynomial in $\mathbb{C}[z]$.

Clearly $h(z) \neq z^{r+1}$, so there is a finite non-empty subset $S \subset \mathbb{C}^\times$, positive integers e_s, for each $s \in S$, and $1 \leq k \leq r$ such that $h(z) = z^k \prod_{s \in S} (z - s)^{e_s}$. Therefore, $A(f_1, \ldots, f_m, g) = 0$ gives $h(f) = A'(f_1, \ldots, f_m, g)$, where $A' \in \mathbb{C}[y_1, \ldots, y_m, z]$ has no term of the form z^i, as Q'_i are constant free.

Now we use condition (1) from Lemma 1. For all $s \in \mathbb{C}^\times$, $f_1, \ldots, f_m, g - s$ have no APS. In particular, this holds for $s \in S$. Then, by Theorem 1.1, for each $s \in S$ there exists a constant-free polynomial $F_s \in \mathbb{C}[y_1, \ldots, y_m, z]$ such that $F_s(f_1, \ldots, f_m, g - s) = 1$. Write $F_s = G_s(y_1, \ldots, y_m) + z H_s(y_1, \ldots, y_m, z)$ with G_s constant-free. Then

$$\left(\prod_{s \in S} (z - s)^{e_s} H_s(y_1, \ldots, y_m, z - s)^{e_s} - \prod_{s \in S} \left(1 - G_s(y_1, \ldots, y_m)\right)^{e_s}\right)(f_1, \ldots, f_m, g) = 0.$$

Hence, there are $H \in \mathbb{C}[y_1, \ldots, y_m, z]$ and constant-free $G \in \mathbb{C}[y_1, \ldots, y_m]$ such that

$$H(f_1, \ldots, f_m, g)\, h(g) = g^k + g^k \cdot G(f_1, \ldots, f_m).$$

Therefore, $g^k = h(g) H(f_1, \ldots, f_m, g) - g^k \cdot G(f_1, \ldots, f_m)$, and hence

$$g^k = A'(f_1, \ldots, f_m, g) H(f_1, \ldots, f_m, g) - g^k \cdot G(f_1, \ldots, f_m),$$

and the polynomial $A'H - z^k G \in \mathbb{C}[y_1, \ldots, y_m, z]$ has no term of the form z^i. To see this note that the least degree of coefficient of z^i in $A'H$ and G is greater than 1. Therefore, there is an $l \geq 1$, and for $1 \leq i \leq l$, there are constant free polynomials $F_i \in \mathbb{C}[y_1, \ldots, y_m]$ such that $g^k = \sum_{i=0}^{l} F_i(f_1, \ldots, f_m)$. ◀

To summarize, we have obtained the following equivalence $\mathsf{AV}(f_1, \ldots, f_m) \subseteq \mathsf{AV}(g) \iff$ there are $r, k, l \geq 1$ with $k \leq r$, and polynomials Q_i and F_j, for $0 \leq i \leq r$ and $0 \leq j \leq l$ in $\mathbb{C}[y_1, \ldots, y_m]$ with Q_r and all F_j constant free such that

$$g^r = \sum_{i=0}^{r} g^i Q_i(f_1, \ldots, f_m), \quad \text{and} \tag{2}$$

$$g^k = \sum_{i=0}^{l} g^i F_i(f_1, \ldots, f_m). \tag{3}$$

Using this, we now show how we can prove the other direction of Theorem 1.2.

Proof of Theorem 1.2 continued. Suppose $l \leq k$, then we can simply rearrange Equation 3 to get $g^k = \sum_{i=0}^{k-1} \frac{F_i}{1 + F_k} g^i$ and we have the desired characterization. Now assume that $l > k$.

