# A note on VNP-completeness and border complexity

**Christian Ikenmeyer**
University of Liverpool
christian.ikenmeyer@liverpool.ac.uk

**Abhiroop Sanyal**
Chennai Mathematical Institute
abhiroop.sanyal@gmail.com



**Abstract**

In 1979 Valiant introduced the complexity class VNP of p-definable families of polynomials, he defined the reduction notion known as p-projection and he proved that the permanent polynomial and the Hamiltonian cycle polynomial are VNP-complete under p-projections.

In 2001 Mulmuley and Sohoni (and independently Bürgisser) introduced the notion of border complexity to the study of the algebraic complexity of polynomials. In this algebraic machine model, instead of insisting on exact computation, approximations are allowed. In this short note we study the set VNPC of VNP-complete polynomials. We show that the complement VNP $\setminus$ VNPC lies dense in VNP. Quite surprisingly, we also prove that VNPC lies dense in VNP. We prove analogous statements for the complexity classes VF, VBP, and VP.

The density of VNP $\setminus$ VNPC holds for several different reduction notions: p-projections, border p-projections, c-reductions, and border c-reductions. We compare the relationship of the VNP-completeness notion under these reductions and separate most of the corresponding sets. Border reduction notions were introduced by Bringmann, Ikenmeyer, and Zuiddam (JACM 2018). Our paper is the first structured study of border reduction notions.

**2012 ACM Subject Classification** Theory of computation → Algebraic complexity theory

**Keywords and phrases** algebraic complexity theory, VNP, border complexity, reductions, completeness, topology

**Funding** *Christian Ikenmeyer*: CI supported by DFG grant IK 116/2-1

**Acknowledgements** We thank Michael Forbes for helpful insights about [13]. Moreover, Theorem 1 was initially only stated for VNP and we thank an anonymous reviewer for noting that it works in higher generality. We thank Josh Grochow for discussions about border complexity and topology that led to significant adjustments in Section 2.2 and the simplification of some proofs.

## 1 Introduction

Valiant's famous determinant versus permanent conjecture [23] states that the algebraic complexity class VBP (polynomials that can be written as determinants of polynomially large matrices of linear polynomials) is strictly contained in the class VNP (polynomials that can be written as Hamilton cycle polynomials of polynomially large matrices of linear polynomials, see Section 2.1). In 2001 Mulmuley and Sohoni in their Geometric Complexity Theory approach towards resolving Valiant's conjecture [20] stated a strengthening of the conjecture (VNP $\not\subseteq \overline{\mathrm{VBP}}$) that is based on *border complexity*, which was stated independently for circuits by Bürgisser [8, hypothesis (12)] (VNP $\not\subseteq \overline{\mathrm{VP}}$). The advantage of working with the closures of complexity classes is that this makes a large set of tools from algebraic geometry

2021-Feb-27

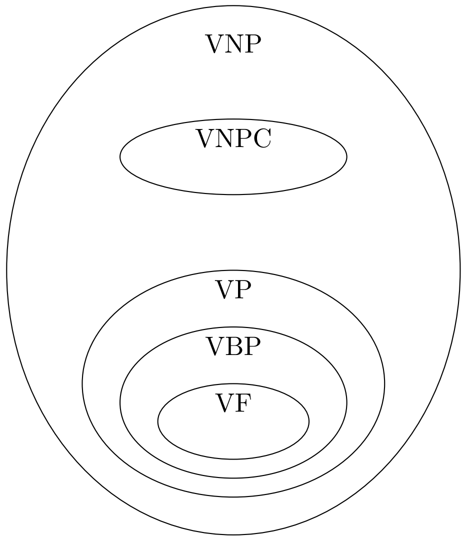



**Figure 1** The known inclusions of the classical algebraic complexity classes. VF is the class of families of polynomials with polynomially sized formulas, VBP is the class of families of polynomials that can be written as polynomially large determinants of matrices of linear polynomials, VP is the class of families of polynomials with polynomially sized circuits. VNPC is the set of VNP-complete families. From a topological perspective such a depiction can be misleading, because VNPC lies dense in VNP and also VNP$\setminus$VNPC lies dense in VNP (under p-projections), see Theorem 1.

and representation theory available, see e.g. [4]. The hope is that VBP and VNP can still be separated in this coarser setting. Indeed, it is a major open question in geometric complexity theory whether or not $\mathrm{VBP} = \overline{\mathrm{VBP}}$, see [10]. If $\mathrm{VBP} = \overline{\mathrm{VBP}}$, then Valiant's conjecture must in principle be provable by algebraic geometry, provided it is true. If $\mathrm{VNP} \subseteq \overline{\mathrm{VBP}}$, then the Geometric Complexity Theory approach fails unsalvageably, while Valiant's conjecture could still be true.

In Boolean complexity theory the relationship between complexity classes is often depicted in diagrams. An analogue for the classical algebraic complexity classes is given in Figure 1. In this paper we see that such a depiction presents misleading topological information: We study the set of VNP-complete polynomials and its complement and see that surprisingly both lie dense in VNP, see Theorem 1. We prove an analogous result for VF, VBP, and VP. This highlights that this topology is very coarse.

