

# On the Limits of Depth Reduction at Depth 3 Over Small Finite Fields

Suryajith Chillara     Partha Mukhopadhyay  
{suryajith, partham}@cmi.ac.in

Chennai Mathematical Institute

**Abstract.** In a surprising recent result, Gupta et al. [GKKS13b] 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  $2^{O(\sqrt{n} \log^{3/2} n)}$ <sup>1</sup>. 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 [GK98] 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 ( $\text{NW}_{n,\epsilon}(X)$ ) 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 [NW94], and is closely related to the polynomials considered in many recent papers where strong depth 4 circuit size lower bounds are shown [KSS13, KLSS14, KS13b, KS14].

## 1 Introduction

In a recent breakthrough, Gupta et al. [GKKS13b] 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  $2^{O(\sqrt{d} \log d \log n \log s)}$ . Using this result, they get a  $\Sigma\Pi\Sigma$  circuit of size  $2^{O(\sqrt{n} \log n)}$  computing the determinant polynomial of a  $n \times n$  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  $\neq 2$ ).

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  $2^{\Omega(n)}$  [GK98]. 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<sup>2</sup>. Over any field, Ryser's formula for Permanent gives a  $\Sigma\Pi\Sigma$  circuit of size  $2^{O(n)}$  (for an exposition of this result, see [Fei09]). Thus, for the permanent polynomial the depth 3 complexity (over fixed-size finite fields) is essentially  $2^{\Theta(n)}$ .

The result of [GKKS13b] 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

<sup>1</sup> 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 [Tav13].

<sup>2</sup> Saptharishi gives a nice exposition of this result in his unpublished survey and he attributes it to Koutis and Srinivasan [Sap13].

of their proof are the well-known monomial formula of Fischer [Fis94] and the duality trick of Saxena [Sax08]. 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 3.1, 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  $\text{IMM}_{n,n}(X)$ ), must be of size  $2^{\Omega(n \log n)}$ .

Previously, Nisan and Wigderson [NW97] 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. [KMN13] 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 [SW01].

Recently Tavenas [Tav13], by improving upon the previous works of Agrawal and Vinay [AV08], and Koiran [Koi12] 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. [KSS13] 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 [NW94]. In a beautiful follow up result, Fournier et al. [FLMS13] proved that a similar lower bound of  $2^{\Omega(\sqrt{n} \log n)}$  is also attainable by the iterated matrix multiplication polynomial (see [CM14], for a unified analysis of the depth 4 lower bounds of [KSS13] and [FLMS13]). The main technique used is *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 [GKKS13a]. Recent work of Kumar and Saraf [KS13a] shows that the depth reduction as shown by Tavenas [Tav13] is optimal even for the homogeneous formulas. This strengthens the result of [FLMS13] 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 [KLSS14,KS13b,KS14].

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  $\text{NW}_{n,\epsilon}(X)$  (see Subsection 3.1, for the definition of the polynomial) is closely related to the polynomial family introduced by Kayal et al. [KSS13]. In fact, from our proof idea it will be clear that the strong depth 3 size lower bound results that we show for  $\text{NW}_{n,\epsilon}(X)$  and  $\text{IMM}_{n,n}(X)$  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  $\text{NW}_{n,\epsilon}(X)$  or  $\text{IMM}_{n,n}(X)$  must be of size at least  $2^{\delta n \log n}$ , where the parameters  $\delta$  and  $\epsilon (< 1/2)$  are in  $(0, 1)$  and depend only on  $q$ .*

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  $2^{o(n \log n)}$ .*

The result of [GK98] only says that over fixed-size finite fields, not all the  $n^{O(1)}$ -variate and  $n$ -degree polynomials in VP can be computed by  $\Sigma\Pi\Sigma$  circuits of size  $2^{o(n)}$ . Our main theorem (Theorem 2) can also be viewed as the first quantitative improvement over the result of [GK98].

### Proof Idea

Our proof technique is quite simple and it borrows ideas mostly from the proof technique of Grigoriev and Karpinski [GK98]. A recurring notion in many papers related to  $\Sigma\Pi\Sigma$  circuits is the notion of *rank* of a product gate. Let  $T = L_1 L_2 \dots L_d$  be a product gate such that each  $L_i$  is an affine linear form over the underlying field. By rank of  $T$ , one simply means the maximum rank of the homogeneous linear system corresponding to set of affine functions  $\{L_1, L_2, \dots, L_d\}$ .

Over fixed-size finite fields,  $\Sigma\Pi\Sigma$  circuits enjoy a nice property that the derivatives of the high rank product gates can be eliminated except for a few erroneous points (denoted by  $E$ ). This property was first observed by Grigoriev and Karpinski in [GK98]. The intuition is simple. If a product gate has many linearly independent functions, then it is likely that a large number of linear functions will be set to zero if we randomly substitute the variables with elements from the field. Then the derivatives (of relatively low order) of the polynomial obtained from the product gate will disappear on a random point with very high probability. To quantify the notion of *high rank*, Grigoriev and Karpinski fixed a threshold for the rank of the product gates. Since they were looking for a  $2^{\Omega(n)}$  lower bound for the Determinant of a  $n \times n$  matrix and the rank of the entire derivative space of the determinant polynomial is  $2^{O(n)}$ , it was natural for them to fix the threshold to be  $\Theta(n)$ . Since the dimension of the derivative spaces of the polynomial families  $\{\text{NW}_{n,\epsilon}(X)\}_{n>0}$  and  $\{\text{IMM}_{n,n}(X)\}_{n>0}$  is  $2^{\Omega(n \log n)}$ , it is possible for us to choose the threshold for the rank of the product gates to be  $\Theta(n \log n)$ . This allows us to bound the size of the error set meaningfully. We formalize this in Lemma 5.