By Lemma 3, we can see that $1 \leq k \leq r$ always. Then we multiply Equation 3 by g^{r-k} on both sides so that the left hand side has exponent r and right hand side has maximum

exponent $l' = l + (r - k)$. Since $l > k$, we have $l' = l + r - k > r$. We will now rename $l' = l$ and thus, we always have $l > r$. We can rewrite Equation 3 as

$$g^r = \sum_{i=0}^{l} g^i F_i(f_1, \ldots, f_m) \tag{4}$$

where $F_0 = \cdots = F_{r-k-1} = 0$. Now, both equations have the same exponent r on the left hand side. Rewrite Equation 2 to get $g^r(1 - Q_r) = \sum_{i=0}^{r-1} g^i Q_i$. Multiplying Equation (4) by $1 - Q_r$, we get

$$\begin{aligned}(1 - Q_r)g^r &= \sum_{i=0}^{l-1} g^i F_i(1 - Q_r) + g^{l-r} F_l g^r (1 - Q_r) \\ &= \sum_{i=0}^{l-1} g^i F_i(1 - Q_r) + g^{l-r} F_l (\sum_{j=0}^{r-1} g^j Q_j) = \sum_{i=0}^{l-1} g^i (F_i(1 - Q_r) + B_i) = \sum_{i=0}^{l-1} g^i H_i\end{aligned}$$

where for $0 \leq i \leq l - r - 1$, $B_i = 0$, and for all $l - r \leq i \leq l - 1$, $B_i = F_l Q_{i-(l-r)}$. Since F_i are constant free, it is easy to see that H_i will be constant free. Hence, starting from Equation 4, where g^r was a linear combination of powers of g up to l we have reduced it to linear combination of powers of g up to $l - 1$ over $\mathbb{C}[f_1, \ldots, f_m]$ such that $g^r = Q_r g^r + \sum_{i=0}^{l-1} H_i(f_1, \ldots, f_m) g^i$ with each H_i, and $Q_r \in \mathbb{C}[y_1, \ldots, y_m]$ being constant free. We can do this inductively as long as $l \geq r$ to eventually get

$$g^r = \sum_{i=0}^{r} g^i F_i(f_1, \ldots, f_m), \tag{5}$$

where $F_i \in \mathbb{C}[y_1, \ldots, y_m]$ is constant free for all i. This can be restated as

$$g^r = \sum_{i=0}^{r-1} g^i \frac{F_i(f_1, \ldots, f_m)}{1 - F_r(f_1, \ldots, f_m)},$$

which is exactly the formulation we desired in Theorem 1.2. ◀

In order to restate our theorem in the language of integral closures, consider the subring $R \coloneqq \mathbb{C}[f_1, \ldots, f_m]$ and the maximal ideal $\mathfrak{m} \coloneqq \langle f_1, \ldots, f_m \rangle$ of R.

▶ Remark 5. Notice that the above ring R differs from the standard polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$. In fact, $R \subseteq \mathbb{C}[x_1, \ldots, x_n]$. Further while $\mathfrak{m}$ is a maximal ideal of R, it might not even be an ideal in $\mathbb{C}[x_1, \ldots, x_n]$.

Let $S \coloneqq R \setminus \mathfrak{m}$. Intuitively, S will contain evaluations at $f_1, \ldots, f_m$ of all polynomials $h \in \mathbb{C}[y_1, \ldots, y_m]$ with constant term not 0. Consider the ring $R_{\mathfrak{m}} \coloneqq S^{-1}R$. It is well known (see [2, Chapter 3]) that in this case $R_{\mathfrak{m}}$ is a local ring, i.e., it will have a unique maximal ideal $\mathfrak{m}R_{\mathfrak{m}}$ which is exactly the set of non units in $R_{\mathfrak{m}}$. It is given by

$$\mathfrak{m}R_{\mathfrak{m}} = \left\{ \frac{h(f_1, \ldots, f_m)}{1 + g(f_1, \ldots, f_m)} \mid h, g \in \mathbb{C}[y_1, \ldots, y_m] \text{ are both constant free} \right\}.$$

We say that an element $g \in \mathbb{C}(x_1, \ldots, x_n)$ is integral over $\mathfrak{m}R_{\mathfrak{m}} \iff$ there is a monic polynomial $h \in R_{\mathfrak{m}}[T]$ with coefficients in the ideal $\mathfrak{m}R_{\mathfrak{m}}$ such that $h(g) = 0$. We are now ready to state our algebro-geometric correspondence in the approximative setting. Thus, Theorem 1.2 can be restated as follows.

