


Functional lower bounds for restricted arithmetic circuits of depth four

Suryajith Chillara 

University of Haifa, Israel.

Abstract

Recently, Forbes, Kumar and Saptharishi [CCC, 2016] proved that there exists an explicit $d^{O(1)}$ -variate and degree d polynomial $P_d \in \text{VNP}$ such that if any depth four circuit C of bounded formal degree d which computes a polynomial of bounded individual degree $O(1)$, that is functionally equivalent to P_d , then C must have size $2^{\Omega(\sqrt{d} \log d)}$.

The motivation for their work comes from Boolean Circuit Complexity. Based on a characterization for ACC^0 circuits by Yao [FOCS, 1985] and Beigel and Tarui [CC, 1994], Forbes, Kumar and Saptharishi [CCC, 2016] observed that functions in ACC^0 can also be computed by algebraic $\Sigma\wedge\Sigma\Pi$ circuits (i.e., circuits of the form – sums of powers of polynomials) of $2^{\log^{O(1)} n}$ size. Thus they argued that a $2^{\omega(\text{poly} \log n)}$ “functional” lower bound for an explicit polynomial Q against $\Sigma\wedge\Sigma\Pi$ circuits would imply a lower bound for the “corresponding Boolean function” of Q against non-uniform ACC^0 . In their work, they ask if their lower bound be extended to $\Sigma\wedge\Sigma\Pi$ circuits.

In this paper, for large integers n and d such that $\omega(\log^2 n) \leq d \leq n^{0.01}$, we show that any $\Sigma\wedge\Sigma\Pi$ circuit of bounded individual degree at most $O\left(\frac{d}{k^2}\right)$ that functionally computes Iterated Matrix Multiplication polynomial $\text{IMM}_{n,d} \in \text{VP}$ over $\{0, 1\}^{n^{2d}}$ must have size $n^{\Omega(k)}$. Since Iterated Matrix Multiplication $\text{IMM}_{n,d}$ over $\{0, 1\}^{n^{2d}}$ is functionally in GapL , improvement of the aforementioned lower bound to hold for quasipolynomially large values of individual degree would imply a fine-grained separation of ACC^0 from GapL .

For the sake of completeness, we also show a syntactic size lower bound against any $\Sigma\wedge\Sigma\Pi$ circuit computing $\text{IMM}_{n,d}$ (for the same regime of d) which is tight over large fields. Like Forbes, Kumar and Saptharishi [CCC, 2016], we too prove lower bounds against circuits of bounded formal degree which functionally compute $\text{IMM}_{n,d}$, for a slightly larger range of individual degree.

1 Introduction

Owing to the difficulty in proving Boolean circuit size lower bounds, Valiant proposed that we prove lower bounds in an “algebraic setting” as the underlying algebraic structure could help us understand the computations better. Valiant further conjectured that any circuit theoretic proof for $P \neq \text{NP}$ would have to be preceded by an analogous result in this more constrained arithmetic model [Val92].

Arithmetic circuits (also called as algebraic circuits) are directed acyclic graphs such that the leaf nodes are labeled by variables or constants from the underlying field, and every non-leaf node is labeled either by a $+$ or \times . Every node computes a polynomial by operating on its inputs with the operation given by its label. The computation flows from the leaves to the output node. Complexity of computation here is quantified by the size of the circuit, which is the number of nodes in it.

It is conjectured that Permanent polynomial does not have polynomial size arithmetic circuits [Val79]. Bürgisser [Bür00] showed that if Permanent polynomial were to have a polynomial sized arithmetic circuit then this would imply $\#P \subseteq \text{FNC}^3/\text{poly}$ which would further imply that $\text{NP} \subseteq P/\text{poly}$ which leads to (1) $\text{PH} \subseteq \Sigma_p^2$ [KL80] and (2) $\text{AM} = \text{MA}$ [AKSS95], both of which go against widely believed conjectures. Thus, a central question in the field of algebraic complexity theory is to show that Permanent polynomial (or any closely related polynomial of interest) needs superpolynomial sized arithmetic circuits to compute it.

Four decades after the problem was formulated, the best known size lower bound is still super linear [BS83]. Over the span of last three decades, researchers have considered restricted arithmetic circuits and here we have seen a great progress towards proving lower bounds under these restrictions (see [SY10, Sap19] for a detailed survey). In a surprising result, Agrawal and Vinay [AV08] showed that it is sufficient to prove subexponential size lower bounds against depth four circuits, to prove super polynomial size lower bounds against general arithmetic circuits.