**An overview of the result of Grigoriev and Karpinski** We now give a high level description of the proof technique in [GK98] to motivate our proof strategy. Roughly speaking, they consider the space  $H$  spanned by  $\Theta(n)$  order derivatives of the determinant. This makes the dimension of  $H$  to be of the order of  $2^{\Theta(n)}$ . For a point  $a \in \mathbb{F}_q^N$ , the subspace  $H_a$  is the space of functions in  $H$  that evaluate to zero on  $a$ . From the rank analysis on the circuit side, they get that the dimension of the space of functions that may not be zero outside the error set  $E$  is bounded. More precisely,  $\text{codim}(\cap_{a \notin E} H_a)$  is small. Grigoriev and Karpinski then considered the group of invertible matrices  $G$  of order  $n \times n$  over  $\mathbb{F}_q$ . For any  $g \in G$ , they define a  $\mathbb{F}_q$ -linear operator  $T_g : H \rightarrow H$  by the formula  $(T_g(f))(a) = f(ga)$ . The fact that the derivative space of the determinant polynomial of a  $n \times n$  matrix is invariant under  $\text{GL}_n(\mathbb{F}_q)$  action was crucially used in defining the map. Then they consider the plane  $P = \cap_{a \in G \setminus E} H_a \subset H$ . Since  $\text{codim}(\cap_{a \notin E} H_a)$  is bounded, the same bound applies for  $\text{codim}(P)$  as well. The most remarkable idea in their work was to prove that  $\text{codim}(\cap_{b \in G} H_b)$  in  $H$  is small given that  $\text{codim}(P)$  is small. Notice that the plane  $P$  is defined only on  $G \setminus E$  and not on the entire group  $G$ . To achieve this, they prove that the full invertible group  $G$  can be covered by taking only a few translates of  $G \setminus E$  from  $G$ . This was done by appealing to a graph theoretic lemma of Lovász [Lov75]. Now, it is not hard to see that we can bound  $\text{codim}(\cap_{b \in G} H_b)$  to a quantity smaller than  $\dim(H)$ . This shows us that there exists a nonzero function in  $H$  that evaluates to zero on the entire group  $G$ . Since the elements in  $H$  are only multilinear polynomials, they finally prove that it is impossible to have such a function in  $H$  by showing that no nonzero multilinear polynomial can vanish over the entire group  $G$ .

**An overview of our result** The group symmetry based argument of [GK98] is tailored to the determinant polynomial and it can not be directly applied to the polynomials that we consider. The main technical contribution of this work is to replace the group symmetry based argument by a new argument that makes the proof strategy robust enough to handle the family of polynomials that we consider. We carefully choose a subspace  $H$  (of sufficiently large dimension) of the derivative spaces of these polynomials which has an additional structure. The subspace  $H$  is spanned by a *downward closed* set of monomials (see, Definition 9). Let  $\mathbb{F}_q$  be the finite field and  $N$  be the number of the variables in the polynomial under consideration. The basic idea is to prove that the dimension of the space  $H$  of the polynomial being considered is more than the dimension of the set of functions in  $H$  which do not evaluate to zero over the entire space  $\mathbb{F}_q^N$ . Since the subspace  $H$  contains only multilinear polynomials, we can then conclude that a nonzero multilinear polynomial in  $H$  will evaluate to zero on entire  $\mathbb{F}_q^N$ , which is not possible by combinatorial nullstellensatz [Alo99].

To implement this, we define a linear map  $T_u : H \rightarrow H$  by  $T_u(f(X)) = f(X - u)$  for any function  $f : \mathbb{F}_q^N \rightarrow \mathbb{F}_q$  and  $u \in \mathbb{F}_q^N$ . The map is well-defined by the downward closed structure of the generating set for  $H$ . Also the map  $T_u$  is one to one for any  $u \in \mathbb{F}_q^N$ . As before, for a point  $a \in \mathbb{F}_q^N$ , the subspace  $H_a$  is the space of functions in  $H$  that evaluates to zero on  $a$ . Let  $P = \bigcap_{a \in \mathbb{F}_q^N \setminus E} H_a$ . Then by Lemma 5, we get that  $\text{codim } P = \text{codim}(\bigcap_{a \in \mathbb{F}_q^N \setminus E} H_a)$  is small. Notice that the plane  $P$  is defined over  $\mathbb{F}_q^N \setminus E$  and not over the entire space  $\mathbb{F}_q^N$ . Similar to the argument in [GK98], we use the graph theoretic lemma of Lovász to prove that the entire space  $\mathbb{F}_q^N$  can be covered by only a few translates of  $\mathbb{F}_q^N \setminus E$ . Then it is simple to observe that  $\text{codim}(\bigcap_{b \in \mathbb{F}_q^N} H_b)$  is small compared to the dimension of  $H$ . As a consequence we get that a nonzero multilinear polynomial in  $H$  must evaluate to zero over  $\mathbb{F}_q^N$ , which is not possible by the combinatorial nullstellensatz.

## 2 Organization

In section 3, we introduce the preliminaries related to arithmetic circuits, and define the polynomial families  $\{\text{NW}_{n,\epsilon}(X)\}_{n>0}$  and  $\{\text{IMM}_{n,n}(X)\}_{n>0}$ . We recall known results related to the derivative space of  $\Sigma\Pi\Sigma$  circuits in Section 4. In section 5, we study the derivative spaces of our polynomial families. We prove Theorem 2 in Section 6. We conclude in Section 7.

## 3 Preliminaries

**Arithmetic Circuits** An arithmetic circuit over a field  $\mathbb{F}$  with the set of variables  $x_1, x_2, \dots, x_n$  is a directed acyclic graph such that the internal nodes are labelled by addition or multiplication gates and the leaf nodes are labelled by the variables or the field elements. The node with fan-out zero is the output gate. An arithmetic circuit computes a polynomial in the polynomial ring  $\mathbb{F}[x_1, x_2, \dots, x_n]$ . Size of an arithmetic circuit is the number of nodes and the depth is the length of a longest path from the root to a leaf node.