We take the methods for proving Theorem 1 as a basis for studying VNP-completeness under different reduction notions, in particular we study border-p-projections, which were recently introduced in [6] with a focus on the border-p-projections of the iterated $2 \times 2$ matrix multiplication polynomial. We get several separations of the power of different reduction notions in Theorem 2. Our paper gives the first analysis of border reduction notions and their relative complexity in comparison to non-border reduction notions. Moreover, our paper is the first to study border oracle complexity.

# 2 Preliminaries

## 2.1 Algebraic Complexity Theory

Fix a field $\mathbb{F}$. An algebraic circuit is defined as a rooted directed acyclic graph which has its leaf vertices labelled with variables $\{x_1, x_2, \ldots, x_n\}$ and field constants and the internal nodes labelled with $\times$ (“multiplication gates”) and $+$ (“addition gates”). By induction over the circuit structure, each internal node computes a polynomial $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. The output of a circuit is defined as the polynomial computed at its root. The size of an algebraic circuit is defined as the number of nodes in the circuit.

A sequence of natural numbers $(t_n)_{n\in\mathbb{N}}$ is called *polynomially bounded* if there exists a polynomial function $p$ such that for all $n \in \mathbb{N}$ we have $t_n \leq p(n)$. A sequence $(f) = (f_n)_{n\in\mathbb{N}}$ of multivariate polynomials is defined to be a $\mathsf{p}$-family if the number of variables in $f_n$ and the degree of $f_n$ are both polynomially bounded. The complexity class VP is defined as the set of all $\mathsf{p}$-families that have algebraic circuits whose size is polynomially bounded. If we only allow *skew* circuits, i.e., circuits for which each multiplication gate is adjacent to a leaf node, then we get the complexity class VBP. If instead we insist on the circuits to be rooted *trees*, then we get the complexity class VF. We have VF $\subseteq$ VBP $\subseteq$ VP, see e.g. [22].

For fixed natural numbers $N$ and $M$, a polynomial $f \in \mathbb{F}[x_1, x_2, \ldots, x_N]$ is said to be a *projection* of another polynomial $g \in \mathbb{F}[y_1, y_2, \ldots, y_M]$ if $f = g(\alpha_1, \alpha_2, \ldots, \alpha_M)$, where $\alpha_i \in \{x_1, x_2, \ldots, x_N\} \cup \mathbb{F}$. This is denoted by $f \leq g$. A $\mathsf{p}$-family $(f)$ is said to be the $\mathsf{p}$-projection of another $\mathsf{p}$-family $(g)$, denoted by $(f) \leq_{\mathsf{p}} (g)$, if there is a polynomially bounded function $t : \mathbb{N} \to \mathbb{N}$ such that $f_n \leq g_{t(n)}$ for all $n$.

$\mathsf{p}$-projections are the first type of reductions introduced by Valiant. Another natural example of reductions are $\mathsf{c}$-reductions, an algebraic analogue of oracle complexity. The oracle complexity $L^g(f)$ of a polynomial $f$ with oracle $g$ is defined as the minimum size of a circuit with $+, \times$, and $g$-oracle gates (the output at these gates is the computation of the polynomial $g$ on the input values. The arity of a $g$-oracle gate equals the number of variables in $g$) that can compute the polynomial $f$. Consider two $\mathsf{p}$-families $(f)$ and $(g)$. The $\mathsf{p}$-family $(f)$ is said to be a $\mathsf{c}$-reduction of $(g)$, denoted by $(f) \leq_{\mathsf{c}} (g)$, if there exists a polynomially bounded function $t : \mathbb{N} \to \mathbb{N}$ such that $L^{g_{t(n)}}(f_n)$ is polynomially bounded.

Let $\mathfrak{S}_n$ denote the symmetric group on $n$ symbols. Let $C_n \subseteq \mathfrak{S}_n$ be the subset of length $n$ cycles. The Hamiltonian cycle family (HC) is the sequence of homogeneous degree $n$ polynomials $\mathrm{HC}_n$ on $n^2$ many variables defined via $\mathrm{HC}_n := \sum_{\pi\in C_n} \prod_{i=1}^n x_{i,\pi(i)}$.

We define the class VNP as the set of all $\mathsf{p}$-families $(f)$ that satisfy $(f) \leq_{\mathsf{p}}$ (HC). This is known to be equivalent to $(f) \leq_{\mathsf{c}}$ (HC). Often a different definition is given that is closer in spirit to the counting complexity class #P, where VNP is defined as a summation of a VP function over the Boolean hypercube, but Valiant [23] showed that these definitions are equivalent. In particular, it is easy to see that VP $\subseteq$ VNP. Valiant's famous conjectures are VF $\neq$ VNP, VBP $\neq$ VNP, and VP $\neq$ VNP. To find candidates outside of VF, VBP or VP, the following notion of VNP-completeness is useful.

