# Almost Cubic Bound for Depth Three Circuits in VP 

Morris Yau＊

November 20， 2016


#### Abstract

In＂An Almost Cubic Lower Bound for $\Sigma \Pi \Sigma$ circuits in VP＂，［BLS16］ present an infinite family of polynomials，$\left\{P_{n}\right\}_{n \in \mathbb{Z}^{+}}$，with $P_{n}$ on $N=\Theta(n \operatorname{polylog}(n))$ variables with degree $N$ being in VP such that every $\Sigma \Pi \sum$ circuit computing $P_{n}$ is of $\operatorname{size} \Omega\left(\frac{N^{3}}{2^{\sqrt{\log N}}}\right)$ ．We present a modified polynomial and perform a tighter analysis to obtain an $\tilde{\Omega}\left(N^{3}\right)$ lower bound．More generally，we show that for every $N$ and $D$ satisfying poly $(N)>D>\log ^{2} N$ ，there exist polyno－ mials $P_{N, D}$ on $N$ variable of degree $D$ in VP that can not be computed by circuits of size $\tilde{\Omega}\left(N^{2} D\right)$ ．


## 1 Introduction

A depth three $\Sigma \Pi \sum$ circuit consists of a layer of sum gates，followed by a layer of multiplication gates，followed by a single sum gate that outputs the computation of the circuit．The fan－in is unbounded，and the circuit size is measured in terms of the number of wires．As such，depth three circuits capture＂sums of products of linear polynomials＂．A recent line of work on depth reduction［AV08，Koi10，GKKS16，Tav15］has shown that moderately strong lower bounds for circuits of depth three implies a super－polynomial lower bound for general circuits．In addition，［Raz13］shows that a strong enough lower bound for set－multilinear depth three circuits implies a super－ polynomial lower bound for general arithmetic formulas．These depth reduc－ tion results build an avenue towards proving super－polynomial lower bounds for general circuits／formulas by leveraging the apparent simple structure of depth three circuits．Unfortunately，it is still an open problem to prove super－ polynomial lower bounds for depth three circuits of fields of characteristic zero．Below we present some of the seminal results in depth three lower bounds．

In［SW02］，Shpilka and Widgerson proved a $\Omega\left(n^{2}\right)$ depth three circuit computing the elementary symmetric polynomials $E S_{Y M_{n}^{d}}\left(x_{1}, x_{2}, \ldots, x_{N}\right)=$

[^0]$\sum_{S \subseteq[N],|S|=d} \prod_{i \in S} x_{i}$ on $n$ variables and degree $d=\Theta(n)$. In the same paper, the authors prove a near quadratic lower bound for the determinant polynomial [SW02]. Restricting the circuit model (homogeneity, multilinearity) and restricting the field characteristic yields better results. Over fixed finite fields, [GR00] proves an exponential lower bound for determinant and in [NW96] it was shown that any homogeneous depth three circuit computing $E S_{Y M}{ }_{n}^{2 d}$ has size $\Omega\left(\left(\frac{n}{4 d}\right)^{d}\right)$. More recently, in [KS15] a $n^{\Omega(\sqrt{d})}$ lower bound was proved for depth three circuits, with bottom fan-in bounded by $n^{\epsilon}$ for any fixed $\epsilon<1$, computing an explicit n-variate polynomial of degree d.

Despite success in many restricted settings (homogenous, degree bounded product gates) the lower bounds in general cases remain relatively weak. Recently [KST16] gave near cubic $\tilde{\Omega}\left(n^{3}\right)$ lower bounds for a polynomial family in VNP, which was followed by [BLS16] who gave a $\Omega\left(\frac{n^{3}}{2^{\sqrt{\log n}}}\right)$ lower bounds for a polynomial family in VP.

In this work we strengthen the latter lower bound to get a polynomial in VP on $N$ variables and degree $D$ satisfying poly $(N)>D>\log ^{2} N$, with size lower bound $\tilde{\Omega}\left(N^{2} D\right)$. Setting $D=N$, this recovers the VNP result up to a $\log ^{4}(N)$ factor. Along the way we present a simplified polynomial and a tighter analysis of its multiplicative complexity. We also expand on the trade off between circuit size as a joint function of the degree of the polynomial and the number of variables - something that does not seem to have been explicitly clarified before.

