Electronic Colloquium on Computational Complexity, Report No. 217 (2026)

Hitting Sets for Polynomials with Small Partial Derivative Spaces

Shubham Bhardwaj* Ramprasad Saptharishi*

28 September 2026

Abstract

We give an explicit hitting set of size $\text{poly}(n, d, r)$ for the class of n-variate degree-d polynomials whose partial derivative space is bounded by r, over any field $\mathbb{F}$ of characteristic zero. In particular, this yields a polynomial sized hitting set for the class of depth-3 powering circuits.

The main technical insight is the construction of a "formal derivation" and properties of the associated Wronskian with respect to this derivation, which was previously studied by Moura [Mou04] in a very different context. The proofs in this paper are elementary and completely self-contained.

AI disclosure: The proof of this result was obtained during conversations [Ast26] with OpenAI GPT-6 Astra. The proof presented in this writeup is a rewriting (in the authors' words) of the proof obtained by the AI model in a form that we believe is understandable to researchers.

1 Introduction

Algebraic circuits are the most natural computational model for studying the complexity of multivariate polynomials via the number of basic operations (additions, multiplications) required to compute it. The field of algebraic complexity broadly deals with the classification of polynomials based on their computational complexity, and also on algorithmic questions regarding polynomials provided via such computations.

Two of the most important aspects of this study are the question of lower bounds (i.e., finding explicit polynomials that cannot be computed by small algebraic circuits), and the algorithmic task of polynomial identity testing (i.e., given a circuit C, algorithmically check if C is computing the zero polynomial). In the context of polynomial identity tests, there are two types of algorithms — whitebox PITs (where the algorithm is given the entire circuit description), or blackbox PITs (where

*Tata Institute of Fundamental Research, Mumbai, India. Email: {shubham.bhardwaj,ramprasad}@tifr.res.in. Research supported by the Department of Atomic Energy, Government of India, under project number RTI400112, and Google and SERB Research Grants.

ISSN 1433-8092

we are only provided evaluation access to the circuit). Although the questions of proving lower bounds and constructing deterministic PITs appear to be of very different flavours, they are intimately connected to each other. Several classical results [HS80, Agr05, KI04, CKS19, GKSS19] show that a strong enough lower bound for circuits can be used to obtain efficient deterministic polynomial identity tests, and vice-versa. Although similar statements when specialised to restricted circuit classes are known in some contexts [DSY09, Oli16, CKS19, BKR+26], this has broadly been a guiding principle for the study of lower bound and PITs for subclasses of circuits. Historically, a polynomial identity test for a class $\mathscr{C}$ has been a successor to a lower bound for the class $\mathscr{C}$, and is often heavily inspired by the techniques used in the lower bound proof. Paradoxically, even 'natural' "barriers" for proving algebraic circuit lower bounds stem from the conjectured existence of *succinct polynomial identity tests* [GKSS17, FSV18].

Over the recent years, there has been quite a lot of progress made towards proving lower bounds for natural subclasses of algebraic circuits, and also constructing whitebox and blackbox PITs for them [AGKS15, GKST15, GG20, LST21, AF22, GOS+26]. One subclass of circuits that has been just shy of a full resolution has been the class of *depth*-3 *powering circuits*.

Depth-3 powering circuits: A depth-3 powering circuit computes a polynomial of the form $f = c_1\ell_1^d + \cdots + c_s\ell_s^d$ where each ℓ_i is a linear polynomial over the underlying variables. This is the circuit analogue of the classical notion of Waring rank, where the Waring rank of a polynomial f is the smallest s such that f can be written as sum of s powers of linear forms. Saxena [Sax08] gave the first lower bound for this class of circuits, and also a polynomial time white-box PIT. A different white-box PIT was also given by Kayal [Kay10]. Agrawal, Saha and Saxena [ASS13], and Forbes and Shpilka [FS13] gave the first $n^{O(\log n)}$-size hitting set for this class (among constructions of quasi-polynomial sized hitting sets for other more general classes), and Forbes, Saptharishi and Shpilka [FSS14] improved this to $n^{O(\log\log n)}$.

The key weakness of the above model that enabled all the lower bounds and PITs was the observation that any k-th order partial derivative of $f = c_1\ell_1^d + \cdots + c_s\ell_s^d$ is a linear combination of $\ell_1^{d-k}, \ldots, \ell_s^{d-k}$ and thus the space of all possible partial derivatives of f (which we shall denote by $\partial^{=*}(f)$) is only $O(sd)$-dimensional. The hitting sets constructed by [ASS13, FSS14] also extend to the (potentially) more general class of polynomials f whose space of all possible partial derivatives is low-dimensional. It continues to remain open if such polynomials with low-dimensional space of partial derivatives admit a not-too-large representation as a depth-3 powering circuit.

The main result of this paper is an explicit polynomial-sized hitting set for this class of polynomials over a characteristic zero field.

