On fixed-polynomial size circuit lower bounds for uniform polynomials in the sense of Valiant

Hervé Fournier [*] Sylvain Perifel [†] Rémi de Verclos [‡]

November 29, 2013

Abstract

We consider the problem of fixed-polynomial lower bounds on the size of arithmetic circuits computing uniform families of polynomials. Assuming the generalised Riemann hypothesis (GRH), we show that for all k, there exist polynomials with coefficients in MA having no arithmetic circuits of size $O(n^k)$ over $\mathbb{C}$ (allowing any complex constant). We also build a family of polynomials that can be evaluated in AM having no arithmetic circuits of size $O(n^k)$. Then we investigate the link between fixed-polynomial size circuit bounds in the Boolean and arithmetic settings. In characteristic zero, it is proved that $\mathsf{NP} \not\subset \mathsf{size}(n^k)$, or $\mathsf{MA} \subset \mathsf{size}(n^k)$, or $\mathsf{NP} = \mathsf{MA}$ imply lower bounds on the circuit size of uniform polynomials in n variables from the class VNP over $\mathbb{C}$, assuming GRH. In positive characteristic p, uniform polynomials in VNP have circuits of fixed-polynomial size if and only if both $\mathsf{VP} = \mathsf{VNP}$ over $\mathbb{F}_p$ and $\mathsf{Mod}_p\mathsf{P}$ has circuits of fixed-polynomial size.

1 Introduction

Baur and Strassen [3] proved in 1983 that the number of arithmetic operations needed to compute the polynomials $x_1^n + \ldots + x_n^n$ is $\Omega(n \log n)$. This is still the best lower bound on uniform polynomials on n variables and of degree $n^{O(1)}$, if uniformity means having circuits computed in polynomial time.

If no uniformity condition is required, lower bounds for polynomials have been known since Lipton [12]. For example, Schnorr [17], improving on [12] and Strassen [18], showed for any k a lower bound $\Omega(n^k)$ on the complexity of a family (P_n) of univariate polynomials of degree polynomial in n – even allowing arbitrary complex constants in the circuits. The starting point of Schnorr's method is to remark that the coefficients of a polynomial computed by a circuit using constants $\alpha = (\alpha_1, \ldots, \alpha_p)$ is given by a polynomial mapping in α. Hence, finding hard polynomials reduces to finding a point outside the image of the mapping associated to some circuit which is universal for a given size. This method has been studied and extended by Raz [15].

In the Boolean setting, this kind of fixed-polynomial lower bounds has already drawn a lot of attention, from Kannan's result [9] proving that for all k, Σ_2^{p} does not have circuits of

[*] Univ Paris Diderot, Sorbonne Paris Cité, Institut de Mathématiques de Jussieu, UMR 7586 CNRS, F-75205 Paris, France. Email: `fournier@math.univ-paris-diderot.fr`.

[†] Univ Paris Diderot, Sorbonne Paris Cité, LIAFA, UMR 7089 CNRS, F-75205 Paris, France. Email: `sylvain.perifel@liafa.univ-paris-diderot.fr`.

[‡] ENS Lyon. F-69342 Lyon, France. Email: `remi.de_joannis_de_verclos@ens-lyon.fr`.

size n^k, to Fortnow, Santhanam and Williams [5], delineating the frontier of Boolean classes which are known to have fixed-polynomial size circuits lower bounds. It might seem easy to prove similar lower bounds in the algebraic world, but the fact that arbitrary constants from the underlying field (e.g. $\mathbb{C}$) are allowed prevents from readily adapting Boolean techniques.

Different notions of uniformity can be thought of, either in terms of the circuits computing the polynomials, or in terms of the complexity of computing the coefficients. For instance, an inspection of the proof of Schnorr's result mentioned above shows that the coefficients of the polynomials can be computed in exponential time. But this complexity is generally considered too high to qualify these polynomials as uniform.

The first problem we tackle is the existence of hard polynomials (i.e. without small circuits over $\mathbb{C}$) but with coefficients that are "easy to compute". The search for a uniform family of polynomials with no circuits of size n^k was pursued recently by Jansen and Santhanam [7]. They show in particular that there exist polynomials with coefficients in MA (thus, uniform in some sense) but not computable by arithmetic circuits of size n^k over $\mathbb{Z}$.[1] Assuming the generalised Riemann hypothesis (GRH), we extend their result to the case of circuits over the complex field. GRH is used to eliminate the complex constants in the circuits, by considering solutions over $\mathbb{F}_p$ of systems of polynomial equations, for a small prime p, instead of solutions over $\mathbb{C}$. In fact, the family of polynomials built by Jansen and Santhanam is also uniform in the following way: it can be evaluated at integer points in MA. Along this line, we obtain families of polynomials without arithmetic circuits of size n^k over $\mathbb{C}$ and that can be evaluated in AM. The arbitrary complex constants prevents us to adapt directly Jansen and Santhanam's method and we need to use in addition the AM protocol of Koiran [10] in order to decide whether a system of polynomial equations has a solution over $\mathbb{C}$.

Another interesting and robust notion of uniformity is provided by Valiant's algebraic class VNP, capturing the complexity of the permanent. The usual definition is non-uniform, but a natural uniformity condition can be required and gives two equivalent characterisations: in terms of the uniformity of circuits and in terms of the complexity of the coefficients. This is one of the notions we shall study in this paper and which is also used by Raz [15] (where the term *explicit* is used to denote uniform families of VNP polynomials). The second problem we study is therefore to give an $\Omega(n^k)$ lower bound on the complexity of an n-variate polynomial in the uniform version of the class VNP. Note that from Valiant's criterion, it corresponds to the coefficients being in GapP, so it is a special case of coefficients that are easy to compute. Even though MA may seem a small class in comparison with GapP (in particular due to Toda's theorem $\mathsf{PH} \subseteq \mathsf{P}^{\#\mathsf{P}}$), the result obtained above does not yield lower bounds for the uniform version of VNP.

We show how fixed-polynomial circuit size lower bound on uniform VNP is connected to various questions in Boolean complexity. For instance, the hypothesis that NP does not have circuits of size n^k for all k, or the hypothesis that MA has circuits of size n^k for some k, both imply the lower bound on the uniform version of VNP assuming GRH. Concerning the question on finite fields, we show an equivalence between lower bounds on uniform VNP and standard problems in Boolean and algebraic complexity.

The paper is organised as follows. Definitions, in particular of the uniform versions of Valiant's classes, and useful known results are given in Section 2. Hard families of polynomials with easy to compute coefficients, or that are easy to evaluate, are built in Section 3. Finally,

[1] Even though this result is not stated explicitly in their paper, it is immediate to adapt their proof to our context.

conditional lower bounds on uniform VNP are presented in the last section.

2 Preliminaries

Arithmetic circuits

An arithmetic circuit over a field K is a directed acyclic graph whose vertices have indegree 0 or 2 and where a single vertex (called the output) has outdegree 0. Vertices of indegree 0 are called inputs and are labelled either by a variable x_i or by a constant $\alpha \in K$. Vertices of indegree 2 are called gates and are labelled by + or ×.