Our main result is as follows.
Theorem 1.1. There exists an explicit polynomial family $P_{N, D}$ computable in $V P$ on $N$ variables of degree $D$ satisfying poly $(N)>D>\log ^{2} N$ such that any depth 3 circuit computing it has size $\tilde{\Omega}\left(N^{2} D\right)$. Setting $D=N$ as in previous works recovers, up to a $\log ^{4}(N)$ factor the $\tilde{\Omega}\left(N^{3}\right)$ bound for polynomials in VNP [KST16]

## 2 Preliminaries

We discuss some of the language and common techniques relating to arithmetic circuits. An extended treatment can be found in the survey [SY10] of Shpilka and Yehudayoff.

Our general organization is as follows. Section (3) constructs a "hard" polynomial and bounds its size for bounded fan-in circuits. Section (4) presents the embedding procedure producing a polynomial that can be analyzed for unbounded fan-in.

### 2.1 Basic Notation

The ideal generated by a set of polynomials of the ring $P$ will be denoted $\langle P\rangle$. We use $\operatorname{poly}(N)$ to denote polynomial in $N$ with an arbitrary constant exponent. A $\Sigma \Pi^{Y} \sum$ circuit computes polynomials that are the sum of the product of at most $Y$ affine linear forms. Similarly, a $\Sigma \Pi^{Q} \Pi^{R} \sum$ circuit consists of a layer of sum gates, followed by two layers of product gates with fan-in bounded by $R$ and $Q$ respectively, followed by a final sum gate. We observe that each $\Sigma \Pi^{Q} \Pi^{R} \sum$ circuit can be converted to a $\Sigma \Pi^{Q R} \sum$ circuit with constant factor overhead in size.

### 2.2 Shifted Partial Derivative Measure

As in previous works, we use a measure $\mu: \mathbb{F}[x] \rightarrow \mathbb{N}$ to capture weakness of a circuit model in opposition to a "hard" family of polynomials giving us a lower bound for the circuit family. Our choice of measure is the "dimension of the shifted partials" introduced in [Kay12]. For polynomial $P \in \mathbb{F}\left[x_{1}, x_{2}, \ldots, x_{N}\right]$, let $\langle P\rangle^{=k}$ be the set of k'th order partials of $P$. Furthermore, let

$$
\begin{equation*}
\langle P\rangle_{\leq \ell}^{=k}:=\left\{f \cdot p \mid \forall \text { monomials } f \text { s.t } \operatorname{deg}(f) \leq \ell, \forall p \in\langle P\rangle^{=k}\right\} \tag{1}
\end{equation*}
$$

Then for $k, \ell \in \mathbb{N}$, the shifted derivative measure is defined to be

$$
\begin{equation*}
\mu_{k, \ell} P=\operatorname{dim}\left(\langle P\rangle=\frac{k}{\leq \ell}\right) \tag{2}
\end{equation*}
$$

Adding the parameter $\ell$ produces this shifted derivative measure that introduces "leeway" into the measure of the "dimension of the partial derivatives" introdued in [NW96]

### 2.3 Circuits under Affine Projections

Given polynomial $P \in \mathbb{F}\left[x_{1}, x_{2}, \ldots, x_{N}\right]$ as above, let $A: \mathbb{F}^{N} \rightarrow \mathbb{F}^{N}$ be an affine linear transform, then it is easy to show that $\mu_{k, \ell} P \circ A \leq \mu_{k, \ell} P$. In which case if $A$ is invertible, then $\mu_{k, \ell} P \circ A=\mu_{k, \ell} P$. The takeaway is that the shifted derivative measure is invariant under invertible affine transforms.

Now let $V$ be a subspace of $\mathbb{F}^{N}$ and $V^{\perp}$ be its complement. Then if $A$ is an affine projection onto the space $V$, then we say $P \circ A$ is a subspace restriction $\left.P\right|_{V}$. If we let $U_{V}$ be the orthogonal projection of $\mathbb{F}^{N}$ to $V$, by the above discussion we observe that $\mu_{k, \ell} P \circ A=\mu_{k, \ell} P \circ U_{V}$. This is useful for the following reason.