Theorem 1.1. *Let $\mathbb{F}$ be a field of characteristic zero. For any $n, r \geq 0$, there is an explicit polynomial map $(G_1(t), \ldots, G_n(t)) \in \mathbb{F}[t]^n$ with $\deg G_i \leq O(nr^2)$ such that if $f(x_1, \ldots, x_n)$ is a polynomial such that*

$\dim \partial^* f \leq r$, *then*

$$f(x_1, \ldots, x_n) = 0 \Leftrightarrow f(G_1(t), \ldots, G_n(t)) = 0.$$

In particular, the above yields a $\mathrm{poly}(n, d, s)$-sized hitting set for the class of size s, degree d depth-3 powering circuits. In fact, $G_i(t)$ can just be instantiated to be the *truncated Taylor series* of $-\ln(1 - it)$:

$$G_i(t) = it + \frac{(it)^2}{2} + \frac{(it)^3}{3} + \cdots + \frac{(it)^B}{B} \quad \text{for } i = 1, \ldots, n$$

where $B = nr^2 + r$.

Using power series for constructing hitting-set generators: The general structure of constructing a hitting-set generator via power series is reminiscent of the randomised PIT algorithms of Chen and Kow [CK97], or Lewin and Vadhan [LV98]. We describe the setting of [CK97] (the setting of [LV98] is very similar with irreducible polynomial playing the role of primes). They show that if $f(x_1, \ldots, x_n)$ is a nonzero polynomial, then

$$f(\pm\sqrt{p_{1,1}} \pm \cdots \pm \sqrt{p_{1,\ell}}, \cdots, \pm\sqrt{p_{n,1}} \pm \cdots \pm \sqrt{p_{n,\ell}}) \neq 0$$

where $p_{i,j}$'s are distinct primes with $\ell = O(\log \deg(f))$. However, an efficient cannot evaluate f at these irrationals of infinite precision. [CK97] show that if the signs are randomly chosen, we can achieve an error of ε as long as we truncate the above irrationals to precision $B(\varepsilon)$. This results in randomised algorithm for PIT where reducing the error is achieved by increasing the precision (and thereby the running time) but keeping the number of random bits fixed.

The PIT in this paper is similar in the sense that the generator is a set of algebraically independent power series $(P_i(t) := -\log(1 - it) \ : \ i \in [n])$. For the class of polynomials with low-dimensional partial derivative space, we show that

$$0 \neq f \implies f(P_1(t), \ldots, P_n(t)) \neq 0 \bmod t^B$$

for a not-too-large B.

Mrinal Kumar pointed out to us that $f(e^{zt}, e^{z^2 t}, \ldots, e^{z^n t}) \neq 0 \bmod t^s$ for any nonzero s-sparse polynomial (thus giving a bivariate, low degree, hitting set generator for sparse polynomials). It would be interesting to see if this applies to a more general class of polynomials.

1.1 Proof overview

Suppose $f(x_1, \ldots, x_n)$ is a nonzero polynomial with low dimensional partial derivative space, and say $g_1, \ldots, g_r$ is a basis of $\partial^{=*}(f)$ with $g_r = f$. Let us consider $f(P_1(t), \ldots, P_n(t))$ for some univariates $P_1, \ldots, P_n$, and we wish to know if $f(P_1(t), \ldots, P_n(t))$ can be divisible by t^B for a large B. Then,

$$\frac{d}{dt}(f \circ P) = \sum_{i=1}^{n} \frac{dP_i}{dt} \cdot (\partial_{x_i} f)(P_1, \ldots, P_n).$$

Inspired by the RHS above, let us define a "derivative operator" D_P given by

$$D_P : \mathbb{F}[t][x_1, \ldots, x_n] \to \mathbb{F}[t][x_1, \ldots, x_n]$$
$$D_P(g(t, x_1, \ldots, x_n)) = \partial_t g + \left(\frac{dP_1}{dt}\right) \cdot \partial_{x_1} g + \cdots + \left(\frac{dP_n}{dt}\right) \cdot \partial_{x_n} g.$$

Thus, if $D := D_P$, we have

$$\frac{d^i}{dt^i}(f \circ P) = D^i(f) \circ P.$$

Thus, if $f \circ P$ was divisible by t^B, then $D^i f \circ P$ is divisible by t^{B-i}.

For any derivation D, there is a well-studied notion of a D-Wronskian of a set of polynomials $g_1, \ldots, g_r$ given by

$$W_D(g_1, \ldots, g_r) = \det \begin{bmatrix} g_1 & g_2 & \cdots & g_r \\ D(g_1) & D(g_2) & \cdots & D(g_r) \\ \vdots & \vdots & \ddots & \vdots \\ D^{r-1}(g_1) & D^{r-1}(g_2) & \cdots & D^{r-1}(g_r) \end{bmatrix}.$$

The above is a polynomial in $t, x_1, \ldots, x_n$ of not-too-large degree. The first observation is that, since the set $\{g_1, \ldots, g_r\}$ is ∂_x-closed (i.e., any $\partial_{x_i} g_j$ can be written as a linear combination of other elements in this set), one can argue that the above D-Wronskian satisfies the property that $\partial_{x_i} W_D(g_1, \ldots, g_r) = 0$ for all $i \in [n]$. In other words, the above is just a pure polynomial in t and does not depend on $x_1, \ldots, x_n$ at all! Thus, we can substitute $x_i \mapsto P_i$ in the above matrix and that does not affect $W_D(g_1, \ldots, g_r)$.