The polynomial computed by a vertex is defined recursively as follows: the polynomial computed by an input is its label; a + gate (resp. × gate), having incoming edges from vertices computing the polynomials f and g, computes the polynomial $f+g$ (resp. fg). The polynomial computed by a circuit is the polynomial computed by its output gate.

A circuit is called *constant-free* if the only constant appearing at the inputs is -1. The *formal degree* of a circuit is defined by induction in the following way: the formal degree of a leaf is 1, and the formal degree of a sum (resp. product) is the maximum (resp. sum) of the formal degree of the incoming subtrees (thus constants "count as variables" and there is no possibility of cancellation).

We are interested in sequences of arithmetic circuits $(C_n)_{n\in\mathbb{N}}$, computing sequences of polynomials $(P_n)_{n\in\mathbb{N}}$ (we shall usually drop the subscript "$n \in \mathbb{N}$").

Definition 1. Let K be a field. If $s : \mathbb{N} \to \mathbb{N}$ is a function, a family (P_n) of polynomials over K is in $\mathsf{asize}_K(s(n))$ if it is computed by a family of arithmetic circuits of size $O(s(n))$ over K.

Similarly, $\mathsf{size}(s(n))$ denotes the set of (Boolean) languages decided by Boolean circuits of size $O(s(n))$.

Arthur-Merlin classes

A language L is in MA if there exist a polynomial $p(n)$ and $A \in \mathsf{P}$ such that for all x:

$$\begin{cases} x \in L \Rightarrow \exists y \in \{0,1\}^{p(|x|)}\ \Pr_{r\in\{0,1\}^{p(|x|)}}[(x,y,r) \in A] \geqslant 2/3; \\ x \notin L \Rightarrow \forall y \in \{0,1\}^{p(|x|)}\ \Pr_{r\in\{0,1\}^{p(|x|)}}[(x,y,r) \in A] \leqslant 1/3. \end{cases}$$

A language L is in AM if there exist a polynomial $p(n)$ and $A \in \mathsf{P}$ such that for all x:

$$\begin{cases} x \in L \Rightarrow \Pr_{r\in\{0,1\}^{p(|x|)}}[\exists y \in \{0,1\}^{p(|x|)}\ (x,y,r) \in A] \geqslant 2/3; \\ x \notin L \Rightarrow \Pr_{r\in\{0,1\}^{p(|x|)}}[\exists y \in \{0,1\}^{p(|x|)}\ (x,y,r) \in A] \leqslant 1/3. \end{cases}$$

We recall that $\mathsf{MA} \subseteq \mathsf{AM} \subseteq \mathsf{PH}$.

Counting classes

A function $f : \{0,1\}^\star \to \mathbb{N}$ is in #P if there exist a polynomial $p(n)$ and a language $A \in \mathsf{P}$ such that for all $x \in \{0,1\}^\star$

$$f(x) = |\{y \in \{0,1\}^{p(|x|)},\ (x,y) \in A\}|.$$

A function $g : \{0,1\}^\star \to \mathbb{Z}$ is in GapP if there exist two functions $f, f' \in \#\mathsf{P}$ such that $g = f - f'$. The class $\mathsf{C_=P}$ is the set of languages $A = \{x,\ g(x) = 0\}$ for some function $g \in \mathsf{GapP}$. The class $\oplus\mathsf{P}$ is the set of languages $A = \{x,\ f(x) \text{ is odd}\}$ for some function $f \in \#\mathsf{P}$. We refer the reader to [6] for more details on counting classes.

Theorem 2 (Lund et al. [13, Corollary 8])**.** *If $\#\mathsf{P}$ has Boolean circuits of polynomial size, then $\mathsf{P}^{\#\mathsf{P}} = \mathsf{MA}$.*

The counting hierarchy CH was introduced in [21]: let $\mathsf{C_1P} = \mathsf{P}^{\mathsf{PP}}$ and $\mathsf{C}_{i+1}\mathsf{P} = \mathsf{PP}^{\mathsf{C}_i\mathsf{P}}$; then $\mathsf{CH} = \bigcup_{i>0} \mathsf{C}_i\mathsf{P}$.

Valiant's classes and their uniform counterpart

Let us first recall the usual definition of Valiant's classes.

Definition 3 (Valiant's classes)**.** Let K be a field. A family (P_n) of polynomials over K is in the class VP_K if the degree of P_n is polynomial in n and (P_n) is computed by a family (C_n) of *polynomial-size* arithmetic circuits over K.

A family $(Q_n(x))$ of polynomials over K is in the class VNP_K if there exists a family $(P_n(x,y)) \in \mathsf{VP}_K$ such that

$$Q_n(x) = \sum_{y \in \{0,1\}^{\ell_n}} P_n(x,y)$$

where ℓ_n denotes the length of y in P_n.

The size of x and y is limited by the circuits for P_n and is therefore polynomial. Note that the only difference between VP_K and $\mathsf{asize}_K(\mathsf{poly})$ is the constraint on the degree of P_n. If the underlying field K is clear, we shall drop the subscript "K" and speak only of VP and VNP. Based on these usual definitions, we now define uniform versions of Valiant's classes.

Definition 4 (Uniform Valiant's classes)**.** Let K be a field. A family of circuits (C_n) is called uniform if the (usual, Boolean) encoding of C_n can be computed in time $n^{O(1)}$. A family of polynomials (P_n) over K is in the class $\mathsf{unif\text{-}VP}_K$ if it is computed by a uniform family of constant-free arithmetic circuits of polynomial formal degree.

A family of polynomials $(Q_n(x))$ over K is in the class $\mathsf{unif\text{-}VNP}_K$ if Q_n has n variables $x = x_1, \ldots, x_n$ and there exists a family $(P_n(x,y)) \in \mathsf{unif\text{-}VP}_K$ such that

$$Q_n(x) = \sum_{y \in \{0,1\}^{\ell_n}} P_n(x,y)$$

where ℓ_n denotes the length of y in P_n.

The uniformity condition implies that the size of the circuit C_n in the definition of $\mathsf{unif\text{-}VP}$ is polynomial in n. Note that $\mathsf{unif\text{-}VP}_K$ and $\mathsf{unif\text{-}VNP}_K$ only depend on the characteristic of the field K (indeed, since no constant from K is allowed in the circuits, these classes are equal to the ones defined over the prime subfield of K).

In the definition of $\mathsf{unif\text{-}VNP}$, we have chosen to impose that Q_n has n variables because this enables us to give a very succinct and clear statement of our questions. This is *not* what is done in the usual non-uniform definition where the number of variables is only limited by the (polynomial) size of the circuit.

The well-known "Valiant's criterion" (see e.g. [4, Proposition 2.20]) is easily adapted to the uniform case in order to obtain the following alternative characterisation of $\mathsf{unif\text{-}VNP}$.

