

# On the Existence of Algebraically Natural Proofs

Prerona Chatterjee

STCS, TIFR

Mumbai, India

prerona.chatterjee.tifr@gmail.com

Mrinal Kumar

Dept. of CS&amp;E, IIT Bombay

Mumbai, India

mrinal@cse.iitb.ac.in

C Ramya

STCS, TIFR

Mumbai, India

c.ramya@tifr.res.in

Ramprasad Saptharishi\*

STCS, TIFR

Mumbai, India

ramprasad@tifr.res.in

Anamay Tengse

STCS, TIFR

Mumbai, India

anamay.tengse@gmail.com

**Abstract**—For every constant  $c > 0$ , we show that there is a family  $\{P_{N,c}\}$  of polynomials whose degree and algebraic circuit complexity are polynomially bounded in the number of variables, that satisfies the following properties:

- For every family  $\{f_n\}$  of polynomials in VP, where  $f_n$  is an  $n$  variate polynomial of degree at most  $n^c$  with bounded integer coefficients and for  $N = \binom{n^c+n}{n}$ ,  $P_{N,c}$  vanishes on the coefficient vector of  $f_n$ .
- There exists a family  $\{h_n\}$  of polynomials where  $h_n$  is an  $n$  variate polynomial of degree at most  $n^c$  with bounded integer coefficients such that for  $N = \binom{n^c+n}{n}$ ,  $P_{N,c}$  does not vanish on the coefficient vector of  $h_n$ .

In other words, there are efficiently computable equations for polynomials in VP that have small integer coefficients. In fact, we also prove an analogous statement for the seemingly larger class VNP. Thus, in this setting of polynomials with small integer coefficients, this provides evidence *against* a natural proof like barrier for proving algebraic circuit lower bounds, a framework for which was proposed in the works of Forbes, Shpilka and Volk [1], and Grochow, Kumar, Saks and Saraf [2].

Our proofs are elementary and rely on the existence of (non-explicit) hitting sets for VP (and VNP) to show that there are efficiently constructible, low degree equations for these classes and also extend to finite fields of small size.

**Keywords**-Computational Complexity; Algebraic Complexity; Algebraically Natural Proofs; Lower Bounds;

## I. INTRODUCTION

The quest for proving strong lower bounds for algebraic circuits is one of the fundamental challenges in algebraic complexity, and maybe the most well studied one. And yet, progress on this problem has been painfully slow and sporadic. Perhaps the only thing more frustrating than the inability to prove such lower bounds is the inability to come up with plausible approaches towards them. This lack of progress on the problem and a dearth of potential approaches towards

it has spurred some work towards understanding the viability of some of the current lower bound approaches; the idea being that a good sense of what approaches will *not* work would aid in the search of approaches that *might* work.

In the broader context of lower bounds in computational complexity, there are various results of this flavor which establish that various families of techniques cannot be used for proving very strong lower bounds, e.g., the barrier of *Relativization* due to Baker, Gill and Solovay [3], that of *Algebraization* due to Aaronson and Wigderson [4] and that of *Natural Proofs* due to Razborov and Rudich [5].<sup>1</sup> While none of these barrier results are directly applicable to the setting of algebraic computation, there have been recent attempts towards generalizing these ideas to the algebraic set up. A key notion in this line of work is the notion of *algebraically natural proofs* alluded to and defined in the works of Aaronson and Drucker [6], Forbes, Shpilka and Volk [1], and Grochow, Kumar, Saks and Saraf [2].

We now discuss this notion, starting with a discussion of *Natural Proofs* which motivated the definition.

### A. The Natural Proofs framework of Razborov and Rudich

Razborov and Rudich [5] noticed that underlying many of the lower bound proofs known in Boolean circuit complexity, there was some common structure. They formalized this common structure via the notion of a *Natural Property*, which we now define.

**Definition I.1.** A subset  $\mathcal{P} \subseteq \{f : \{0,1\}^n \rightarrow \{0,1\}\}$  of Boolean functions is said to be a natural property useful against a class  $\mathcal{C}$  of Boolean circuits if the following are true.

- **Usefulness.** Any Boolean function  $f : \{0,1\}^n \rightarrow \{0,1\}$  that can be computed by a Boolean circuit

<sup>1</sup>Sometimes, these results are conditional, as in [5].

in  $\mathcal{C}$  does not have the property  $\mathcal{P}$ .

- **Constructivity.** Given the truth table of a Boolean function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ , whether or not it has the property  $\mathcal{P}$  can be decided in time polynomial in the length of the input, i.e. in time  $2^{O(n)}$ .
- **Largeness.** For all large enough  $n$ , at least a  $2^{-O(n)}$  fraction of all  $n$  variate Boolean functions have the property  $\mathcal{P}$ .  $\diamond$

A proof that a certain family of Boolean functions cannot be computed by circuits in  $\mathcal{C}$  is said to be a *natural lower bound proof* if the proof (perhaps implicitly) proceeds via establishing a natural property useful against  $\mathcal{C}$ , and showing that the candidate hard function has this property. Razborov and Rudich then showed that most of the Boolean circuit lower bound proofs that we know, e.g., lower bounds for  $\text{AC}^0$  circuits [7], [8] or lower bounds for  $\text{AC}^0[\oplus]$  circuits [9], [10] fit into this framework (maybe with some work) and hence are *natural* in this sense. Further, they argue that under standard cryptographic assumptions, the proof of a lower bound against any sufficiently rich circuit class (such as the class  $\text{P/poly}$ ) cannot be natural! Thus, under standard cryptographic assumptions, most of the current lower bound techniques are not strong enough to show super-polynomial lower bounds for general Boolean circuits.

We now move on to discuss a relatively recent analog of the notion of Natural Proofs, formalized in the context of algebraic computation.

### B. Algebraically Natural Proofs

Algebraic complexity is the study of computational questions about multivariate polynomials as formal objects. The basic model of computation here, an algebraic circuit, is an algebraic analog of a Boolean circuit with the gates of the circuit being labeled by  $+$  (sum) and  $\times$  (product) gates as opposed to Boolean functions.<sup>2</sup> The algebraic analog of  $\text{P/poly}$  is the class  $\text{VP}$  of polynomial families  $\{f_n\}$ , where  $f_n$  is an  $n$  variate polynomial of degree and algebraic circuit size  $\text{poly}(n)$ . A fundamental question in this setting is to come up with explicit families of polynomials, i.e. polynomials in the class  $\text{VNP}$  (the algebraic analog of  $\text{NP/poly}$ ), which are not in  $\text{VP}$ . While the state of the art of lower bounds for algebraic circuits is a bit better than that for Boolean circuits, with slightly super linear lower bounds having been shown by Strassen [11] and Baur & Strassen [12], this lower bound has seen no improvements for nearly four decades. This absence of progress has led to some research towards understanding

the limitations of the current proof techniques in proving strong lower bounds for algebraic circuits.

Considering that algebraic circuits seem like a fairly general and powerful model of computation, it is tempting to think that the *natural proofs barrier* of Razborov and Rudich [5] also extends to this setting. This problem turns out to be a non-trivial one, and indeed it is not known whether their results extend to algebraic circuits. This question is closely related to the question of whether cryptographically secure algebraic pseudorandom functions can be computed by small and low degree algebraic circuits and there does not seem to be substantial evidence one way or the other on this. We refer the reader to [6] and [1] for a more detailed discussion on this issue.

In the last few years, this question of trying to find an algebraic analog of the barrier results in [5] has received substantial attention. It was observed by various authors [6], [13], [1], [2] that most of the currently known proofs of algebraic circuit lower bounds fit into a common unifying framework, not unlike that in [5], although of a more algebraic nature. Indeed, these proofs also implicitly go via defining a property for the set of all polynomials and using this property to separate the hard polynomial from the easy ones. Moreover, the notions of *largeness* and *constructivity* in Definition I.1 also seem to extend to these proofs.

