Information and Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

On the limits of depth reduction at depth 3 over small finite fields

Suryajith Chillara *,[1], Partha Mukhopadhyay

Chennai Mathematical Institute, Siruseri, India

ARTICLE INFO

Article history:
Received 14 November 2014
Available online xxxx

ABSTRACT

In a surprising recent result, Gupta–Kamath–Kayal–Saptharishi have proved that over $\mathbb{Q}$ any $n^{O(1)}$-variate and n-degree polynomial in **VP** can also be computed by a depth three $\Sigma\Pi\Sigma$ circuit of size $2^{O(\sqrt{n}\log^{3/2} n)}$.[2] Over fixed-size finite fields, Grigoriev and Karpinski proved that any $\Sigma\Pi\Sigma$ circuit that computes the determinant (or the permanent) polynomial of a $n \times n$ matrix must be of size $2^{\Omega(n)}$. In this paper, for an explicit polynomial in **VP** (over fixed-size finite fields), we prove that any $\Sigma\Pi\Sigma$ circuit computing it must be of size $2^{\Omega(n\log n)}$. The explicit polynomial that we consider is the iterated matrix multiplication polynomial of n generic matrices of size $n \times n$. The importance of this result is that over fixed-size fields there is *no depth reduction technique* that can be used to compute all the $n^{O(1)}$-variate and n-degree polynomials in **VP** by depth 3 circuits of size $2^{o(n\log n)}$. The result of Grigoriev and Karpinski can only rule out such a possibility for $\Sigma\Pi\Sigma$ circuits of size $2^{o(n)}$.

We also give an example of an explicit polynomial ($\mathrm{NW}_{n,\epsilon}(X)$) in **VNP** (which is not known to be in **VP**), for which any $\Sigma\Pi\Sigma$ circuit computing it (over fixed-size fields) must be of size $2^{\Omega(n\log n)}$. The polynomial we consider is constructed from the combinatorial design of Nisan and Wigderson, and is closely related to the polynomials considered in many recent papers (by Kayal–Saha–Saptharishi, Kayal–Limaye–Saha–Srinivasan, and Kumar–Saraf), where strong depth 4 circuit size lower bounds are shown.

1. Introduction

In a recent breakthrough, Gupta et al. [1] have proved that over $\mathbb{Q}$, if an $n^{O(1)}$-variate polynomial of degree d is computable by an arithmetic circuit of size s, then it can also be computed by a depth three $\Sigma\Pi\Sigma$ circuit of size $2^{O(\sqrt{d\log d\log n\log s})}$.[3] Using this result, they prove the existence of a $\Sigma\Pi\Sigma$ circuit of size $2^{O(\sqrt{n}\log n)}$ computing the determinant polynomial of an $n \times n$ matrix (over $\mathbb{Q}$). Before this result, no depth 3 circuit for Determinant of size smaller than $2^{O(n\log n)}$ was known (over any field of characteristic $\neq 2$).

* Corresponding author.
E-mail addresses: suryajith@cmi.ac.in (S. Chillara), partham@cmi.ac.in (P. Mukhopadhyay).

1 Supported by TCS research fellowship.

2 In a nice follow-up work, Tavenas has improved the upper bound to $2^{O(\sqrt{n}\log n)}$. The main ingredient in his proof is an improved depth 4 reduction.

3 Gupta et al. [1], using the depth reduction of Koiran [2], show that if a polynomial is computed by an algebraic branching program of size s, then it can also be computed by a depth three circuit of size $2^{O(\sqrt{d\log n\log s})}$. The determinant polynomial of a $n \times n$ matrix has an algebraic branching program of size poly(n).

http://dx.doi.org/10.1016/j.ic.2017.04.007
0890-5401/

The situation is very different over *fixed-size finite fields*. Grigoriev and Karpinski proved that over fixed-size finite fields, any depth 3 circuit for the determinant polynomial of a $n \times n$ matrix must be of size $2^{\Omega(n)}$ [3]. Although Grigoriev and Karpinski proved the lower bound result only for the determinant polynomial, it is a folklore result that some modification of their argument can show a similar depth 3 circuit size lower bound for the permanent polynomial as well.[4] Over any field, Ryser's formula for Permanent gives a $\Sigma\Pi\Sigma$ circuit of size $2^{O(n)}$ [5] (for an exposition of this result, see [6]). Thus, for the permanent polynomial the depth 3 complexity (over fixed-size finite fields) is essentially $2^{\Theta(n)}$.

The result of [1] is obtained through an ingenious depth reduction technique but their technique is tailored to the fields of zero characteristic. In particular, the main technical ingredients of their proof are the well-known monomial formula of Fischer [7] and the duality trick of Saxena [8]. These techniques do not work over finite fields. Looking at the contrasting situation over $\mathbb{Q}$ and the fixed-size finite fields, a natural question is to ask whether one can find a new depth reduction technique over fixed-size finite fields such that any $n^{O(1)}$-variate and degree n polynomial in **VP** can also be computed by a $\Sigma\Pi\Sigma$ circuit of size $2^{o(n \log n)}$.