A depth four circuit¹ (denoted by $\Sigma\Pi\Sigma\Pi$) computes polynomials that can also be expressed as a sum of products of polynomials.

$$P(X) = \sum_{i=1}^{s_1} \prod_j Q_{i,j}.$$

Syntactic lower bounds: We say that a polynomial P has a syntactic circuit size lower bound of s against class \mathcal{C} of circuits if no circuit in \mathcal{C} of size strictly smaller than s syntactically computes P .

Strong syntactic size lower bounds for depth four circuits were proven in restricted settings: Bounded fan-in [GKKS14, KSS14, FLMS15, CM19, KS15], Homogeneous [KLSS14, KS14, KLSS17, KS17b], Multilinear [RY09, CLS19], and Multi-r-ic [KST18, Chi20b, Chi20a]. In a breakthrough, Limaye, Srinivasan and Tavenas recently proved superpolynomial size lower bounds against all constant depth circuits [LST21]. Prior to that the best known lower bound for depth four circuits was super-quadratic [GST20] (which improves upon super-linear lower bounds due to Shoup and Smolensky [SS97] and Raz [Raz10]).

Functional lower bounds: For a set $B \subseteq \mathbb{F}$, we say that two polynomials $P(x_1, \dots, x_N)$ and $Q(x_1, \dots, x_N)$ are functionally equivalent over B^N if $P(\mathbf{a}) = Q(\mathbf{a})$ for all $\mathbf{a} \in B^N$. We say that a circuit C functionally computes a polynomial $P \in \mathbb{F}[x_1, \dots, x_N]$ over B^N if the output polynomial $f \in \mathbb{F}[x_1, \dots, x_N]$ of C is functionally equivalent to P over B^N .

We say that a polynomial P has a functional size lower bound of s against a class \mathcal{C} of circuits if no polynomial that is computed by circuits in \mathcal{C} of size strictly less than s , is functionally equivalent to P over B^n for any $B \subseteq \mathbb{F}$.

Forbes, Kumar and Saptharishi [FKS16] proved exponential functional lower bounds for a polynomial in VNP against depth four circuits of bounded formal degree and bounded individual degree $O(1)$. Formally, they showed that there is an explicit polynomial P_d of degree d over $\approx d^3$ variables such that no depth four circuit of bounded formal degree d and size smaller than $2^{c(\sqrt{d} \log d)}$ (for a small constant c) that computes a polynomial of bounded individual degree at most $O(1)$ can be functionally equivalent to P_d . Apart from this work, strong functional lower bounds are known against depth three circuits over finite fields [GR00], multilinear formulas [Raz06, Raz04, RY08, RY09, CELS18, CLS19], and set-multilinear formulas [NW97, LST21].

The motivation for the work of [FKS16] comes from Boolean circuit complexity. ACC^0 circuits are constant depth Boolean circuits that have AND, OR, NOT and MOD gates. Allender and Gore [AG94] showed that *uniform* ACC^0 circuits of subexponential size cannot compute Permanent. In a major breakthrough, Williams [Wil14] showed that there exists a function in NEXP such that it cannot be computed by polynomial sized *nonuniform* ACC^0 circuits. Recently Murray and Williams [MW20] further improved the situation to show that there exists a function in NQP such that it needs superpolynomial size ACC^0 circuits to compute it.

Beigel and Tarui [BT94] showed that every language L in the class ACC^0 can be recognized by a family of depth two² deterministic circuits with a symmetric function gate at the root and $2^{\log^{O(1)} n}$

¹Generally speaking, a depth four circuit can also be of the form $\Pi\Sigma\Pi\Sigma$ but we follow the convention that the root node is a $+$ node. Under such a convention $\Pi\Sigma\Pi\Sigma$ circuit is a depth five circuit.

²Here the variables can appear negated at the leaves that feed into the AND gates. Even though it is stated as depth two in the paper, the longest leaf to root path in this circuit is of length 3. Leaf node \rightarrow AND \rightarrow root.

many AND gates of fan-in $\log^{O(1)} n$ in the second layer. Over large fields, Forbes, Kumar and Saptharishi [FKS16] observed that given this Boolean circuit, there is an algebraic circuit of depth four which computes polynomials of the form – sum of $2^{\log^{O(1)} n}$ many powers of polynomials each of whose monomials are supported on at most $\log^{O(1)} n$ many variables such that outputs of both of these circuits are functionally equivalent.

$\Sigma \wedge \Sigma \Pi$ circuits are depth four circuits that compute polynomials which can be expressed as sums of powers of polynomials. $\Sigma \wedge \Sigma \Pi^{[t]}$ circuits are depth four circuits that compute polynomials which can be expressed as sums of powers of polynomials each of whose monomials are supported on at most t many variables.