We now formally define this unifying framework. We start by defining the notion of a *proof polynomial* or a *defining equation*, which takes as input coefficient vectors of other polynomials.

**Definition I.2** (Proof polynomials/equations for a class). *For some  $n, d \in \mathbb{N}$ , let  $\mathcal{C}_{n,d}$  be a class of  $n$ -variate polynomials of total degree at most  $d$ ; i.e.  $\mathcal{C}_{n,d} \subseteq \mathbb{F}[\mathbf{x}]^{\leq d}$ .*

*Then for  $N = \binom{n+d}{n}$ , a nonzero polynomial  $P_N(\mathbf{Z})$  is called a proof against  $\mathcal{C}_{n,d}$  if for all  $f(\mathbf{x}) \in \mathcal{C}_{n,d}$ , we have that  $P_N(\text{coeff}(f)) = 0$ , where  $\text{coeff}(f)$  is the coefficient vector of  $f$ .*  $\diamond$

Intuitively, non-vanishing of the proof polynomial (against a class  $\mathcal{C}$ ) on the coefficient vector of a given polynomial  $f$  is a proof that  $f$  is not in  $\mathcal{C}$ . This framework comes up very naturally in the context of algebraic geometry (and geometric complexity theory), where a proof polynomial is just a *defining equation* of the variety obtained by taking the coefficient vectors of every polynomial in the class  $\mathcal{C}$  and looking at their Zariski Closure. Getting our hands on a defining equation of a variety gives us a plausible way to test and certify non-membership in the variety, in other words, to prove a lower bound.

This notion of a *proof polynomial against a class* is an analog of the the notion of *natural properties useful against a class* in [5]. Moreover, since a nonzero

<sup>2</sup>See Definition II.1 for a formal definition.

polynomial does not vanish very often on a random input from a large enough grid, it follows that a nonzero proof polynomial against a class  $\mathcal{C}$  will be nonzero on the coefficient vector of a ‘‘random polynomial’’. Here by a random polynomial we mean a polynomial whose coefficients are independent and uniformly random elements from some large enough set in the underlying field. With appropriate quantitative bounds, this observation can be formalized to give an appropriate algebraic analog of the notion of *largeness*. Lastly, the algebraic circuit complexity of the proof polynomial gives a natural algebraic analog of the notion of *constructivity*. Intuitively, any algebraic circuit lower bound which goes via defining a nonzero proof polynomial of polynomially bounded degree that can be efficiently computed by an algebraic circuit is an *Algebraically Natural Proof* of a lower bound.

We now formally define this notion. Note that since we are interested in asymptotic bounds, we have to work with families of polynomials. So, as a first step, we extend [Definition I.2](#) to polynomial families.

**Definition I.3** (Proofs against a class of polynomial families). *Let  $\mathcal{C}$  be a class of polynomial families  $\{\{f_n\} : f_n \in \mathcal{C}_{n,d_n}\}$ , and let  $\{P_N\}$  be a polynomial family.*

*The family  $\{P_N\}$  is said to be a proof against  $\mathcal{C}$  if there is an  $n_0$ , such that for all  $n \geq n_0$  the polynomial  $P_N$  is a proof against  $\mathcal{C}_{n,d_n}$  where  $N = \binom{n+d_n}{n}$ . That is,  $P_N$  is a proof against  $\mathcal{C}_{n,d_n}$  for all large enough  $n$ .*  $\diamond$

We now formally define an algebraically natural proof.

**Definition I.4** (Algebraically natural proofs [[1](#), [2](#)]). *Let  $\mathcal{C}$  be a class of polynomial families  $\{\{f_{n,d}\} : f_{n,d} \in \mathcal{C}_{n,d}\}$ .*

*Then, for a class  $\mathcal{D}$  of polynomials, we say that  $\mathcal{C}$  has  $\mathcal{D}$ -natural proofs if there is a family  $\{P_N\} \in \mathcal{D}$  which is a proof against  $\mathcal{C}$ .*  $\diamond$

In the rest of this paper, whenever we say a natural proof, without specifying the class  $\mathcal{D}$ , we mean a VP-natural proof.

Analogous to the abstraction of *natural proofs* for Boolean circuit lower bounds, this framework of *algebraically natural proofs* turns out to be rich and general enough that almost all of our current proofs of algebraic circuit lower bounds are in fact algebraically natural, or can be viewed in this framework with a little work [[14](#)]. Thus, this definition seems like an important first step towards understanding the strengths and limitations of many of our current lower bound techniques in algebraic complexity.

The immediate next question to ask is whether algebraically natural proofs are rich enough to give strong

algebraic circuit lower bounds. The works of Forbes *et al.* [[1](#)] and Grochow *et al.* [[2](#)] argue that under an appropriate (but non-standard) pseudorandomness assumption, this is not true, i.e., algebraically natural proof techniques cannot be used to show strong lower bounds for algebraic circuits. To discuss this formally, we need the following definition of *succinct hitting sets*.

**Definition I.5** (Succinct hitting sets for a class of polynomials (Informal)). *For some  $n, d \in \mathbb{N}$ , let  $\mathcal{C}_{n,d}$  be a class of  $n$ -variate polynomials of total degree at most  $d$ ; i.e.  $\mathcal{C}_{n,d} \subseteq \mathbb{F}[x]^{\leq d}$ .*

*Then for  $N = \binom{n+d}{n}$ , we say that a class of  $N$  variate polynomials  $\mathcal{D}_N$  has  $\mathcal{C}_{n,d}$ -succinct hitting sets if for all  $0 \neq P(\mathbf{Z}) \in \mathcal{D}_N$ , there exists some  $f \in \mathcal{C}_{n,d}$  such that  $P_N(\text{coeff}(f)) \neq 0$ .*  $\diamond$

As with [Definition I.3](#), this definition naturally extends to polynomial families. It follows from the definitions that non-existence of  $\mathcal{D}$ -natural proofs against a class  $\mathcal{C}$  is equivalent to the existence of  $\mathcal{C}$ -succinct hitting sets for the class  $\mathcal{D}$ .

Forbes, Shpilka and Volk [[1](#)] showed that for various restricted circuit classes  $\mathcal{C}$  and  $\mathcal{D}$ , the class  $\mathcal{D}$  has  $\mathcal{C}$  succinct hitting sets. Or equivalently, lower bounds for  $\mathcal{C}$  cannot be proved via proof polynomial families in  $\mathcal{D}$ . However, this question has remained unanswered for more general circuit classes  $\mathcal{C}$  and  $\mathcal{D}$ . In particular, if we take both  $\mathcal{C}$  and  $\mathcal{D}$  to be VP, we do not seem to have significant evidence on the existence of VP succinct hitting sets for VP. In [[1](#)], the authors observed that showing VP succinct hitting sets for VP would immediately imply non-trivial deterministic algorithms for polynomial identity testing, which via well known connections between algebraic hardness and derandomization will in turn imply new lower bounds [[15](#)], [[16](#)]. Thus, the problem of proving an unconditional barrier result for algebraically natural proof techniques via this route seems as hard as proving new circuit lower bounds! It is, however, conceivable that one can show such a barrier conditionally. And in some more structured settings, such as for the case of matrix completion, such results are indeed known [[17](#)]. However, the following concrete problem has continued to remain open.