Focusing on the last column of the matrix $W_D(g_1, \ldots, g_r) \circ P$, since we assumed that $f \circ P = 0 \bmod t^B$, we observe that every entry in the last column is divisible by t^{B-r+1}. Thus, in particular $W_D(g_1, \ldots, g_r)$ must be divisible by t^{B-r+1}. However, we know that $W_D(g_1, \ldots, g_r)$ is a polynomial in t of suitably bounded degree (and composing by P does not increase the degree at all since the

polynomial did not depend on x at all). If B is set to be sufficiently large, we have our contradiction.

Unless of course, $W_D(g_1, \ldots, g_r)$ happens to be the zero polynomial, and we get nothing! Thus, we would like D to have the property that $W_D(g_1, \ldots, g_r) \neq 0$. Standard Wronskians capture linear independence, and it seems reasonable to hope that $g_1, \ldots, g_r$ being linearly independent should allow us to argue that $W_D(g_1, \ldots, g_r) \neq 0$. For this, however, we need some properties satisfied by the derivative operator D, namely that its kernel is just the base field $\mathbb{F}$. More formally, if

$$\{h \in \mathbb{F}(t)(x_1, \ldots, x_n) \ : \ D(h) = 0\} = \mathbb{F},$$

then $W_D(g_1, \ldots, g_r) = 0$ if and only if $g_1, \ldots, g_r$ are $\mathbb{F}$-linearly dependent.

Flipping this around, suppose we had a convenient "derivative operator" $D = \partial_t + \sum_{i=1}^{n} b_i(t)\partial_{x_i}$ that has the property that $\ker(D) = \mathbb{F}$, then we can reverse-engineer $P_1(t), \ldots, P_n(t)$ such that $\frac{dP_i}{dt} = b_i(t)$ and the above argument essentially goes through. In this write-up, we work with a specific derivative operator

$$\tilde{D} := \partial_t + \sum_{i=1}^{n} \frac{i}{1 - it} \cdot \partial_{x_i}$$

which indeed has the property that $\ker(\tilde{D}) = \mathbb{F}$ (Lemma 2.6). A derivative operator of a similar shape, and its associated Wronskian, appears to have been studied by Moura [Mou04] in a very different context. For this choice, we have $P_i(t) = -\ln(1 - it)$. Of course, these are infinite power series, and the $b_i(t)$'s are rational functions and not polynomials. But both of these are minor technicalities that are easily fixed.

Remark 1.2. *To be more precise, the properties we need from $\tilde{D}$ for our proof are that* $\ker \tilde{D} = \mathbb{F}$ *and that $\tilde{D}$ commutes with ∂_{x_i} for all i. The latter property essentially forces $\tilde{D}$ to be of the form $a(t)\partial_t + \sum_i b_i(t)\partial_{x_i}$, and the above derivation is the simplest of this form that satisfies* $\ker \tilde{D} = \mathbb{F}$. ◊

Notation

- Throughout this paper we assume that we will be working with a field of characteristic zero. We use $\mathbb{F}[\![t]\!]$ to denote the ring of formal power series in t
- We use $\partial_{x_i}(f)$ as a shorthand for $\frac{\partial f}{\partial x_i}$.
- We abuse notation and sometimes use x to denote the tuple $(x_1, \ldots, x_n)$. Notations such as $\deg_x$ or $\mathrm{Hom}_x^{=d}$ will denote the degree or homogeneous component with respect to the variables $(x_1, \ldots, x_n)$.

2 Derivations and D-Wronskians

Definition 2.1 (Derivations)**.** *Let $R = \mathbb{F}(t)[x_1, \ldots, x_n]$ and let $\mathbb{K} = \mathrm{Frac}(R) = \mathbb{F}(t)(x_1, \ldots, x_n)$. A map $D : R \to R$ is said to be a* derivation *if*

- *D is $\mathbb{F}$-linear, i.e. $D(\alpha f + \beta g) = \alpha D(f) + \beta D(g)$ for $\alpha, \beta \in \mathbb{F}$ and $f, g \in R$,*
- *D satisfies the Leibniz product rule, i.e. $D(fg) = fD(g) + gD(f)$.*

A derivation D over $R = \mathbb{F}(t)[x_1, \ldots, x_n]$ extends uniquely to a derivation over $\mathbb{K} = \mathrm{Frac}(R)$ by defining $D(B^{-1}) = -B^{-2} \cdot D(B)$ for any $0 \neq B \in R$, thus extending as

$$D(A/B) = \frac{B \cdot D(A) - A \cdot D(B)}{B^2}.$$

For a derivation D, we define its field[1] of constants *to be the set* $\ker D = \{h \in \mathbb{K} : D(h) = 0\}$. *We shall say that D has a* trivial field of constants *if* $\ker D = \mathbb{F}$. ◊

The notion of D-Wronskian, which is a generalisation of standard Wronskians in the context of a derivation, was studied by Moura [Mou04] in the context of hyperelliptic integrals. The following lemma shows that D-Wronskians also capture linear independence, provided D has a trivial field of constants.