**Depth 3 Circuits** Usually a depth 3 circuit over a field  $\mathbb{F}$  is denoted by  $\Sigma\Pi\Sigma$ . The circuit has an addition gate at the top, a middle layer of multiplication gates, and then a level of addition gates at the bottom. A  $\Sigma\Pi\Sigma$  circuit with  $s$  multiplication gates computes a polynomial of the following form.

$$C(X) = \sum_{i=1}^s \prod_{j=1}^{d_i} L_{i,j}(x_1, \dots, x_n)$$

where  $L_{i,j}$ s are affine linear functions over  $\mathbb{F}$  and  $\{x_1, x_2, \dots, x_n\}$  are the variables appearing in the polynomial.

**Combinatorial Nullstellensatz** We recall the following theorem from [Alo99].

**Theorem 4.** *Let  $f(x_1, x_2, \dots, x_n)$  be a polynomial in  $n$  variables over an arbitrary field  $\mathbb{F}$ . Suppose that the degree of  $f$  as a polynomial in  $x_i$  is at most  $t_i$ , for  $1 \leq i \leq n$  and let  $S_i \subseteq \mathbb{F}$  such that  $|S_i| \geq t_i + 1$ . If  $f(a_1, a_2, \dots, a_n) = 0$  for all  $n$ -tuples in  $S_1 \times S_2 \times \dots \times S_n$ , then  $f = 0$ .*

### 3.1 The Polynomial Families

A multivariate polynomial family  $\{f_n(X) \in \mathbb{F}[x_1, x_2, \dots, x_n] : n \geq 1\}$  is in the class VP if  $f_n$  has degree at most  $\text{poly}(n)$  and can be computed by an arithmetic circuit of size  $\text{poly}(n)$ . It is in VNP if it can be expressed as

$$f_n(X) = \sum_{Y \in \{0,1\}^m} g_{n+m}(X, Y)$$

where  $m = |Y| = \text{poly}(n)$  and  $g_{n+m}$  is a polynomial in VP.

**The Polynomial Family from the Combinatorial Design** Let  $\mathbb{F}$  be any field<sup>3</sup>. For integers  $n > 0$  ranging over prime powers and  $0 < \epsilon < 1$ , we define a polynomial family  $\{\text{NW}_{n,\epsilon}(X)\}_{n>0}$  in  $\mathbb{F}_q[X]$  as follows.

$$\text{NW}_{n,\epsilon}(X) = \sum_{a(z) \in \mathbb{F}_n[z]} x_{1a(1)} x_{2a(2)} \dots x_{na(n)}$$

where  $a(z)$  runs over all univariate polynomials of degree  $< \epsilon n$ . The finite field  $\mathbb{F}_n$  is naturally identified with the numbers  $\{1, 2, \dots, n\}$ . Notice that the number of monomials in  $\text{NW}_{n,\epsilon}(X)$  is  $n^{\epsilon n}$ . From the explicitness of the polynomial, it is clear that  $\{\text{NW}_{n,\epsilon}(X)\}_{n>0}$  is in VNP for any  $\epsilon \in (0, 1)$ . In [KSS13], a very similar family of polynomials was introduced where the degree of the univariate polynomial was bounded by  $\epsilon\sqrt{n}$ .

**The Iterated Matrix Multiplication Polynomial** The iterated matrix multiplication polynomial of  $n$  generic  $n \times n$  matrices  $X^{(1)}, X^{(2)}, \dots, X^{(n)}$  is the  $(1, 1)$ th entry of the product of the matrices. More formally, let  $X^{(1)}, X^{(2)}, \dots, X^{(n)}$  be  $n$  generic  $n \times n$  matrices with disjoint sets of variables and  $x_{ij}^{(k)}$  be the variable in  $X^{(k)}$  indexed by  $(i, j) \in [n] \times [n]$ . Then the iterated matrix multiplication polynomial (denoted by the family  $\{\text{IMM}_{n,n}(X)\}_{n>0}$ ) is defined as follows.

$$\text{IMM}_{n,n}(X) = \sum_{i_1, i_2, \dots, i_{n-1} \in [n]} x_{1i_1}^{(1)} x_{i_1 i_2}^{(2)} \dots x_{i_{n-2} i_{n-1}}^{(n-1)} x_{i_{n-1} 1}^{(n)}$$

Notice that  $\text{IMM}_{n,n}(X)$  is a  $n^2(n-2) + 2n$ -variate polynomial of degree  $n$ . For our application, we consider  $n = 2m$  where  $m$  ranges over the positive integers. Over any field  $\mathbb{F}$ , the polynomial family  $\{\text{IMM}_{n,n}(X)\}_{n>0}$  can be computed in VP. This can be seen by observing that  $\text{IMM}_{n,n}(X)$  can be computed by a  $\text{poly}(n)$  sized algebraic branching program.

<sup>3</sup> In the lower bound proof for  $\text{NW}_{n,\epsilon}(X)$ , we will consider  $\mathbb{F}$  to be any fixed finite field  $\mathbb{F}_q$ .

## 4 The Derivative Space of $\Sigma\Pi\Sigma$ Circuits Over Small Fields

In this section we fix the field  $\mathbb{F}$  to be a fixed-size finite field  $\mathbb{F}_q$ . Let  $C$  be a  $\Sigma\Pi\Sigma$  circuit of top fan-in  $s$  computing a  $N = n^{O(1)}$ -variate polynomial of degree  $n$ . Consider a  $\Pi$  gate  $T = L_1 L_2 \dots L_d$  in  $C$ . Let  $r$  be the rank of the (homogeneous)-linear system corresponding to  $\{L_1, L_2, \dots, L_d\}$  by viewing each  $L_i$  as a vector in  $\mathbb{F}_q^{N+1}$ . Fix a threshold for the rank of the system of linear functions  $r_0 = \beta n \ln n$ , where  $\beta > 0$  is a constant to be fixed later in the analysis. In our application, the parameter  $N$  is at least  $n^2$ , so the threshold for the rank is meaningful. W.l.o.g, let  $\{L_1, L_2, \dots, L_r\}$  be a set of affine linear forms in  $\{L_1, L_2, \dots, L_d\}$  whose homogeneous system forms a maximal independent set of linear functions. The following analysis has been reworked from [GK98] to fix the parameters. It shows that the derivative space of a  $\Sigma\Pi\Sigma$  circuit can be approximated by just the derivative space of the low rank product gates of the circuit over a large subset of  $\mathbb{F}_q^N$ .