A $\mathsf{p}$-family $(f)$ is defined to be VNP-$\mathsf{p}$-complete if $(f) \in$ VNP and (HC) $\leq_{\mathsf{p}} (f)$. The set of all VNP-$\mathsf{p}$-complete $\mathsf{p}$-families is denoted by VNPC($\leq_{\mathsf{p}}$). Analogously, a $\mathsf{p}$-family $(f)$ is defined to be VNP-$\mathsf{c}$-complete if $(f) \in$ VNP and (HC) $\leq_{\mathsf{c}} (f)$. The set of all VNP-$\mathsf{c}$-complete $\mathsf{p}$-families is denoted by VNPC($\leq_{\mathsf{c}}$).

The main motivation behind VNP-completeness comes from the following simple observation: If we would find $(g)$ such that both $(g) \in$ VNPC($\leq_{\mathsf{p}}$) and $(g) \in$ VP, then for all $(f) \in$ VNP we would have $(f) \leq_{\mathsf{p}}$ (HC) $\leq_{\mathsf{p}} (g)$, and by transitivity $(f) \leq_{\mathsf{p}} (g)$, which implies $(f) \in$ VP, thus VP $=$ VNP. Analgously for VF and VBP instead of VP.

A $\mathsf{p}$-family $(f)$ is defined to be VF-$\mathsf{p}$-complete if $(f) \in$ VF and $(g) \leq_{\mathsf{p}} (f)$ for every $(g) \in$ VF. The set of all VF-$\mathsf{p}$-complete $\mathsf{p}$-families is denoted by VFC($\leq_{\mathsf{p}}$). The iterated $3 \times 3$ matrix multiplication polynomial family is an example of an element in VFC($\leq_{\mathsf{p}}$), see [2]. A $\mathsf{p}$-family $(f)$ is defined to be VBP-$\mathsf{p}$-complete if $(f) \in$ VBP and $(g) \leq_{\mathsf{p}} (f)$ for every $(g) \in$ VBP. The set of all VBP-$\mathsf{p}$-complete $\mathsf{p}$-families is denoted by VBPC($\leq_{\mathsf{p}}$). The determinant polynomial family is an example of an element in VBPC($\leq_{\mathsf{p}}$), see [22]. A $\mathsf{p}$-family $(f)$ is defined to be VP-$\mathsf{p}$-complete if $(f) \in$ VP and $(g) \leq_{\mathsf{p}} (f)$ for every $(g) \in$ VP. The set of all VP-$\mathsf{p}$-complete $\mathsf{p}$-families is denoted by VPC($\leq_{\mathsf{p}}$). There exist specific graph homomorphism polynomial families that are in VPC($\leq_{\mathsf{p}}$), see the recent [18]. The search for natural problems in VPC($\leq_{\mathsf{p}}$) was in fact a long-standing open problem.

## 2.2 Border complexity

In this section we define so-called *border complexity analogues* to the reduction notions in Section 2.1. This was first done explicitly in [6]. In our definitions we will use the polynomial ring $\mathbb{F}[\varepsilon]$ and the field extension $\mathbb{F}(\varepsilon)$. The reduction notions from Section 2.1 are interpreted over this field extension. Therefore, even if $g$ is a polynomial over $\mathbb{F}$, we can have $f \leq g$ with a polynomial $f$ over $\mathbb{F}(\varepsilon)$.

A polynomial $f$ over $\mathbb{F}$ is called a *border projection* of a polynomial $g$ over $\mathbb{F}$ (denoted by $f \trianglelefteq g$) if $f + \varepsilon \cdot h \leq g$ for some polynomial $h$ over $\mathbb{F}[\varepsilon]$. Clearly $f \leq g$ implies $f \trianglelefteq g$. We extend this definition to sequences of polynomials as follows. A sequence of polynomials $(f)$ is defined to be a *border* $\mathsf{p}$*-projection* of another sequence of polynomials $(g)$, denoted by $(f) \trianglelefteq_{\mathsf{p}} (g)$, if there is a polynomially bounded function $t : \mathbb{N} \to \mathbb{N}$ such that $f_n \trianglelefteq g_{t(n)}$ for all $n$.

The border oracle complexity $\overline{L^g}(f)$ of a polynomial $f$ over $\mathbb{F}$ with oracle access to a polynomial $g$ over $\mathbb{F}$ is defined as the smallest $c$ such that there exists a polynomial $h$ over $\mathbb{F}[\varepsilon]$ such that $L^g_{\mathbb{F}(\varepsilon)}(f + \varepsilon \cdot h) \leq c$, where $L^g_{\mathbb{F}(\varepsilon)}$ denotes the oracle complexity over the field $\mathbb{F}(\varepsilon)$. Clearly $\overline{L^g}(f) \leq L^g(f)$ for all $f$ and $g$. Consider two $\mathsf{p}$-families $(f)$ and $(g)$. The $\mathsf{p}$-family $(f)$ is said to be a border $\mathsf{c}$-reduction of $(g)$, denoted by $(f) \trianglelefteq_{\mathsf{c}} (g)$, if there exists a polynomially bounded function $t : \mathbb{N} \to \mathbb{N}$ such that $\overline{L^{g_{t(n)}}}(f_n)$ is polynomially bounded.