▶ **Theorem 2.1.** *Let $f_1, \ldots, f_m, g \in \mathbb{C}[x_1, \ldots, x_n]$. Then $\mathsf{AV}(g) \supseteq \mathsf{AV}(f_1, \ldots, f_n)$ if and only if g is integral over $\mathfrak{m}R_{\mathfrak{m}}$.*

▶ Remark 6. A natural question, is, can we get even simpler characterizations that the one in Theorem 2.1? However, we show two natural candidates do not suffice to fully characterize AV containment.

- *g can't just be characterized by an integral closure without localization:* We show that this is not possible. Consider, $f_1 = xy, f_2 = wz, f_3 = yz-1, g = xz$. Then $\mathsf{AV}(g) \supseteq \mathsf{AV}(f_1, f_2, f_3)$ but $g(1 + f_3) = f_1 f_2$.
- *g can't just be characterized by a radical ideal in the local ring:* A "radical-type" characterization would be of the form $g^r = \frac{F(f_1,\ldots,f_m)}{1+G(f_1,\ldots,f_m)}$. However, we show that this is also not always possible. Consider $f_1 = x^2 - xy, f_2 = y, g = x$, then $g^2 = f_1 + g \cdot f_2$. In fact, $\mathfrak{m}$ is maximal so its radical is itself. Therefore, we really need to use integral closure, just using the radical will not be enough.

We can now see that Theorem 2.1 gives us a very nice characterization analogous to the strong Hilbert's Nullstellensatz (SHN). Recall that SHN says that given polynomials $f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$, a polynomial g vanishes on vanishing set of $f_1, \ldots, f_m$ is equivalent to saying g lies in the radical ideal of $f_1, \ldots, f_m$. Similarly, Theorem 2.1 says that g approximatively vanishes on the common approximative vanishing set of $f_1, \ldots, f_m$ if and only if g is integral over a maximal ideal of a natural fractional subring of $\mathbb{C}(x_1, \ldots, x_n)$ determined by $f_1, \ldots, f_m$.

▶ Remark 7. Conventionally, an element in the integral closure of an ideal implies the element is in the radical of the ideal. Suppose we have some ring R and its ideal I. Let

$$g^r = \sum_{i=0}^{r-1} a_i g^i$$

where $a_i \in I$. Then, it simply implies $g^r \bmod I = 0$ and g lies in the radical of ideal I. This is because g, a_i are coming from the same underlying structure R. However, in our case while the maximal ideal $\mathfrak{m}R_{\mathfrak{m}}$ originates from the ring $R = \mathbb{C}[f_1, \ldots, f_m]$, the polynomial g is instead coming from the larger polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$. Hence, $a_i g^i$ is not necessarily a part of ideal I and hence it might be the case that $a_i g^i \bmod I \neq 0$. Thus, g might not lie in the radical.

Integral closure over $\mathfrak{m}R_{\mathfrak{m}}$ forms an $R_{\mathfrak{m}}$-module: Define $\overline{\mathfrak{m}R_{\mathfrak{m}}}$ to be the integral closure of $\mathfrak{m}R_{\mathfrak{m}}$ in $\mathbb{C}(x_1, \ldots, x_n)$. Let $f, g \in \overline{\mathfrak{m}R_{\mathfrak{m}}}$, then $\mathsf{AV}(f+g) \supseteq \mathsf{AV}(f) \cap \mathsf{AV}(g) \supseteq \mathsf{AV}(f_1, \ldots, f_m)$. Hence $f + g \in \overline{\mathfrak{m}R_{\mathfrak{m}}}$. Now for $r \in R_{\mathfrak{m}}$, $\mathsf{AV}(rf) \supseteq \mathsf{AV}(f) \cup \mathsf{AV}(r) \supseteq \mathsf{AV}(f_1, \ldots, f_m)$. Hence $rf \in \overline{\mathfrak{m}R_{\mathfrak{m}}}$ and $\overline{\mathfrak{m}R_{\mathfrak{m}}}$ is an $R_{\mathfrak{m}}$-module. Clearly, the natural inclusion $R \hookrightarrow R_{\mathfrak{m}}$ makes $\overline{\mathfrak{m}R_{\mathfrak{m}}} \cap \mathbb{C}[x_1, \ldots, x_n]$ an R-module.