Lemma 2.2 (Wronskians with respect to derivatives with trivial field of constants)**.** *Suppose D is a derivation that has a trivial field of constants. Then, for any $g_1, \ldots, g_m \in R$, we have that $g_1, \ldots, g_m$ are $\mathbb{F}$-linearly independent if and only if the D-Wronskian (denoted by $W_D(g_1, \ldots, g_m)$ below) is nonzero:*

$$W_D(g_1, \ldots, g_m) = \det \begin{bmatrix} g_1 & g_2 & \cdots & g_m \\ D(g_1) & D(g_2) & \cdots & D(g_m) \\ \vdots & \vdots & \ddots & \vdots \\ D^{m-1}(g_1) & D^{m-1}(g_2) & \cdots & D^{m-1}(g_m) \end{bmatrix}$$

Proof. One direction is clear — if $g_1, \ldots, g_m$ are linearly dependent then clearly $W_D(g_1, \ldots, g_m) = 0$.

Thus, we are left to show that $W_D(g_1, \ldots, g_m) = 0$ implies that $g_1, \ldots, g_m$ are linearly dependent. The proof would be by induction on m (the base case of $m = 1$ is immediate). Assume that $m \geq 2$ and $W_D(g_1, \ldots, g_m) = 0$. If M refers to the matrix of the D-Wronskian, this implies that there is some nonzero $\boldsymbol{c} = (c_1, \ldots, c_m) \in \mathbb{K}^m$ such that $M\boldsymbol{c} = 0$. If $c_m = 0$, then $(c_1, \ldots, c_{m-1})$ is a nonzero kernel for the $(m-1) \times (m-1)$ D-Wronskian matrix of $g_1, \ldots, g_{m-1}$ which would force by induction that $g_1, \ldots, g_{m-1}$ are dependent. Thus, we may assume without loss of generality that $c_m = 1$ (by scaling $\boldsymbol{c}$ if necessary).

[1] Literature also uses the phrase 'ring of constants' to refer to this. It is not hard to check that it is indeed a field.

Since $M\boldsymbol{c} = 0$, we have

$$\begin{aligned}
&\text{For } i = 0, \ldots, m-1, \quad \sum c_j \cdot D^i(g_j) = 0 \\
\therefore \text{For } i = 0, \ldots, m-2, \quad 0 = D\left(\sum_{j=1}^{m} c_j D^i(g_j)\right) &= \sum_{j=1}^{m} \left(D(c_j) \cdot D^i(g_j) + c_j \cdot D^{i+1}(g_j)\right) \\
&= \sum_{j=1}^{m} D(c_j) \cdot D^i(g_j) \\
&= \sum_{j=1}^{m-1} D(c_j) \cdot D^i(g_j).
\end{aligned}$$

Thus, $(D(c_1), \ldots, D(c_{m-1}))$ is a kernel vector for the D-Wronskian matrix of $g_1, \ldots, g_{m-1}$. By induction, we know this matrix is invertible and hence $D(c_1) = D(c_2) = \cdots = D(c_{m-1}) = 0$ which forces each $c_i \in \mathbb{F}$ (and $c_m = 1$). Thus, focusing on just the first row of M we have that $c_1 g_1 + \cdots + c_m g_m = 0$ and thus we have an $\mathbb{F}$-linear dependency between $g_1, \ldots, g_m$. □

2.1 A concrete derivation with trivial field of constants

For this paper, we would need a derivation D that has a trivial field of constants over $\mathbb{K} = \text{Frac}(R)$. Note that D having a trivial kernel over the ring $R = \mathbb{F}(t)[x_1, \ldots, x_n]$ does not necessarily imply that the kernel is trivial over $\mathbb{K}$ also (a standard example is $D = \partial_t + x^2\partial_x$ which has a trivial kernel over R but $D(t + \frac{1}{x}) = 0$).

Definition 2.3. *Let $\tilde{D} : R \to R$ be the derivation given by*

$$\tilde{D} := \partial_t + \sum_{i=1}^{n} \frac{i}{1 - it} \cdot \partial_{x_i}$$

and, clearing denominators, define

$$D := Q(t) \cdot \tilde{D} = Q(t) \cdot \partial_t + \sum_{i=1}^{n} b_i(t) \cdot \partial_{x_i} \tag{2.4}$$

where $Q(t) = \prod_{i=1}^{n}(1 - it)$ and $b_i(t) = i \cdot Q(t)/(1 - it) = i \prod_{j \neq i}(1 - jt)$. ◊

Remark. *There appears to be a rich literature on the study of* derivation fields *with numerous examples of derivations that have a trivial field of constants. The derivation defined above appears to be a special case of a broader class of derivations called Shamsuddin derivations. Nowicki's book [Now94] provides a fairly comprehensive study of this field.* ◊

The following is a simple observation about the degrees of $D(g)$ compared to g.

Observation 2.5 (Degree bounds when acted by D)**.** *For any $g \in \mathbb{F}[t][x_1, \ldots, x_n]$, we have*

- $\deg_x D(g) \leq \deg_x g$
- $\deg_t D(g) \leq n + \deg_t g$.

Proof. Follows immediately from definition since $\deg Q(t) = n$ and $\deg b_i(t) = n - 1$. □

We now present the key property of D, which is that it has a trivial field of constants.