Proposition 1 (Valiant's criterion)**.** *In characteristic zero, a family (P_n) is in* $\mathsf{unif\text{-}VNP}$ *iff P_n has n variables, a polynomial degree and its coefficients are computable in* GapP*; that is, the function mapping $(c_1, \ldots, c_n)$ to the coefficient of $X_1^{c_1} \cdots X_n^{c_n}$ in P_n is in* GapP*.*

The same holds in characteristic $p > 0$ with coefficients in "$\mathsf{GapP} \mod p$"[2]*.*

Over a field K, a polynomial $P(x_1, \ldots, x_n)$ is said to be a projection of a polynomial $Q(y_1, \ldots, y_m)$ if $P(x_1, \ldots, x_n) = Q(a_1, \ldots, a_m)$ for some choice of $a_1, \ldots, a_m \in \{x_1, \ldots, x_n\} \cup K$. A family (P_n) reduces to (Q_n) (via projections) if P_n is a projection of $Q_{q(n)}$ for some polynomially bounded function q.

The permanent polynomial is defined by

$$\mathrm{per}_n(x_{1,1}, \ldots, x_{n,n}) = \sum_{\sigma} \prod_{i=1}^{n} x_{i,\sigma(i)},$$

where the sum is on all permutations $\sigma \in S_n$. The family (per_n) is known to be VNP-complete (for projections) over any field of characteristic different from 2. The Hamiltonian Circuit polynomial is defined by

$$\mathrm{HC}_n(x_{1,1}, \ldots, x_{n,n}) = \sum_{\sigma} \prod_{i=1}^{n} x_{i,\sigma(i)},$$

where the sum is on all cycles $\sigma \in S_n$ (i.e. on all the Hamiltonian cycles of the complete graph over $\{1, \ldots, n\}$). The family (HC_n) is known to be VNP-complete (for projections) over any field [20].

Elimination of complex constants in circuits

The method used to handle polynomial systems over $\mathbb{C}$ is based on the theorem below. The satisfiability of such a system over $\mathbb{C}$ is reduced to its satisfiability over small finite fields $\mathbb{F}_p$: for this we need to assume the generalised Riemann hypothesis. This conjecture is widely believed to be true and implies precise results on the distribution of prime numbers. The following theorem shows in particular that if a system of polynomial equations with integer coefficients has a solution over the complex field then it has a solution modulo a small enough prime number p. Without the generalised Riemann hypothesis, this number p would be too large to derive our results. The following theorem is a weakening of [10] adapted to our purpose.

Theorem 5 (Koiran [10, Theorems 1 and 8])**.** *Let S be a system of polynomial equations*

$$P_1(x_1, \ldots, x_n) = 0, \ldots, P_r(x_1, \ldots, x_n) = 0$$

over n unknowns, with coefficients in $\mathbb{Z}$ and with the following parameters: $r \leqslant 2^{n^a}$ for some a, coefficients with absolute value bounded by $2^{2^{n^a}}$ and for all i, the degree of P_i is at most 2^{n^a}.

Assume GRH. There exist integers $m = n^{O(a)}$ and $x_0 = 2^{n^{O(a)}}$ such that the following holds. Let E be the set of primes p smaller than x_0 such that S has a solution modulo p.

- *If S is not satisfiable over $\mathbb{C}$, then $|E| \leqslant 2^{m-2}$;*

[2] This is equivalent to the fact that for all $v \in \mathbb{F}_p$, the set of monomials having coefficient v is in $\mathsf{Mod}_p\mathsf{P}$.

- *If S is satisfiable over $\mathbb{C}$, then $|E| \geqslant m2^m$.*

Furthermore, if S is satisfiable over $\mathbb{C}$, then it is satisfiable over $\mathbb{F}_p$ for some $2^{n^a} < p < 2^{n^{O(a)}}$.

We shall also need an upper bound on the following problem HN (named after Hilbert's Nullstellensatz):

Input A system $S = \{P_1 = 0, \ldots, P_m = 0\}$ of n-variate polynomial equations with integer coefficients, each polynomial $P_i \in \mathbb{Z}[x_1, \ldots, x_n]$ being given as a constant-free arithmetic circuit.

Question Does the system S have a solution in $\mathbb{C}^n$?

Theorem 6 (Koiran [11])**.** *Assuming GRH is true, HN $\in$ AM.*

Let us now state a consequence of VNP having small arithmetic circuits over the complex field.

Theorem 7 (Bürgisser [4, Corollary 4.6])**.** *Assume GRH. If $(per_n) \in \mathsf{asize}_{\mathbb{C}}(n^{O(1)})$ then $\#\mathsf{P}$ has Boolean circuits of polynomial size.*

Finally, we shall need several times the following straightforward consequence of Theorem 7, Theorem 2 and Toda's theorem.

Corollary 1. *Assume GRH. If $(per_n) \in \mathsf{asize}_{\mathbb{C}}(n^{O(1)})$, then $\mathsf{PH} = \mathsf{MA}$.*

3 Hard polynomials with coefficients in MA

We begin with lower bounds on polynomials with coefficients in PH before bringing them down to MA.

Hard polynomials with coefficients in PH

Theorem 8. *Assume GRH is true. For any constant k, there is a family (P_n) of univariate polynomials with coefficients in $\{0, 1\}$ satisfying:*

- $\deg(P_n) = n^{O(1)}$ *(polynomial degree);*
- *the coefficients of P_n are computable in PH, that is, on input $(1^n, i)$ we can decide in PH if the coefficient of x^i is 1;*
- *(P_n) is not computed by arithmetic circuits over $\mathbb{C}$ of size n^k.*

Proof. Fix k. By Schnorr [17], there exists a sequence of univariate polynomials with coefficients in $\{0, 1\}$, degree $d = n^{3k}$ and without circuits of size n^k over $\mathbb{C}$.

As we explain in the next paragraph, the problem CS of whether a polynomial $\sum_{i=0}^{d} a_i X^i$ given by its integer coefficients (in binary) has an arithmetic circuit of size n^k over $\mathbb{C}$ belongs to PH. Then, as in Kannan's proof [9], we can define in $\mathsf{PH}^{\mathrm{CS}}$ the smallest tuple of coefficients $(a_0, \ldots, a_d) \in \{0, 1\}^{d+1}$ (in the lexicographic order) such that $\sum_{i=0}^{d} a_i X^i$ has no arithmetic circuit of size n^k over $\mathbb{C}$. This gives the family (P_n) of the theorem.