Integral closure over $\mathfrak{m}R_{\mathfrak{m}}$ is finitely generated: The next proposition proves that $\overline{\mathfrak{m}R_{\mathfrak{m}}}$ is a finitely generated as an $R_{\mathfrak{m}}$-module. In order to do so, we show that the set of elements of $\mathbb{C}(x_1, \ldots, x_n)$ algebraic over $C(f_1, \ldots, f_m)$ is a finite extension of $C(f_1, \ldots, f_m)$. Then we use that $R_{\mathfrak{m}}$ is an integral Noetherian Nagata domain, i.e., the integral closure of $R_{\mathfrak{m}}$ in a finite extension of its field of fractions is finitely-generated $R_{\mathfrak{m}}$-module (for details see [28, Definition 31(A)]).

▶ **Proposition 2.2.** *Let $R := \mathbb{C}[f_1, \ldots, f_m] \subset \mathbb{C}[x_1, \ldots, x_n]$ and let $\mathfrak{m} = (f_1, \ldots, f_m) \subset R$ be a maximal ideal. Let $\overline{R_{\mathfrak{m}}}$ be the integral closure of $R_{\mathfrak{m}}$ inside $\mathbb{C}(x_1, \ldots, x_n)$. Then $\overline{R_{\mathfrak{m}}}$ is a finitely generated $R_{\mathfrak{m}}$-module.*

Furthermore, the $R_{\mathfrak{m}}$-module

$$\overline{\mathfrak{m}R_{\mathfrak{m}}} \coloneqq \{f \in \overline{R_{\mathfrak{m}}} \mid \exists\ r \geq 1 \text{ and } a_0, \ldots, a_{r-1} \in \mathfrak{m}R_{\mathfrak{m}} \text{ s.t. } f^r = \sum_{i=0}^{r-1} a_i f^i\}$$

is a finitely generated $R_{\mathfrak{m}}$-module.

Proof. Let $K := \mathrm{Frac}(R) = \mathrm{Frac}(R_{\mathfrak{m}}) = \mathbb{C}(f_1, \ldots, f_m) \subset L := \mathbb{C}(x_1, \ldots, x_n)$. Let

$$E := \{\ell \in L : \ \ell \text{ is algebraic over } K\}$$

be the algebraic closure of K in L. Let $r := \mathrm{trdeg}_{\mathbb{C}} K$ (equivalently, $r = \mathrm{trdeg}_{\mathbb{C}} \mathbb{C}(f_1, \ldots, f_m)$). Since $\mathrm{trdeg}_{\mathbb{C}} L = n$, we have $\mathrm{trdeg}_K L = n - r$. Choose a transcendence basis $g_1, \ldots, g_{n-r} \in L$ of L over K. Then L is algebraic over $K(g_1, \ldots, g_{n-r})$. Since the field $L = \mathbb{C}(x_1, \ldots, x_n)$ is a finitely generated algebra over $K(g_1, \ldots, g_{n-r})$, by [2, Proposition 7.9] it is a finite algebraic extension. However, $K(g_1, \ldots, g_{n-r}) \cap E = K$ and therefore, $[E : K] = [EK(g_1, \ldots, g_{n-r}) : K(g_1, \ldots, g_{n-r})] \leq [L : K(g_1, \ldots, g_{n-r})] < \infty$.

If $t \in L$ is integral over $R_{\mathfrak{m}}$, then t is algebraic over K, i.e., $t \in E$. Therefore, the elements of L integral over R are exactly the elements of E integral over R.

Since R is a finitely generated $\mathbb{C}$-algebra, it is a Nagata ring, and localizing preserves the Nagata property [28, Definition 31(A)]; hence $R_{\mathfrak{m}}$ is Noetherian integral domain that is also Nagata. By the Nagata property, $\overline{R_{\mathfrak{m}}}$ is a finite (hence finitely generated) $R_{\mathfrak{m}}$-module.