**Low rank gates :  $r \leq r_0$**  Over the finite field  $\mathbb{F}_q$ , we have  $x^q = x$ . We express  $T : \mathbb{F}_q^N \rightarrow \mathbb{F}_q$  as a linear combination of  $\{L_1^{e_1} L_2^{e_2} \dots L_r^{e_r} : e_i < q \text{ for all } i \in [r]\}$ . Since, the derivatives of all orders lie in the same space, the dimension of the set of partial derivatives of  $T$  of all orders is bounded by  $q^r \leq q^{r_0}$ .

**High rank gates :  $r > r_0$**  Let the rank of a high rank gate  $T$  be  $y\beta n \ln n$  where  $y \geq 1$ . We assign values to the variables uniformly at random from  $\mathbb{F}_q$  and compute the probability that at most  $n$  linearly independent functions evaluate to zero.

$$\begin{aligned} \Pr_{a \in \mathbb{F}_q^N} [\text{at most } n \text{ linearly independent functions evaluate to zero}] &= \sum_{i=0}^n \binom{r}{i} \left(\frac{1}{q}\right)^i \left(1 - \frac{1}{q}\right)^{r-i} \\ &\leq n \binom{r}{n} \left(\frac{1}{q}\right)^n \left(1 - \frac{1}{q}\right)^{r-n} \end{aligned}$$

The above inequality follows from the fact that  $r > 2n$  and thus the binomial terms under the summation are monotonically increasing. Hence, if we differentiate  $T$  with respect to any set of variables of size at most  $n$  and restrict all the variables to values from  $\mathbb{F}_q$ , the gate  $T$  may not vanish over a set of points  $E_T$  whose size is estimated below.

$$|E_T| \leq n \binom{r}{n} \left(\frac{1}{q}\right)^n \left(1 - \frac{1}{q}\right)^{r-n} q^N$$

Over all the gates, let  $E$  be the set of points over which some of the product gates with large rank may not evaluate to zero. Then by a union bound, we get that  $|E| \leq s|E_T|$ . If  $s \leq e^{\delta n \ln n}$  then we have the following estimate.

$$\begin{aligned} |E| &\leq e^{\delta n \ln n} n \binom{r}{n} \left(\frac{1}{q}\right)^n \left(1 - \frac{1}{q}\right)^{r-n} q^N \\ &\leq e^{\delta n \ln n} n \left(\frac{er}{n}\right)^n e^{-\frac{r-n}{q}} q^N \\ &= q^N e^{\delta n \ln n + n + n \ln \frac{r}{n} + \ln n - \frac{r-n}{q}} \\ &= q^N e^{\delta n \ln n + n + n \ln \frac{y\beta n \ln n}{n} + \ln n - \frac{y\beta n \ln n - n}{q}} \end{aligned}$$

To bound the above estimate meaningfully, we need  $\delta n \ln n$  to be strictly less than  $\frac{y\beta}{q} \ln n - n \ln y$ . That is,

$$\delta < \frac{y\beta}{q} - \frac{\ln y}{\ln n} \quad (1)$$

Once we satisfy the relation given by the inequality 1, we can upper bound the size of  $E$  as  $|E| < q^N \mu^{n \ln n}$  for some suitably fixed constant  $\mu$  between 0 and 1. Now it is clear that over  $\mathbb{F}_q^N \setminus E$ , the derivative space is spanned by the derivatives of the low rank gates. We summarize it in the following lemma.

**Lemma 5.** *Let  $\mathbb{F}_q$  be a fixed-size finite field. Then there exist constants  $0 < \delta(q), \beta(q), \mu(q) < 1$  such that the following is true. Let  $C$  be a  $\Sigma\Pi\Sigma$  circuit of top fan-in  $s \leq e^{\delta n \ln n}$  computing a  $N = n^{O(1)}$ -variate and  $n$ -degree polynomial  $f(\mathbf{X})$  over the finite field  $\mathbb{F}_q$ . Then, there exists a set  $E \subset \mathbb{F}_q^N$  of size at most  $q^N \mu^{n \ln n}$  such that the dimension of the space spanned by the derivatives of order  $\leq n$  of  $C$  restricted to  $\mathbb{F}_q^N \setminus E$  is  $\leq s q^{\beta n \ln n}$ .*

It is worth (re)-emphasizing that, when we consider the derivatives, what we really mean is the formal derivatives of  $C$  as polynomials. In the above lemma we view the derivatives as functions from  $\mathbb{F}_q^N \rightarrow \mathbb{F}_q$ . Then it follows from the above analysis that the dimension of the space spanned by the functions corresponding to the derivatives of order  $\leq n$  of  $C$  restricted to  $\mathbb{F}_q^N \setminus E$  is  $\leq s q^{\beta n \ln n}$ . This way of viewing derivatives either as *formal polynomials* or as *functions* is implicit in the work of [GK98]. In Section 6, we show how to fix the parameters  $\delta, \beta$ , and  $\mu$  which depend only on the field size  $q$ .

## 5 Derivative Spaces of the Polynomial Families

In this section, we study the derivative spaces of  $\text{NW}_{n,\epsilon}(\mathbf{X})$  and  $\text{IMM}_{n,n}(\mathbf{X})$  polynomials. Instead of considering the full derivative spaces, we focus on a set of carefully chosen derivatives and consider the subspaces spanned by them.