Let us now show that CS $\in$ PH. If $C(X, \alpha_1, \ldots, \alpha_t)$ is an arithmetic circuit using constants $\alpha_1, \ldots, \alpha_t \in \mathbb{C}$, we call its *skeleton* the circuit $C(X, u_1, \ldots, u_t)$ where the constants $\alpha_1, \ldots, \alpha_t$ are replaced with different formal variables $u_1, \ldots, u_t$. The polynomial $\sum_{i=0}^{d} a_i X^i$ is computed by an arithmetic circuit of size n^k over $\mathbb{C}$ if and only if there exist a circuit skeleton $C(X, u_1, \ldots, u_t)$ of size n^k and $\alpha_1, \ldots, \alpha_t \in \mathbb{C}$ for which the coefficients of $C(X, \alpha_1, \ldots, \alpha_t)$ are $a_0, \ldots, a_d$. Computing the homogeneous components of C gives circuits $C_i(u_1, \ldots, u_t)$ $(0 \leqslant i \leqslant d)$ of size $O(dn^k)$ for the coefficients of $X^0, X^1, \ldots, X^d$ in $C(X, u_1, \ldots, u_t)$. The system $\{C_i(u_1, \ldots, u_t) = a_i \ : \ 0 \leqslant i \leqslant d\}$ with unknowns $u_1, \ldots, u_t$ has a solution over $\mathbb{C}$ if and only if $\sum_{i=0}^{d} a_i X^i$ is computed by some instantiation of the skeleton $C(X, u_1, \ldots, u_t)$. By Theorem 6, if we assume GRH then deciding if this system has a solution is in AM. Hence, CS $\in \mathsf{NP}^{\mathsf{AM}} \subseteq \mathsf{PH}$. □

Alternatively, one could show the existence of n-variate polynomials, with 0-1 coefficients in PH, with total degree $O(k)$ and without circuits of size n^k over $\mathbb{C}$.

Hard polynomials with coefficients in MA

Allowing n variables and degree $n^{O(1)}$, we can even obtain lower bounds for polynomials with coefficients in MA.

Corollary 2. *Assume GRH is true. For any constant k, there is a family (P_n) of polynomials on n variables, of degree $n^{O(1)}$, with coefficients in $\{0, 1\}$ computable in MA, and such that $(P_n) \notin \mathsf{asize}_{\mathbb{C}}(n^k)$.*

Proof. If the permanent family (per_n) does not have circuits of polynomial size over $\mathbb{C}$, consider the following variant with n variables: $\mathrm{per}'_n(x_1, \ldots, x_n) = \mathrm{per}_{\lfloor\sqrt{n}\rfloor}(x_1, \ldots, x_{\lfloor\sqrt{n}\rfloor^2})$. This is a family whose coefficients are in P (hence in MA) and without circuits of size n^k.

On the other hand, if the permanent family (per_n) has circuits of polynomial size over $\mathbb{C}$, then $\mathsf{PH} = \mathsf{MA}$ under GRH by Corollary 1. Therefore the family of polynomials of Theorem 8 has its coefficients in MA. □

Hard polynomials that can be evaluated in AM

A family of polynomials $(P_n(x_1, \ldots, x_n))$ is said to be evaluable in AM if

$$\{(a_1, \ldots, a_n, i, b) \mid \text{the } i\text{-th bit of } P_n(a_1, \ldots, a_n) \text{ is } b\} \in \mathsf{AM},$$

where $a_1, \ldots, a_n, i$ are integers given in binary and $b \in \{0, 1\}$.

What is the relationship between polynomials with easy-to-compute coefficients and polynomials that are easy to evaluate? For univariate polynomials with a polynomial degree and integer coefficients of polynomial size, these two notions can be related as follows. For a complexity class C, if a polynomial is evaluable in C, the bits of its coefficients are in P^{C} by interpolation. Conversely, if the bits of its coefficients are in C, the polynomial can be evaluated in P^{C}. For multivariate polynomials, it seems there is no implication between these two notions. Some polynomials have easy-to-compute coefficients but are believed to be hard to evaluate: this is the case of the permanent. Conversely, although it seems difficult to produce an example of an easy-to-evaluate polynomial with hard-to-compute coefficients, there are easy-to-evaluate polynomials whose *partial* coefficients are hard: for example, the coefficient of $x_1 \ldots x_n$ in $\prod_{i=1}^{n} \sum_{j=1}^{n} y_{i,j} x_j$ is the permanent of the matrix $(y_{i,j})$.

In the next proposition, we show how to obtain hard polynomials which can be evaluated in AM. The method is based on Santhanam [16] and Koiran [11]. The protocol described below heavily relies on the technique used in [11, Theorem 2] to prove that $\mathrm{HN} \in \mathsf{AM}$. However, this two-round protocol is not used as a black box since the system of equations considered in our proof is of exponential size and handled implicitly.

Lemma 1 (Kabanets and Impagliazzo [8]). *The language*

$$L = \{(C, n, p) \ : \ \textit{the arithmetic circuit } C \textit{ computes } per_n \textit{ over } \mathbb{F}_p\}$$

belongs to coRP.

Theorem 9. *Assume GRH is true. For any constant k, there is a family (P_n) of polynomials on n variables, with coefficients in $\{0,1\}$, of degree $n^{O(1)}$, evaluable in AM and such that $(P_n) \notin \mathsf{asize}_{\mathbb{C}}(n^k)$.*

Proof. We adapt the method of Santhanam [16] to the case of circuits with complex constants.

If the permanent has polynomial-size circuits over $\mathbb{C}$, then $\mathsf{PH} = \mathsf{MA}$ by Corollary 1. Hence the family of polynomials of Theorem 8 is evaluable in $\mathsf{MA} \subseteq \mathsf{AM}$.

Otherwise, call $s(n)$ the minimal size of a circuit over $\mathbb{C}$ for per_n. The n-tuple of variables $(x_1, \ldots, x_n)$ is split in two parts (y, z) in the unique way satisfying $0 < |y| \leqslant |z|$ and $|z|$ a power of two. Remark therefore that $|y|$ can take all the values from 1 to $|z|$ depending on n. We now define the polynomial $P_n(y, z)$:

$$\begin{cases} P_n(y,z) = \mathrm{per}_{\sqrt{|y|}}(y) & \text{if } |y| \text{ is a square and } s(\sqrt{|y|}) \leqslant n^{2k} \\ P_n(y,z) = 0 & \text{otherwise.} \end{cases}$$

The variables z are only used as padding to bring down the complexity of the permanent below n^{2k}.

Let us first show that (P_n) does not have circuits of size n^k. By hypothesis there exist infinitely many n such that $s(n) > (3n^2)^{2k}$: let n_0 be one of them and take m the least power of two such that $s(n_0) \leqslant (m + n_0^2)^{2k}$, which implies $m \geqslant 2n_0^2$. Let $n_1 = m + n_0^2$: by definition of (P_n), we have $P_{n_1}(y,z) = \mathrm{per}_{n_0}(y)$. By definition of m, $s(n_0) > (m/2 + n_0^2)^{2k} > (n_1/2)^{2k} > n_1^k$. This means that per_{n_0}, and hence P_{n_1}, does not have circuits of size n_1^k.

We now show that (P_n) can be evaluated in AM. We give an MAMA protocol which is enough since $\mathsf{MAMA} = \mathsf{AM}$ (see [2]).