**Question I.6.** *For every constant  $c > 0$ , does there exist a nonzero polynomial family  $\{P_{N,c}\}$  in VP such that for all large enough  $n$ , the following is true?*

*For every family of polynomials  $\{f_n\}_n$  in VP, such that  $f_n$  is an  $n$  variate polynomial of degree  $n^c$ ,  $P_{N,c}$  vanishes on the coefficient vector of  $f_n$  for  $N = \binom{n+n^c}{n}$ .*

In other words, does VP have proof polynomials in VP? As discussed earlier, a negative answer to this question is equivalent to the existence of VP succinct

hitting sets for VP and will imply that it is not possible to prove super-polynomial lower bounds for algebraic circuits via algebraically natural lower bound proofs.

An equivalent interpretation of this relation between succinct hitting sets and algebraically natural proofs is via the geometric notion of equations of algebraic varieties. [Question I.6](#) is precisely the question of understanding whether the Zariski closure of VP has equations which have degree and circuit complexity polynomial in their number of variables? Even though this is true for many of the restricted circuit classes for which we currently have lower bounds (as observed in [1]), perhaps hoping that this extends to richer and more general circuit classes is too much to ask for?

We are now ready to state our results.

### C. Our results

In our main results, we make progress towards answering [Question I.6](#) in the affirmative. We prove the following theorems.

*Equations for polynomials in VP with coefficients of small complexity:*

**Theorem I.7.** *Let  $c > 0$  be any constant. There is a polynomial family  $\{P_{N,c}\} \in \text{VP}_{\mathbb{Q}}^3$  such that for all large  $n$  and  $N = \binom{n+n^c}{n}$ , the following are true.*

- *For every family  $\{f_n\} \in \text{VP}_{\mathbb{C}}$ , where  $f_n$  is an  $n$  variate polynomial of degree at most  $n^c$  and coefficients in  $\{-1, 0, 1\}$ , we have*

$$P_{N,c}(\overline{\text{coeff}}(f_n)) = 0,$$

*where  $\overline{\text{coeff}}(f_n)$  is the coefficient vector of  $f_n$ .*

- *There exists a family  $\{h_n\}$  of  $n$  variate polynomials and degree at most  $n^c$  with coefficients in  $\{-1, 0, 1\}$  such that*

$$P_{N,c}(\overline{\text{coeff}}(h_n)) \neq 0.$$

We remark that even though [Theorem I.7](#) is stated for polynomials with coefficients in  $\{-1, 0, 1\}$ , the theorem holds for polynomials with coefficients as large as  $N$ . However, for brevity, we will confine the discussion in this paper to polynomials with coefficients in  $\{-1, 0, 1\}$ .

We also prove an analogous theorem for finite fields of small size.

**Theorem I.8.** *Let  $\mathbb{F}$  be any finite field of constant size and  $c > 0$  be any constant. There is a polynomial family  $\{P_{N,c}\} \in \text{VP}_{\mathbb{F}}$  such that for all large enough  $n$  and  $N = \binom{n+n^c}{n}$ , the following are true.*

- *For every  $\{f_n\} \in \text{VP}_{\mathbb{F}}$ , where  $f_n$  is an  $n$  variate polynomial of degree at most  $n^c$ , we have*

$$P_{N,c}(\overline{\text{coeff}}(f_n)) = 0.$$

<sup>3</sup>For a field  $\mathbb{F}$ ,  $\text{VP}_{\mathbb{F}}$  denotes the class VP where the coefficients of the polynomials are from the field  $\mathbb{F}$ .

- *There exists a family  $\{h_n\}$  of  $n$  variate polynomials and degree at most  $n^c$  with coefficients in  $\mathbb{F}$  such that*

$$P_{N,c}(\overline{\text{coeff}}(h_n)) \neq 0.$$

Furthermore, we also prove analogous statements for the larger class VNP, which we now state.

*Equations for polynomials in VNP with coefficients of small complexity:*

**Theorem I.9.** *Let  $c > 0$  be any constant. There is a polynomial family  $\{Q_{N,c}\} \in \text{VNP}_{\mathbb{Q}}$  such that for all large  $n$  and  $N = \binom{n+n^c}{n}$ , the following are true.*

- *For every family  $\{f_n\} \in \text{VNP}_{\mathbb{C}}$ , where  $f_n$  is an  $n$  variate polynomial of degree at most  $n^c$  and coefficients in  $\{-1, 0, 1\}$ , we have*

$$Q_{N,c}(\overline{\text{coeff}}(f_n)) = 0.$$

- *There exists a family  $\{h_n\}$  of  $n$  variate polynomials and degree at most  $n^c$  with coefficients in  $\{-1, 0, 1\}$  such that*

$$Q_{N,c}(\overline{\text{coeff}}(h_n)) \neq 0.$$

**Theorem I.10.** *Let  $\mathbb{F}$  be any finite field of constant size and  $c > 0$  be any constant. There is a polynomial family  $\{Q_{N,c}\} \in \text{VNP}_{\mathbb{F}}$  such that for all large enough  $n$  and  $N = \binom{n+n^c}{n}$ , the following are true.*

- *For every family  $\{f_n\} \in \text{VNP}_{\mathbb{F}}$ , where  $f_n$  is an  $n$  variate polynomial of degree at most  $n^c$ , we have*

$$Q_{N,c}(\overline{\text{coeff}}(f_n)) = 0.$$

- *There exists a family  $\{h_n\}$  of  $n$  variate polynomials and degree at most  $n^c$  with coefficients in  $\mathbb{F}$  such that*

$$Q_{N,c}(\overline{\text{coeff}}(h_n)) \neq 0.$$

### D. Discussion and relations to prior work

As is evident from the statements, our main theorems make some progress towards answering [Question I.6](#) in the affirmative, at least in the setting of small finite fields and for polynomials with small integer coefficients, in a fairly strong sense. In fact, as [Theorem I.9](#) and [Theorem I.10](#) show, in the context of polynomials with coefficients of low complexity, not just VP but even the seemingly larger class VNP has efficiently computable low degree<sup>4</sup> equations.

Many of the families of polynomials commonly studied in algebraic complexity have integer coefficients with absolute values bounded by 1, and fall in the setting of the results here. Moreover, the condition of

<sup>4</sup>Throughout this paper, by a *low degree* polynomial family, we mean a polynomial family whose degree is polynomially bounded in its number of variables.

computing polynomials with bounded coefficients is a semantic condition on a model, in the sense that even though the final output of the circuit is required to have bounded coefficients, the circuit is free to use arbitrary constants from  $\mathbb{C}$  in the intermediate computation. Thus, it is conceivable that we might be able to prove a super-polynomial lower bound on the algebraic circuit size for the permanent polynomial via an algebraically natural proof constructible in VP, thereby separating VP and VNP. However, since analogs of [Theorem I.7](#) and [Theorem I.8](#) are also true for VNP, any such separation of VNP and VP will have to rely on more fine grained information on the equations, and not just their degree and algebraic circuit size. Unfortunately, our proofs are all existential and do not give a sense of what the polynomial families  $\{P_{N,c}\}$  (or  $\{Q_{N,c}\}$ ) might look like.

We also note that in the light of some of the prior work, the results here are perhaps a bit surprising. The classes of polynomials in VP and VNP with small coefficients (or over small finite fields), are seemingly rich and complex sets, and the main theorems here show (unconditionally) that they have equations which are also efficiently computable. As discussed earlier in this introduction, this property is known to be true for many structured subclasses of algebraic circuits (for example, homogeneous circuits of depth 3 and 4, multilinear formulas, polynomials of small Waring rank). However, it is unclear if this property extends to more general circuit classes, in particular VP (or VNP).