We can summarize the afore mentioned discussion formally as follows.

Lemma 1 (Lemma 3.2, [FKS16]). *Let \mathbb{F} be any field of characteristic zero or at least $\exp(\omega(\text{poly}(\log n)))$. If a function $f : \{0, 1\}^n \mapsto \{0, 1\}$ is in ACC^0 then there exists a polynomial $P_f \in \mathbb{F}[x_1, \dots, x_n]$ such that*

- P_f and f are functionally equivalent over $\{0, 1\}^n$, and
- P_f can be computed by a $\Sigma \wedge \Sigma \Pi$ circuit of top fan-in at most $2^{\log^{O(1)} n}$ and bottom support at most $\log^{O(1)} n$.

Thus, to show a lower bound against ACC^0 circuits in the Boolean setting, it is sufficient to show a functional lower bound of $\exp(\omega(\text{poly}(\log n)))$ for a polynomial P would imply that the Boolean part³ of P is not in ACC^0 .

Lemma 2 (Lemma 3.3, [FKS16]). *Let \mathbb{F} be any field of characteristic zero or at least $\exp(\omega(\text{poly}(\log n)))$. Then a $\exp(\omega(\text{poly}(\log n)))$ functional size lower bound for a $n^{O(1)}$ -variate and $n^{O(1)}$ degree polynomial $P \in \mathbb{F}[X]$ against $\Sigma \wedge \Sigma \Pi^{\text{poly}(\log(n))}$ circuits over \mathbb{F} would imply that Boolean part of P is not in ACC^0 .*

Forbes, Kumar and Saptharishi [FKS16] through an open question in their paper ask if such functional lower bounds can also be proved for $\Sigma \wedge \Sigma \Pi$ circuits. We in this paper show strong functional lower bounds against all $\Sigma \wedge \Sigma \Pi$ circuits which output polynomials of bounded individual degree.

A circuit C is said to have a bounded individual degree⁴ r if the polynomial output by the circuit C has degree at most r with respect to each of its variables.

Theorem 3 (Functional Lower Bounds for $\Sigma \wedge \Sigma \Pi$ circuits of Bounded Individual Degree). *Let n be a large integer. Let d, k and r be such that $\omega(\log^2 n) \leq d \leq n^{0.01}$ and $r \leq \frac{d}{1201k^2}$. Any depth four $\Sigma \wedge \Sigma \Pi$ circuit of bounded individual degree r computing a function equivalent to $\text{IMM}_{n,d}$ on $\{0, 1\}^{n^2 d}$, must have size at least $n^{\Omega(k)}$.*

Note that there is a trade-off between the lower bound on the circuit size and the upper bound on the range of r this lower bound can be achieved for.

Since Iterated Matrix Multiplication $\text{IMM}_{n,d}$ over $\{0, 1\}^{n^2 d}$ is functionally⁵ in GapL [Vin91, Section 6], improvement of the afore mentioned lower bound to hold for quasipolynomially large values of individual degree would imply a fine-grained separation of ACC^0 from GapL .

³Bürgisser [Bür00] defined the boolean part of a polynomial $P(x_1, \dots, x_n)$ (denoted by $\text{BP}(P)$) to be a function that agrees with P over all evaluations over $\{0, 1\}^n$.

⁴Not to be confused with the multi- r -ic circuits dealt with in [KS17a, KST18, Chi20b, Chi20a].

⁵Bürgisser [Bür00] showed that boolean part of any polynomial in VP lies in FNC^3/poly , and in particular $\text{IMM}_{n,d} \in \text{VP}$. On the other hand, Vinay [Vin91] identified that this problem of computing Iterated Matrix Product of integer matrices (denoted by ITMATPROD) is in fact in the class GapL which consists of all problems that are logspace reducible to determinant computation of an integer matrix. This is a better characterization as $\text{GapL} \subseteq \text{NC}^2 \subseteq \text{FNC}^3/\text{poly}$.

By a divide and conquer construction, we get a depth four $\Sigma\Pi\Sigma\Pi$ circuit of size $n^{O(\sqrt{d})}$ that computes $\text{IMM}_{n,d}$ such that the fan-in of both the product gates is equal to \sqrt{d} . Using the identity

$$m! \cdot x_1 x_2 \dots x_m = \sum_{S \subseteq [m]} \left(\sum_{i \in S} x_i \right)^m \cdot (-1)^{m-|S|}$$

(attributed to Fischer [Fis94] and Ryser [Rys63] in [GKKS16]), over large fields this circuit can be converted into a $\Sigma\wedge\Sigma\Pi$ circuit of size $n^{O(\sqrt{d})}$. We will now show a lower bound of $n^{\Omega(\sqrt{d})}$ for $\text{IMM}_{n,d}$ against any $\Sigma\wedge\Sigma\Pi$ circuits. From the afore mentioned discussion, this lower bound is optimal up to a constant in the exponent over large fields.