Recall that the variables $x = (x_1, \ldots, x_n)$ of P_n are split into (y, z) as above. If $|y|$ is not a square, then $P_n(x) = 0$ and Arthur will accept if and only if $b = 0$. We now assume $|y|$ is a square and let $t = \sqrt{|y|}$.

In the protocol, Merlin will send a constant-free circuit $C(y, u)$ of size $s \leqslant n^{2k}$ where $|y| = t^2$ and u is a tuple of variables. From this circuit we define a system of polynomial equations

$$S = \left\{ C(\varepsilon, u) = \mathrm{per}_t(\varepsilon) \ : \ \varepsilon \in \{0, \ldots, 2^s\}^{|y|} \right\},$$

where the unknowns are u.

If the variables u can be replaced by complex numbers α such that $C(y, \alpha)$ computes the permanent over the complex field, then S is obviously satisfiable. Conversely, if S is satisfiable, there exists $\alpha \in \mathbb{C}^{|u|}$ such that $C(y, \alpha)$ computes the permanent over $\{0, \ldots, 2^s\}^{|y|}$; since the degree of the polynomial computed by the circuit $C(y, \alpha)$ is at most 2^s, $C(y, \alpha)$ is equal to the permanent by interpolation (e.g. Schwartz-Zippel lemma).

The system S has the following parameters: the number of variables is $|u|$ which is at most s, the degree of each equation is bounded by 2^s, the number of equations is $2^{O(s|y|)} = 2^{O(s^2)}$ and the absolute value of each coefficient is $2^{2^{s^{O(1)}}}$. Hence, by Theorem 5, there are integers $m = s^{O(1)}$ and $x_0 = 2^{s^{O(1)}}$ such that the following holds. Let E be the set of primes p smaller than x_0 such that S has a solution modulo p.

- If S is not satisfiable over $\mathbb{C}$, then $|E| \leqslant 2^{m-2}$;
- If S is satisfiable over $\mathbb{C}$, then $|E| \geqslant m2^m$.

Testing if $|E|$ is large or small will be done via the following probabilistic argument from [11]. For an integer $p \leqslant x_0$, let $\hat{p} \in \mathbb{F}_2{}^{\log x_0}$ denote the binary representation of p. For some matrices A_j over $\mathbb{F}_2$ of size $m \times \log x_0$, the predicate $\phi(A_1, \ldots, A_m)$ is defined as

$$\exists p_0, p_1, \ldots, p_m \in E \ : \ \psi(A_1, \ldots, A_m, p_0, \ldots, p_m)$$

where

$$\psi(A_1, \ldots, A_m, p_0, \ldots, p_m) \equiv \bigwedge_{j=1}^{m} (A_j\hat{p}_0 = A_j\hat{p}_j \wedge p_0 \neq p_j)\,.$$

If A_j are seen as hashing functions, the predicate ϕ above expresses that there are enough collisions between elements of E. It is proved in [11] that if $|E| \leqslant 2^{m-2}$, the probability that $\phi(A_1, \ldots, A_m)$ holds is at most $1/2$ when the matrices A_j are chosen uniformly at random, whereas it is 1 when $|E| \geqslant m2^m$. Checking if $p_j \in E$ will be done by testing if a circuit computes the permanent over $\mathbb{F}_{p_j}$.

We are now ready to explain the MAMA protocol to evaluate the family (P_n). Let $(a_1, \ldots, a_n, i, b)$ be the input. As for $(x_1, \ldots, x_n)$, we split $(a_1, \ldots, a_n)$ into (a', a'') such that $|a'| = |y| = t^2$. The protocol is the following:

- Merlin sends a constant-free circuit $C(y, u)$ of size $s \leqslant n^{2k}$ where u is a tuple of variables. The circuit $C(y, u)$ is the skeleton of a circuit supposedly computing per_t over $\mathbb{C}$ (that is, there is a way to replace the formal variables u with elements from $\mathbb{C}$ such that the circuit computes per_t).
- Arthur sends to Merlin random matrices $A_1, \ldots, A_m$ over $\mathbb{F}_2$.
- Merlin sends prime integers $p_0, \ldots, p_m$ together with constants $\alpha_{p_j} \in \mathbb{F}_{p_j}^{|u|}$ for C, for all $0 \leqslant j \leqslant m$. He also sends a prime number $p \geqslant t!M^t$ (where M is the largest value in $a' = (a_1, \ldots, a_{t^2})$) and constants $\alpha_p \in \mathbb{F}_p^{|u|}$ for C.
- Arthur checks that $\psi(A_1, \ldots, A_m, p_0, \ldots, p_m)$ is true. Then he checks that all p_j and p are primes and that the circuits $C(y, \alpha_{p_j})$ and $C(y, \alpha_p)$ compute the permanent modulo $p_0, \ldots, p_m, p$ using Lemma 1. If any of these tests fails, Arthur accepts iff $b = 0$. Otherwise, he computes $C(a', \alpha_p)$ and accepts iff its i-th bit is equal to b.

If $s(|y|) \leqslant n^{2k}$, then $P_n(y, z) = \mathrm{per}_t(y)$. We show that Merlin can convince Arthur with probability 1. Merlin sends a correct skeleton C: since $|E| \geqslant m2^m$, there are prime integers $p_0, \ldots, p_m \in E$ such that $\psi(A_1, \ldots, A_m, p_0, \ldots, p_m)$ holds. Merlin sends such numbers p_j

together with the correct constants for the circuit C to compute the permanent modulo p_j. He also sends p with the correct constants for the permanent modulo p: p and the constants are guaranteed to exist by Theorem 5. In the fourth round, all the verifications are satisfied with probability 1 and Arthur computes the permanent modulo p (which is larger than the permanent of the input) and therefore gives the right answer.

On the other hand, if $s(|y|) > n^{2k}$ then $|E| \leqslant 2^{m-2}$. Whatever Merlin sends as prime numbers p_j, the probability (over the matrices A_j) that all p_j belong to E and produce a collision is at most $1/2$. Since the error when testing if $p_j \in E$ can be made as small as we wish (testing if $C(y, \alpha_{p_j})$ computes $\mathrm{per}_t(y) \mod p_j$ is done in coRP by Lemma 1), the probability that the whole protocol gives the wrong answer in this case is bounded by $2/3$. $\square$

4 Conditional lower bounds for uniform VNP

Recall that by definition, the n-th polynomial of a family in $\mathsf{unif\text{-}VNP}$ has exactly n variables (as opposed the usual definition of VNP where it is $n^{O(1)}$), which makes the results in this section non trivial.

In characteristic zero

In this whole subsection we assume GRH is true. Our main result is that if for all k, $\mathsf{C_{=}P}$ has no circuits of size n^k, then the same holds for $\mathsf{unif\text{-}VNP}$ (in characteristic zero). For the clarity of exposition, we first prove the weaker result where the assumption is on the class NP instead.