Now for the final part, we note that $\overline{\mathfrak{m}R_{\mathfrak{m}}}$ is a submodule of a finitely generated module $\overline{R_{\mathfrak{m}}}$ over the Noetherian ring $R_{\mathfrak{m}}$, and we are done. ◀

3 Proof of SAN ∈ PSPACE

In this section, we prove our other main result where we show that the computational problem SAN can be decided in PSPACE. Degree bounds for annihilating polynomials go back to Perron [33] and have been extended further in [3, 21]. We use these bounds together with the "random reductions trick" of GSS to obtain our algorithm. We now present these two key results for completeness.

▶ **Theorem 3.1** (Annihilator bound, Theorem 11, [21]). *Let $h_1, \ldots, h_\ell \in \mathbb{C}[x_1, \ldots, x_n]$ be of degree at most d, and suppose the algebraic rank (transcendence degree) of $\{h_1, \ldots, h_\ell\}$ is r. Then there exists a nonzero annihilating polynomial for $(h_1, \ldots, h_\ell)$ of degree at most $(r+1)d^r$, and there are examples where the minimal annihilator has degree at least d^r.*

▶ **Theorem 3.2** (Random reductions, Theorem 4.6, [17]). *With high probability, we have*

1. *Transcendence degree of $g_1, \ldots, g_{k+1}$ over $\mathbb{C}$ is k.*
2. *The constant term of every annihilator for $g_1, \ldots, g_{k+1}$ is zero* if and only if *the constant term of every annihilator of $f_1, \ldots, f_m$ is zero*

▶ **Theorem.** SAN *is in* PSPACE.

As discussed earlier in Section 1.3, apriori it is not clear how to use the geometric criterion obtained in Lemma 1, or the integral closure formulation obtained in Theorem 1.2 to obtain a PSPACE upper bound. However, leveraging the additional structure of our formulation along with Theorem 3.1, 3.2 we can match the PSPACE upper bound of WAN. We cannot directly use the annihilator obtained from the algebraic characterization in Theorem 1.2 (shown in Equation 5), as we have no guarantees about the degree bound there, since Theorem 3.1 only establishes the singly exponential degree bound for the minimal annihilator of the system

of polynomials, not *all* annihilators. However, we can now use Theorem 3.2 to ensure that it is sufficient to look at the minimal annihilator. Given any system of polynomials, we first calculate its transcendence degree ρ in PSPACE using linear algebra [33, 34, 4]. Then, we reduce to $\rho+1$ polynomials which are random linear combinations which preserve the non-emptiness of AV. Since the annihilator ideal of ℓ polynomials $h_1,\ldots,h_\ell$ is principal if the transcendence degree of the system is $\ell-1$ [17, 21], we can now bound the degree of this generator by Theorem 3.1.

Proof. We achieve the proof by giving a singly-exponential degree upper bound in the equivalent criterion of SAN restated below (see Equation 5).

$$g^r = \sum_{i=0}^{r} g^i F_i(f_1,\ldots,f_m),$$

We got this by combining the criteria obtained in Lemma 2 and Lemma 3, and we show that both of these can be reformulated to have singly exponential degree bounds.

First, we re-inspect the proof of Lemma 2. We started with the condition: $f_1,\ldots,f_m,y,1-yg$ have no common APS, and using the above discussion we can reduce to a system of polynomials $g_1,\ldots,g_{\rho+1}$ where $g_j = c_{j,1}f_1+\cdots+c_{j,m}f_m+c_{j,m+1}y+c_{j,m+2}(1-yg)$, and $A(g_1,\ldots,g_{\rho+1})=1$ such that $A(z_1,\ldots,z_{\rho+1})$ is constant-free. Let d' be the maximum degree of the polynomials $f_1,\ldots,f_m,g$, then clearly degree of each g_j is bounded above by $d=d'+1$. Hence, A has degree bounded by $D=(\rho+1)d^\rho$ by Theorem 3.1, where ρ is the transcendence degree of $f_1,\ldots,y,1-yg$. Similar to proof of Lemma 2, since $A(g_1,\ldots,g_{\rho+1})=1$ holds in $\mathbb{C}[x_1,..,x_n,y]$, it holds in $\mathbb{C}(x_1,\ldots,x_n)[y]$. Hence, we can set $y=\frac{1}{g}$. After this substitution, each