Lemma 2.6 (D has trivial field of constants)**.** *Let D be the derivation from Definition 2.3. Then, for all $h \in \mathbb{K} = \mathrm{Frac}(R)$, we have that $D(h) = 0$ if and only if $h \in \mathbb{F}$. In other words, D has a trivial field of constants.*

Proof. We will first show that for all $h \in R = \mathbb{F}(t)[x_1, \ldots, x_n]$ we have $D(h) = 0$ if and only if $h \in \mathbb{F}$. Suppose $h \in R$ with $D(h) = 0$. Let h_i denote the degree i (in x) homogeneous component of h and let $\deg_x h = d$. If $d = 0$, we are done and so we may assume that $d \geq 1$. Focusing on the degree d part of $D(h) = 0$, we have

$$\begin{aligned} 0 = \mathrm{Hom}_x^{=d}(D(h)) &= Q(t) \cdot \partial_t h_d \\ \implies \partial_t h_d &= 0. \end{aligned}$$

Thus, the highest-degree homogeneous part of h is t-free. Now focusing on the homogeneous part of degree $d - 1$, we have

$$\begin{aligned} 0 = \mathrm{Hom}_x^{=d-1}(D(h)) &= Q(t) \cdot \left(\partial_t h_{d-1} + \sum_{i=1}^{n} \frac{i}{1 - it} \cdot \partial_{x_i} h_d \right) \\ \implies \partial_t h_{d-1} &= -\sum_{i=1}^{n} \frac{i}{1 - it} \cdot \partial_{x_i} h_d. \end{aligned}$$

Note that h_d is independent of t and thus so is $\partial_{x_i} h_d$. Hence, if $\partial_{x_i} h_d \neq 0$, then the RHS has a simple pole (of order 1) at $t = 1/i$ but $\partial_t h_{d-1}$ can never have simple poles. (To see this, write the *partial fraction* decomposition of $h_{d-1} \in \mathbb{F}(t)$ as

$$h_{d-1}(t) = p(t) + \sum_{a} \sum_{j \geq 1} \frac{c_{a,j}}{(t - a)^j}$$

for some polynomial $p(t)$ and constants $c_{a,j} \in \mathbb{F}$ for finitely many a. Differentiating term by term, $p(t)$ contributes a polynomial and thus no poles, while each term $c_{a,j}(t - a)^{-j}$ contributes $-jc_{a,j}(t - a)^{-j-1}$ and thus a pole of order $j + 1$ at a. Hence, $\partial_t h_{d-1}$ has no pole of order exactly 1 at any point.) Thus, the only way the above can be zero is if $\partial_{x_i} h_d = 0$ for all $i \in [n]$, which is absurd when $d \geq 1$. Thus, $d = 0$ and hence $h \in \mathbb{F}$.

To extend this to the fraction field, suppose $h = A/B$ where $A, B \in \mathbb{F}(t)[x_1, \ldots, x_n]$ with A and B being coprime, with $D(h) = 0$. Then,

$$\begin{aligned} D(A) = D(B \cdot h) &= BD(h) + hD(B) \\ &= h \cdot D(B) = \frac{A}{B} \cdot D(B) \\ \implies B \cdot D(A) &= A \cdot D(B). \end{aligned}$$

Since A and B are coprime, this implies that B divides $D(B)$ and A divides $D(A)$. Since $\deg_x D(A) \leq \deg_x A$ this implies that $D(A) = cA$ and $D(B) = cB$ for some $c \in \mathbb{F}(t)$. Consider the highest degree (in x) part A_d of A, and let $\alpha(t)$ be the coefficient of some degree-d (in x) monomial m of A. Then, by tracing the coefficient of m in the equality $D(A) = cA$, we get

$$\begin{aligned} Q(t) \cdot \partial_t \alpha &= c \cdot \alpha \\ \implies D\left(\frac{A}{\alpha}\right) &= \frac{D(A)}{\alpha} + A \cdot D(1/\alpha) = \frac{D(A)}{\alpha} - \frac{A \cdot Q(t) \cdot \partial_t \alpha}{\alpha^2} \\ &= A \cdot \left(\frac{c}{\alpha} - \frac{Q(t) \cdot \partial_t \alpha}{\alpha^2}\right) = 0. \end{aligned}$$

But since $\frac{A}{\alpha} \in \mathbb{F}(t)[x_1, \ldots, x_n]$, we have that $\frac{A}{\alpha} \in \mathbb{F}$. Similarly, $\frac{B}{\alpha} \in \mathbb{F}$, and thus $\frac{A}{B} \in \mathbb{F}$ as well. □

2.2 Relating D to the map P

We now connect the above derivation to the map $(P_1, \ldots, P_n)$ with $P_i = \sum_{j \geq 1} \frac{(it)^j}{j} = -\ln(1 - it)$. Note that P_i's are power series in t. For any polynomial $f(t, x_1, \ldots, x_n) \in \mathbb{F}[t][x_1, \ldots, x_n]$, the composition $f \circ P = f(P_1, \ldots, P_n)$ is a well-defined element of $\mathbb{F}[\![t]\!]$.

Lemma 2.7 (Relating D to the map P)**.** *Let $P_i(t) \in \mathbb{F}[\![t]\!]$ be defined as $\sum_{j \geq 1} \frac{(it)^j}{j}$, the Taylor series of $-\ln(1 - it)$, and let $P = (P_1, \ldots, P_n)$. Then, for any $f(t, x_1, \ldots, x_n) \in \mathbb{F}[t][x_1, \ldots, x_n]$, we have*

$$Q(t) \cdot \frac{d}{dt}(f \circ P) = D(f) \circ P$$

as elements of $\mathbb{F}[\![t]\!]$.