Lemma 2. *If there exists k such that $\mathsf{unif\text{-}VNP} \subseteq \mathsf{asize}_{\mathbb{C}}(n^k)$, then there exists ℓ such that $\mathsf{NP} \subseteq \mathsf{size}(n^\ell)$.*

Proof. Let us assume that $\mathsf{unif\text{-}VNP} \subseteq \mathsf{asize}_{\mathbb{C}}(n^k)$. Let $L \in \mathsf{NP}$. There is a polynomial q and a polynomial time computable relation $\phi : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}$ such that for all $x \in \{0,1\}^n$, $x \in L$ if and only if $\exists y \in \{0,1\}^{q(n)}\ \phi(x,y) = 1$.

We define the polynomial P_n by

$$P_n(X_1,\dots,X_n) = \sum_{x\in\{0,1\}^n} \left(\sum_{y\in\{0,1\}^{q(n)}} \phi(x,y) \right) \prod_{i=1}^{n} X_i^{x_i}(1-X_i)^{1-x_i}.$$

Note that for $x \in \{0,1\}^n$, $P_n(x)$ is the number of elements y in relation with x via ϕ. By Valiant's criterion (Proposition 1), the family (P_n) belongs to $\mathsf{unif\text{-}VNP}$ in characteristic 0. By hypothesis, there exists a family of arithmetic circuits (C_n) over $\mathbb{C}$ computing (P_n), with C_n of size $t = O(n^k)$.

Let $\alpha = (\alpha_1,\dots,\alpha_t)$ be the complex constants used by the circuit C_n: then $P_n(X_1,\dots,X_n) = C_n(X_1,\dots,X_n,\alpha)$. Take one unknown Y_i for each α_i and one additional unknown Z, and consider the following system S:

$$\begin{cases} \left(\prod_{x\in L\cap\{0,1\}^n} C_n(x,Y)\right)\cdot Z = 1 \\ C_n(x,Y) = 0 \text{ for all } x \in \{0,1\}^n \setminus L. \end{cases}$$

Let $\beta = \left(\prod_{x\in L\cap\{0,1\}^n} C_n(x,\alpha)\right)^{-1}$. Then (α,β) is a solution of S over $\mathbb{C}$.

The system S has $t+1 = O(n^k)$ unknowns. The degree of $C_n(x,Y)$ is bounded by 2^t; hence the degree of S is at most $2^{O(n^k)}$. Moreover, the absolute value of the coefficients of the polynomials in S is bounded by $2^{2^{O(n^k)}}$. Since the system S has the solution (α,β) over $\mathbb{C}$, by Theorem 5 it has a solution over $\mathbb{F}_p$ for $p = 2^{n^{O(k)}}$. (Note that introducing one equation $C_n(x,Y)Z_x = 0$ for each $x \in L \cap \{0,1\}^n$ in the system S instead of the single equation above would not work since it would require to introduce an exponential number of new variables Z_x.)

Consider such a prime number p and (α',β') a solution of the system S over $\mathbb{F}_p$. By definition of S, when the circuit C_n is evaluated over $\mathbb{F}_p$, the following is satisfied:

$$\begin{cases} \forall x \in L \cap \{0,1\}^n, & C_n(x,\alpha') \neq 0, \\ \forall x \in \{0,1\}^n \setminus L, & C_n(x,\alpha') = 0. \end{cases}$$

Computations over $\mathbb{F}_p$ can be simulated by Boolean circuits, using $\log_2 p$ bits to represent an element of $\mathbb{F}_p$, and $O(\log^2 p)$ gates to simulate an arithmetic operation. This yields Boolean circuits of size n^ℓ for $\ell = O(k)$ to decide the language L. □

Theorem 10. *Assume GRH is true. Suppose one of the following conditions holds:*

1. $\mathsf{NP} \not\subset \mathsf{size}(n^k)$ *for all* k*;*
2. $\mathsf{C_=P} \not\subset \mathsf{size}(n^k)$ *for all* k*;*
3. $\mathsf{MA} \subset \mathsf{size}(n^k)$ *for some* k*;*
4. $\mathsf{NP} = \mathsf{MA}$.

Then $\mathsf{unif\text{-}VNP} \not\subset \mathsf{asize}_{\mathbb{C}}(n^k)$ *for all* k*.*

Proof. The first point is proved in Lemma 2.

The second point subsumes the first since $\mathsf{coNP} \subseteq \mathsf{C_=P}$. It can be proved in a very similar way. Indeed consider $L \in \mathsf{C_=P}$ and $f \in \mathsf{GapP}$ such that $x \in L \iff f(x) = 0$, and its associated family of polynomials

$$P_n(X_1,\ldots,X_n) = \sum_{x\in\{0,1\}^n} f(x)\prod_{i=1}^{n} X_i^{x_i}(1-X_i)^{1-x_i}$$

as in the proof of Lemma 2. Then for all $x \in \{0,1\}^n$, $P_n(x) = 0$ iff $x \in L$. The family (P_n) belongs to $\mathsf{unif\text{-}VNP}$ and thus, assuming $\mathsf{unif\text{-}VNP} \subset \mathsf{asize}_{\mathbb{C}}(n^k)$, has arithmetic circuits (C_n) over $\mathbb{C}$ of size $t = O(n^k)$. Constants of $\mathbb{C}$ are replaced with elements of a small finite field by considering the system:

$$\begin{cases} C_n(x,Y) = 0 \text{ for all } x \in L \cap \{0,1\}^n \\ \left(\prod_{x\in\{0,1\}^n\setminus L} C_n(x,Y)\right) \cdot Z = 1. \end{cases}$$

The end of the proof is similar.

For the third point, let us assume $\mathsf{unif\text{-}VNP} \subset \mathsf{asize}_{\mathbb{C}}(\mathsf{poly})$. Then the uniform family (per_n) has circuits of polynomial size over $\mathbb{C}$. Therefore under GRH, $\mathsf{PH} = \mathsf{MA}$ by Corollary 1. This implies $\mathsf{MA} \not\subset \mathsf{size}(n^k)$ for all k since $\mathsf{PH} \not\subset \mathsf{size}(n^k)$ for all k [9].

For the last point, assume $\mathsf{NP} = \mathsf{MA}$. If NP is without n^k-size circuits for all k, then the conclusion comes from the first point. Otherwise MA has n^k-size circuits for some k and the conclusion follows from the previous point. □

For any constant c, the class $\mathsf{P}^{\mathsf{NP}[n^c]}$ is the set of languages decided by a polynomial time machine making $O(n^c)$ calls to an NP oracle. It is proven in [5] that $\mathsf{NP} \subset \mathsf{size}(n^k)$ implies $\mathsf{P}^{\mathsf{NP}[n^c]} \subset \mathsf{size}(n^{ck^2})$. Hence, it is enough to assume fixed-polynomial lower bounds on this larger class $\mathsf{P}^{\mathsf{NP}[n^c]}$ for some c to get fixed-polynomial lower bounds on $\mathsf{unif\text{-}VNP}_{\mathbb{C}}$.