A $\mathsf{p}$-family $(f)$ is defined to be VNP-border-$\mathsf{p}$-complete if $(f) \in$ VNP and (HC) $\trianglelefteq_{\mathsf{p}} (f)$. The set of all VNP-border-$\mathsf{p}$-complete $\mathsf{p}$-families is denoted by VNPC($\trianglelefteq_{\mathsf{p}}$). Analogously, a $\mathsf{p}$-family $(f)$ is defined to be VNP-border-$\mathsf{c}$-complete if $(f) \in$ VNP and (HC) $\trianglelefteq_{\mathsf{c}} (f)$. The set of all VNP-border-$\mathsf{c}$-complete $\mathsf{p}$-families is denoted by VNPC($\trianglelefteq_{\mathsf{c}}$).

In geometric complexity theory the common type of reduction is similar to $\mathsf{p}$-projections and border-$\mathsf{p}$-projections, but instead of replacing variables with constants and variables, variables are replaced by affine linear polynomials. All proofs in this paper also work with this version of $\mathsf{p}$-projections and border-$\mathsf{p}$-projections.

Let $C$ be a complexity class definable by circuits over $\mathbb{F}$ and $\mathbb{F}(\varepsilon)$ such as VF, VBP, VP, or VNP. A $\mathsf{p}$-family $(g)$ over $\mathbb{F}$ is defined to lie in the closure $\overline{C}$ of such a class $C$ over $\mathbb{F}$ if there exists a function $e : \mathbb{N} \to \mathbb{N}$ and a $\mathsf{p}$-family $(h)$ over $\mathbb{F}[\varepsilon]$ such that $(h) \in C(\mathbb{F}(\varepsilon))$ and for every $n \in \mathbb{N}$ and $i \leq e(n)$ there exist polynomials $f_{n,i}$ over $\mathbb{F}$ with

$$h_n := g_n + \varepsilon f_{n,1} + \cdots + \varepsilon^e f_{n,e}.$$

The class $\overline{\text{VNPC}(\leq_{\mathsf{p}})}$ is not defined by circuits. A $\mathsf{p}$-family $(f)$ over $\mathbb{F}$ is defined to be in $\overline{\text{VNPC}(\leq_{\mathsf{p}})}$ if (HC) $\leq_{\mathsf{p}} (f) + \varepsilon \cdot (g)$ for some $\mathsf{p}$-family $(g)$ over $\mathbb{F}[\varepsilon]$. Analogously for $\leq_{\mathsf{c}}$, $\trianglelefteq_{\mathsf{p}}$, and $\trianglelefteq_{\mathsf{c}}$. The class $\overline{\text{VNP} \setminus \text{VNPC}(\leq_{\mathsf{p}})}$ is also not defined by circuits. A $\mathsf{p}$-family $(f)$ is defined to be in $\overline{\text{VNP} \setminus \text{VNPC}(\leq_{\mathsf{p}})}$ if $(f) + \varepsilon \cdot (g) \in \text{VNP}(\mathbb{F}(\varepsilon))$ for some $\mathsf{p}$-family $(g)$ over $\mathbb{F}[\varepsilon]$ and (HC) $\not\leq_{\mathsf{p}} (f) + \varepsilon \cdot (g)$. Analogously for $\leq_{\mathsf{c}}$, $\trianglelefteq_{\mathsf{p}}$, and $\trianglelefteq_{\mathsf{c}}$, but we will not study these three notions in this context. The closures of VFC, VBPC, VPC, VF $\setminus$ VFC, VBP $\setminus$ VBPC, VP $\setminus$ VPC are defined analogously by replacing VNP and using the respective complete polynomials.

As noted in [6], taking the closure is not a *closure operator* in the usual sense of the definition. Still, we define a sub $C \subsetneq C'$ to be *dense in* $C'$ if $\overline{C} = C'$. For all the sets VF, VBP, VP, VNP, it is a major open question if they are equal to their closure, see [10].

## 3 Main results

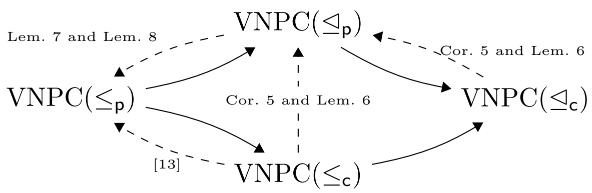
Using a fairly elementary proof we obtain the following surprising density results.

