Electronic Colloquium on Computational Complexity, Report No. 168 (2026)

A Note on Deterministic PIT for $\Sigma^{[3]}\Pi\Sigma\Pi^{[\delta]}$ Circuits

Zeyu Guo*

September 5, 2026

Abstract

Guo and Wang gave a deterministic polynomial-time black-box identity test for $\Sigma^{[3]}\Pi\Sigma\Pi^{[\delta]}$ circuits over fields of arbitrary characteristic, for constant δ, assuming that one product gate is squarefree. This note communicates an observation suggested by a large language model: the squarefreeness assumption can be removed by combining the normalization argument of Guo and Wang with the Mason–Stothers theorem.

1 Introduction

Garg, Oliveira, and Sengupta [GOS25] gave a deterministic polynomial-time black-box polynomial identity testing (PIT) algorithm for $\Sigma^{[3]}\Pi\Sigma\Pi^{[\delta]}$ circuits over fields of characteristic zero, for every constant δ. Guo and Wang [GW25] proved such a result over fields of arbitrary characteristic under the additional assumption that one of the three product gates is squarefree. Their argument uses constructive normalization of algebraic curves.

A large language model pointed out to us that the squarefreeness assumption in our result can be removed by combining the argument of Guo–Wang with the Mason–Stothers theorem [Mas84, Sto81], also known as the function field analogue of the ABC conjecture. In this note, we communicate this result. The resulting hitting set has size $(nd)^{O_\delta(1)}$, where n is the number of variables and d bounds the degrees of the product gates, and works over arbitrary fields.

After removing a common gcd and common Frobenius powers, we use the following dichotomy. If some irreducible factor of a product gate does not divide the output polynomial, the normalization argument of [GW25] applies without a squarefreeness assumption. Otherwise, the radical of the product of the three summands divides the nonzero output. Its degree is consequently at most the degree of a summand. A line restriction that preserves the distinct factors and their multiplicities cannot turn this sum into an identity: the Mason–Stothers theorem would give the opposite strict inequality.

The Mason–Stothers theorem and its variants have also appeared in recent work on algebraic computation. Shpilka and Tal [ST26] use a strengthening of the theorem in their deterministic PIT and reconstruction algorithms for $\Sigma^{[r]}\wedge^{[d]}\Sigma^{[s]}\Pi^{[\delta]}$ circuits over fields of characteristic zero or sufficiently large characteristic. Kedlaya and Kopparty [KK24, Section 2.2, Item 6] also remark that their lemma on consecutive zero coefficients in polynomial powers can be deduced from the Mason–Stothers theorem.

2 Removing the Squarefreeness Assumption

Let $\mathbb{F}$ be a field and let $\overline{\mathbb{F}}$ be its algebraic closure. All factorizations and squarefreeness statements below are over $\overline{\mathbb{F}}$. A hitting set for a class of polynomials is a set containing a nonzero evaluation

*The Ohio State University. Email: zguotcs@gmail.com.

ISSN 1433-8092

of every nonzero member of the class. As in [GW25], evaluation points may lie in an extension field of $\mathbb{F}$. Explicitness and running time are understood in the algebraic model used there.

For integers $n, d, \delta \geq 1$, let $\mathcal{C}^{\hom}_{n,d,\delta}$ be the class of polynomials admitting a representation

$$F = \sum_{i=0}^{k-1} F_i \qquad \text{with} \qquad F_i = c_i \prod_{j=1}^{m_i} f_{i,j} \tag{1}$$

where $k \leq 3$, $c_i \in \overline{\mathbb{F}}^{\times}$, the $f_{i,j}$ are nonconstant homogeneous polynomials of degree at most δ, and all F_i have the same degree $D \leq d$. Empty products are allowed. We work with circuits over $\overline{\mathbb{F}}$, which also include circuits originally defined over $\mathbb{F}$.

We first recall the homogeneous theorem of Guo–Wang.