An unconditional lower bound in characteristic zero

In this part we do not allow arbitrary constants in circuits. We consider instead circuits with -1 as the only scalar that can label the leaves. For $s : \mathbb{N} \to \mathbb{N}$, let $\mathsf{asize}_0(s(n))$ be the family of polynomials computed by families of unbounded degree constant-free circuits of size $O(s(n))$ (in characteristic zero). Note that the formal degree of these circuits are not polynomially bounded: hence, large constants produced by small arithmetic circuits can be used.

We first need a result of [1]. Let PosCoefSLP be the following problem: on input (C, i) where C is a constant-free circuit with one variable x and i is an integer, decide whether the coefficient of x^i in the polynomial computed by C is positive.

Theorem 11 (Allender et al. [1]). *PosCoefSLP is in* CH*.*

The following result extends Theorem 2 to CH.

Lemma 3. *If* $\#\mathsf{P}$ *has polynomial size circuits, then* $\mathsf{CH} = \mathsf{MA}$*.*

Proof. If $\#\mathsf{P}$ has circuits of polynomial size, then by Theorem 2, $\mathsf{C}_1\mathsf{P} = \mathsf{P}^{\mathsf{PP}} = \mathsf{P}^{\#\mathsf{P}} = \mathsf{MA}$.

Assume we have proved $\mathsf{C}_i\mathsf{P} = \mathsf{MA}$: then $\mathsf{C}_{i+1}\mathsf{P} = \mathsf{PP}^{\mathsf{C}_i\mathsf{P}} = \mathsf{PP}^{\mathsf{MA}}$. But $\mathsf{PP}^{\mathsf{PH}} = \mathsf{P}^{\mathsf{PP}}$ by [19] (see also [6, Corollary 4.17]). Hence $\mathsf{C}_{i+1}\mathsf{P} = \mathsf{P}^{\mathsf{PP}} = \mathsf{MA}$. It follows that $\mathsf{CH} = \mathsf{MA}$. □

Theorem 12. $\mathsf{unif\text{-}VNP} \not\subset \mathsf{asize}_0(n^k)$ *for all* k*.*

Proof. If the permanent family does not have constant-free arithmetic circuits of polynomial size, then the variant with n variables $\mathrm{per}'_n(x_1, \dots, x_n) = \mathrm{per}_{\lfloor\sqrt{n}\rfloor}(x_1, \dots, x_{\lfloor\sqrt{n}\rfloor^2})$ matches the statement.

Otherwise $\#\mathsf{P}$ has polynomial size circuits, hence $\mathsf{CH} = \mathsf{MA}$ by Lemma 3. For a given constant-free circuit C computing a univariate polynomial $P = \sum_{i=0}^d a_i x^i$, its "sign condition" is defined as the series $(b_i)_{i\in\mathbb{N}}$ where $b_i \in \{0,1\}$, $b_i = 1$ iff $a_i > 0$.

Note that for some constant α, there are at most $2^{n^{\alpha k}}$ different sign conditions of constant-free circuits of size n^k (at most one per circuit). Hence there exists a sign condition

$$(b_0, \dots, b_{n^{\alpha k}}, 0, 0, \dots)$$

such that any polynomial with such a sign condition is not computable by constant-free circuits of size n^k. We define $b_0, \dots, b_{n^{\alpha k}}$ to be the lexicographically first such bits.

We can express these bits as the first in lexicographic order such that for every constant-free circuit C, there exists i such that:

$$b_i = 0 \text{ iff the coefficient of } x^i \text{ in } C \text{ is positive.}$$

Therefore they can be computed in $\mathsf{PH}^{\mathrm{PosCoefSLP}}$, hence in CH by Theorem 11, hence in MA since $\mathsf{CH} = \mathsf{MA}$. By reducing the probability of error in the MA protocol, this means that there exists a polynomial-time function $a : \{0,1\}^\star \to \{0,1\}$ such that:

$$\begin{cases} \exists y \sum_r a(i,y,r) \geqslant (1 - 2^{-|y|-1})N & \text{if } b_i = 1 \\ \forall y \sum_r a(i,y,r) \leqslant 2^{-|y|-1}N & \text{if } b_i = 0, \end{cases}$$

where y and r are words of polynomial size, and where $N = 2^{|r|}$. Now, the following polynomial family:

$$P_n(x) = \sum_{i=0}^{n^{\alpha k}} \Big((\sum_{y,r} a(i,y,r)) - N/2 \Big) x^i$$

is in $\mathsf{unif}\text{-}\mathsf{VNP}$ and has sign condition $(b_0, \dots, b_{n^{\alpha k}}, 0, 0, \dots)$. □

In positive characteristic

This subsection deals with fixed-polynomial lower bounds in positive characteristic. The results are presented in characteristic 2 but they hold in any positive characteristic p (replacing $\oplus\mathsf{P}$ with $\mathsf{Mod}_p\mathsf{P}$). We recall that the permanent family is not VNP-complete in characteristic 2. That is why we use the Hamiltonian circuit family (HC_n) instead.

Lemma 4. *Consider the polynomial*

$$P(X_1, \dots, X_n) = \sum_{y_1,\dots,y_p \in \{0,1\}} C(X_1, \dots, X_n, y_1, \dots, y_p)$$

where C is an arithmetic circuit of size s computing a polynomial of total degree at most d (with respect to all the variables $X_1 \dots, X_n, y_1, \dots, y_p$). Then P is a projection of $HC_{(sd)^{O(1)}}$.

Proof. This lemma follows from a careful inspection of the proof of VNP-completeness of the Hamiltonian circuit polynomial given in Malod [14]. We give some more details below.

From the fact that $\mathsf{VNP} = \mathsf{VNP}_\mathsf{e}$ [4, Theorem 2.13], we can write P as a Boolean sum of formulas, i.e.

$$P(X_1, \dots, X_n) = \sum_{z_1,\dots,z_q \in \{0,1\}} F(X_1, \dots, X_n, z_1, \dots, z_q).$$

Moreover, $q = s^{O(1)}$ and an inspection of the proof of $\mathsf{VNP} = \mathsf{VNP}_e$ given in [14] shows that the size of the formula F is $(sd)^{O(1)}$. By [14, Lemme 8], a formula is a projection of the Hamiltonian circuit polynomial of linear size. This yields

$$P(X_1, \dots, X_n) = \sum_{z_1,\dots,z_q \in \{0,1\}} \mathrm{HC}_{s'}(a_1, \dots, a_{s'})$$

where $s' = (sd)^{O(1)}$ and $a_i \in \{X_1, \dots, X_n, z_1, \dots, z_q, -1, 0, 1\}$. At last, in order to write this exponential sum as a projection of a not too large Hamiltonian circuit, a sum gadget of size $O(q)$ and $O(s')$ XOR gadgets of size $O(1)$ are needed [14, Théorème 7]. Hence, the polynomial P is a projection of $\mathrm{HC}_{(sd)^{O(1)}}$. □