The central barrier to proving lower bounds for bounded depth circuits is the unbounded fan-in. The key idea is then to restrict the polynomial with an affine transform $A$ to an affine subspace $V$ so that the product gates with large fan-in can be pruned. We are then left with a bounded fan-in circuit which we can analyze. However, we must now compute the measure of the polynomial $P \circ A$. We do this precisely by noting that $\mu_{k, \ell} P \circ A=\mu_{k, \ell} P \circ U_{V}$ and construct $P$ so that its shifted derivative measure is easy to compute under orthogonal affine restrictions. In some sense we are "embedding" a polynomial for which we can analyze its shifted derivative measure within $P$. Section 2 constructs the embedded polynomial and section 4 details how the subspace restrictions are performed in practice.

## 3 Embedded Polynomial

First we construct a polynomial in VP for which we can analyze its shifted derivative measure and bound its circuit size for constant depth circuits with bounded fan-in.

### 3.1 Polynomial Construction

Let $X$ be a $b$-by- $n$ matrix of formal variables as shown below.

$$
X=\left[\begin{array}{cccc}
x_{11} & x_{12} & \ldots & x_{1 n}  \tag{3}\\
x_{21} & x_{22} & \ldots & x_{2 n} \\
\ldots \ldots & \ldots & \ldots & \ldots \\
x_{b 1} & x_{b 2} & \ldots & x_{b n}
\end{array}\right]
$$

Let $J=\left(j_{1}, j_{2}, . ., j_{b}\right)$ for $J \in[n]^{b}$. Then define the function $\operatorname{Permute}(X)$ to be

$$
\begin{equation*}
\operatorname{Permute}(X)=\prod_{i=1}^{b} \sum_{j=1}^{n} x_{i j}^{\frac{D}{b}}=\sum_{J \in[n]^{b}} x_{1 j_{1}}^{\frac{D}{b}} x_{2 j_{2}}^{\frac{D}{b}} \ldots x_{b j_{b}}^{\frac{D}{b}} \tag{4}
\end{equation*}
$$

Notice that $\operatorname{Permute}(X)$ has $N=n b$ variables and has degree $D$. For $b=$ $\log n$, $\operatorname{Permute}(X)$ is in VP by inspecting the sum and product in the definition.

### 3.2 Bounding Measure for Target Polynomial

The first lemma was first presented as Proposition 9 in [AG13]. If polynomial $f \in \mathbb{F}\left[x_{1}, \ldots, x_{N}\right]$ is of the form $f=\sum_{i=1}^{s} \prod_{j=1}^{Q} G_{i j}\left(x_{1}, x_{2}, \ldots, x_{N}\right)$ where each $G_{i j}$ is a polynomial of degree no greater than $R$, then the following inequality bounds the size of $s$.
Lemma 3.1. For all $k, \ell \in \mathbb{N}$ let the shifted partial derivative measure $\mu_{k, \ell} f=$ $\operatorname{dim}\left(\langle f\rangle_{\leq \ell}^{k}\right)$. Then for $k<Q$ the following lower bounds the size of $s$

$$
\begin{equation*}
\frac{\mu_{k, \ell} f}{\binom{Q+k}{k}\binom{N+\ell+k(R-1)}{\ell+k(R-1)}} \leq s \tag{5}
\end{equation*}
$$

With respect to circuits, $s$ is the size of the top fan-in which is what we'll be using as a lower bound for circuit size. $Q$ can then be interpreted as the top layer product gate fan-in. So long as each product gate has a fanin consisting of polynomials of degree no greater than $R$, the above lemma holds. Summarizing these remarks, we find that the left hand side of the inequality is dependent only on the circuit model, and that $k$ and $\ell$ are chosen for analytical convenience.

The next lemma has several formulations. We will present the formulation in Lemma 3 of [CM13].

First, we define a distance metric between any pair of monomials $g$ and $g^{\prime}$ of identical degree. Let $h$ be the monomial of minimum degree divisible by both $g$ and $g^{\prime}$. Then let $\left|g \Delta g^{\prime}\right|=\operatorname{deg}(h)-\operatorname{deg}(g)$ which is well defined because $\operatorname{deg}(g)=\operatorname{deg}\left(g^{\prime}\right)$.
Lemma 3.2. Let $f \in \mathbb{F}\left[x_{1}, x_{2}, . ., x_{N}\right]$ be a polynomial, then the following inequality lower bounds the shifted partial derivative measure $\mu_{k, l} f$ for all $k, l \in \mathbb{N}$. If $S \subseteq \partial_{k}\langle f\rangle$ is a set of monomials satisfying for distinct $g, g^{\prime} \in S$, $\left|g \Delta g^{\prime}\right| \geq \tau$ then

$$
\begin{equation*}
|S|\binom{N+\ell}{\ell}-|S|^{2}\binom{N+\ell-\tau}{\ell-\tau} \leq \mu_{k, \ell} f \tag{6}
\end{equation*}
$$