$$g_j = \frac{1}{g}\Big(g(\sum_{i=1}^{m} c_{j,i}f_i)+b_j\Big) = \frac{gq_j(f_1,\ldots,f_m)+b_j}{g}$$

where $b_j\in\mathbb{C}, q_j\in\mathbb{C}[y_1,\ldots,y_m]$ such that q_j is constant-free. Abusing notation, we will now call such polynomials q_j constant-free in $\mathbb{C}[f_1,\ldots,f_m]$. Any monomial of $A(z_1,\ldots,z_{\rho+1})$ is of the form $\alpha\prod_{i=1}^{\rho+1} z_i^{a_i}$ where $t=\sum_i a_i\le D$ and $\alpha\in\mathbb{C}$. On substitution, this monomial becomes $\alpha\frac{1}{g^t}(gq_j+b_j)^{a_j} = \alpha\frac{1}{g^t}(g^tv_t+g^{t-1}v_{t-1}+\ldots+v_0)$ where, v_j are constant-free elements in $\mathbb{C}[f_1,\ldots,f_m]$ for all $1\le j\le t$, and $v_0=b_1^{a_1}\cdots b_{\rho+1}^{a_{\rho+1}}\in\mathbb{C}$. Further, degree of each v_j is bounded by D in terms of f_i. In particular, $A(g_1,\ldots,g_{k+1})=1$ under this substitution gives $\sum_{t=1}^{D}\frac{1}{g^t}(g^tp_{t,t}+\cdots+p_{t,0})=1$ where $p_{t,1},...,p_{t,t}$ are constant free polynomials in $\mathbb{C}[f_1,...,f_m]$ and $p_{t,0}\in\mathbb{C}$ for all $1\le t\le D$. Further, degree of each p_i is bounded by D. Thus, this becomes

$$g^D = (g^Dp_{D,D}+\cdots+p_{D,0})+g(g^{D-1}p_{D-1,D-1}+\cdots+p_{D-1,0})+\cdots+g^{D-1}(gp_{1,1}+p_{1,0})$$

In particular, the coefficient of g^D is $p_{D,D}+p_{D-1,D-1}+\ldots+p_{1,1}$. Since each of these $p_{a,a}$ is constant-free, there will be no term of cg^D for some $c\in\mathbb{C}$ in the right hand side of the equation. In particular, we get an annihilator $g^D = g^DQ_D+g^{D-1}Q_{D-1}\cdots+Q_0$ where Q_D is constant-free and degree of each Q_i is bounded by D. This is exactly like the formulation we obtained in Lemma 2, with the *additional constraint* that D and degree of each Q_i is singly exponential in the input parameters.

Now, we re-inspect the proof of Lemma 3 using this annihilator as a starting point. The corresponding $h(z)$ we get will be a degree $D+1$ polynomial in z and hence has at most D non-zero roots. For each $F_s(f_1,\ldots,f_m,g-s)=1$ in the proof, we now instead use