Theorem 13. *The following are equivalent:*

- $\mathsf{unif}\text{-}\mathsf{VNP}_{\mathbb{F}_2} \subset \mathsf{asize}_{\mathbb{F}_2}(n^k)$ *for some k;*
- $\mathsf{VP}_{\mathbb{F}_2} = \mathsf{VNP}_{\mathbb{F}_2}$ *and* $\oplus\mathsf{P} \subset \mathsf{size}(n^k)$ *for some k.*

Proof. Suppose that $\mathsf{unif}\text{-}\mathsf{VNP}_{\mathbb{F}_2} \subset \mathsf{asize}_{\mathbb{F}_2}(n^k)$. Then the Hamiltonian polynomials (HC_n) (in n^2 variables) have $O(n^{2k})$ size circuits and thus $\mathsf{VP} = \mathsf{VNP}$ over $\mathbb{F}_2$. Let $L \in \oplus\mathsf{P}$ and the corresponding function $f \in \#\mathsf{P}$ so that

$$x \in L \iff f(x) \text{ is odd.}$$

Consider the sequence of polynomials $P_n \in \mathbb{F}_2[X_1, \ldots, X_n]$ associated to L:

$$P_n(X_1, \ldots, X_n) = \sum_{x \in \{0,1\}^n} f(x) \prod_{i=1}^{n} X_i^{x_i} (1 - X_i)^{1-x_i}.$$

This family belongs to $\mathsf{unif\text{-}VNP}$ over $\mathbb{F}_2$. Hence, P_n has $O(n^k)$ size circuits. It can be simulated by a Boolean circuit of the same size within a constant factor, and yields $O(n^k)$ size circuits for L. Hence $\oplus\mathsf{P} \subset \mathsf{size}(n^k)$.

For the converse, suppose that $\oplus\mathsf{P} \subset \mathsf{size}(n^k)$ and $\mathsf{VP}_{\mathbb{F}_2} = \mathsf{VNP}_{\mathbb{F}_2}$, and let $(P_n) \in \mathsf{unif\text{-}VNP}_{\mathbb{F}_2}$. We can write

$$P_n(X_1, \ldots, X_n) = \sum_{m_1, \ldots, m_n \in \{0, \ldots, d\}} \phi(m_1, \ldots, m_n) \prod_{i=1}^{n} X_i^{m_i}$$

where d is a bound on the degree of each variable of P_n. Since the coefficients of P_n belong to $\oplus\mathsf{P}$, they can be computed by Boolean circuits of size $O(\tilde{n}^k)$ with $\tilde{n} = n \log n$ (by our hypothesis on circuit size for $\oplus\mathsf{P}$ languages and the fact that the function ϕ takes $n \log d$ bits).

These Boolean circuits can in turn be simulated by (Boolean) sums of arithmetic circuits of size and formal degree $O(\tilde{n}^k)$ by the usual method (see e.g. the proof of Valiant's criterion in [4]).

Hence we have written $P_n = \sum_{\tilde{m}} \psi(\tilde{m}) X^{\tilde{m}}$, i.e. P_n is a sum over $O(\tilde{n}^k)$ variables in $\mathbb{F}_2$ of an arithmetic circuit ψ of size $O(\tilde{n}^k)$, and the degree of ψ is $O(\tilde{n}^k)$. By Lemma 4, P_n is a projection of $\mathrm{HC}_{\tilde{n}^{O(k)}}$. By hypothesis, the uniform family (HC_n) has $O(n^k)$ arithmetic circuits. Hence, (P_n) has arithmetic circuits of size $n^{O(k^2)}$. □

Acknowledgements

We thank Guillaume Malod for useful discussions (in particular on Lemma 4) and Thomas Colcombet for some advice on the presentation.

References

[1] Eric Allender, Peter Bürgisser, Johan Kjeldgaard-Pedersen, and Peter Bro Miltersen. On the complexity of numerical analysis. *SIAM J. Comput.*, 38(5):1987–2006, 2009.

[2] José Luis Balcázar, Josep Díaz, and Joaquim Gabarró. *Structural complexity. II*, volume 22 of *EATCS Monographs on Theoretical Computer Science*. Springer-Verlag, Berlin, 1990.

[3] Walter Baur and Volker Strassen. The complexity of partial derivatives. *Theor. Comput. Sci.*, 22:317–330, 1983.

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

[5] Lance Fortnow, Rahul Santhanam, and Ryan Williams. Fixed-polynomial size circuit bounds. In *IEEE Conference on Computational Complexity*, pages 19–26, 2009.

[6] Lane A. Hemaspaandra and Mitsunori Ogihara. *The complexity theory companion.* Texts in Theoretical Computer Science. An EATCS Series. Springer-Verlag, Berlin, 2002.

[7] Maurice J. Jansen and Rahul Santhanam. Stronger lower bounds and randomness-hardness trade-offs using associated algebraic complexity classes. In *STACS*, pages 519–530, 2012.

[8] Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1-2):1–46, 2004.

[9] Ravi Kannan. Circuit-size lower bounds and non-reducibility to sparse sets. *Information and Control*, 55(1-3):40–56, 1982.

[10] Pascal Koiran. Hilbert's Nullstellensatz is in the polynomial hierarchy. *J. Complexity*, 12(4):273–286, 1996.

[11] Pascal Koiran. Hilbert's Nullstellensatz is in the polynomial hierarchy. Technical Report 96-27, DIMACS, July 1996.

[12] Richard J. Lipton. Polynomials with 0-1 coefficients that are hard to evaluate. In *FOCS*, pages 6–10, 1975.

[13] Carsten Lund, Lance Fortnow, Howard J. Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. *J. ACM*, 39(4):859–868, 1992.

[14] Guillaume Malod. *Polynômes et coefficients.* PhD thesis, Université Claude Bernard Lyon 1, 2003. http://tel.archives-ouvertes.fr/tel-00087399.

[15] Ran Raz. Elusive functions and lower bounds for arithmetic circuits. *Theory of Computing*, 6(1):135–177, 2010.

[16] Rahul Santhanam. Circuit lower bounds for Merlin–Arthur classes. *SIAM J. Comput.*, 39(3):1038–1061, 2009.

[17] Claus-Peter Schnorr. Improved lower bounds on the number of multiplications/divisions which are necessary of evaluate polynomials. *Theor. Comput. Sci.*, 7:251–261, 1978.

[18] Volker Strassen. Polynomials with rational coefficients which are hard to compute. *SIAM J. Comput.*, 3(2):128–149, 1974.

[19] Seinosuke Toda. PP is as hard as the polynomial-time hierarchy. *SIAM J. Comput.*, 20(5):865–877, 1991.

[20] Leslie G. Valiant. Completeness classes in algebra. In *STOC*, pages 249–261, 1979.

[21] Klaus W. Wagner. The complexity of combinatorial problems with succinct input representation. *Acta Inf.*, 23(3):325–356, 1986.