Theorem 4 (Syntactic Lower Bounds for $\Sigma\wedge\Sigma\Pi$ circuits). *Let n and d be a large integers such that $\omega(\log^2 n) \leq d \leq n^{0.01}$. Any depth four $\Sigma\wedge\Sigma\Pi$ circuit computing $\text{IMM}_{n,d}$ must have size at least $n^{\Omega(\sqrt{d})}$.*

Recall that Forbes, Kumar and Saptharishi [FKS16] proved functional lower bounds for a polynomial in VNP against depth four circuits of bounded formal degree whose output polynomials are of bounded individual degree $O(1)$. Here shall prove functional lower bounds for a polynomial in VP against depth four circuits of bounded formal degree whose output polynomials are of bounded individual degree $O(\log n)$.

Formal degree of a circuit is the maximum degree of any polynomial that could be computed by this circuit structure sans the constants nor cancellations. Formal degree of a circuit is inductively defined as follows: for a leaf node w , the formal degree 1 if it is labeled by a variable and 0 otherwise. Formal degree of a sum node is the maximum over all the formal degrees of its children, and formal degree of a product node is equal to the sum over all the formal degrees of its children.

Theorem 5 (Functional Lower Bounds for $\Sigma\Pi\Sigma\Pi$ Circuits of Bounded Formal Degree). *Let n , d and r be integers such that $\omega(\log^2 n) \leq d \leq n^{0.01}$ and $r \leq \frac{\log n}{12}$. Any depth four $\Sigma\Pi\Sigma\Pi$ circuit of formal degree d and bounded individual degree r that computes a function equivalent to $\text{IMM}_{n,d}$ on $\{0, 1\}^{n^2 d}$, must have size at least $n^{\Omega(\sqrt{\frac{d}{r}})}$.*

We would to remark that the afore mentioned bound and the bound for similar circuits in [FKS16] can be made to work for formal degree that is slightly larger than d .

Related Work

For the sake of brevity, we shall denote the $\Sigma\wedge\Sigma\Pi$ circuits of bounded individual degree r by $(\Sigma\Pi\Sigma\Pi)^{\leq r}$. We in this table summarize our results in comparison to the work of [FKS16].

Circuit model	Work	Hard multilinear polynomial family	Lower Bound	Range of parameters
$(\Sigma\Pi\Sigma\Pi)^{\leq r}$ & formal degree d	[FKS16]	Nisan-Wigderson polynomial $\text{NW}_{m,d} \in \text{VNP}$ with md many variables and degree d	$2^{\Omega(\sqrt{d} \log(md))}$	$m = \Theta(d^2)$, and $r \leq O(1)$.
$(\Sigma\Pi\Sigma\Pi)^{\leq r}$ & formal degree d	This work	Iterated Matrix Multiplication polynomial $\text{IMM}_{n,d} \in \text{VP}$ with $n^2 d$ many variables and degree d	$n^{\Omega(\sqrt{\frac{d}{r}})}$	$\omega(\log^2 n) \leq d \leq n^{0.01}$, and $r \leq \frac{\log n}{12}$.
$(\Sigma\wedge\Sigma\Pi)^{\leq r}$	This work	$\text{IMM}_{n,d}$	$n^{\Omega(k)}$	$\omega(\log^2 n) \leq d \leq n^{0.01}$, and $r \leq \frac{d}{1201k^2}$.

Our work is inspired by [FKS16]'s line of research and depends on the techniques introduced by them. We take their research a bit further.

Complexity measure and proof overview

Let the variable set X be partitioned into two fixed, disjoint sets Y and Z . Let $\sigma_Y : \mathbb{F}[Y \sqcup Z] \mapsto \mathbb{F}[Z]$ be a linear map such that for any polynomial $P(Y, Z)$, $\sigma_Y(P) \in \mathbb{F}[Z]$ is obtained by setting every variable from Y to zero and leaving the variables from Z untouched.