### The derivative space of $\{\text{NW}_{n,\epsilon}(\mathbf{X})\}_{n>0}$ polynomial family

A set of variables  $D = \{x_{i_1 j_1}, x_{i_2 j_2}, \dots, x_{i_t j_t}\}$  is called an admissible set if  $i_k$ s (for  $1 \leq k \leq t$ ) are all distinct and  $\epsilon n \leq t \leq n$ . Let  $H$  be the subspace spanned by the set of the partial derivatives of the polynomial  $\text{NW}_{n,\epsilon}(\mathbf{X})$  with respect to the admissible sets of variables. More formally,

$$H := \mathbb{F}_q\text{-span} \left\{ \frac{\partial \text{NW}_{n,\epsilon}(\mathbf{X})}{\partial D} : D \text{ is an admissible set of variables} \right\}$$

Since the monomials of the  $\text{NW}_{n,\epsilon}(\mathbf{X})$  polynomial are defined by the univariate polynomials of degree  $< \epsilon n$ , each partial derivative with respect to such a set  $D$  yields a multilinear monomial. If we choose  $\epsilon$  such that  $n - \epsilon n > \epsilon n$  (i.e.  $\epsilon < 1/2$ ), then after the differentiation, all the monomials of length  $n - \epsilon n$  are distinct. This follows from the fact that the monomials are generated from the image of the univariate polynomials of degree  $< \epsilon n$ .

Let us treat these monomials as functions from  $\mathbb{F}_q^{n^2} \rightarrow \mathbb{F}_q$ . The following lemma says that the functions corresponding to any set of distinct monomials are linearly independent.

**Lemma 6.** *Let  $m_1(\mathbf{X}), m_2(\mathbf{X}), \dots, m_k(\mathbf{X})$  be any set of  $k$  distinct multilinear monomials in  $\mathbb{F}_q[x_1, x_2, \dots, x_N]$ . For  $1 \leq i \leq k$ , let  $f_i : \mathbb{F}_q^N \rightarrow \mathbb{F}_q$  be the function corresponding to the monomial  $m_i(\mathbf{X})$ , i.e.  $f_i(\mathbf{X}) = m_i(\mathbf{X})$ . Then,  $f_i$ s are linearly independent in the  $q^N$  dimensional vector space over  $\mathbb{F}_q$ .*

*Proof.* If  $f_i$ s are not linearly independent then  $\sum_{i=1}^k \lambda_i f_i = 0$  for  $\bar{\lambda} = (\lambda_1, \lambda_2, \dots, \lambda_k) \in \mathbb{F}_q^k \setminus \{\bar{0}\}$ . Then, the nonzero multilinear polynomial  $\sum_{i=1}^k \lambda_i m_i(X)$  evaluates to zero on  $\mathbb{F}_q^N$ , which contradicts Theorem 4.  $\square$

Consider the derivatives of  $NW_{n,\epsilon}(X)$  corresponding to the sets  $\{x_{1a(1)}, x_{2a(2)}, \dots, x_{\epsilon na(\epsilon n)}\}$  for all univariate polynomials  $a$  of degree  $< \epsilon n$ . From Lemma 6, it follows that  $\dim(H) \geq n^{\epsilon n} = e^{\epsilon n \ln n}$ . W.l.o.g, we can assume that the constant function  $\mathbf{1} : \mathbb{F}_q^N \rightarrow \mathbb{F}_q$  given by  $\forall x, \mathbf{1}(x) = 1$  is also in  $H$ . This corresponds to the derivatives of order  $n$ .

### The derivative space of $\{\text{IMM}_{n,n}(X)\}_{n>0}$ polynomial family

For our application, we consider  $n = 2m$  where  $m$  ranges over the positive integers. Consider the set of matrices  $X^{(1)}, X^{(3)}, \dots, X^{(2m-1)}$  corresponding to the odd places. Let  $S$  be any set of  $m$  variables chosen as follows. Choose any variable from the first row of  $X^{(1)}$  and choose any one variable from each of the matrices  $X^{(3)}, \dots, X^{(2m-1)}$ . We call such a set  $S$  an admissible set.

If we differentiate  $\text{IMM}_{n,n}(X)$  with respect to two different admissible sets of variables  $S$  and  $S'$ , then we get two different monomials of length  $m$  each. This follows from the structure of the monomials in the  $\text{IMM}_{n,n}(X)$  polynomial, whenever we fix two variables from  $X^{(i-1)}$  and  $X^{(i+1)}$ , the variable from  $X^{(i)}$  gets fixed. So the number of such monomials after differentiation is exactly  $n^{2m-1} = e^{(n-1) \ln n}$ .

Let  $m_S$  be the monomial obtained after differentiating  $\text{IMM}_{n,n}(X)$  by the set of variables in  $S$  and  $\text{var}(m_S)$  be the set of variables in  $m_S$ . Consider the derivatives of  $\text{IMM}_{n,n}(X)$  with respect to the following sets of variables.

$$\{S \cup T : T \subseteq \text{var}(m_S)\} \text{ where } S \text{ ranges over all admissible sets.}$$

Let  $H$  be the subspace spanned by these derivatives. More formally,

$$H := \mathbb{F}_q\text{-span} \left\{ \frac{\partial \text{IMM}_{n,n}(X)}{\partial D} : D = S \cup T \text{ where } T \subseteq \text{var}(m_S); S \text{ is an admissible set} \right\}$$

As before, we can assume that the constant function  $\mathbf{1}$  is in  $H$ . From Lemma 6, we know that  $\dim(H) \geq e^{(n-1) \ln n}$ . Now to unify the arguments for  $NW_{n,\epsilon}(X)$  and  $\text{IMM}_{n,n}(X)$  polynomials, we introduce the following notion.

### Downward closed property

**Definition 7.** A set of multilinear monomials  $\mathcal{M}$  is said to be downward closed if the following property holds. If  $m(X) \in \mathcal{M}$  and multilinear monomial  $m'(X)$  is such that  $\text{var}(m'(X)) \subseteq \text{var}(m(X))$ , then  $m'(X) \in \mathcal{M}$ .

Now we consider a downward closed set of monomials  $\mathcal{M}$  over  $N$  variables. These monomials can be viewed as functions from  $\mathbb{F}_q^N$  to  $\mathbb{F}_q$ . W.l.o.g, we assume that the constant function is also in  $\mathcal{M}$  (constant function corresponds to a monomial with an empty set of variables). Let  $H$  be the subspace spanned by these functions in  $\mathcal{M}$ .