Theorem 2.1 (Guo–Wang [GW25, Theorem 1.1])**.** *There is an explicit hitting set of size $(nd)^{O_\delta(1)}$ for the polynomials in $\mathcal{C}^{\hom}_{n,d,\delta}$ admitting a representation (1) in which at least one F_i is squarefree.*

In [GW25], squarefreeness is used to find an irreducible factor θ of a summand that does not divide the output. Specifically, in the proof of [GW25, Lemma 5.5], after excluding the case $F_1 + F_2 = cF_0$, the equality of degrees gives $F_0 \nmid F_1 + F_2$. Since F_0 is squarefree, some irreducible factor θ of F_0 does not divide $F_1 + F_2$, and hence does not divide F. Once the existence of such a factor θ is assumed, the subsequent arguments do not require squarefreeness. The following lemma records this consequence of the proofs in [GW25].

Lemma 2.2 (Implicit in the proofs of [GW25, Lemmas 5.5, 5.7, and 5.8])**.** *There is an explicit set $H_{\mathrm{fac}} \subseteq \overline{\mathbb{F}}^n$ of size $(nd)^{O_\delta(1)}$ with the following property. Suppose $F = F_0 + F_1 + F_2 \in \mathcal{C}^{\hom}_{n,d,\delta}$ and there is an irreducible polynomial θ dividing some F_i but not dividing F. Then H_{fac} contains a nonzero evaluation of F. No squarefreeness assumption is imposed on the F_i.*

Without squarefreeness, a factor θ as in Lemma 2.2 need not exist. It remains to handle the case where every irreducible factor of $F_0F_1F_2$ divides F. We address this case using the Mason–Stothers theorem.

First, we need an explicit family of affine lines such that restriction to a suitable line preserves the degrees, squarefreeness, and pairwise coprimality of the factors.

Lemma 2.3 (Preserving factors on a line)**.** *For $n, s, \delta \geq 1$, there is an explicit family $\mathcal{L}$ of affine maps $\ell : \overline{\mathbb{F}} \to \overline{\mathbb{F}}^n$, of size $(ns)^{O_\delta(1)}$, such that for every collection of $r \leq s$ pairwise nonassociate irreducible polynomials $\theta_1, \ldots, \theta_r \in \overline{\mathbb{F}}[x_1, \ldots, x_n]$ of degrees at most δ, some $\ell \in \mathcal{L}$ satisfies*

(i) $\deg(\theta_i \circ \ell) = \deg \theta_i$ *for all i;*
(ii) *every $\theta_i \circ \ell$ is squarefree;*
(iii) *the $\theta_i \circ \ell$ are pairwise coprime.*

Proof. Write $\ell(t) = a + tb$ with $2n$ parameters (a, b). The desired conditions are ensured by the nonvanishing of the leading coefficient $\mathrm{lc}_t\, \theta_i(a + tb)$, the discriminant $\mathrm{Disc}_t\, \theta_i(a + tb)$, and the resultant $\mathrm{Res}_t\big(\theta_i(a + tb), \theta_j(a + tb)\big)$ for all relevant i and j. These are $O(s^2 + s)$ nonzero polynomials in the coordinates of a and b, each of degree $O(\delta^2)$ and hence with at most $(2n)^{O(\delta^2)}$ monomials. We can use the explicit hitting-set construction of Klivans and Spielman [KS01] for sparse polynomials to hit these polynomials simultaneously. The resulting set of pairs (a, b), and thus the family $\mathcal{L}$, has size $(ns)^{O_\delta(1)}$. □

We use the following characteristic-free version of the Mason–Stothers theorem; see [Jeo14].

Theorem 2.4 (Mason–Stothers)**.** *Let $a, b, c \in \overline{\mathbb{F}}[t]$ be nonzero pairwise coprime polynomials satisfying $a + b + c = 0$. If a', b', c' are not all zero, then*

$$\max\{\deg a, \deg b, \deg c\} < \deg \mathrm{rad}(abc).$$

We now address the case where every irreducible factor of $F_0F_1F_2$ divides F. We further assume that $\gcd(F_0, F_1, F_2) = 1$; a circuit satisfying this condition is called *simple*. The reduction to simple circuits is given in the proof of Theorem 2.6.