$F_s(g'_1, \ldots, g'_{\rho+1}) = 1$ where the g'_j are now random linear combinations of $f_1, \ldots, f_m, g-s$ and ρ is their transcendence degree. The degree of F_s will be bounded by D. In particular, each g'_j can be written as $g'_j = p_j + b'_j(g-s)$ where each $p_j \in \mathbb{C}[f_1, \ldots, f_m]$ is linear in f_i and is constant-free, and $b'_j \in \mathbb{C}$. Any monomial of F_s would be of the form $\gamma \prod_{j=1}^{\rho+1}(p_j + b'_j(g-s))^{a'_j}$ where $\sum a'_j = t \leq D$ and $\gamma \in \mathbb{C}$. Thus, any monomial is of the type $(g-s)^t a'_t + (g-s)^{t-1} q'_{t-1} + \ldots + q'_0$ where each q'_i is constant-free in $\mathbb{C}[f_1, \ldots, f_m]$ with degree bounded by $D-i$, and $a'_t \in \mathbb{C}$. Using this we can rewrite $F_s(g'_1, \ldots, g'_{\rho+1})$ as $Q(f_1, \ldots, f_m) + (g-s)P(f_1, \ldots, f_m, g)$ where degree of Q in f_i is bounded by D and degree of P in f_i, g is bounded by D. Also, Q is constant-free in $\mathbb{C}[f_1, \ldots, f_m]$. Using this annihilator in the proof of Lemma 3, the next step is to multiply these for all the roots of $h(z)$, which are at most D. Further, we then multiply with g^k where k is also bounded by D (since k was the multiplicity of 0 as a root of $h(z)$). Thus, finally we get $H(f_1, \ldots, f_m, g)h(g) = g^k + g^k G(f_1, \ldots, f_m)$ where degree of H, G is bounded above by D^2 and G is constant-free in $\mathbb{C}[f_1, \ldots, f_m]$. We can again replace $h(g)$ like in the original proof and get

$$g^k = \sum_{i=0}^{l} g^i F_i(f_1, .., f_m)$$

where l and degree of F_i is bounded by $D' = D^2 + D$, and each F_i is constant-free.

We now show that the obtained bounds are sufficient to put SAN in PSPACE. First thing to note is that $D = (\rho+1)d^\rho$. Since ρ was the transcendence degree of the a system of at most $m+2$ polynomials in $n+1$ variables, $\rho \leq n+1$. Hence, k, D, D' is atmost singly exponential in the input parameters. We can thus set up an exponential-sized system of linear equations in the same way as for computing annihilator using Perron's bound [17, 34, 33], which can be solved in PSPACE [4, 31, 10, 5] ◀

4 Conclusion

In this work, we provide an analog of the SHN for approximative roots of a system of polynomials. Further, we provide a PSPACE upper bound for testing the same, matching the best known upper bound for the Weak Approximative Nullstellensatz. We believe that this work opens up several interesting areas of study in the geometry of approximative roots. Most prominently, defining the notion of dimension to estimate the size of a set of approximative roots is particularly interesting. Similarly, examining how intersection theory of curves translates to this setting is also very intriguing. From a computational perspective, improving the complexity bounds for WAN and SAN, and algorithmically obtaining the generators of the integral closure obtained in Theorem 1.2 is also interesting.

References

1 Matthias Aschenbrenner and Anton Leykin. Degree bounds for gröbner bases in algebras of solvable type. *Journal of Pure and Applied Algebra*, 213(8):1572–1588, 2009. doi:10.1016/j.jpaa.2009.01.004.

2 Michael F. Atiyah and I. G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley, Reading, MA, 1969.

3 Michael Beecken, Johannes Mittmann, and Nitin Saxena. Algebraic independence and blackbox identity testing. *Information and Computation*, 222:2–19, 2013. doi:10.1016/j.ic.2012.10.002.

4 Stuart J Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Information processing letters*, 18(3):147–150, 1984.

5 Allan Borodin, Joachim von zur Gathem, and John Hopcroft. Fast parallel matrix and gcd computations. In *23rd annual symposium on foundations of computer science (sfcs 1982)*, pages 65–71. IEEE, 1982.

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

7 John F. Canny. Some algebraic and geometric computations in PSPACE. Technical Report CSD-88-439, Computer Science Division, University of California, Berkeley, 1988.

8 A. L. Chistov and D. Yu. Grigor'ev. Complexity of quantifier elimination in the theory of algebraically closed fields. In *Mathematical Foundations of Computer Science 1984 (MFCS'84)*, volume 176 of *Lecture Notes in Computer Science*, pages 17–31. Springer, 1984. doi:10.1007/BFb0030287.

9 David Cox, John Little, Donal O'shea, and Moss Sweedler. *Ideals, varieties, and algorithms*. Springer, 1997.

10 Laszlo Csanky. Fast parallel matrix inversion algorithms. In *16th Annual Symposium on Foundations of Computer Science (sfcs 1975)*, pages 11–12. IEEE, 1975.