Proof. Note that $\frac{dP_i}{dt} = \frac{i}{1-it}$. Then, by the chain rule of derivatives,

$$\begin{aligned} \frac{d}{dt} f(t, P_1, \ldots, P_n) &= \partial_t f + \sum_{i=1}^{n} ((\partial_{x_i} f) \circ P) \cdot \frac{dP_i}{dt} \\ &= \partial_t f + \sum_{i=1}^{n} ((\partial_{x_i} f) \circ P) \cdot \frac{i}{1 - it} \\ &= \frac{1}{Q(t)} \cdot (D(f) \circ P). \end{aligned}$$

□

Corollary 2.8. *For any $B \geq i \geq 0$ and $f(t, x_1, \ldots, x_n) \in \mathbb{F}[t][x_1, \ldots, x_n]$, if $f \circ P = 0 \bmod t^B$ then $D^i(f) \circ P = 0 \bmod t^{B-i}$.*

Proof. The proof follows by induction on i via applications of Lemma 2.7. The case of $i = 0$ is trivial. Assume that $D^i(f) \circ P = t^{B-i} \cdot h(t)$ for some $h(t) \in \mathbb{F}[\![t]\!]$. Then,

$$\begin{aligned} D^{i+1}(f) \circ P &= D(D^i(f)) \circ P = Q(t) \cdot \frac{d}{dt}\left(D^i(f) \circ P\right) \\ &= Q(t) \cdot \frac{d}{dt}(t^{B-i} \cdot h(t)) \\ &= 0 \bmod t^{B-(i+1)}. \end{aligned}$$

That completes the inductive step, and thus the proof of the corollary. □

2.3 D-Wronskian of a derivative-closed set

The following is a simple yet important observation that makes the above machinary applicable to the setting of polynomials of low dimensional partial derivative space.

Lemma 2.9 (Wronskian of derivative-closed sets are x-independent)**.** *Let $D : R \to R$ be the derivation defined in Definition 2.3, and let $g_1, \ldots, g_m \in \mathbb{F}[x_1, \ldots, x_n]$ be a set of polynomials such that for all $i \in [m]$ and $j \in [n]$ we have that $\partial_{x_j} g_i \in \mathbb{F}\text{-span}(g_1, \ldots, g_m)$. Then, the D-Wronskian $W_D(g_1, \ldots, g_m)$ is a rational function in t and is independent of the x_i's.*

Furthermore, if $g_1, \ldots, g_m$ are linearly independent and D is a derivation with a trivial field of constants, then $W_D(g_1, \ldots, g_m)$ is a nonzero element of $\mathbb{F}(t)$.

Proof. As taking partial derivatives with respect to any x_i reduces the degree in x_i, we may assume that $g_1, \ldots, g_m$ are arranged in increasing order of degree. Thus,

$$\partial_{x_i} g_k = \sum_{j=1}^{k-1} c_{ijk} g_j$$

for some constants $c_{ijk} \in \mathbb{F}$. Also, since g_k does not depend on t we have $\partial_t g_k = 0$ and hence

$$\begin{aligned} \partial_{x_i}(D(g_k)) &= \partial_{x_i}\left(Q(t) \cdot \partial_t g_k + Q(t) \cdot \sum_{j=1}^{n} \frac{j}{1-jt} \cdot \partial_{x_j} g_k\right) \\ &= \partial_{x_i}\left(Q(t) \cdot \sum_{j=1}^{n} \frac{j}{1-jt} \cdot \partial_{x_j} g_k\right) \\ &= Q(t) \cdot \sum_{j=1}^{n} \frac{j}{1-jt} \cdot \partial_{x_i} \partial_{x_j} g_k \\ &= D(\partial_{x_i} g_k). \end{aligned}$$

Therefore, we have $\partial_{x_i}(D^\ell(g_k)) = D^\ell(\partial_{x_i} g_k)$ and hence

$$\partial_{x_i}(D^\ell(g_k)) = D^\ell\left(\sum_{j=1}^{k-1} c_{ijk} g_j\right) = \sum_{j=1}^{k-1} c_{ijk} D^\ell(g_j)$$

Thus, if C_k is the k-th column of the Wronskian matrix, we have that

$$\partial_{x_i} C_k = \sum_{j=1}^{k-1} c_{ijk} C_j$$

Hence taking partial derivatives of $W_D(g_1, g_2, \ldots, g_m)$ with respect to x_i and using the product rule for determinants, we have

$$\begin{aligned}
\partial_{x_i} W_D(g_1, g_2, \ldots, g_m) &= \sum_{k=1}^{m} \det(C_1, \ldots, C_{k-1}, \partial_{x_i} C_k, C_{k+1}, \ldots, C_m) \\
&= \sum_{k=1}^{m} \sum_{j<k} c_{ijk} \det(C_1, \ldots, C_{k-1}, C_j, C_{k+1}, \ldots, C_m) \\
&= 0.
\end{aligned}$$

Thus, since $\partial_{x_i} W_D(g_1, \ldots, g_m) = 0$ for each $i \in [n]$, we have that $W_D(g_1, \ldots, g_m)$ must indeed be independent of the x_i's and is just a rational function in t.