Lemma 2.5 (The case where every factor divides the sum)**.** *Let $F = F_0 + F_1 + F_2 \neq 0$, where the F_i are nonzero homogeneous polynomials of a common degree $d > 0$, with $\gcd(F_0, F_1, F_2) = 1$. Suppose every irreducible factor of $F_0F_1F_2$ divides F. In positive characteristic p, suppose additionally that the F_i are not all p-th powers. If an affine line map ℓ satisfies the three conditions of Lemma 2.3 for all distinct factors of $F_0F_1F_2$, then $F \circ \ell \neq 0$.*

Proof. The F_i are pairwise coprime. Indeed, a factor dividing two summands also divides F by hypothesis, and hence divides the third, contradicting the common gcd being one. Put $R = \operatorname{rad}(F_0F_1F_2)$. Since $R \mid F \neq 0$ and $\deg F = d$, we have $\deg R \leq d$.

Write $\overline{F}_i = F_i \circ \ell$. The line conditions give $\deg \overline{F}_i = d$, $\gcd(\overline{F}_i, \overline{F}_j) = 1$ (for $i \neq j$), and $\deg \operatorname{rad}(\overline{F}_0\overline{F}_1\overline{F}_2) = \deg R$. Their derivatives are not all zero. This is immediate in characteristic zero. In characteristic p, at least one factor of one F_i has multiplicity not divisible by p, since $\overline{\mathbb{F}}$ is a perfect field and that F_i is not a p-th power. The line preserves this multiplicity at each root of the corresponding restricted factor, so the corresponding $\overline{F}_i$ is not a p-th power and has nonzero derivative. If $\overline{F}_0 + \overline{F}_1 + \overline{F}_2 = 0$, Theorem 2.4 gives $d < \deg R$, contradicting $\deg R \leq d$. □

We can now remove the squarefreeness hypothesis entirely.

Theorem 2.6 (Homogeneous circuits without squarefreeness)**.** *For every field $\mathbb{F}$ and every $n, d, \delta \geq 1$, there is an explicit hitting set $H \subseteq \overline{\mathbb{F}}^n$ of size $(nd)^{O_\delta(1)}$ for $\mathcal{C}^{\hom}_{n,d,\delta}$. No restriction is imposed on the multiplicities of the factors.*

Proof. Explicit hitting sets for circuits with at most two summands are known, e.g., using Lemma 2.3, so we focus on circuits with three summands. First construct a hitting set H_0 for nonzero sums $F = F_0 + F_1 + F_2$ whose summands have a common positive degree at most d, have common gcd one, and, in characteristic p, are not all p-th powers. If an irreducible factor of a summand does not divide F, apply Lemma 2.2. Otherwise, apply Lemma 2.5 together with Lemma 2.3, using $s = 3d$, and evaluate at $d + 1$ distinct parameter values on each line. Taking the union of these evaluations with H_{fac} gives H_0 of size $(nd)^{O_\delta(1)}$.

Now consider an arbitrary nonzero sum $F = F_0 + F_1 + F_2$ in $\mathcal{C}^{\hom}_{n,d,\delta}$. Let $G = \gcd(F_0, F_1, F_2)$ and $Q_i = F_i/G$ for $i \in \{0, 1, 2\}$. In characteristic p, if the Q_i are nonconstant, let q be the largest power of p dividing all irreducible-factor multiplicities in all three Q_i. Otherwise, including in characteristic zero, set $q = 1$. Since $\overline{\mathbb{F}}$ is a perfect field, we may write $Q_i = P_i^q$ over $\overline{\mathbb{F}}$, and hence

$$F = G(P_0 + P_1 + P_2)^q.$$

The P_i have common gcd one and a common degree at most d, and their irreducible factors have degree at most δ. If the common degree of the P_i is positive, then in positive characteristic the P_i are not all p-th powers by the maximality of q. Thus H_0 hits $P_0 + P_1 + P_2$; the nonzero constant case is immediate.