For a polynomial $P(x_1, \dots, x_N)$, let $\text{mult}(P)$ be defined to be equal to $P \bmod \{(x_i^2 - x_i) \mid i \in [N]\}$. Similarly, let $\text{mult}(V)$ for a subspace V of polynomials in $\subseteq \mathbb{F}[x_1, \dots, x_N]$, be defined as follows.

$$\text{mult}(V) = \{\text{mult}(P) \mid P \in V\}.$$

For a polynomial $P(Y, Z)$ and a set $S \subseteq \mathbb{F}$, let $\text{Eval}_S^{[Y \cup Z]}(P)$ denote the vector of evaluations of polynomial P over $S^{|Y \cup Z|}$ as follows.

$$\text{Eval}_S^{[Y \cup Z]}(P(Y, Z)) = (P(\mathbf{a}))_{\mathbf{a} \in S^{|Y \cup Z|}}.$$

This definition can be extended to a set V of polynomials over $\mathbb{F}[Y \cup Z]$ as follows.

$$\text{Eval}_S^{[Y \cup Z]}(V) = \left\{ \text{Eval}_S^{[Y \cup Z]}(P(Y, Z)) \mid P(Y, Z) \in V \right\}.$$

We use $\partial_Y^{\leq k} P$ to denote the set of all partial derivatives of P of order at most k with respect to monomials over variables just from Y , and $Z^{\ell} \cdot \sigma_Y(\partial_Y^{\leq k} P)$ to refer to the set of polynomials obtained by multiplying each polynomial in $\sigma_Y(\partial_Y^{\leq k} P)$ with monomials of degree equal to ℓ in Z variables.

Main measure – Multilinear Shifted Evaluation Dimension ($\text{mSED}_{k,\ell}^{[Y,Z]}$): Forbes, Kumar and Saptharishi [FKS16] defined Shifted Evaluation Dimension which counts the dimension of space of vectors each of which is a list of evaluations of polynomials $\{0, 1\}^{|X|}$ where these polynomials are Z -shifts of partial evaluations.

$$\text{SED}_{k,\ell}^{[Y,Z]}(P(Y, Z)) = \dim \left(\text{Eval}_{\{0,1\}^{|Z|}} \left\{ Z^{\ell} \cdot \mathbb{F}\text{-span} \left\{ P(\mathbf{a}, Z) \mid \mathbf{a} \in \{0, 1\}_{\leq k}^{|Y|} \right\} \right\} \right)$$

We just make a minor modification to this measure to better relate our measure with the measure of Projected Shifted Skew Partial derivatives ([Chi20b, Chi20a]) and this helps us obtain bounds that we could not get before.

$$\text{mSED}_{k,\ell}^{[Y,Z]}(P(Y, Z)) = \dim \left(\text{Eval}_{\{0,1\}^{|Z|}} \left\{ \text{mult} \left(Z^{\ell} \cdot \mathbb{F}\text{-span} \left\{ P(\mathbf{a}, Z) \mid \mathbf{a} \in \{0, 1\}_{\leq k}^{|Y|} \right\} \right) \right\} \right)$$

In spirit, it is still the measure of [FKS16] and thus we do not consider this to be a new measure. We just make a minor modification to relate this measure with their measure of Projected Shifted Skew Partial derivatives ([Chi20b, Chi20a]) and this helps us obtain bounds that we could not get before.

By unfurling the above definition, we can see that if two N -variate polynomials $P_1(Y, Z)$ and $P_2(Y, Z)$ (defined on the same variable sets) are functionally equivalent over $\{0, 1\}^N$ then $\text{mSED}_{k,\ell}^{[Y,Z]}(P_1(Y, Z)) = \text{mSED}_{k,\ell}^{[Y,Z]}(P_2(Y, Z))$. Note that two polynomials which are not functionally equivalent over \mathbb{F}^N can end up being functionally equivalent over $\{0, 1\}^N$ but to show that two polynomials are not functionally equivalent, it is sufficient to show that they are not functionally equivalent over $\{0, 1\}^N$.

The crux of our work henceforth is to show that the polynomial of interest, $\text{IMM}_{n,d}$ is not functionally equivalent over $\{0, 1\}^{n^2 d}$ to the polynomials that are output by the $\Sigma/\Delta\Pi$ circuits of bounded

individual degree. That is, we need to show that $\text{mSED}_{k,\ell}^{[Y,Z]}(\text{IMM}_{n,d}(Y,Z))$ is much larger than $\text{mSED}_{k,\ell}^{[Y,Z]}(C(Y,Z))$ where C is a $\Sigma\wedge\Sigma\Pi$ circuit of small size and bounded individual degree.

Though two N -variate polynomials P_1 and P_2 that are functionally equivalent over $\{0,1\}^N$ have the same (multilinear) shifted evaluation dimension, the dimension of their partial derivative spaces can be very different (see [FKS16, Section 1.2.1] for an example). However in certain special cases Forbes, Kumar and Saptharishi [FKS16] do manage to relate the shifted evaluation dimension, and a partial derivate based measure well enough for their proof to work. We shall do something very similar.