And if $g_1, \ldots, g_m$ are linearly independent and D has a trivial field of constants, then Lemma 2.2 asserts that $W_D(g_1, \ldots, g_m)$ is in fact a nonzero element of $\mathbb{F}(t)$. □

Remark. *The lemma holds more generally for any derivation D of the form $a_0(t)\partial_t + \sum_i a_i(t)\partial_{x_i}$ that satisfies $D(\partial_{x_i} f) = \partial_{x_i} D(f)$.* ◊

3 Constructing the hitting set

Now we have all the ingredients to prove Theorem 1.1. We state it here in a slightly different form from which Theorem 1.1 would readily follow.

Theorem 3.1. *Suppose $0 \neq f(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$ such that $\dim \partial^{=*}(f) \leq r$. Let $P_1(t), \ldots, P_n(t) \in \mathbb{F}[\![t]\!]$ be defined as*

$$P_i(t) = \sum_{j \geq 1} \frac{(it)^j}{j}$$

Then, $f(P_1(t), \cdots, P_n(t)) \neq 0 \bmod t^B$ for $B = nr^2 + r$.

Theorem 1.1 follows from the above since we may truncate each P_i to the first B terms and retain the nonzeroness of f.

Proof of Theorem 3.1. For simplicity, let us assume that $\dim \partial^{=*} f = r$ (else we will replace r with the actual dimension in the proof below). Let $g_1, g_2, \ldots, g_r$ be a basis of the space V_f of all partial derivatives of f in increasing order of degree with $g_r = f$. Let $P(t) = (P_1(t), P_2(t), \ldots, P_n(t))$ where $P_i(t) = -\ln(1 - it)$ for $i = 1, \ldots, n$.

Assume on the contrary that $f \circ P$ is divisible by t^B for $B = nr^2 + r$. Consider the D-Wronskian $W_D(g_1, \ldots, g_r)$. By Lemma 2.6, we know D has a trivial field of constants, and Lemma 2.2 asserts that $W_D(g_1, \ldots, g_r)$ is nonzero since $g_1, \ldots, g_r$ are linearly independent. Since each entry $D^i(g_j)$ of the Wronskian matrix is in fact a polynomial in $t, x_1, \ldots, x_n$, we have that $W_D(g_1, \ldots, g_r)$ is a nonzero element of $\mathbb{F}[t, x_1, \ldots, x_n]$. Furthermore, by Lemma 2.9, it is independent of x and hence $W_D(g_1, \ldots, g_r) = w(t)$ is nonzero polynomial in t. By Observation 2.5, row i of the D-Wronskian matrix of $W_D(g_1, \ldots, g_r)$ has polynomials of degree at most $n \cdot (i-1)$ in t and therefore $w(t)$ is a nonzero polynomial of degree at most nr^2.

On the other hand, $W_D(g_1, \ldots, g_r) \circ P = w(t)$ (since w is independent of x-variables), and the last column of the matrix is the vector $[f \circ P, Df \circ P, D^2 f \circ P, \cdots, D^{r-1} f \circ P]$. By Corollary 2.8, this entire column is therefore divisible by $t^{B-(r-1)}$. Therefore, $w(t)$ is divisible by $t^{B-(r-1)}$, but this is impossible if $B \geq nr^2 + r$ since $w(t)$ is a polynomial of degree at most nr^2.

Thus we have that $f \circ P \neq 0 \bmod t^{nr^2+r}$. □

Acknowledgements: We'd like to thank several members in the community (especially Robert Andrews, Umang Bhaskar, Prerona Chatterjee, Prahladh Harsha, Mrinal Kumar, Anamay Tengse) for numerous philophical discussions on whether to not to publish this.

References

[AF22] Robert Andrews and Michael A. Forbes. Ideals, determinants, and straightening: proving and using lower bounds for polynomial ideals. In *STOC '22: 54th Annual ACM SIGACT Symposium on Theory of Computing, Rome, Italy, June 20 - 24, 2022*, pages 389–402. ACM, 2022.

[AGKS15] Manindra Agrawal, Rohit Gurjar, Arpita Korwar, and Nitin Saxena. Hitting-Sets for ROABP and Sum of Set-Multilinear Circuits. *SIAM Journal of Computing*, 44(3):669–697, 2015. Pre-print available at `arXiv:1406.7535`.

[Agr05] Manindra Agrawal. Proving Lower Bounds Via Pseudo-random Generators. In *Proceedings of the 25th International Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2005)*, volume 3821 of *Lecture Notes in Computer Science*, pages 92–105. Springer, 2005.

[ASS13] Manindra Agrawal, Chandan Saha, and Nitin Saxena. Quasi-polynomial hitting-set for set-depth-Δ formulas. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC 2013)*, pages 321–330, 2013. `eccc:TR12-113`.

[Ast26] OpenAI GPT 6 Astra. Building a polynomial hitting set, 2026.

[BKR+26] Somnath Bhattacharjee, Mrinal Kumar, Shanthanu S. Rai, Varun Ramanathan, Ramprasad Saptharishi, and Shubhangi Saraf. Closure under Factorization from a Result of Furstenberg. In *Proceedings of the 58th Annual ACM Symposium on Theory of Computing, STOC 2026, Salt Lake City, UT, USA, June 22-26, 2026*, pages 174–185. ACM, 2026.