Indeed, following the work of Forbes *et al.* [1] and Grochow *et al.* [2], much of the research on this problem [1], [17], [18] has focused on proving the *non-existence* of efficiently computable equations for VP, and this line of work has made interesting progress in this direction for many structured and special instances of problems of this nature. The results in [17], [18] draw connections between the existence of efficiently constructible equations of a variety and the problem of testing (non)membership in it and use the conditional hardness of the (non)membership testing problem for certain varieties to rule out the existence of efficiently computable equations for them. More precisely, Bläser *et al.* [17] show that if all the equations for the variety of matrices with zero permanent is constructible by small constant-free algebraic circuits, then the non-membership problem for this variety can be decided in the class  $\exists\text{BPP}$ . Thus, unless  $P^{\#P} \subseteq \exists\text{BPP}$ , the equations of this variety does not have small, low degree constant free algebraic circuits. In a subsequent work [18], the results of [17] are generalized to *min-rank* or *slice-rank* varieties. However, in the bounded coefficient setting (and over small finite fields), our results show that the contrary is true, and VP does have efficiently

computable low degree equations. We also remark that because of the setting of bounded integer coefficients or small finite fields in this work, this natural connection between variety non-membership and equations of varieties discussed in [17], [18] appears to break down.

A positive result on the complexity of equations of naturally occurring varieties in algebraic complexity appears in a recent work of Kumar and Volk [19] where they show polynomial degree bounds on the equations of the Zariski closure of the set of non-rigid matrices and small linear circuits over all large enough fields. However, we do not know if any of these low degree equations can be *efficiently* computed by an algebraic circuit.

*Other related work:* Many of the algebraic circuit lower bounds (e.g. lower bounds for depth-3 and depth-4 circuits, and lower bounds for multilinear models) are obtained by considering the rank of certain matrices as a complexity measure. In their recent works, Efremenko, Garg, Oliveira and Wigderson [20] and Garg, Makam, Oliveira and Wigderson [21], discuss limitations of some of these rank based methods towards proving lower bounds. In particular, Efremenko *et al.* [20] show that some of these rank based methods cannot prove lower bounds better than  $\Omega_d(n^{\lfloor d/2 \rfloor})$  on tensor rank (resp., Waring rank) for a  $d$ -dimensional tensor of side  $n$ . Building on [20], in [21], the authors demonstrate that one *cannot* hope to significantly improve the known lower bounds for tensor rank for  $d$  dimensional tensors by lifting lower bounds on tensors in fewer dimensions. However, we note that a general algebraically natural proof of a lower bound does not necessarily fit into the framework of [20], [21], and so these limitations for the so called *rank methods* do not seem to immediately extend to algebraically natural proofs in general. As discussed earlier, in the light of the results here, it is conceivable that we might be able to improve the state of the art for general algebraic circuit lower bounds, using techniques that are algebraically natural.

For Boolean circuits, Chow [22] circumvents the natural proofs barrier in [5] by providing (under standard cryptographic assumptions) an explicit *almost natural proof* that is useful against  $P/\text{poly}$  as well as constructive in nearly linear time, but compromises on the largeness condition. Furthermore, Chow [22] shows the unconditional existence of a natural property useful against  $P/\text{poly}$  (infinitely often) constructive in linear size that has a weakened largeness condition. In some sense, [Theorem I.8](#) and [Theorem I.7](#) are analogous to the work of Chow [22], albeit in the algebraic world.

*On the largeness criterion:* In the definitions of algebraically natural proofs [2], [1], the authors observe that in the algebraic setting, an analog of the *largeness* criterion in [Definition I.1](#) is often available for free;

the reason being that a nonzero defining equation for any class of polynomials vanishes on a very small fraction of all polynomials over any sufficiently large field. However, this trade-off becomes a bit subtle when considering polynomials over finite fields of small size, or polynomials with bounded integer coefficients. In particular, as we observe in the course of the proofs of our results, we still have a large number of polynomials whose coefficients will keep  $\{P_{N,c}\}$  (and  $\{Q_{N,c}\}$ ) nonzero, although this set is no longer a significant fraction of the set of all polynomials.

*Putting Our Results in Context:* Given the absence of conclusive evidence both for and against the existence of algebraically natural proofs for VP, we believe that some comments on the consequences of our results are in order.

As alluded to in the previous section, most of the prior work related to Question I.6 has focused on looking for evidence that the answer to it is negative, i.e. VP does not have efficiently computable and low degree equations if certain strong hitting sets exist. The main results of this paper highlight the possibility of there being interesting upper bounds for the equations for natural algebraic complexity classes, again using the existence of hitting sets. Although the results in this paper do not prove the existence of efficiently computable equations for VP, they do provide some useful context with respect to other results that hint towards potential barriers. Especially in the context of proving super-polynomial lower bounds against algebraic circuits, Theorem I.7 and Theorem I.8 can be seen as evidence for efficacy of “natural lower bound techniques”.

It is worth noting that our results do not suggest that proving super-polynomial lower bounds is easy. The equations constructed in this paper rely on hitting sets for VP (or VNP), and explicit hitting sets have, historically, always been preceded by strong lower bounds against corresponding models. Our results merely suggest that perhaps as of now it is imprudent to dismiss the possibility of proving interesting lower bounds for rich subclasses of algebraic circuits via natural proof strategies.

#### E. An overview of the proof

At a high level, the idea behind our results is to try and come up with a *non-trivial* property of polynomials which every polynomial with a small circuit satisfies. By a non-trivial property, we mean that there should exist (nonzero) polynomials which do not have this property. The hope is that once we have such a property (which is nice enough), one can try to transform this into a defining equation via an appropriate *algebraization*. The property that we finally end up using is the existence of (non-explicit) *hitting sets* for polynomials with small

circuits.

A hitting set for a class  $\mathcal{C}$  of polynomials over a field  $\mathbb{F}$  is a set of points  $\mathcal{H}$ , such that every nonzero polynomial in  $\mathcal{C}$  evaluates to a nonzero value on at least one point in  $\mathcal{H}$ . We then turn this property of *not-vanishing-everywhere on  $\mathcal{H}$*  into a defining equation in some settings to get our main theorems.

To make things a bit more formal, let us consider the map  $\Phi_{\mathcal{H}}$ , defined by the hitting set  $\mathcal{H}$  of  $\mathcal{C}$  on the set of all polynomials, that maps any given polynomial  $f$  to its evaluations over the points in  $\mathcal{H}$ . It is clear from the above observation that any nonzero polynomial in the kernel of  $\Phi_{\mathcal{H}}$  is guaranteed to be outside  $\mathcal{C}$ . Thus, if there were a nonzero polynomial that vanishes on all polynomials  $f \notin \ker(\mathcal{H})$ , we have a defining equation for  $\mathcal{C}$ .

Moreover, if such a polynomial happened to have its degree and circuit complexity polynomially bounded in its number of variables, we would have our main theorems. However, note that *not* being in the kernel of a linear map seems to be a tricky condition to check via a polynomial (as opposed to the complementary property of *being* in the kernel, which can be easily checked via a polynomial). To prove our theorems, we get past this issue in the setting of small finite fields, and for polynomials over  $\mathbb{C}$  with bounded integer coefficients.

Over a finite field  $\mathbb{F}$ , a univariate polynomial that maps every nonzero  $x \in \mathbb{F}$  to zero and vice versa, already exists in  $q(x) = 1 - x^{|\mathbb{F}|-1}$ . Therefore, for a given polynomial  $f$ , the defining equation essentially outputs  $\prod_{\mathbf{h} \in \mathcal{H}} q(f(\mathbf{h}))$ . Clearly, for a polynomial  $f$ ,  $\prod_{\mathbf{h} \in \mathcal{H}} q(f(\mathbf{h}))$  is zero if and only if  $f$  evaluates to a nonzero value on at least one point in  $\mathcal{H}$ .

To generalize this to other fields, we wish to find a “low-degree” univariate  $q(x)$  that maps nonzero values to 0, and zero to a nonzero value. We observe that in the setting when the polynomials in  $\mathcal{C}$  have integer coefficients of bounded magnitude, we can still obtain such a univariate polynomial, and in turn a non-trivial defining equation. Indeed, if  $q$  were such a univariate, we essentially output  $\prod_{\mathbf{h} \in \mathcal{H}} q(f(\mathbf{h}))$ , for a given polynomial  $f$ . This step relies on a simple application of the Chinese Remainder Theorem.