Let C be a $\Sigma\wedge\Sigma\Pi$ circuit of bounded individual degree at most r that computes a polynomial that is functionally equivalent to a homogeneous and degree d set-multilinear polynomial $P(X)$ defined over the sets $X = X_1 \sqcup \dots \sqcup X_d$ such that $Y = X_{i_1} \sqcup \dots \sqcup X_{i_k}$ (for a fixed subset $\{i_1, \dots, i_k\} \subseteq [d]$) and $Z = X \setminus Y$. Similar to [FKS16], we show that we can bound the multilinear shifted evaluation dimension on the above and below by an auxiliary measure that counts the dimension of a space of a specially chosen syntactic polynomials. For every value of k, ℓ and r , we can show that

$$\text{PSSPD}_{k,\ell}^{[Y,Z]}(P(Y,Z)) \leq \text{mSED}_{k,\ell}^{[Y,Z]}(P(Y,Z)) = \text{mSED}_{k,\ell}^{[Y,Z]}(C(Y,Z)) \leq \text{PSSPD}_{r,k,\ell}^{[Y,Z]}(C(Y,Z)).$$

Upon instantiating the above expression with explicit homogeneous and set-multilinear polynomial $\text{IMM}_{n,d}(Y,Z)$, and if for a suitable setting of values of k, ℓ and r , we get that $\text{PSSPD}_{k,\ell}^{[Y,Z]}(\text{IMM}_{n,d}(Y,Z))$ is much larger than $\text{PSSPD}_{r,k,\ell}^{[Y,Z]}(C(Y,Z))$ where C is a $\Sigma\wedge\Sigma\Pi$ circuit that computes polynomials of bounded individual degree r of size s , then we can infer that $\text{IMM}_{n,d}(Y,Z)$ cannot be functionally computed by this class of circuits, thus giving us a functional size lower bound of s for this explicit polynomial.

Auxiliary measure – Projected Skew Shifted Partial Derivatives ($\text{PSSPD}_{k,\ell}^{[Y,Z]}$): The following is a measure⁶ borrowed from [Chi20a] which was used to prove syntactic lower bounds for multi- r -ic depth four circuits.

$$\text{PSSPD}_{k,\ell}^{[Y,Z]}(P(Y,Z)) = \dim \left(\mathbb{F}\text{-span} \left\{ \text{mult} \left(Z^{\ell} \cdot \sigma_Y \left(\partial_Y^{\leq k} P \right) \right) \right\} \right).$$

We currently do not know how to directly obtain a bound on $\text{PSSPD}_{r,k,\ell}^{[Y,Z]}(C(Y,Z))$ to a value that is much smaller than $\text{PSSPD}_{k,\ell}^{[Y,Z]}(\text{IMM}_{n,d}(Y,Z))$. To resolve this issue, we use random restrictions $V \leftarrow D$ to convert our $\Sigma\wedge\Sigma\Pi$ circuit C of size $s \leq n^{\frac{t}{2}}$ that computes a polynomial P of bounded individual degree to a $\Sigma\wedge\Sigma\Pi$ circuit C' of size s and of bottom fan-in at most t that still computes the restricted polynomial P' , with a high probability. We can now bound $\text{PSSPD}_{r,k,\ell}^{[Y,Z]}(C(Y,Z))$ to a value that is much smaller than $\text{PSSPD}_{k,\ell}^{[Y,Z]}((\text{IMM}_{n,d}(Y,Z))|_V)$. This trick is omnipresent in this line of work [KLSS14, KS14, KLSS17, KS17b, KST18, FKS16, Chi20b, Chi20a].

We then borrow the lower bound on $\text{PSSPD}_{k,\ell}^{[Y,Z]}(P'(Y,Z))$ (where P' is the polynomial obtained from $\text{IMM}_{n,d}$ after restrictions) from [Chi20a].

We would like to remark that $\text{mult}(P)$ for a polynomial $P(x_1, \dots, x_N)$ was defined to be $P \bmod \{x_i^2 : i \in [N]\}$ in [Chi20b, Chi20a] instead of $P \bmod \{x_i^2 - x_i : i \in [N]\}$ as defined here. We use this new definition of mult because $\text{mSED}_{k,\ell}^{[Y,Z]}(P_1(Y,Z))$ may not be equal to $\text{mSED}_{k,\ell}^{[Y,Z]}(P_2(Y,Z))$ under the older definition of $\text{mult}(P) = P \bmod \{x_i^2 : i \in [N]\}$ even though $P_1(Y,Z)$ and $P_2(Y,Z)$ are functionally equivalent.