11 Theo de Jong. An algorithm for computing the integral closure. volume 26, pages 273–277, 1998. doi:10.1006/jsco.1998.0211.

12 Thomas Dubé. The structure of gröbner bases and the complexity of buchberger's algorithm. *SIAM Journal on Computing*, 19(4):750–773, 1990. doi:10.1137/0219053.

13 Antonio J Engler and Alexander Prestel. *Valued fields*. Springer, 2005.

14 Michael A Forbes and Amir Shpilka. Explicit noether normalization for simultaneous conjugation via polynomial identity testing. In *International Workshop on Approximation Algorithms for Combinatorial Optimization*, pages 527–542. Springer, 2013.

15 Michael A. Forbes and Amir Shpilka. A PSPACE construction of a hitting set for the closure of small algebraic circuits. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing (STOC 2018)*, pages 1180–1192, 2018. doi:10.1145/3188745.3188792.

16 Mika Göös, Alexandros Hollender, Siddhartha Jain, Gilbert Maystre, William Pires, Robert Robere, and Ran Tao. Separations in proof complexity and tfnp. *Journal of the ACM*, 71(4):1–45, 2024.

17 Zeyu Guo, Nitin Saxena, and Amit Sinhababu. Algebraic dependencies and pspace algorithms in approximative complexity over any field. *Theory of Computing*, 15(1):1–30, 2019.

18 Deirdre Haskell and Yoav Yaffe. Ganzstellensätze in theories of valued fields. *Journal of Mathematical Logic*, 8(01):1–22, 2008.

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

20 Doug J. Ierardi. The complexity of quantifier elimination in the theory of an algebraically closed field. Technical Report TR89-1030, Cornell University, 1989.

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

22 Elisabeth Leonie Kayser. Computational complexity of polynomial subalgebras. In *Proceedings of the 2025 International Symposium on Symbolic and Algebraic Computation*, ISSAC '25, page 337–344, New York, NY, USA, 2025. Association for Computing Machinery. doi:10.1145/3747199.3747578.

23 Simon Kochen. Integer valued rational functions over the p-adic numbers: A p-adic analogue of the theory of real fields. In *Proc. Symp. Pure Math*, volume 12, pages 57–73, 1969.

24 Pascal Koiran. Hilbert's nullstellensatz is in the polynomial hierarchy. *Journal of complexity*, 12(4):273–286, 1996.

25 János Kollár. Sharp effective nullstellensatz. *Journal of the American Mathematical Society*, pages 963–975, 1988.

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

27 Noa Lavi. A ganzstellensatz for semialgebraic sets and a boundedness criterion for rational functions. *Communications in Algebra*, 44(1):26–39, 2016. doi:10.1080/00927872.2014.930473.

28 Hideyuki Matsumura. *Commutative Algebra*. 2022. Revised and modernized edition; typeset by the TEXromancers. Original edition: 1980. URL: https://aareyanmanzoor.github.io/assets/matsumura-CA.pdf.

29 Ernst W. Mayr and Albert R. Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. In *Advances in Mathematics*, 1982.

30 James S Milne. *Algebraic geometry*. Allied Publishers, 2012.

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

32 Ketan D. Mulmuley. Geometric complexity theory V: Equivalence between blackbox derandomization of PIT and derandomization of noether's normalization lemma. In *Proceedings of the 53rd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2012)*, pages 629–638, 2012.

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

34 Arkadiusz Płoski. Algebraic dependence of polynomials after o. perron and some applications. *Computational Commutative and Non-Commutative Algebraic Geometry*, pages 167–173, 2005.

35 Alexander Prestel and Cydara C Ripoll. Integral-valued rational functions on valued fields. *manuscripta mathematica*, 73(1):437–452, 1991.

36 JL Rabinowitsch. Zum hilbertschen nullstellensatz. *Mathematische Annalen*, 102(1):520–520, 1930.

37 Wolmer V. Vasconcelos. *Integral Closure: Rees Algebras, Multiplicities, Algorithms*. Springer Monographs in Mathematics. Springer, 2005.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il