In order to show that the equations are non-trivial in the sense that there exist polynomials with bounded integer coefficients which do not pass this test, we need to show that there are nonzero polynomials with bounded integer coefficients which vanish everywhere on the hitting set  $\mathcal{H}$ . We show this via a well known lemma of Siegel<sup>5</sup>, which uses a simple pigeon hole argument to show that an under-determined system of homogeneous linear equations where the constraint

<sup>5</sup>A statement of the lemma can be found [here](#). Refer to [23] for details.

matrix has small integer entries has a nonzero solution with small integer entries.

As it turns out, our proofs do not use much about the class  $\text{VP}$  except for the existence of small hitting sets for polynomials in the class. It is not hard to observe that this property is also true for the seemingly larger class  $\text{VNP}$  and hence the results here also extend to  $\text{VNP}$ .

We remark that given the hitting set  $\mathcal{H}$  explicitly, the construction of the defining equation is completely explicit. In other words, the non-explicitness in our construction comes only from the fact that we do not have explicit constructions of hitting sets for algebraic circuits.

*Organization of the paper:* We begin with some notations and preliminaries in [Section II](#) before moving on to prove [Theorem I.8](#) in [Section III](#) and [Theorem I.7](#) in [Section IV](#). In [Section V](#), we observe that these results also generalize to  $\text{VNP}$ , and finally conclude with some open questions in [Section VI](#).

## II. NOTATION AND PRELIMINARIES

### A. Notation

We use  $\{f_n\}_{n \in \mathbb{N}}$  to denote families of polynomials. We drop the index set whenever it is clear from context. For a given polynomial  $f$ , we denote by  $\deg(f)$  its degree. For a polynomial  $f(\mathbf{x}, \mathbf{y}, \dots)$  on multiple sets of variables, we use  $\deg_{\mathbf{x}}(f)$ ,  $\deg_{\mathbf{y}}(f)$ , etc. to denote the degree in the variables from the respective sets.

We use  $\mathbb{F}[\mathbf{x}]^{\leq d}$  to denote polynomials over the field  $\mathbb{F}$  in variables  $\mathbf{x}$  of degree at most  $d$ , and use  $\mathbf{x}^{\leq d}$  to denote the set of all monomials in variables  $\mathbf{x}$  of degree at most  $d$ .

For a given polynomial  $f \in \mathbb{F}[\mathbf{x}]^{\leq d}$  and a monomial  $m \in \mathbf{x}^{\leq d}$ , we use  $\text{coeff}_m(f)$  to refer to the coefficient of  $m$  in  $f$ . We further use  $\overline{\text{coeff}}(f)$  to denote the vector<sup>6</sup> of coefficients of  $f$ .

### B. Algebraic circuits and complexity classes

Let us first formally define algebraic circuits.

**Definition II.1** (Algebraic circuits). *An algebraic circuit is specified by a directed acyclic graph, with leaves (indegree zero; also called inputs) labeled by field constants or variables, and internal nodes labeled by + or  $\times$ . The nodes with outdegree zero are called the outputs of the circuit. Computation proceeds in the natural way, where inductively each + gate computes the sum of its children and each  $\times$  gate computes the product of its children.*

The size of the circuit is defined as the number of nodes in the underlying graph.  $\diamond$

<sup>6</sup>We do not explicitly mention the monomial ordering used for this vector representation, since all our statements work for any monomial ordering.

We also define the class  $\text{VP}$  and its “slices” formally.

**Definition II.2** ( $\text{VP}$  and  $\text{VP}_{\mathbb{F}}^{[c]}$ ). *A family of polynomials  $\{f_n\}$  over a field  $\mathbb{F}$  is said to be in  $\text{VP}_{\mathbb{F}}$  (or just  $\text{VP}$  when the field is clear from context) if there exist constants  $c_1, c_2$  such that*

- $f_n$  is an  $n$ -variate polynomial,
- $\deg(f_n) \leq n^{c_1}$  for all large enough  $n$ ,
- $f_n$  is computable by an algebraic circuit of size at most  $n^{c_2}$ , for all large enough  $n$ .

Even though  $f_n \in \mathbb{F}[\mathbf{x}]$ , the circuit computing  $f_n$  may employ constants from a larger extension field  $\mathbb{K} \supset \mathbb{F}$ .

For the ease of notation, we also consider “slices” of  $\text{VP}$  with  $d = n^c$  for a fixed constant  $c$ . To this end, we will define  $\text{VP}_{\mathbb{F}}^{[c]}$  to denote

$$\text{VP}_{\mathbb{F}}^{[c]} := \left\{ \{f_n\} \in \text{VP}_{\mathbb{F}} : f_n \in \mathbb{F}[x_1, \dots, x_n]^{\leq n^c} \right\}.$$

We also consider polynomials  $\{f_n\}$  over integers whose coefficients are in  $\{-1, 0, 1\}$ . However, it is important to note that even in this setting the bound is only on the coefficients of  $f_n$ ; the circuit computing  $f_n$  may use arbitrary constants from the underlying field, or an extension.  $\diamond$

Finally, let us formally define the class  $\text{VNP}$  and its “slices”.

**Definition II.3** ( $\text{VNP}$  and  $\text{VNP}_{\mathbb{F}}^{[c]}$ ). *A family of polynomials  $\{f_n\}$  over a field  $\mathbb{F}$  is said to be in  $\text{VNP}_{\mathbb{F}}$  (or just  $\text{VNP}$  when the field is clear from context) if there exist constants  $c_1, c_2$  such that*

- $f_n$  is an  $n$ -variate polynomial,
- $\deg(f_n) \leq n^{c_1}$  for all large enough  $n$ ,
- for  $m \leq n^{c_2}$  there exists an  $(n+m)$ -variate polynomial  $g_{n+m}(\mathbf{x}, \mathbf{y})$  of degree at most  $n^{c_2}$  which has an algebraic circuit of size at most  $n^{c_2}$ , that satisfies

$$f_n(\mathbf{x}) = \sum_{\mathbf{a} \in \{0,1\}^m} g_{n+m}(\mathbf{x}, \mathbf{a})$$

Again, the circuit computing  $g_{n+m} \in \mathbb{F}[\mathbf{x}, \mathbf{y}]$  may employ constants from a larger extension field  $\mathbb{K} \supset \mathbb{F}$ .

Analogous to  $\text{VP}_{\mathbb{F}}^{[c]}$ , we will define  $\text{VNP}_{\mathbb{F}}^{[c]}$  to denote

$$\text{VNP}_{\mathbb{F}}^{[c]} := \left\{ \{f_n\} \in \text{VNP}_{\mathbb{F}} : f_n \in \mathbb{F}[x_1, \dots, x_n]^{\leq n^c} \right\}.$$

Just as with  $\text{VP}$ , we also consider polynomials  $\{f_n\}$  over integers whose coefficients are in  $\{-1, 0, 1\}$ . Here again the bound is only on the coefficients of  $f_n$  and the corresponding circuits may use arbitrary constants from the underlying field, or an extension.  $\diamond$

### C. Some Preliminaries

For our proofs, we will need the following notion of universal circuits defined by Raz [24] that gives

a construction of a universal circuit such that any polynomial computed by a small circuit is a simple projection of the universal circuit.