[CK97] Zhi-Zhong Chen and Ming-Yang Kao. Reducing Randomness via Irrational Numbers. In *Proceedings of the 29th Annual ACM Symposium on Theory of Computing (STOC 1997)*, pages 200–209, 1997.

[CKS19] Chi-Ning Chou, Mrinal Kumar, and Noam Solomon. Closure Results for Polynomial Factorization. *Theory of Computing*, 15(13):1–34, 2019.

[DSY09] Zeev Dvir, Amir Shpilka, and Amir Yehudayoff. Hardness-Randomness Tradeoffs for Bounded Depth Arithmetic Circuits. *SIAM J. Comput.*, 39(4):1279–1293, 2009.

[FS13] Michael A. Forbes and Amir Shpilka. Quasipolynomial-Time Identity Testing of Noncommutative and Read-Once Oblivious Algebraic Branching Programs. In *Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2013)*, pages 243–252, 2013. Full version at `arXiv:1209.2408`.

[FSS14] Michael A. Forbes, Ramprasad Saptharishi, and Amir Shpilka. Hitting sets for multilinear read-once algebraic branching programs, in any order. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing (STOC 2014)*, pages 867–875, 2014.

[FSV18] Michael A. Forbes, Amir Shpilka, and Ben Lee Volk. Succinct Hitting Sets and Barriers to Proving Lower Bounds for Algebraic Circuits. *Theory of Computing*, 14(1):1–45, 2018.

[GG20] Zeyu Guo and Rohit Gurjar. Improved Explicit Hitting-Sets for ROABPs. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2020, Virtual Conference, August 17-19, 2020*, volume 176 of *LIPIcs*, pages 4:1–4:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

[GKSS17] Joshua A. Grochow, Mrinal Kumar, Michael E. Saks, and Shubhangi Saraf. Towards an algebraic natural proofs barrier via polynomial identity testing. *CoRR*, abs/1701.01717, 2017. Pre-print available at `arXiv:1701.01717`.

[GKSS19] Zeyu Guo, Mrinal Kumar, Ramprasad Saptharishi, and Noam Solomon. Derandomization from Algebraic Hardness: Treading the Borders. In *60th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2019, Baltimore, Maryland, USA, November 9-12, 2019*, pages 147–157. IEEE Computer Society, 2019.

[GKST15] Rohit Gurjar, Arpita Korwar, Nitin Saxena, and Thomas Thierauf. Deterministic Identity Testing for Sum of Read-once Oblivious Arithmetic Branching Programs. In *Proceedings of the 30th Annual Computational Complexity Conference (CCC 2015)*, pages 323–346, 2015. `arXiv:1411.7341`.

[GOS+26] Abhibhav Garg, Rafael Oliveira, Akash Kumar Sengupta, Nir Shalmon, and Amir Shpilka. Rank Bounds and Polynomial-Time PIT for Σˆk Π Σ Π^2 Circuits. In *41st Computational Complexity Conference, CCC 2026, Lisbon, Portugal, August 3-6, 2026*, volume 383 of *LIPIcs*, pages 17:1–17:18. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2026.

[HS80] Joos Heintz and Claus-Peter Schnorr. Testing Polynomials which Are Easy to Compute (Extended Abstract). In *Proceedings of the 12th Annual ACM Symposium on Theory of Computing (STOC 1980)*, pages 262–272. ACM, 1980.

[Kay10] Neeraj Kayal. Algorithms for Arithmetic Circuits. *Electronic Colloquium on Computational Complexity (ECCC)*, 2010.

[KI04] Valentine Kabanets and Russell Impagliazzo. Derandomizing Polynomial Identity Tests Means Proving Circuit Lower Bounds. *Computational Complexity*, 13(1-2):1–46, 2004. Preliminary version in the *35th Annual ACM Symposium on Theory of Computing (STOC 2003)*.

[LST21] Nutan Limaye, Srikanth Srinivasan, and Sébastien Tavenas. Superpolynomial Lower Bounds Against Low-Depth Algebraic Circuits. In *Proceedings of the 62nd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2021)*, pages 804–814. IEEE, 2021. Preliminary version in the Electronic Colloquium on Computational Complexity (ECCC), Technical Report TR21-081.

[LV98] Daniel Lewin and Salil P. Vadhan. Checking Polynomial Identities over any Field: Towards a Derandomization? In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC 1998)*, pages 438–447, 1998.

[Mou04] Claire Moura. On the multiplicity of hyperelliptic integrals. *Nonlinearity*, 17(6):2057–2068, August 2004.

[Now94] Andrzej Nowicki. *Polynomial derivations and their rings of constants*. 10 1994.

[Oli16] Rafael Oliveira. Factors of low individual degree polynomials. *Comput. Complex.*, 25(2):507–561, 2016.

[Sax08] Nitin Saxena. Diagonal Circuit Identity Testing and Lower Bounds. In *Proceedings of the 35th International Colloquium on Automata, Languages and Programming (ICALP 2008)*, pages 60–71, 2008. Pre-print available at `eccc:TR07-124`.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il