For any  $u \in \mathbb{F}_q^N$ , define an operator  $T_u$  such that  $(T_u(f))(X) = f(X-u)$  for any function  $f : \mathbb{F}_q^N \rightarrow \mathbb{F}_q$ . The following proposition is simple to prove.

**Proposition 8.** Let  $H$  be the subspace spanned by a downward closed set of monomials  $\mathcal{M}$  over the set of variables  $\{x_1, x_2, \dots, x_N\}$ . Then for any  $u \in \mathbb{F}_q^N$ ,  $T_u$  is a linear map from  $H$  to  $H$ . Moreover, the map  $T_u$  is one-one for any  $u \in \mathbb{F}_q^N$ .

*Proof.* Let  $g(X)$  be an arbitrary function in  $H$  which can be expressed as follows:  $g(X) = \sum_{i \geq 1} c_i m_i(X)$  where  $m_i(X) \in \mathcal{M}$ , and  $c_i \in \mathbb{F}_q$  for all  $i \geq 1$ .

$$(T_u(g))(X) = g(X - u) = \sum_{i \geq 1} c_i m_i(X - u)$$

It is sufficient to prove that  $m(X - u) \in H$  where  $m(X) \in \mathcal{M}$ . We can express  $m(X - u)$  as follows.

$$m(X - u) = \sum_{S \subseteq \text{var}(m(X))} c_S \prod_{x_r \in S} x_r$$

where  $c_S \in \mathbb{F}_q$ . For every  $S \subseteq \text{var}(m(X))$ ,  $\prod_{x_r \in S} x_r \in \mathcal{M}$  because  $\mathcal{M}$  is downward closed. Since the choice of  $S$  was arbitrary,  $m(X - u) \in H$ . It is obvious that  $T_u$  is a linear map.

To see that  $T_u$  is a one-one map, consider any nonzero function  $g(X)$  in  $H$  which can be defined as  $g(X) = \sum_{i \geq 1} c_i m_i(X)$  where  $m_i(X) \in \mathcal{M}$ , and  $c_i \in \mathbb{F}_q$  for all  $i \geq 1$ . Now, we notice that the highest degree monomials always survive in  $T_u(g(X))$ . Hence, the kernel of the map  $T_u$  is trivial for all  $u \in \mathbb{F}_q^N$ .  $\square$

It is not difficult to observe that the derivative spaces that we select for  $\text{NW}_{n,\epsilon}(X)$  and  $\text{IMM}_{n,n}(X)$  are spanned by downward closed sets of monomials.

**Lemma 9.** *The generator sets for the derivative subspaces  $H$  for  $\text{NW}_{n,\epsilon}(X)$  and  $\text{IMM}_{n,n}(X)$  polynomials are downward closed.*

*Proof.* Let us consider the  $\text{NW}_{n,\epsilon}(X)$  polynomial first. Let  $m \in H$  be any monomial and  $D$  be the admissible set such that  $m = \frac{\partial \text{NW}_{n,\epsilon}(X)}{\partial D}$ . Let  $m'$  be any monomial such that  $\text{var}(m') \subseteq \text{var}(m)$ . Then  $m' = \frac{\partial \text{NW}_{n,\epsilon}(X)}{\partial D'}$  where  $D' = D \cup (\text{var}(m) \setminus \text{var}(m'))$ .

Similarly for the  $\text{IMM}_{n,n}(X)$  polynomial, consider any  $m \in H$ . Then  $m = \frac{\partial \text{IMM}_{n,n}(X)}{\partial D}$  and  $D = S \cup T$  for an admissible set  $S$  and  $T \subseteq \text{var}(m_S)$ . If  $m'$  is any monomial such that  $\text{var}(m') \subseteq \text{var}(m)$ , then  $m' = \frac{\partial \text{IMM}_{n,n}(X)}{\partial D'}$  where  $D' = S \cup (T \cup (\text{var}(m) \setminus \text{var}(m')))$ . Clearly  $T \cup (\text{var}(m) \setminus \text{var}(m')) \subseteq \text{var}(m_S)$ .  $\square$

## 6 A Covering Argument

In this section, we adapt the covering argument of [GK98] to prove the lower bound results. In [GK98], the covering argument was given over the set of invertible matrices. Here we adapt their argument suitably over the entire space  $\mathbb{F}_q^N$ . As defined in the section 5, the subspace  $H$  represents the chosen derivative subspace of either the  $\text{NW}_{n,\epsilon}(X)$  polynomial or the  $\text{IMM}_{n,n}(X)$  polynomial.

Define the subspace  $H_a := \{f \in H : f(a) = 0\}$  for  $a \in \mathbb{F}_q^N$ . Let us recall that  $E$  is the set of points over which some of the product gates with large rank may not evaluate to zero. Let the set of points  $\mathbb{F}_q^N \setminus E$  be denoted by  $A$ . Then Lemma 5 says that in  $H$ , we get that  $\text{codim}(\bigcap_{a \in A} H_a) < s q^{r_0}$ . We note the following simple observation.

**Proposition 10.** *For any  $u, a \in \mathbb{F}_q^N$ , we have that  $T_u(H_a) = H_{u+a}$ .*

*Proof.* Let  $f(X)$  be any function in  $H_a$ .  $(T_u(f))(X) = f(X - u)$ . Since  $f(a) = 0$ ,  $f(a + u - u) = 0$ , it implies that  $T_u(H_a) \subseteq H_{u+a}$ .