Putting Lemma 0.1 and 0.2 together we obtain

$$
\begin{equation*}
\frac{|S|\binom{N+\ell}{\ell}-|S|^{2}\binom{N+\ell-\tau}{\ell-\tau}}{\binom{Q+k}{k}\binom{N+\ell+k(R-1)}{\ell+k(R-1)}} \leq s \tag{7}
\end{equation*}
$$

Now we must determine the size of a set $S$ satisfying the properties of Lemma 0.2 with a corresponding minimum distance $\tau$ for our polynomial Permute ( $X$ ). Consider the following, we set $k=b=\log n$, and define $\partial_{J} \operatorname{Permute}(X)$ for $J=\left(j_{1}, j_{2}, \ldots, j_{k}\right) \in[n]^{k}$ to be the $k$ 'th order derivative obtained by differentiating $\operatorname{Permute}(X)$ by $x_{1 j_{1}} x_{2 j_{2}} \ldots x_{k j_{k}}$. Then

$$
\begin{equation*}
\partial_{J} \operatorname{Permute}(X)=x_{1 j_{1}}^{\frac{D}{\log n}-1} x_{2 j_{2}}^{\frac{D}{\log n}-1} \ldots x_{k j_{k}}^{\frac{D}{\log n}-1} \tag{8}
\end{equation*}
$$

Then we define $S:=\left\{\partial_{J} \operatorname{Permute}(X) \mid \forall J \in[n]^{k}\right\}$ which gives us $|S|=n^{k}$. Furthermore, for any distinct $J, J^{\prime} \in[n]^{k}, J$ and $J^{\prime}$ differ in some coordinate $j_{i}$ implying $\tau=\frac{D}{\log n}-1$. Armed with our values of $|S|$ and $\tau$, we can set the circuit parameters $Q, R$ and the shifted derivative parameters $k, \ell$ and compute a lower bound on bounded fan-in depth four circuits.

### 3.3 Calculation

Lemma 3.3. For any $\Sigma \Pi^{Q} \Pi^{R} \sum$ circuit computing Permute $(X)$, if we set the values for the circuit parameters $Q=n^{1-\frac{5}{\log n}}, R=\frac{\tau}{\log ^{2} n}$ and the shifted derivative parameters $k=\log n, l=\frac{n \log n}{2^{\frac{\log ^{2} n+1}{\tau}}-1}$, then the top fan-in $s$ is greater than $N^{4}$. Adjusting the constant in the definition of $Q$ gives us an poly $(N)$ bound of arbitrary constant degree.

Proof. Plugging these parameters into (5) we find

$$
\begin{equation*}
\frac{n^{k}\binom{N+\ell}{\ell}-n^{2 k}\binom{N+\ell-\tau}{\ell-\tau}}{\binom{Q+k}{k}\binom{N+\ell+k(R-1)}{\ell+k(R-1)}} \leq s \tag{9}
\end{equation*}
$$

We apply standard binomial inequalities to obtain

$$
\begin{equation*}
\frac{n^{k}\binom{N+\ell}{\ell}-n^{2 k}\binom{N+\ell}{\ell}\left(\frac{N+\ell}{\ell}\right)^{-\tau}}{\binom{Q+k}{k}\binom{N+\ell}{\ell}\left(\frac{N+\ell}{\ell}\right)^{k(R-1)}} \leq s \tag{10}
\end{equation*}
$$

And remove the $\binom{N+\ell}{\ell}$ term to obtain

$$
\begin{equation*}
\frac{n^{k}-n^{2 k}\left(\frac{N+\ell}{\ell}\right)^{-\tau}}{\binom{Q+k}{k}\left(\frac{N+\ell}{\ell}\right)^{k(R-1)}} \leq s \tag{11}
\end{equation*}
$$

Now our setting of $\ell$ gives us $\left(\frac{N+\ell}{\ell}\right)^{-\tau}=\frac{1}{2} n^{-k}$ so that the numerator reduces to

$$
\begin{equation*}
n^{k}-n^{2 k}\left(\frac{N+\ell}{\ell}\right)^{-\tau}=\frac{1}{2} n^{k} \tag{12}
\end{equation*}
$$