**Lemma II.4** (Universal circuit, [24]). *Let  $\mathbb{F}$  be any field and  $n, s \geq 1$  and  $d \geq 0$ . Then there exists an algebraic circuit  $\mathcal{U}$  of size  $\text{poly}(n, d, s)$  computing a polynomial in  $\mathbb{F}[x_1, \dots, x_n, y_1, \dots, y_r]$  with  $r \leq \text{poly}(n, d, s)$  such that:*

- $\deg_x(\mathcal{U}(\mathbf{x}, \mathbf{y})) \leq d$ ;
- $\deg_y(\mathcal{U}(\mathbf{x}, \mathbf{y})) \leq \text{poly}(d)$ ;
- for any  $f \in \mathbb{F}[x_1, \dots, x_n]$  with  $\deg_x(f) \leq d$  that is computable by an algebraic circuit of size  $s$ , there exists an  $\mathbf{a} \in \mathbb{F}^r$  such that  $f(\mathbf{x}) = \mathcal{U}(\mathbf{x}, \mathbf{a})$ .

We will also be using the well-known Polynomial Identity Lemma.

**Lemma II.5** (Polynomial Identity Lemma, [25], [26], [27], [28]). *Let  $f \in \mathbb{F}[x_1, x_2, \dots, x_n]$  be a nonzero polynomial of degree at most  $d$  and let  $S$  be a subset of  $\mathbb{F}$  (or an extension of  $\mathbb{F}$ ). Then, the number of zeros of  $f$  on the grid  $S^n$  is at most  $d|S|^{n-1}$ .*

### III. CONSTRUCTIBLE EQUATIONS FOR VP OVER SMALL FINITE FIELDS

We expand on our main theorem for finite fields in this section. We skip the proofs due to space constraints, and we therefore encourage the reader to refer to the full version [29] for a full proof of our result. As mentioned in the introduction, our proof uses the existence of non-explicit hitting sets for small circuits. This fact appears to be folklore but we state below the version that can be found in Forbes' thesis [30].

**Lemma III.1** (Folklore (cf. Lemma 3.2.14 in [30])). *Let  $\mathbb{F}$  be a finite field with  $|\mathbb{F}| \geq d^2$ . Let  $\mathcal{C}(n, d, s)$  be the class of polynomials in  $\mathbb{F}[x_1, \dots, x_n]$  of degree at most  $d$  that are computable by fan-in 2 algebraic circuits of size at most  $s$ . Then, there is a non-explicit hitting set for  $\mathcal{C}$  of size at most  $\lceil 2s \cdot (\log n + 2 \log s + 4) \rceil$ .*

The above shows that over large enough finite fields, there are non-explicit hitting sets of size  $O(s^2)$  (when  $n, d \leq s$ ). We now use this to prove Theorem I.8 which we restate below.

**Theorem I.8.** *Let  $\mathbb{F}$  be any finite field of constant size and  $c > 0$  be any constant. There is a polynomial family  $\{P_{N,c}\} \in \text{VP}_{\mathbb{F}}$  such that for all large enough  $n$  and  $N = \binom{n+n^c}{n}$ , the following are true.*

- For every  $\{f_n\} \in \text{VP}_{\mathbb{F}}$ , where  $f_n$  is an  $n$  variate polynomial of degree at most  $n^c$ , we have

$$P_{N,c}(\overline{\text{coeff}}(f_n)) = 0.$$

- There exists a family  $\{h_n\}$  of  $n$  variate polynomials and degree at most  $n^c$  with coefficients in  $\mathbb{F}$  such

that

$$P_{N,c}(\overline{\text{coeff}}(h_n)) \neq 0.$$

### IV. CONSTRUCTIBLE EQUATIONS FOR VP WITH COEFFICIENTS IN $\{-1, 0, 1\}$

We will now give more details about Theorem I.7. Again we omit the proofs due to space constraints, and encourage the reader to refer to the full version [29] for the full proofs of the claims in this section. As before, our proof uses the existence of non-explicit hitting sets for circuits of small size. When the underlying field is  $\mathbb{C}$ , their existence is known due to the results of Heintz and Schnorr [15] which additionally also give hitting sets of low bit-complexity. We therefore begin by stating their result in the language of this paper.

**Lemma IV.1** ([15](Theorem 4.4)). *There are (non-explicit) hitting sets  $\mathcal{H}$  for  $\mathcal{C}(n, d, s)$  (the set of all  $n$ -variate polynomials with degree at most  $d$  and computable by algebraic circuits of size at most  $s$ ), such that  $\mathcal{H} \subset [sd^3]^n$  and  $|\mathcal{H}| = \text{poly}(n, s)$ .*

We then use the result above to prove our main theorem, which we restate below.

**Theorem I.7.** *Let  $c > 0$  be any constant. There is a polynomial family  $\{P_{N,c}\} \in \text{VP}_{\mathbb{Q}}^7$  such that for all large  $n$  and  $N = \binom{n+n^c}{n}$ , the following are true.*

- For every family  $\{f_n\} \in \text{VP}_{\mathbb{C}}$ , where  $f_n$  is an  $n$  variate polynomial of degree at most  $n^c$  and coefficients in  $\{-1, 0, 1\}$ , we have

$$P_{N,c}(\overline{\text{coeff}}(f_n)) = 0,$$

where  $\overline{\text{coeff}}(f_n)$  is the coefficient vector of  $f_n$ .

- There exists a family  $\{h_n\}$  of  $n$  variate polynomials and degree at most  $n^c$  with coefficients in  $\{-1, 0, 1\}$  such that

$$P_{N,c}(\overline{\text{coeff}}(h_n)) \neq 0.$$

As mentioned earlier, the proof generalizes in a straightforward manner for polynomial families  $\{f_n\} \in \text{VP}_{\mathbb{Z}}^{[c]}$  whose coefficients are bounded by  $N$ . We state this for polynomials whose coefficients are in  $\{-1, 0, 1\}$  just to avoid cumbersome notation.

### V. EQUATIONS FOR VNP

We shall now state the VNP analogs of Theorem I.7 and Theorem I.8. We omit the proofs again for brevity, and encourage the readers to refer to the full version [29] for details. First, we have the following definition.

<sup>7</sup>For a field  $\mathbb{F}$ ,  $\text{VP}_{\mathbb{F}}$  denotes the class VP where the coefficients of the polynomials are from the field  $\mathbb{F}$ .

**Definition V.1** (Definability of Polynomials). For  $s \geq 1$ , a polynomial  $f_n$  is said to be  $s$ -definable if there exists a polynomial  $g_s \in \mathcal{C}(s, s, s)$  such that for  $m = s - n$ ,

$$f_n(\mathbf{x}) = \sum_{\alpha \in \{0,1\}^m} g_s(\mathbf{x}, \alpha).$$

Further, let us denote by  $\mathcal{D}(n, d, s)$  the class of all  $n$ -variate polynomials of degree  $d$  that are  $s$ -definable.  $\diamond$

**Remark V.2.** Note that for every family  $\{f_n\} \in \text{VNP}$ , there is a polynomially bounded function  $s(n) > n, d(n)$  such that  $f_n$  is  $s(n)$ -definable, for all large  $n$ .  $\diamond$

#### A. VNP over Small Finite Fields

As in the VP case, we will need the existence of non-explicit hitting sets. A slight modification to the proof of Lemma 3.2.14 in [30]) gives us the following statement.

**Lemma V.3.** Let  $\mathbb{F}$  be a finite field with  $|\mathbb{F}| \geq d^2$ . Let  $\mathcal{D}(n, d, s)$  be the class of polynomials in  $\mathbb{F}[x_1, \dots, x_n]$  of degree at most  $d$  that are  $s$ -definable. Then, there is a non-explicit hitting set  $\mathcal{H}$  for  $\mathcal{D}(n, d, s)$  of size at most  $\lceil 2s \cdot (3 \log s + 4) \rceil$ .