The lower bound on $\text{PSSPD}_{k,\ell}^{[Y,Z]}(P'(Y,Z))$ in [Chi20a] continues to hold despite this change of definition.

⁶This measure is an amalgamation of measures – dimension of Projected Shifted Partial derivatives of [KLSS14] and dimension of Skew Shifted Partial derivatives of [KST18].

2 Preliminaries

Notation:

- We use $[n]$ to refer to the set $\{1, 2, \dots, n\}$.
- For a polynomial f and a monomial m of degree k , we use $\partial_m^k f$ to refer to the k th partial derivative of the polynomial f with respect to the monomial m .
- For a polynomial f , we use $\partial_Y^{\leq k}(f)$ to refer to the space of partial derivatives of order at most k of f with respect to monomials of degree at most k in variables from Y .
- We use Z^{ℓ} and $Z^{\leq \ell}$ to refer to the set of all the monomials of degree equal to ℓ and at most ℓ , respectively, in variables Z .
- We use $Z_{ML}^{\leq t}$ to refer to the set of all the multilinear monomials of degree at most t in Z variables.
- For sets A and B of polynomials, we define the product $A \cdot B$ to be the set $\{f \cdot g \mid f \in A \text{ and } g \in B\}$.
- For a monomial m we use $\text{Supp}(m)$ to refer to the set of variables that appear in it.
- We use $Z_{\{\leq t\}}$ to refer to the set of all monomials m in Z variables such that $|\text{Supp}(m)| \leq t$.

Claim 6. *Let $W \subseteq \mathbb{F}[X]$ be a subspace of multilinear polynomials. Then $\dim(W) = \dim(\text{Eval}_{\{0,1\}}^{[X]}(W))$.*

Proof. Proof of this claim follows from the facts that every multilinear polynomial in W has a unique evaluation vector, and access to evaluations of a multilinear polynomial over all of $\{0, 1\}^{[X]}$ uniquely determines it. \square

Proposition 7. *For two sets A and B of polynomials,*

1. $\text{mult}(A \cdot B) = \text{mult}(\text{mult}(A) \cdot \text{mult}(B))$, and
2. $\dim(\text{mult}(\text{mult}(A) \cdot \text{mult}(B))) \leq \dim(\text{mult}(A) \cdot \text{mult}(B))$.

The proof of this proposition easily follows from the fact that mult is a many to one map and not one to many.

Definition 8 (Homogeneous polynomials). *A polynomial P of degree d is said to be homogeneous if it can be expressed as a linear combination of just the monomials of degree equal to d .*

Definition 9 (Set-multilinear polynomials). *A polynomial P is said to be set-multilinear with respect to a set of variables X , under the partition $X = X_1 \sqcup X_2 \sqcup \dots \sqcup X_d$ if every monomial m in the monomial support of P is such that $|\text{MonSupp}(m) \cap X_i| \leq 1$ for all $i \in [d]$.*

Definition 10 (Multi- r -ic polynomials). *A polynomial P is said to be multi- r -ic polynomial if the degree of the polynomial with respect to each of its variables is at most r .*

The following lemma (from [GKKS14]) is key to the asymptotic estimates required for the lower bound analyses.

Lemma 11 (Lemma 6, [GKKS14]). *Let $a(n), f(n), g(n) : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$ be integer valued functions such that $(f + g) = o(a)$. Then,*

$$\ln \frac{(a + f)!}{(a - g)!} = (f + g) \ln a \pm O\left(\frac{(f + g)^2}{a}\right)$$

We shall now state a few lemmas that help us relate both the complexity measures introduced above.

Lemma 12 (Observation 4.5 in [FKS16]). *Let $X = X_1 \sqcup \dots \sqcup X_d$ and $|X| = N$. Let $Y = X_1 \sqcup \dots \sqcup X_k$ for some $k \ll d$. Let P be a homogeneous set multilinear polynomial of degree d with respect to the partition $X_1 \sqcup \dots \sqcup X_d$. Let $m = Y^e$ be a set multilinear monomial⁷ of degree k over Y . Then,*

$$\frac{\partial^k P}{\partial Y^e} = P(\mathbf{e}, Z).$$

Corollary 13 (Similar to Corollary 4.6 in [FKS16]). *For a homogeneous and set multilinear polynomial $P(Y, Z)$ which is as defined as in Lemma 12, and for all values of parameters k and ℓ ,*

$$\text{PSSPD}_{k,\ell}^{[Y,Z]}(P(Y, Z)) \leq \text{mSED}_{k,\ell}^{[Y,Z]}(P(Y, Z)).$$