The denominator reduces to

$$
\begin{equation*}
s\binom{Q+k}{k}\left(\frac{N+\ell}{\ell}\right)^{k R}=s\binom{Q+k}{k} n^{\frac{k^{2} R}{\tau}} 2^{\frac{k R}{\tau}} \tag{13}
\end{equation*}
$$

Now combining numerator and denominator we obtain

$$
\begin{equation*}
s \geq \frac{\frac{1}{2} n^{k}}{\binom{Q+k}{k} n^{\frac{k^{2} R}{\tau}} 2^{\frac{k R}{\tau}}} \geq \frac{\frac{1}{2} n^{k}}{\binom{Q+k}{k} n} \geq \frac{\frac{1}{2} n^{k}}{Q^{k} n} \geq \frac{\frac{1}{2} n^{k}}{n^{\left(1-\frac{5}{\log n}\right) k} n}=\frac{1}{2} n^{4} \tag{14}
\end{equation*}
$$

This concludes our analysis of $\operatorname{Permute}(X)$. We can obtain any polynomial lower bound by adjusting the constant parameter 5 in the setting of $Q$ which is all we need for the subspace restrictions detailed next.

## 4 Putting it Together

We give present the technique of subspace restrictions following the general presentation in [BLS16, KST16]. The proof idea is to construct an explicit polynomial $F_{N^{\prime}, D^{\prime}}$ in VP with $N^{\prime}=\Theta(N \log N)$ variables and degree $D^{\prime}=\Theta(D \log N)$ where any circuit computing $F_{N^{\prime}, D^{\prime}}$ satisfies the property that restricting any $N$ product gates yields a circuit computing Permute (X). So long as $\operatorname{Permute}(X)$ must be computed by a $\operatorname{poly}(N)$ sized circuit with some large constant degree, then $F_{N^{\prime}, D^{\prime}}$ must be computed by a $\Omega(N Q R)=$ $\tilde{\Omega}\left(N^{2} D\right)=\tilde{\Omega}\left(N^{\prime 2} D^{\prime}\right)$ sized circuit. Note, it is for $F_{N^{\prime}, D^{\prime}}$, not Permute $(X)$, for which we produce our almost cubic lower bound. First we present the construction of $F_{N^{\prime}, D^{\prime}}$, then we present the subspace restriction procedure, and finally we prove Theorem 0.1.

### 4.1 Polynomial Embedding

Permute ( $X$ ) takes $N=n \log n$ variables. We now introduce the formal variables $W=\left\{w_{1}, w_{2}, \ldots, w_{2 N}\right\}$ and $U=\left\{U_{1}, U_{2}, \ldots, U_{N}\right\}$. Where each $U_{i} \in U$ is a collection of $q$ variables $U_{i}=\left\{u_{i 1}, u_{i 2}, \ldots, u_{i q}\right\}$ for $q=C \log n$ for constant factor $C$. Now let $M=\left\{m_{1}, m_{2}, \ldots, m_{2 N}\right\}$ be $2 N$ pairwise distinct subsets of [C $\log n$ ] where each $m_{i} \in M$ is of size $\left|m_{i}\right|=C^{\prime} \log n$. . Then for $i \in[2 N]$ and $j \in N$, we define $\phi_{i}\left(U_{j}\right)=\prod_{y \in m_{i}} u_{j y}$. Now we are ready to define $F_{N^{\prime}, D^{\prime}}(U, W)$.
Let $V$ be a set of $N$ formal variables, defined as follows

$$
V=\left[\begin{array}{cccc}
\phi_{1}\left(U_{1}\right) & \phi_{2}\left(U_{1}\right) & \ldots & \phi_{2 N}\left(U_{1}\right)  \tag{15}\\
\phi_{1}\left(U_{2}\right) & \phi_{2}\left(U_{2}\right) & \ldots & \phi_{2 N}\left(U_{2}\right) \\
\ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \\
\phi_{1}\left(U_{N}\right) & \phi_{2}\left(U_{N}\right) & \ldots & \phi_{2 N}\left(U_{N}\right)
\end{array}\right]\left[\begin{array}{c}
w_{1} \\
w_{2} \\
\vdots \\
w_{2 N}
\end{array}\right]
$$

Then we define

$$
\begin{equation*}
F_{N^{\prime}, D^{\prime}}(U, W)=\operatorname{Permute}(V) \tag{16}
\end{equation*}
$$

Their is slight notational abuse since we initially defined Permute to be a function taking a matrix of $N$ variables but $V$ is a vector. It is to be understood that in writing $\operatorname{Permute}(V)$ we implicitly arrange $V$ into a matrix.