▶ **Theorem 1.** *Let $\le$ be one of $\le_{\mathsf{p}}$, $\le_{\mathsf{c}}$, $\trianglelefteq_{\mathsf{p}}$, or $\trianglelefteq_{\mathsf{c}}$. Then the set $\mathrm{VNPC}(\le)$ is a dense subset of $\mathrm{VNP}$. Moreover, the complement $\mathrm{VNP} \setminus \mathrm{VNPC}(\le_{\mathsf{p}})$ is a dense subset of $\mathrm{VNP}$. Additionally, $\mathrm{VFC}(\le)$ and $\mathrm{VF} \setminus \mathrm{VFC}(\le_{\mathsf{p}})$ are both dense in $\mathrm{VF}$; $\mathrm{VBPC}(\le)$ and $\mathrm{VBP} \setminus \mathrm{VBPC}(\le_{\mathsf{p}})$ are both dense in $\mathrm{VBP}$; and $\mathrm{VPC}(\le)$ and $\mathrm{VP} \setminus \mathrm{VPC}(\le_{\mathsf{p}})$ are both dense in $\mathrm{VP}$.*

We leave it as an open problem if $\mathrm{VNP} \setminus \mathrm{VNPC}(\le)$ is dense in VNP for the other three reduction notions. Oracle complexity is obviously too coarse to study VF-completeness, VBP-completeness, or VP-completeness.

As a second result we initiate the comparison of classical and border reduction notions. We give an almost complete separation of the sets of VNP-complete polynomials under the different reduction notions as follows.

▶ **Theorem 2.** *Over $\mathbb{F} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ we have the following diagram of inclusions (solid arrows) and non-inclusions (dashed arrows).*




The inclusions (solid arrows) are obvious. The non-inclusions are proved in the respective lemmas as annotated in the figure.

## 4 Related work

The relative power of algebraic reduction notions has been studied before: [13] show with a short argument that

$$\mathrm{VNPC}(\le_{\mathsf{p}}) \subsetneqq \mathrm{VNPC}(\le_{\mathsf{c}}).$$

They do not study border complexity though.

Border complexity has already been an object of study in algebraic complexity theory for bilinear maps since 1980 (see [3]) and is still a very active area of research today [17, 16]. The study of border complexity for polynomials has recently gained significant momentum, see for example [10, 15, 6, 5]. In fact, [6] prove that $\mathrm{VFC}(\le_{\mathsf{p}}) \subsetneqq \mathrm{VFC}(\trianglelefteq_{\mathsf{p}})$. Their proof is based on a fairly involved analysis in [1].

The Boolean world knows many types of reductions. Their relative power has been analyzed for example in [11, 12]. The notion of $\mathsf{c}$-reductions in algebraic complexity theory is relatively new [7]. The difference between $\mathsf{p}$-projections and $\mathsf{c}$-reductions plays a prominent role in [19].

## 5 Proof of Theorem 1

We start with an observation of [13] that we state simultaneously for VNP, VF, VBP, and VP. It is clear that the result holds in much higher generality.

▶ **Proposition 3** ([13]). *Fix any field $\tilde{\mathbb{F}}$. Given a* p*-family $(f)$ over $\tilde{\mathbb{F}}$ such that each $f_n$ has the following form: $f_n = q(rg_n + cg_n^2)$ for some* p*-family $(g)$ over $\tilde{\mathbb{F}}$, some fixed polynomial $r$ over $\tilde{\mathbb{F}}$ of any degree $d_2$, some fixed polynomial $q$ over $\tilde{\mathbb{F}}$ of even degree $d_1$ that is also a perfect square, and some constant $c \in \tilde{\mathbb{F}}$. Let $s$ be a univariate polynomial of odd degree $> d_1 + 2d_2$. Then for all $n$: $s \not\leq f_n$. In particular for the constant family $(s)$ we have $(s) \not\leq_{\mathsf{p}} (f)$.*

**Proof.** The proof is a very minor generalization of [13, Lemma 3.2]. Consider a univariate polynomial $s(y)$ of odd degree $M > d_1 + 2d_2$. Let $deg_y(h)$ denote the degree of a polynomial $h$ in the variable $y$, when considered as a polynomial over the polynomial ring in all its other constituent variables. We claim that $s$ cannot be written as a projection of $f_n$, for any $n$. Let $\gamma$ be any linear projection map. Then, $deg_y(\gamma(f_n)) \leq \mathsf{max}[deg_y(\gamma(q \cdot r \cdot g_n)), deg_y(\gamma(q \cdot g_n^2))]$. Also, note that $deg_y(\gamma(q)) \leq d_1$ and $deg_y(\gamma(r)) \leq d_2$.

If $deg_y(\gamma(g_n)) \leq d_2$, then $deg_y(\gamma(f_n)) \leq d_1 + 2d_2$. If $\gamma(f_n) = s(y)$, this contradicts the fact that $s(y)$ has degree $M$.

Otherwise, $deg_y(\gamma(f_n)) = deg_y(\gamma(q \cdot g_n^2))$. But $q \cdot g_n^2$ is a perfect square polynomial, hence $\deg_y(\gamma(f_n))$ is even, but $s(y)$ has odd degree. Hence, $\gamma(f_n) \neq s(y)$. ◀

**Proof of Theorem 1.** First we prove that $\mathrm{VNPC}(\leq_{\mathsf{p}})$ is dense in VNP. Let $(f) \in \mathrm{VNP}$ be arbitrary. Define

$$h_n := f_n + \varepsilon y(\mathrm{HC}_n - f_n),$$

a polynomial over $\mathbb{F}(\varepsilon)$. Let $\gamma$ denote the projection map $\gamma : y \mapsto \frac{1}{\varepsilon}$. We observe $\gamma(h_n) = \mathrm{HC}_n$ and hence $(\mathrm{HC}) \leq_{\mathsf{p}} (f) + \varepsilon \cdot (g)$ with $g_n = y(\mathrm{HC}_n - f_n)$. Therefore $(f) \in \overline{\mathrm{VNPC}(\leq_{\mathsf{p}})}$.