By Remark V.2, we have that over large enough finite fields, there are non-explicit hitting sets of size  $O(s^2)$  for VNP. Since the proof of Theorem I.8 does not use any property of VP except for the existence of non-trivial hitting sets, we get the following theorem. The proof is omitted, since it is exactly the same except we use Lemma V.3 instead of Lemma III.1.

**Theorem I.10.** Let  $\mathbb{F}$  be any finite field of constant size and  $c > 0$  be any constant. There is a polynomial family  $\{Q_{N,c}\} \in \text{VP}_{\mathbb{F}}$  such that for all large enough  $n$  and  $N = \binom{n+n^c}{n}$ , the following are true.

- For every family  $\{f_n\} \in \text{VNP}_{\mathbb{F}}$ , where  $f_n$  is an  $n$ -variate polynomial of degree at most  $n^c$ , we have

$$Q_{N,c}(\overline{\text{coeff}}(f_n)) = 0.$$

- There exists a family  $\{h_n\}$  of  $n$  variate polynomials and degree at most  $n^c$  with coefficients in  $\mathbb{F}$  such that

$$Q_{N,c}(\overline{\text{coeff}}(h_n)) \neq 0.$$

#### B. Polynomials in VNP with Small Integer Coefficients

Our argument will be identical to that in Section IV, for which we will need a statement analogous to Lemma IV.1 showing the existence of non-explicit hitting sets for VNP with small bit-complexity. We show this by first giving a universal map for the polynomials in VNP, analogous to Lemma II.4; for which we need the following lemma.

**Lemma V.4** (Coefficient Vectors of Definable Polynomials). Let  $f \in \mathbb{C}[\mathbf{x}]$  be an  $n$ -variate polynomial of degree  $d$  that is  $s$ -definable. Then there exists an  $s$ -variate polynomial  $g$  and a linear map  $L_{n,d,s}$ , such that  $\overline{\text{coeff}}(f) = L(\overline{\text{coeff}}(g))$ . Furthermore, the map  $L$  depends solely on  $n, d$  and  $s$ .

**Lemma V.5** (Universal Map for Definable Polynomials). Let  $s \geq n \geq 1$  and  $d \geq 0$ . Then for  $N = \binom{n+d}{n}$  there exists a polynomial map  $\mathcal{U}(\mathbf{y}) : \mathbb{C}^r \rightarrow \mathbb{C}^N$  with  $r \leq \text{poly}(n, d, s)$  such that:

- $\deg(\mathcal{U}(\mathbf{y})) \leq \text{poly}(s)$ ;
- for any  $f \in \mathbb{C}[x_1, \dots, x_n]$  with  $\deg_x(f) \leq d$  that is  $s$ -definable, there exists an  $\mathbf{a} \in \mathbb{C}^r$  such that  $\overline{\text{coeff}}(f) = \mathcal{U}(\mathbf{a})$ .

We then prove the existence of non-explicit hitting sets of small bit-complexity even for the class of efficiently definable polynomials with small integer coefficients. We do this by first bounding the number of polynomials in VNP with small coefficients, using the map from Lemma V.5 in conjunction with the following lemma, which is a slight modification of a result of Hrubeš and Yehudayoff [31, Claim 3.6].

**Lemma V.6** ([31]). Let  $V \in \mathbb{C}^n$  be an irreducible algebraic variety of dimension  $k$  and degree  $r$ . Suppose  $F = (F_1, \dots, F_m)$  with  $F_i \in \mathbb{F}[x_1, \dots, x_n]^{\leq d}$  be a polynomial map. Then, for  $\Delta \subset \mathbb{Z}$ ,

$$|F(V) \cap \Delta^m| \leq r \cdot (|\Delta| \cdot d)^k.$$

We can then use the *Polynomial Identity Lemma* Lemma II.5 along with a counting argument, to prove the existence of non-explicit hitting sets of small size and low bit complexity, for polynomials in VNP with small coefficients.

**Lemma V.7.** Let  $\Delta \subset \mathbb{Z}$ . There are (non-explicit) hitting sets  $\mathcal{H}$  for  $\mathcal{D}(n, d, s)$  (the set of all  $n$ -variate polynomials with degree at most  $d$ , that are  $s$ -definable) with coefficients in  $\Delta$ , such that  $\mathcal{H} \subset [ds|\Delta|]^n$  and  $|\mathcal{H}| = \text{poly}(s)$ .

We can now prove the following theorem along the lines of Theorem I.7. The proof of Theorem I.7 almost directly extends here, as it does not assume anything about VP except for the existence of non-explicit hitting sets of small bit-complexity, which here is given by Lemma V.7.

**Theorem I.9.** Let  $c > 0$  be any constant. There is a polynomial family  $\{Q_{N,c}\} \in \text{VP}_{\mathbb{Q}}$  such that for all large  $n$  and  $N = \binom{n+n^c}{n}$ , the following are true.

- For every family  $\{f_n\} \in \text{VNP}_{\mathbb{C}}$ , where  $f_n$  is an  $n$  variate polynomial of degree at most  $n^c$  and

coefficients in  $\{-1, 0, 1\}$ , we have

$$Q_{N,c}(\overline{\text{coeff}}(f_n)) = 0.$$

- There exists a family  $\{h_n\}$  of  $n$  variate polynomials and degree at most  $n^c$  with coefficients in  $\{-1, 0, 1\}$  such that

$$Q_{N,c}(\overline{\text{coeff}}(h_n)) \neq 0.$$

**Remark V.8.** In the setting of small integer coefficients (or over small finite fields), there exist constructible low degree equations for both VP and VNP. However, this does not mean that the framework of algebraically natural proofs cannot be used for separating VP and VNP. It is worth noting that the equations for VP and VNP that are constructive in VP seem to be different from each other as they use different universal map constructions. This also highlights the fact that any separation of VP and VNP (in the bounded coefficient setting) cannot rely solely on the degree and circuit size of their equations, but might need to look more carefully at the structure and properties of these equations. ◇

## VI. OPEN PROBLEMS

We conclude with some open questions.

- The most natural question here is to extend the results in this paper to the entire class VP over all fields. Our proofs crucially use the complexity of the coefficients and it is not clear if ideas from this paper can be used for such an extension. A first step towards this generalization would be to understand the complexity of equations for constant-free versions of the classes VP and VNP namely  $\text{VP}^0$  and  $\text{VNP}^0$ .
- In general, proving non-trivial upper (and lower) bounds on the circuit complexity and degree of equations of varieties associated with natural algebraic models is an interesting question. In addition to proving such bounds for VP as mentioned in the item above, it is also of great interest to prove such bounds for other models, like formulas or algebraic branching programs.

## ACKNOWLEDGEMENTS

The authors from TIFR acknowledge support of the Department of Atomic Energy, Government of India, under project number RTI4001.

Mrinal thanks Rahul Santhanam and Ben Lee Volk for many insightful conversations about algebraic natural proofs and succinct hitting sets.

All the authors thank Ben Lee Volk for his helpful comments on an earlier draft of this paper.

We are also grateful to the anonymous reviewers of the conference for their valuable comments and suggestions.