First we observe that $F_{N^{\prime}, D^{\prime}}(U, W)$ has $N^{\prime}=C N \log N+2 N=\Theta(N \log N)$ variables. Furthermore, the degree $D^{\prime}=C^{\prime} D \log N=\Theta(D \log N)$. Since the sets $m_{i} \in M$ are pairwise distinct, for each subset $A \in[2 N]$ satisfying $|A|=N$ there exists a setting of the variables in $U$ such that $F_{N^{\prime}, D^{\prime}}(U, W)=\operatorname{Permute}\left(\chi_{A}(W)\right)$ where $\chi_{A}(W)$ selects $N$ variables from $W$ corresponding to $A$. Therefore, we call the $W$ 's "relevant" variables and the $U$ 's "indicator" variables that we eventually set to be $\{0,1\}$. We restate this critical property in the following lemma.
Lemma 4.1. For each subset $A \in[2 N]$ satisfying $|A|=N$, there exists a setting of the variables in $U$ such that $F_{N^{\prime}, D^{\prime}}(U, W)=\operatorname{Permute}\left(\chi_{A}(W)\right)$ where $\chi_{A}(W)$ selects $N$ variables from $W$ corresponding to $A$.

### 4.2 Affine Subspace Restriction

Here we finish proving Theorem 0.1. For any $\Sigma \Pi \sum$ circuit computing $F_{N^{\prime}, D^{\prime}}(U, W)$ we say a product gate is "heavy" if its fan-in consists of more than $Q R$ sum gates that have a relevant variable $w_{i} \in W$ in their fan-in. Then there are two cases.
case 1: If there are more than $N=\Theta(n \log n)$ product gates with fan-in greater than $Q R=n^{1-\frac{5}{\log n}} \frac{\tau}{\log ^{2} n}=\frac{n D}{32 \log ^{2} n}$, then we have an $N \frac{n D}{32 \log ^{2} n}=$ $\Omega\left(\frac{N^{2} D}{\operatorname{polylog}(N)}\right)$ lower bound on the number of wires in the circuit and we're done.
case 2: Consider a $\Sigma \Pi \sum$ circuit with top fan-in $s$ computing $F_{N^{\prime}, D^{\prime}}(U, W)$. If there are fewer than $N$ heavy product gates than we remove them in the following manner. Let $P(U, W)$ be a heavy product gate, then choose any sum gate $L(U, W)$ in the fan-in of $P(U, W)$ that is the affine sum of variables including a relevant $w_{i} \in W$. Therefore we can write $L(U, W)=\alpha w_{i}+L^{\prime}(U, W)$ where $L^{\prime}(U, W)$ is an affine linear form not involving $w_{i}$. Then rewiring the circuit so that $w_{i}=\frac{-1}{\alpha} L^{\prime}(U, W)$ removes the sum gate $L(U, W)$ and the product gate $P(U, W)$. Repeating this process at most $N$ times for all heavy product gates we are eventually left with a $\Sigma \Pi^{Q R} \sum$ circuit which we then pull apart to a $\Sigma \Pi^{Q} \Pi^{R} \sum$ circuit (Note: pulling the product apart does not change the size of the top fan-in). Now let $Y \in[2 N]$ be the set of indices corresponding to the unrestricted variables in $W$, and let $A \subseteq Y$ be a subset of the unrestricted variables of size $|A|=N$. Then by lemma 0.5 we can set the $U$ 's so that $F_{N^{\prime}, D^{\prime}}(U, W)=\operatorname{Permute}\left(\chi_{A}(W)\right)$. Taken together, we have a $\Sigma \Pi^{Q} \Pi^{R} \sum$ circuit with some top fan-in $s^{\prime}$ computing our hard polynomial $\operatorname{Permute}\left(\chi_{A}(W)\right)$. In the process of converting from $\Sigma \Pi \Sigma$ to $\Sigma \Pi^{Q} \Pi^{R} \Sigma$ we have performed affine restrictions and set the variables in $U$, operations that can only decrease the size of the top fan-in. Therefore $s>s^{\prime}$, and by lemma 0.4 we know $s>s^{\prime}>N^{4}$.