The polynomial G is a product of at most d irreducible factors of degree at most δ, counted with multiplicity. The construction of Klivans–Spielman [KS01], used in the proof of Lemma 2.3, therefore gives an explicit set H_1 of size $(nd)^{O_\delta(1)}$ that hits every such G.

A standard technique then yields a hitting set for $F = G(P_0 + P_1 + P_2)^q$: take $d + 1$ distinct points on every line joining a point of H_0 to a point of H_1. The resulting set has size $(nd)^{O_\delta(1)}$. □

The homogeneity assumption can also be removed as in [GW25]. We present a proof here for completeness.

Corollary 2.7 (Arbitrary $\Sigma^{[3]}\Pi\Sigma\Pi^{[\delta]}$ circuits)**.** *Let $\mathbb{F}$ be any field. The class of polynomials*

$$F = \sum_{i=0}^{k-1} c_i \prod_{j=1}^{m_i} f_{i,j}, \qquad k \leq 3,$$

where $\deg f_{i,j} \leq \delta$ and every product gate has degree at most d, has an explicit hitting set of size $(nd)^{O_\delta(1)}$ in $\overline{\mathbb{F}}^n$. In particular, for constant δ, this gives deterministic polynomial-time black-box PIT over arbitrary fields, without homogeneity or squarefreeness assumptions.

Proof. Homogenize all summands to the same degree $D \leq d$ with a new variable x_0. Each homogenized summand is a product of homogenized bottom factors and possibly repeated copies of x_0, so the bottom degree bound remains δ. The homogenized sum $\widetilde{F}$ is nonzero if and only if F is nonzero. Apply Theorem 2.6 in $n+1$ variables.

To dehomogenize the hitting set H, fix a set $T \subseteq \overline{\mathbb{F}}^{\times}$ of size $d+1$ and use

$$H^* = \{(a_1/t, \ldots, a_n/t) : (a_0, a_1, \ldots, a_n) \in H,\ t \in T\}.$$

If $\widetilde{F}(a_0, a_1, \ldots, a_n) \neq 0$, the polynomial $\widetilde{F}(t, a_1, \ldots, a_n)$ is nonzero and has degree at most d. It is therefore nonzero at some $t \in T$, and $\widetilde{F}(t, a_1, \ldots, a_n) = t^D F(a_1/t, \ldots, a_n/t)$. Thus H^* is a hitting set, with only a factor of $d+1$ increase in size. □

References

[GOS25] Abhibhav Garg, Rafael Oliveira, and Akash Kumar Sengupta. Rank bounds and PIT for depth-4 circuits with top fan-in 3 and constant bottom fan-in via a non-linear Edelstein–Kelly theorem. In *2025 IEEE 66th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 2143–2169. IEEE, 2025.

[GW25] Zeyu Guo and Siki Wang. Deterministic depth-4 PIT and normalization, 2025. arXiv:2504.15143.

[Jeo14] Sangtae Jeong. Two generalized abc theorems for $\mathbb{F}_q[t]$. *Journal of Number Theory*, 139:80–90, 2014.

[KK24] Kiran S. Kedlaya and Swastik Kopparty. On the degree of polynomials computing square roots mod p. In Rahul Santhanam, editor, *39th Computational Complexity Conference (CCC 2024)*, volume 300 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 25:1–25:14, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[KS01] Adam R. Klivans and Daniel A. Spielman. Randomness efficient identity testing of multivariate polynomials. In *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing*, pages 216–223. ACM, 2001.

[Mas84] R. C. Mason. Equations over function fields. In Hendrik Jager, editor, *Number Theory Noordwijkerhout 1983*, volume 1068 of *Lecture Notes in Mathematics*, pages 149–157. Springer, Berlin, Heidelberg, 1984.

[ST26] Amir Shpilka and Yann Tal. Polynomial identity testing and reconstruction for depth-4 powering circuits of high degree, 2026. arXiv:2602.20832.

[Sto81] W. W. Stothers. Polynomial identities and Hauptmoduln. *The Quarterly Journal of Mathematics*, 32(3):349–370, 1981.

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il