Question 1. *Over any fixed-size finite field $\mathbb{F}_q$, is it possible to compute any $n^{O(1)}$-variate and n-degree polynomial in* **VP** *by a $\Sigma\Pi\Sigma$ circuit of size $2^{o(n \ln n)}$?*

Note that any $n^{O(1)}$-variate and n-degree polynomial can be trivially computed by a $\Sigma\Pi\Sigma$ circuit of size $2^{O(n \log n)}$ by writing it explicitly as a sum of all $n^{O(n)}$ possible monomials.

We give a negative answer to the aforementioned question by showing that over fixed-size finite fields, any $\Sigma\Pi\Sigma$ circuit computing the iterated matrix multiplication polynomial (which is in **VP** for any field) must be of size $2^{\Omega(n \log n)}$ (see Subsection 2.3, for the definition of the polynomial). More precisely, we prove that any $\Sigma\Pi\Sigma$ circuit computing the iterated matrix multiplication polynomial of n generic $n \times n$ matrices (denoted by $\mathrm{IMM}_{n,n}(\mathrm{X})$), must be of size $2^{\Omega(n \log n)}$.

Previously, Nisan and Wigderson [9] proved a size lower bound of $\Omega(n^{d-1}/d!)$ for any homogeneous $\Sigma\Pi\Sigma$ circuit computing the iterated matrix multiplication polynomial over d generic $n \times n$ matrices. Kumar et al. [10] improved the bound to $\Omega(n^{d-1}/2^d)$. These results work over any field. Over fields of zero characteristic, Shpilka and Wigderson proved a near quadratic lower bound for the size of depth 3 circuits computing the trace of the iterated matrix multiplication polynomial [11].

Recently Tavenas [12], by improving upon the previous works of Agrawal and Vinay [13], and Koiran [2] proved that any $n^{O(1)}$-variate, n-degree polynomial in **VP** has a depth four $\Sigma\Pi^{[O(\sqrt{n})]}\Sigma\Pi^{[\sqrt{n}]}$ circuit of size $2^{O(\sqrt{n} \log n)}$. Subsequently, Kayal et al. [14] proved a size lower bound of $2^{\Omega(\sqrt{n} \log n)}$ for a polynomial in **VNP** which is constructed from the combinatorial design of Nisan and Wigderson [15]. In a beautiful follow up result, Fournier et al. [16] proved that a similar lower bound of $2^{\Omega(\sqrt{n} \log n)}$ is also attainable by the iterated matrix multiplication polynomial (see [17], for a unified analysis of the depth 4 lower bounds of [14] and [16]). The main technique used was *the method of shifted partial derivatives* which was used to prove $2^{\Omega(\sqrt{n})}$ size lower bound for $\Sigma\Pi^{[O(\sqrt{n})]}\Sigma\Pi^{[\sqrt{n}]}$ circuits computing Determinant or Permanent polynomial [18]. Recent work of Kumar and Saraf [19] shows that the depth reduction as shown by Tavenas [12] is optimal even for the homogeneous formulas. This strengthens the result of [16] who proved the optimality of depth reduction for the circuits. Very recently, a series of papers show strong depth 4 lower bounds even for homogeneous depth 4 formulas with no bottom fan-in restriction [20–22].

Similar to the situation at depth 4, we also give an example of an explicit n^2-variate and n-degree polynomial in **VNP** (which is not known to be in **VP**) such that over fixed-size finite fields, any depth three $\Sigma\Pi\Sigma$ circuit computing it must be of size $2^{\Omega(n \log n)}$. This polynomial family, denoted by $\mathrm{NW}_{n,\epsilon}(\mathrm{X})$ (see Subsection 2.2, for the definition of the polynomial) is closely related to the polynomial family introduced by Kayal et al. [14]. In fact, from our proof idea it will be clear that the strong depth 3 size lower bound results that we show for $\mathrm{NW}_{n,\epsilon}(\mathrm{X})$ and $\mathrm{IMM}_{n,n}(\mathrm{X})$ polynomials are not really influenced by the fact that the polynomials are either in **VNP** or **VP**. Rather, the bounds are determined by a combinatorial property of the subspaces generated by a set of carefully chosen derivatives.

Our main theorem is the following.

Theorem 2. *Over any fixed-size finite field $\mathbb{F}_q$, any depth three $\Sigma\Pi\Sigma$ circuit computing the polynomials $\mathrm{NW}_{n,\epsilon}(\mathrm{X})$ or $\mathrm{IMM}_{n,n}(\mathrm{X})$ must be of size at least $2^{\delta n \log n}$, where the parameters δ and ϵ $(< 1/2)$ are in $(0, 1)$ and depend only on q.*

In section 6, we set the parameter δ to $\frac{1}{20q \log q}$ and it follows from the subsequent calculations that $\epsilon < \delta + 0.1$. As an important consequence of the above theorem, we have the following corollary.

Corollary 3. *Over any fixed-size finite field $\mathbb{F}_q$, there is no depth reduction technique that can be used to compute all the $n^{O(1)}$-variate and n-degree polynomials in* **VP** *by depth 3 circuits of size $2^{o(n \log n)}$.*

[4] Saptharishi gives a nice exposition of this result in his survey and he attributes it to Koutis and Srinivasan [4].

Please cite this article in press as: S. Chillara, P. Mukhopadhyay, On the limits of depth reduction at depth 3 over small finite fields, Inf. Comput. (2017), http://dx.doi.org/10.1016/j.ic.2017.04.007