Taking the minimum of case 1 and case 2 we obtain the size of any $\Sigma \Pi \Sigma$ circuit computing $F_{N^{\prime}, D^{\prime}}(U, W)$ is greater than $\min \left(\frac{N^{2} D}{\operatorname{polylog}(N)}, N^{4}\right)=\tilde{\Omega}\left(N^{\prime 2} D^{\prime}\right)$ where we understand that $N^{4}$ can be any $\operatorname{pol} y(N)$. As a final comment, the $\tilde{\Omega}$ hides a $\log ^{6} N$ factor, whereas the VNP result in [KST16] is almost cubic by a $\log ^{2} N$ factor. Removal of this final $\log ^{4} N$ can be done if the we do not incur the $\log N$ costs in the polynomial embedding, which would bring the VP result to match the VNP bounds.

## Acknowledgements

We thank Madhu Sudan for directing us to this line of work, for his supervision, guidance, advice, and for many invaluable discussions.

## References

[AG13] Neeraj Kayal Ramprasad Saptharishi Ankit Gupta, Pritish Kamath. Approaching the chasm at depth four. In Conference on Computational Complexity. IEEE, June 2013.
[AV08] Manindra Agrawal and V. Vinay. Arithmetic circuits: A chasm at depth four. 2013 IEEE 54th Annual Symposium on Foundations of Computer Science, 00(undefined):67-75, 2008.
[BLS16] Nikhil Balaji, Nutan Limaye, and Srikanth Srinivasan. An almost cubic lower bound for $\Sigma \Pi \Sigma$ circuits computing a polynomial in VP. Electronic Colloquium on Computational Complexity (ECCC), 23:143, 2016.
[CM13] Suryajith Chillara and Partha Mukhopadhyay. Depth-4 lower bounds, determinantal complexity: A unified approach. arXiv preprint arXiv:1308.1640, 2013.
[GKKS16] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Arithmetic circuits: A chasm at depth 3. SIAM Journal on Computing, 45(3):1064-1079, 2016.
[GR00] D. Grigoriev and A. Razborov. Exponential lower bounds for depth 3 arithmetic circuits in algebras of functions over finite fields. Applicable Algebra in Engineering, Communication and Computing, 10(6):465-487, 2000.
[Kay12] Neeraj Kayal. An exponential lower bound for the sum of powers of bounded degree polynomials. Electronic Colloquium on Computational Complexity (ECCC), 19:81, 2012.
[Koi10] Pascal Koiran. Arithmetic circuits: the chasm at depth four gets wider. CoRR, abs/1006.4700, 2010.
[KS15] Neeraj Kayal and Chandan Saha. Lower bounds for depth three arithmetic circuits with small bottom fanin. In Proceedings of the 30th Conference on Computational Complexity, CCC '15, pages 158-182, Germany, 2015. Schloss Dagstuhl-LeibnizZentrum fuer Informatik.
[KST16] Neeraj Kayal, Chandan Saha, and Sébastien Tavenas. An Almost Cubic Lower Bound for Depth Three Arithmetic Circuits. In Yuval Rabani Ioannis Chatzigiannakis, Michael Mitzenmacher and Davide Sangiorgi, editors, 43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016), volume 55 of Leibniz International Proceedings in Informatics (LIPIcs), pages 33:1-33:15, Dagstuhl, Germany, 2016. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.
[NW96] Noam Nisan and Avi Wigderson. Lower bounds on arithmetic circuits via partial derivatives. Computational Complexity, 6(3):217-234, 1996.
[Raz13] Ran Raz. Tensor-rank and lower bounds for arithmetic formulas. J. ACM, 60(6):40:1-40:15, November 2013.
[SW02] Amir Shpilka and Avi Wigderson. Depth-3 arithmetic circuits over fields of characteristic zero. Comput. Complex., 10(1):1-27, January 2002.
[SY10] Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. Found. Trends Theor. Comput. Sci., 5(3\&\#8211;4):207-388, March 2010.
[Tav15] Sébastien Tavenas. Improved bounds for reduction to depth 4 and depth 3. Information and Computation, 240:2-11, 2015. \{MFCS\} 2013.


[^0]:    ＊Harvard John A．Paulson School of Engineering and Applied Sciences，Department of Computer Science