The result for the other reduction types is immediate, because p-projections are the weakest notion of reduction we consider, in particular $\mathrm{VNPC}(\leq_{\mathsf{p}}) \subseteq \mathrm{VNPC}(\leq_{\mathsf{c}})$, $\mathrm{VNPC}(\leq_{\mathsf{p}}) \subseteq \mathrm{VNPC}(\trianglelefteq_{\mathsf{p}})$, and $\mathrm{VNPC}(\leq_{\mathsf{p}}) \subseteq \mathrm{VNPC}(\trianglelefteq_{\mathsf{c}})$.

For the other part, let $(f) \in \mathrm{VNP}$ be arbitrary. Define

$$h_n := f_n + \varepsilon f_n^2$$

a polynomial over $\mathbb{F}(\varepsilon)$. Obviously, $(h) \in \mathrm{VNP}(\mathbb{F}(\varepsilon))$, but according to Proposition 3 (taking $\tilde{\mathbb{F}} = \mathbb{F}(\varepsilon)$, $r = q = 1$ and $c = \varepsilon$), we have $(s) \not\leq_{\mathsf{p}} (h)$ for the constant family $(s)$ and hence $(\mathrm{HC}) \not\leq_{\mathsf{p}} (h)$.

The analogous statements about VF, VBP, and VP that are claimed in the theorem are proved in exactly the same way by replacing (HC) by a complete polynomial family for the respective class. ◀

## 6 Proof of Theorem 2

We start with a classical lemma about taking roots.

▶ **Lemma 4.** *Suppose $g = f^r$ for some $f \in \mathbb{F}[\overline{\mathbf{x}}]$ of degree $d$ and constant $r$, where $\overline{\mathbf{x}}$ denotes a set of variables. Then $f$ can be computed by a $g$-oracle circuit of size poly$(d)$. In particular, if $g_n = f_n^r$ for all $n$, then $(f) \leq_{\mathsf{c}} (g)$.*

**Proof.** (The proof follows that of a special case of [14], the proof technique borrows from [24] and [9]). Consider a polynomial $g = f^r$, where $f$ has degree $d$. Notice that for every infinite field $\mathbb{F}$ and every nonzero polynomial $f$ over $\mathbb{F}[\overline{\mathbf{x}}]$, there exists $\overline{\alpha} \in \mathbb{F}^{|\overline{\mathbf{x}}|}$, such that $f(\overline{\alpha}) \neq 0$. Also, shifting the variables $f(\overline{\mathbf{x}}) \mapsto f(\overline{\mathbf{x}} + \alpha)$ is an invertible operation since you may re-shift at the input nodes of the circuit. Thus, by appropriately shifting we may assume w.l.o.g. that $g(\mathbf{0}) \neq 0$. Rescaling at the output node is also an invertible operation, so we may assume w.l.o.g. that $g(\mathbf{0}) = 1$. Then, we can write:

$$f = (1 + (g - 1))^{1/r}$$

Using the binomial theorem for rational coefficients, this gives us:

$$(1 + (g - 1))^{1/r} = 1 + \frac{1}{r}(g - 1) + \binom{1/r}{2}(g - 1)^2 + \cdots + \binom{1/r}{d}(g - 1)^d + \cdots$$

Since $g(\mathbf{0}) = 1$, then $g - 1 = 0 \bmod (\overline{\mathbf{x}})$. Thus, $(g - 1)^i$ has trailing monomial degree larger than $d$ for $i \geq d + 1$. So,

$$f = 1 + \frac{1}{r}(g - 1) + \binom{1/r}{2}(g - 1)^2 + \cdots + \binom{1/r}{d}(g - 1)^d \mod \left(\overline{\mathbf{x}}^{d+1}\right)$$

where $\overline{\mathbf{x}}^{d+1}$ denotes the set of all monomials of degree $d + 1$. We have the oracle circuit for $g$. The modular operation can be done via Strassen's homogenization trick [21]. Specifically, each homogeneous part can be written as a linear combination of $(d + 1)$ $\mathsf{p}$-projections of $g$. Thus, computing roots using oracle gates is possible with circuits of size $\mathrm{poly}(d)$. This proves the first part. The second part follows from the fact that $\mathsf{p}$-families have polynomially bounded degrees. ◀

As an immediate corollary we obtain:

▶ **Corollary 5.** $(\mathrm{HC}^2) \in \mathrm{VNPC}(\leq_{\mathsf{c}})$.