## REFERENCES

- [1] M. A. Forbes, A. Shpilka, and B. L. Volk, “Succinct hitting sets and barriers to proving lower bounds for algebraic circuits,” *Theory of Computing*, vol. 14, no. 1, pp. 1–45, 2018. [Online]. Available: <https://doi.org/10.4086/toc.2018.v014a018>
- [2] J. A. Grochow, M. Kumar, M. E. Saks, and S. Saraf, “Towards an algebraic natural proofs barrier via polynomial identity testing,” *CoRR*, vol. abs/1701.01717, 2017. [Online]. Available: <http://arxiv.org/abs/1701.01717>
- [3] T. Baker, J. Gill, and R. Solovay, “Relativizations of the  $\mathcal{P} = ? \mathcal{NP}$  question,” *SIAM Journal on Computing*, vol. 4, no. 4, pp. 431–442, 1975. [Online]. Available: <https://doi.org/10.1137/0204037>
- [4] S. Aaronson and A. Wigderson, “Algebrization: A new barrier in complexity theory,” *ACM Trans. Comput. Theory*, vol. 1, no. 1, Feb. 2009. [Online]. Available: <https://doi.org/10.1145/1490270.1490272>
- [5] A. A. Razborov and S. Rudich, “Natural proofs,” *J. Comput. Syst. Sci.*, vol. 55, no. 1, pp. 24–35, 1997. [Online]. Available: <https://doi.org/10.1006/jcss.1997.1494>
- [6] S. Aaronson and A. Drucker, “Arithmetic natural proofs theory is sought,” Shtetl Optimized: Scott Aaronson’s Blog, 2008. [Online]. Available: <https://www.scottaaronson.com/blog/?p=336>
- [7] M. Furst, J. B. Saxe, and M. Sipser, “Parity, circuits, and the polynomial-time hierarchy,” *Mathematical systems theory*, vol. 17, no. 1, pp. 13–27, 1984. [Online]. Available: <https://doi.org/10.1007/BF01744431>
- [8] J. Håstad, “Almost optimal lower bounds for small depth circuits,” in *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*, ser. STOC ’86. New York, NY, USA: Association for Computing Machinery, 1986, p. 6–20. [Online]. Available: <https://doi.org/10.1145/12130.12132>
- [9] A. A. Razborov, “Lower bounds on the size of bounded depth circuits over a complete basis with logical addition,” *Mathematical notes of the Academy of Sciences of the USSR*, vol. 41, no. 4, pp. 333–338, 1987. [Online]. Available: <http://dx.doi.org/10.1007/BF01137685>
- [10] R. Smolensky, “Algebraic methods in the theory of lower bounds for boolean circuit complexity,” in *Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC 1987)*, 1987, pp. 77–82.
- [11] V. Strassen, “Die Berechnungskomplexität von elementarsymmetrischen Funktionen und von Interpolationskoeffizienten,” *Numerische Mathematik*, vol. 20, no. 3, pp. 238–251, 1973.
- [12] W. Baur and V. Strassen, “The complexity of partial derivatives,” *Theoretical Computer Science*, vol. 22, pp. 317–330, 1983.

- [13] J. A. Grochow, "Unifying known lower bounds via geometric complexity theory," *Comput. Complex.*, vol. 24, no. 2, pp. 393–475, 2015. [Online]. Available: <https://doi.org/10.1007/s00037-015-0103-x>
- [14] J. Grochow, 2013, <http://cstheory.stackexchange.com/questions/19261/degree-restriction-for-polynomials-in-mathsfpv/19268#19268>.
- [15] J. Heintz and C.-P. Schnorr, "Testing Polynomials which Are Easy to Compute (Extended Abstract)," in *Proceedings of the 12th Annual ACM Symposium on Theory of Computing (STOC 1980)*, 1980, pp. 262–272.
- [16] V. Kabanets and R. Impagliazzo, "Derandomizing polynomial identity tests means proving circuit lower bounds," *Computational Complexity*, vol. 13, no. 1-2, pp. 1–46, 2004, Preliminary version in the 35th Annual ACM Symposium on Theory of Computing (STOC 2003).
- [17] M. Bläser, C. Ikenmeyer, G. Jindal, and V. Lysikov, "Generalized matrix completion and algebraic natural proofs," in *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, 2018, pp. 1193–1206. [Online]. Available: <https://doi.org/10.1145/3188745.3188832>
- [18] M. Bläser, C. Ikenmeyer, V. Lysikov, A. Pandey, and F. Schreyer, "Variety membership testing, algebraic natural proofs, and geometric complexity theory," *CoRR*, vol. abs/1911.02534, 2019. [Online]. Available: <http://arxiv.org/abs/1911.02534>
- [19] M. Kumar and B. L. Volk, "A polynomial degree bound on defining equations of non-rigid matrices and small linear circuits," *CoRR*, vol. abs/2003.12938, 2020. [Online]. Available: <https://arxiv.org/abs/2003.12938>
- [20] K. Efremenko, A. Garg, R. Oliveira, and A. Wigderson, "Barriers for rank methods in arithmetic complexity," in *9th Innovations in Theoretical Computer Science Conference, ITCS 2018, January 11-14, 2018, Cambridge, MA, USA*, ser. LIPIcs, A. R. Karlin, Ed., vol. 94. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018, pp. 1:1–1:19. [Online]. Available: <https://doi.org/10.4230/LIPIcs.ITCS.2018.1>
- [21] A. Garg, V. Makam, R. Oliveira, and A. Wigderson, "More barriers for rank methods, via a "numeric to symbolic" transfer," in *60th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2019, Baltimore, Maryland, USA, November 9-12, 2019*, D. Zuckerman, Ed. IEEE Computer Society, 2019, pp. 824–844. [Online]. Available: <https://doi.org/10.1109/FOCS.2019.00054>
- [22] T. Y. Chow, "Almost-natural proofs," *J. Comput. Syst. Sci.*, vol. 77, no. 4, pp. 728–737, 2011. [Online]. Available: <https://doi.org/10.1016/j.jcss.2010.06.017>
- [23] C. L. Siegel, "Über einige anwendungen diophantischer approximationen," in *On Some Applications of Diophantine Approximations*, U. Zannier, Ed. Springer, 2014, pp. 81–138. [Online]. Available: [https://doi.org/10.1007/978-88-7642-520-2\\_2](https://doi.org/10.1007/978-88-7642-520-2_2)
- [24] R. Raz, "Elusive functions and lower bounds for arithmetic circuits," *Theory of Computing*, vol. 6, no. 1, pp. 135–177, 2010. [Online]. Available: <https://doi.org/10.4086/toc.2010.v006a007>
- [25] Ø. Ore, "Über höhere kongruenzen," *Norsk Mat. Forenings Skrifter*, vol. 1, no. 7, p. 15, 1922.
- [26] R. A. DeMillo and R. J. Lipton, "A Probabilistic Remark on Algebraic Program Testing," *Information Processing Letters*, vol. 7, no. 4, pp. 193–195, 1978. [Online]. Available: [http://dx.doi.org/10.1016/0020-0190\(78\)90067-4](http://dx.doi.org/10.1016/0020-0190(78)90067-4)
- [27] J. T. Schwartz, "Fast Probabilistic Algorithms for Verification of Polynomial Identities," *Journal of the ACM*, vol. 27, no. 4, pp. 701–717, 1980.
- [28] R. Zippel, "Probabilistic algorithms for sparse polynomials," in *Symbolic and Algebraic Computation, EUROSAM '79, An International Symposium on Symbolic and Algebraic Computation*, ser. Lecture Notes in Computer Science, vol. 72. Springer, 1979, pp. 216–226. [Online]. Available: [http://dx.doi.org/10.1007/3-540-09519-5\\_73](http://dx.doi.org/10.1007/3-540-09519-5_73)
- [29] P. Chatterjee, M. Kumar, C. Ramya, R. Saptharishi, and A. Tengse, "On the existence of algebraically natural proofs," *CoRR*, vol. abs/2004.14147, 2020. [Online]. Available: <https://arxiv.org/abs/2004.14147>
- [30] M. Forbes, "Polynomial Identity Testing of Read-Once Oblivious Algebraic Branching Programs," Ph.D. dissertation, Massachusetts Institute of Technology, 2014. [Online]. Available: <http://hdl.handle.net/1721.1/89843>
- [31] P. Hrubeš and A. Yehudayoff, "Arithmetic complexity in ring extensions," *Theory of Computing*, vol. 7, no. 8, pp. 119–129, 2011.