Now consider any function  $g(X) \in H_{u+a}$ . Define the function  $h(X) = g(X + u)$ . It is easy to see that  $h(X) \in H$ . Thus,  $h(a) = 0$  and so  $h(X) \in H_a$ . Also,  $T_u(h(X)) = g(X)$ . Hence,  $H_{u+a} \subseteq T_u(H_a)$ .  $\square$

Let  $P = \bigcap_{a \in A} H_a$ . Let  $S \subset \mathbb{F}_q^N$  be a set such that we can cover the entire space  $\mathbb{F}_q^N$  by the shifts of  $A$  with the elements from  $S$ .

$$\bigcup_{u \in S} u + A = \mathbb{F}_q^N$$

Now by applying the map  $T_u$  to  $P$  which is one-one, we get the following.

$$T_u(P) = \bigcap_{a \in A} T_u(H_a) = \bigcap_{b \in u+A} H_b$$

By a further intersection over  $S$ , we get the following.

$$\bigcap_{u \in S} T_u(P) = \bigcap_{u \in S} \bigcap_{b \in u+A} H_b = \bigcap_{b \in \mathbb{F}_q^N} H_b \quad (2)$$

From Equation 2, we get the following estimate.

$$\text{codim} \left( \bigcap_{b \in \mathbb{F}_q^N} H_b \right) = \text{codim} \left( \bigcap_{u \in S} T_u(P) \right) \leq |S| \text{codim}(P) \leq |S| s q^{r_0} \quad (3)$$

The  $\text{codim} \left( \bigcap_{b \in \mathbb{F}_q^N} H_b \right)$  refers to the dimension of the set of functions in  $H$  which do not evaluate to zero over all the points in  $\mathbb{F}_q^N$ .

Next, we show an upper-bound estimate for the size of the set  $S$ . This follows from a simple adaptation of the dominating set based argument given in [GK98].

### Upper bound on the size of the set $S$

Consider the directed graph  $G = (V, R)$  defined as follows. The points in  $\mathbb{F}_q^N$  are the vertices of the graph. For  $u_1, u_2 \in \mathbb{F}_q^N$ , the edge  $u_1 \rightarrow u_2$  is in  $R$  iff  $u_2 = u_1 + b$  for any  $b \in A$ . Clearly the in-degree and out-degree of any vertex are equal to  $|A|$ . Now, we recall Lemma 2 of [GK98] to estimate the size of  $S$ .

**Lemma 11 (Lovász, [Lov75]).** *Let  $(V, R)$  be a directed (regular) graph with  $|V| = m$  vertices and with the in-degree and the out-degree of each vertex both equal to  $d$ . Then there exists a subset  $U \subset V$  of size  $O(\frac{m}{d} \log(d+1))$  such that for any vertex  $v \in V$  there is a vertex  $u \in U$  forming an edge  $(u, v) \in R$ .*

Let  $c_0$  be the constant fixed by the lemma in its  $O()$  notation. By Lemma 11, we get the following estimate.

$$\begin{aligned} |S| &\leq c_0 \frac{|\mathbb{F}_q^N|}{|A|} \log(|A| + 1) \\ &\leq c_0 \frac{q^N}{q^N - |E|} \log(q^N - |E| + 1) \\ &\leq c_0 (\log q) N \frac{q^N}{q^N - |E|} \\ &= O(N) \quad (\text{for fixed } q) \end{aligned}$$

The last equation follows from the estimate for  $|E|$  from the section 4.

**Fixing the parameters** Consider the inequality 1 which is  $\delta < \frac{y\beta}{q} - \frac{\ln y}{\ln n}$ . Fix the values for  $\beta, \delta$ , and  $\mu$  in Lemma 5 as follows. Set  $\beta = \frac{1}{10 \ln q}$ ,  $\delta = \frac{1}{20q \ln q}$ ,  $\nu = \frac{\delta}{2}$ , and  $\mu = e^{-\nu}$ . Consider the function  $g(y) = y - \frac{10q \ln q}{\ln n} \ln y - 0.50$ . Since  $g(y)$  is a monotonically increasing function (for  $n$  appropriately larger than a threshold value depending on  $q$ <sup>4</sup>) which takes the value of 0.50 at  $y = 1$ ,  $g(y) > 0$  for  $y \geq 1$  and thus  $\delta < \frac{y\beta}{q} - \frac{\ln y}{\ln n}$  for the chosen values of  $\beta$  and  $\delta$ . Also,  $\frac{y\beta}{q} - \frac{\ln y}{\ln n} - \delta > \nu$  and thus  $|E| \leq q^N \mu^{n \ln n}$ .

From Section 5, we know that  $\dim(H)$  for  $\text{NW}_{n,\epsilon}(X)$  is at least  $e^{\epsilon n \ln n}$ . Consider the upper bound on  $\text{codim} \left( \bigcap_{b \in \mathbb{F}_q^N} H_b \right)$  given by the inequality 3. If we choose  $\epsilon$  in such a way that  $e^{\epsilon n \ln n} > |S| s q^{r_0}$ , then there will be a multilinear polynomial  $f$  in  $H$  such that  $f$  will evaluate to zero over all points in  $\mathbb{F}_q^N$ .

$$\begin{aligned} \dim(H) &> n^{\epsilon n} = e^{\epsilon n \ln n} \\ \implies e^{\epsilon n \ln n} &> |S| s q^{r_0} = e^{\delta n \ln n + (\beta \ln q) n \ln n + \ln N} \end{aligned}$$

Considering the terms of the order of  $n \ln n$  in the exponent, it is enough to choose  $\epsilon (< 1/2)$  such that the following holds.

$$\begin{aligned} \epsilon &> \delta + \beta \ln q \\ &= \frac{1}{20q \ln q} + \frac{1}{10} \end{aligned}$$

Since the  $\dim(H)$  for  $\text{IMM}_{n,n}(X)$  is  $\geq e^{(n-1) \ln n}$ , the chosen values of  $\beta$  and  $\delta$  clearly suffice. Finally, we recall from Theorem 4 that no non-zero multilinear polynomial can be zero over  $\mathbb{F}_q^N$ . Thus, we get the main theorem (restated from Section 1).

**Theorem 12.** *For any fixed-size finite field  $\mathbb{F}_q$ , any depth three  $\Sigma\Pi\Sigma$  circuit computing the polynomials  $\text{NW}_{n,\epsilon}(X)$  or  $\text{IMM}_{n,n}(X)$  must be of size at least  $2^{\delta n \log n}$  where the parameters  $\delta$  and  $\epsilon (< 1/2)$  are in  $(0, 1)$  and depend only on  $q$ .*

It is straightforward to observe that the lower bound analysis holds for any polynomial for which we can find a subspace (of sufficiently large dimension) of its derivative space spanned by a downward closed set of monomials.