**Proof.** By Lemma 4 we have $(\mathrm{HC}) \leq_{\mathsf{c}} (\mathrm{HC}^2)$. Since $(\mathrm{HC}) \in \mathrm{VNPC}(\leq_{\mathsf{c}})$, for every $(f) \in \mathrm{VNP}$ we have $(f) \leq_{\mathsf{c}} (\mathrm{HC})$. By transitivity we have $(f) \leq_{\mathsf{c}} (\mathrm{HC}^2)$. Therefore $(\mathrm{HC}^2) \in \mathrm{VNPC}(\leq_{\mathsf{c}})$. ◀

▶ **Lemma 6.** $(\mathrm{HC}^2) \notin \mathrm{VNPC}(\trianglelefteq_{\mathsf{p}})$.

**Proof.** $(\mathrm{HC}^2) \in \mathrm{VNPC}(\trianglelefteq_{\mathsf{p}})$ is equivalent to $(\mathrm{HC}) \trianglelefteq_{\mathsf{p}} (\mathrm{HC}^2)$. Since the constant $\mathsf{p}$-family $(x)$ satisfies $(x) \trianglelefteq_{\mathsf{p}} (\mathrm{HC})$, if we prove that $(x) \ntrianglelefteq_{\mathsf{p}} (\mathrm{HC}^2)$, then $(\mathrm{HC}) \ntrianglelefteq_{\mathsf{p}} (\mathrm{HC}^2)$ by transitivity. Indeed, $(x) \trianglelefteq_{\mathsf{p}} (\mathrm{HC}^2)$ is equivalent to the existence of a polynomially bounded function $t : \mathbb{N} \to \mathbb{N}$ and a $\mathsf{p}$-family $(g)$ over $\mathbb{F}[\varepsilon]$ such that $\forall n : x + \varepsilon g_n \leq (\mathrm{HC}_{t(n)})^2$. All projections of $(\mathrm{HC}_{t(n)})^2$ are squares over $\mathbb{F}(\varepsilon)$, but for any $g_n$ over $\mathbb{F}[\varepsilon]$, $x + \varepsilon g_n$ is not a square of a polynomial over $\mathbb{F}(\varepsilon)$, which can be seen as follows. For the sake of contradiction, assume that $x + \varepsilon g_n = f^2$ for some polynomial $f$ over $\mathbb{F}(\varepsilon)$. Without loss of generality, we can assume that $f$ is univariate, i.e., $f = \sum_{i=0}^{d} c_i x^i$, because otherwise we could set all other variables to 0, which is a ring homomorphism. We denote by $g[i]$, the coefficient of $x^i$ in any polynomial $g$. Clearly, we have $c_0^2 = \varepsilon \cdot g_n[0]$. Suppose $c_0 \neq 0$. Therefore, $c_0$ is an element of degree greater than 0 in $\mathbb{F}[\varepsilon]$. Now, we consider the coefficient of $x^d$ on both sides. Clearly:

$$2c_d c_0 + \sum_{\substack{0<i,j<d \\ i+j=d}} c_i c_j = \varepsilon \cdot g_n[d]$$

So, $c_d c_0$ is a rational function of the form $\frac{p(\varepsilon)}{q(\varepsilon)}$ where both $p$ and $q$ are in $\mathbb{F}[\varepsilon]$ and $q$ does not divide $p$. Thus, $c_d = \frac{p(\varepsilon)}{r(\varepsilon)}$ where $r(\varepsilon)$ in $\mathbb{F}[\varepsilon]$ has degree greater than 0 and $r$ does not divide $p$. Now consider the coefficient of $x^{2d}$ on both sides. We get:

$$\frac{p^2(\varepsilon)}{r^2(\varepsilon)} = f^2[2d] = \varepsilon \cdot g_n[2d]$$

But $g_n[2d]$ is in $\mathbb{F}[\varepsilon]$. This gives us a contradiction! So, $c_0 = 0$. But then, $f = x \cdot h$ where $h$ is another polynomial over $\mathbb{F}(\varepsilon)$. Then, we have:

$$x + \varepsilon g_n = x^2 h^2$$

which is clearly not possible since the left-hand side has a linear term. This completes the proof. ◀

We now construct $(P) \in \mathrm{VNPC}(\trianglelefteq_{\mathsf{p}}) \setminus \mathrm{VNPC}(\leq_{\mathsf{p}})$ via

$$P_n := z^2(y\mathrm{HC}_n + y^2\mathrm{HC}_n^2)$$

where $y$ and $z$ are variables outside the set of variables in $\mathrm{HC}_n$, for all $n$.

▶ **Lemma 7.** $(P) \notin \mathrm{VNPC}(\leq_{\mathsf{p}})$

**Proof.** This is a direct consequence of Proposition 3. ◀

▶ **Lemma 8.** $(P) \in \mathrm{VNPC}(\trianglelefteq_{\mathsf{p}})$.

**Proof.** Consider the projection map $\gamma_\varepsilon$:

$$y \mapsto \varepsilon^2 \quad \text{and} \quad z \mapsto \tfrac{1}{\varepsilon}$$

We have $\gamma_\epsilon(P_n) \leq P_n$ and $\gamma_\epsilon(P_n) = \mathrm{HC}_n + \varepsilon^2\mathrm{HC}_n^2$, hence $\mathrm{HC}_n \trianglelefteq P_n$ for all $n$ and thus $(\mathrm{HC}) \trianglelefteq_{\mathsf{p}} (P)$. ◀

## References


1 Eric Allender and Fengming Wang. On the power of algebraic branching programs of width two. *Comput. Complex.*, 25(1):217–253, March 2016.

2 Michael Ben-Or and Richard Cleve. Computing algebraic formulas using a constant number of registers. *SIAM Journal on Computing*, 21(1):54–58, 1992.

3 D. Bini. Relations between exact and approximate bilinear algorithms. applications. *CALCOLO*, 17(1):87–97, Jan 1980.

4 Markus Bläser and Christian Ikenmeyer. Introduction to geometric complexity theory. `http://pcwww.liv.ac.uk/~iken/teaching_sb/summer17/introtogct/gct.pdf`, 2018.

5 Markus Bläser, Christian Ikenmeyer, Meena Mahajan, Anurag Pandey, and Nitin Saurabh. Algebraic Branching Programs, Border Complexity, and Tangent Spaces. In Shubhangi Saraf, editor, *35th Computational Complexity Conference (CCC 2020)*, volume 169 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 21:1–21:24, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

6 Karl Bringmann, Christian Ikenmeyer, and Jeroen Zuiddam. On algebraic branching programs of small width. *J. ACM*, 65(5):32:1–32:29, 2018.

7 Peter Bürgisser. *Completeness and reduction in algebraic complexity theory*, volume 7 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2000.

8 Peter Bürgisser. The complexity of factors of multivariate polynomials. *Found. Comput. Math.*, 4(4):369–396, 2004.

9 Pranjal Dutta, Nitin Saxena, and Amit Sinhababu. Discovering the roots: uniform closure results for algebraic classes under factoring. In Ilias Diakonikolas, David Kempe, and Monika Henzinger, editors, *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 1152–1165. ACM, 2018.

10 Joshua A. Grochow, Ketan D. Mulmuley, and Youming Qiao. Boundaries of VP and VNP. In Ioannis Chatzigiannakis, Michael Mitzenmacher, Yuval Rabani, and Davide Sangiorgi, editors, *43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016)*, volume 55 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 34:1–34:14, Dagstuhl, Germany, 2016. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

11 L.A. Hemaspaandra and Ogihara M. *The Complexity Theory Companion*. Springer, 2002.

12 John M. Hitchcock and A. Pavan. Comparing reductions to np-complete sets. *Information and Computation*, 205(5):694 – 706, 2007.

13 Christian Ikenmeyer and Stefan Mengel. On the relative power of reduction notions in arithmetic circuit complexity. *Inf. Process. Lett.*, 130:7–10, 2018.

14 Erich Kaltofen. Single-factor hensel lifting and its application to the straight-line complexity of certain polynomials. In Alfred V. Aho, editor, *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA*, pages 443–452. ACM, 1987.

15 Mrinal Kumar. On top fan-in vs formal degree for depth-3 arithmetic circuits. arXiv:1804.03303, 2018.

16 Joseph M Landsberg and Mateusz Michałek. A $2n^2$-$\log_2$ n -1 lower bound for the border rank of matrix multiplication. *International Mathematics Research Notices*, 2018(15):4722–4733, 03 2017.

17 Joseph M. Landsberg and Giorgio Ottaviani. New lower bounds for the border rank of matrix multiplication. *Theory of Computing*, 11(11):285–298, 2015.

18 Meena Mahajan and Nitin Saurabh. Some complete and intermediate polynomials in algebraic complexity theory. *Theory of Computing Systems*, 62(3):622–652, 2018.

19 Meena Mahajan and Nitin Saurabh. Some complete and intermediate polynomials in algebraic complexity theory. *Theory of Computing Systems*, 62(3):622–652, Apr 2018.

20 K.D. Mulmuley and M. Sohoni. Geometric Complexity Theory. I. An approach to the P vs. NP and related problems. *SIAM J. Comput.*, 31(2):496–526, 2001.

21 Volker Strassen. Vermeidung von Divisionen. *Journal für die reine und angewandte Mathematik*, 264:184–202, 1973.

22 Seinosuke Toda. Classes of arithmetic circuits capturing the complexity of computing the determinant. *IEICE Transactions on Information and Systems*, 75(1):116–124, 1992.

23 Leslie G. Valiant. Completeness classes in algebra. In *Conference Record of the Eleventh Annual ACM Symposium on Theory of Computing (Atlanta, Ga., 1979)*, pages 249–261. ACM, New York, 1979.

24 Leslie G. Valiant. Negation can be exponentially powerful. In Michael J. Fischer, Richard A. DeMillo, Nancy A. Lynch, Walter A. Burkhard, and Alfred V. Aho, editors, *Proceedings of the 11h Annual ACM Symposium on Theory of Computing, April 30 - May 2, 1979, Atlanta, Georgia, USA*, pages 189–196. ACM, 1979.