## 7 Conclusion

In this paper, over fixed-size finite fields, we show a tight lower bound on the size of  $\Sigma\Pi\Sigma$  circuits computing a polynomial in VP. More precisely, we show that the iterated matrix multiplication polynomial obtained by multiplying  $n$  generic  $n \times n$  matrices requires  $\Sigma\Pi\Sigma$  circuit of size  $2^{\Omega(n \log n)}$  over any fixed-size finite field. Additionally, we show a similar tight lower bound for an explicit polynomial in VNP constructed from Nisan-Wigderson design. Our proof technique is inspired by the classical result of Grigoriev-Karpinski [GK98] where they proved a  $2^{\Omega(n)}$  size lower bound for  $\Sigma\Pi\Sigma$  circuits computing Determinant (or Permanent) polynomial of a  $n \times n$  matrix over fixed-size finite fields. The main technical novelty in our work is to replace the group symmetry based argument of Grigoriev-Karpinski by a new argument which is robust enough to handle both the polynomials  $\text{IMM}_{n,n}(X)$  and  $\text{NW}_{n,\epsilon}(X)$ .

Then main interesting open problem is to prove that over the fixed-size fields, any  $\Sigma\Pi\Sigma$  circuit computing the determinant polynomial for a  $n \times n$  matrix must be of size  $2^{\Omega(n \log n)}$ . For an optimist,

<sup>4</sup> In general, it should be understood throughout the paper that we consider  $n$  greater than any appropriate threshold value whenever necessary.

the task will be to find a  $\Sigma\Pi\Sigma$  circuit of size  $2^{o(n \log n)}$  for the determinant polynomial. It seems that we need significantly new ideas and techniques to make progress either on the lower bound side or on the upper bound side.

## References

- [Alo99] Noga Alon. Combinatorial nullstellensatz. *Combinatorics, Probability and Computing*, 8, 1999.
- [AV08] Manindra Agrawal and V Vinay. Arithmetic circuits: A chasm at depth four. In *Proceedings-Annual Symposium on Foundations of Computer Science*, pages 67–75. IEEE, 2008.
- [CM14] Suryajith Chillara and Partha Mukhopadhyay. Depth-4 lower bounds, determinantal complexity: A unified approach. In *STACS*, pages 239–250, 2014.
- [Fei09] Uri Feige. The permanent and the determinant. 2009.
- [Fis94] Ismor Fischer. Sums of like powers of multivariate linear forms. *Mathematics Magazine*, 67(1):59–61, 1994.
- [FLMS13] Hervé Fournier, Nutan Limaye, Guillaume Malod, and Srikanth Srinivasan. Lower bounds for depth 4 formulas computing iterated matrix multiplication. *To appear in the proceedings of STOC 2014. Electronic Colloquium on Computational Complexity (ECCC)*, 20:100, 2013.
- [GK98] Dima Grigoriev and Marek Karpinski. An exponential lower bound for depth 3 arithmetic circuits. In *STOC*, pages 577–582, 1998.
- [GKKS13a] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Approaching the chasm at depth four. In *IEEE Conference on Computational Complexity*, pages 65–73, 2013.
- [GKKS13b] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Arithmetic circuits: A chasm at depth three. In *FOCS*, pages 578–587, 2013.
- [KLSS14] Neeraj Kayal, Nutan Limaye, Chandan Saha, and Srikanth Srinivasan. An exponential lower bound for homogeneous depth four arithmetic formulas. *To appear in the proceedings of STOC 2014. Electronic Colloquium on Computational Complexity (ECCC)*, 21:5, 2014.
- [KMN13] Mrinal Kumar, Gaurav Maheshwari, and Jayalal Sarma M. N. Arithmetic circuit lower bounds via maxrank. In *ICALP (1)*, pages 661–672, 2013.
- [Koi12] Pascal Koiran. Arithmetic circuits: The chasm at depth four gets wider. *Theor. Comput. Sci.*, 448:56–65, 2012.
- [KS13a] Mrinal Kumar and Shubhangi Saraf. The limits of depth reduction for arithmetic formulas: It’s all about the top fan-in. *To appear in the proceedings of STOC 2014. Electronic Colloquium on Computational Complexity (ECCC)*, 20:153, 2013.
- [KS13b] Mrinal Kumar and Shubhangi Saraf. Superpolynomial lower bounds for general homogeneous depth 4 arithmetic circuits. *To appear in the proceedings of ICALP 2014. Electronic Colloquium on Computational Complexity (ECCC)*, 20:181, 2013.
- [KS14] Mrinal Kumar and Shubhangi Saraf. On the power of homogeneous depth 4 arithmetic circuits. *Electronic Colloquium on Computational Complexity (ECCC)*, 21:045, 2014.
- [KSS13] Neeraj Kayal, Chandan Saha, and Ramprasad Saptharishi. A super-polynomial lower bound for regular arithmetic formulas. *To appear in the proceedings of STOC 2014. Electronic Colloquium on Computational Complexity (ECCC)*, 20:91, 2013.
- [Lov75] László Lovász. On the ratio of optimal integral and fractional covers. *Discrete mathematics*, 13(4):383–390, 1975.
- [NW94] Noam Nisan and Avi Wigderson. Hardness vs randomness. *J. Comput. Syst. Sci.*, 49(2):149–167, 1994.
- [NW97] Noam Nisan and Avi Wigderson. Lower bounds on arithmetic circuits via partial derivatives. *Computational Complexity*, 6(3):217–234, 1997.
- [Sap13] Ramprasad Saptharishi. Personal communication. 2013.
- [Sax08] Nitin Saxena. Diagonal circuit identity testing and lower bounds. In *ICALP (1)*, pages 60–71, 2008.
- [SW01] Amir Shpilka and Avi Wigderson. Depth-3 arithmetic circuits over fields of characteristic zero. *Computational Complexity*, 10(1):1–27, 2001.
- [Tav13] Sébastien Tavenas. Improved bounds for reduction to depth 4 and depth 3. In *MFCS*, pages 813–824, 2013.