Proof. From the definition of the polynomial as defined in Lemma 12, it is easy to see that $\sigma_Y(\partial^{<k}P) = 0$. Further from Lemma 12, we know that

$$\begin{aligned} \sigma_Y(\partial_Y^{\leq k}P) &= \left\{ P(\mathbf{e}, Z) \mid \mathbf{e} \in \{0, 1\}_{=k}^{|Y|} \text{ indexes a set multilinear monomial over } Y \right\} \\ &\subseteq \left\{ P(\mathbf{e}, Z) \mid \mathbf{e} \in \{0, 1\}_{\leq k}^{|Y|} \right\} \end{aligned}$$

Multiplying both sides with the set $Z^{\leq \ell}$, we get the following.

$$Z^{\leq \ell} \cdot \sigma_Y(\partial_Y^{\leq k}P) \subseteq Z^{\leq \ell} \cdot \left\{ P(\mathbf{e}, Z) \mid \mathbf{e} \in \{0, 1\}_{\leq k}^{|Y|} \right\}.$$

Note that this inclusion continues to hold even after a multilinear projection.

$$\text{mult}(Z^{\leq \ell} \cdot \sigma_Y(\partial_Y^{\leq k}P)) \subseteq \text{mult}\left(Z^{\leq \ell} \cdot \left\{ P(\mathbf{e}, Z) \mid \mathbf{e} \in \{0, 1\}_{\leq k}^{|Y|} \right\}\right).$$

Now taking the evaluation perspective of all the multilinear polynomials in the subspaces on both sides, we get that

$$\text{Eval}_{\{0,1\}}^{[Z]}(\text{mult}(Z^{\leq \ell} \cdot \sigma_Y(\partial_Y^{\leq k}P))) \subseteq \text{Eval}_{\{0,1\}}^{[Z]}(\text{mult}\left(Z^{\leq \ell} \cdot \left\{ P(\mathbf{e}, Z) \mid \mathbf{e} \in \{0, 1\}_{\leq k}^{|Y|} \right\}\right))$$

and thus

$$\dim\left(\text{Eval}_{\{0,1\}}^{[Z]}(\text{mult}(Z^{\leq \ell} \cdot \sigma_Y(\partial_Y^{\leq k}P)))\right) \leq \text{mSED}_{k,\ell}^{[Y,Z]}(P(Y, Z)).$$

Putting this together with Claim 6, we get the following.

$$\begin{aligned} \text{PSSPD}_{k,\ell}^{[Y,Z]}(P(Y, Z)) &= \dim\left(\mathbb{F}\text{-span}\left\{\text{mult}\left(Z^{\leq \ell} \cdot \sigma_Y\left(\partial_Y^{\leq k}f\right)\right)\right\}\right) \\ &= \dim\left(\mathbb{F}\text{-span}\left\{\text{mult}\left(Z^{\leq \ell} \cdot \sigma_Y\left(\partial_Y^{\leq k}f\right)\right)\right\}\right) \\ &= \dim\left(\text{Eval}_{\{0,1\}}^{[Z]}(\text{mult}(Z^{\leq \ell} \cdot \sigma_Y(\partial_Y^{\leq k}P)))\right) \\ &\leq \text{mSED}_{k,\ell}^{[Y,Z]}(P(Y, Z)). \end{aligned}$$

□

⁷Here \mathbf{e} is a $|Y|$ -long vector that indicates the support of multilinear monomials. Y^e is a shorthand representation of $y_1^{e_1} y_2^{e_2} \dots y_{|Y|}^{e_{|Y|}}$.

Lemma 14 (Lemma 4.7 in [FKS16]). *Let $P(Y, Z)$ be a multi- r -ic polynomial. Then for every choice of parameters k and ℓ , we have*

$$\left\{ P(\mathbf{e}, Z) \mid \mathbf{e} \in \{0, 1\}_{\leq k}^{|Y|} \right\} \subseteq \mathbb{F}\text{-span} \left\{ \sigma_Y(\partial_Y^{\leq rk} P) \right\}.$$

Corollary 15 (Similar to Lemma 4.8 in [FKS16]). *For a multi- r -ic polynomial $P(Y, Z)$,*

$$\text{mSED}_{k, \ell}^{[Y, Z]}(P(Y, Z)) \leq \text{PSSPD}_{r, k, \ell}^{[Y, Z]}(P(Y, Z)).$$

Proof.

$$\left\{ P(\mathbf{e}, Z) \mid \mathbf{e} \in \{0, 1\}_{\leq k}^{|Y|} \right\} \subseteq \mathbb{F}\text{-span} \left\{ \sigma_Y(\partial_Y^{\leq rk} P) \right\}$$

Multiplying these polynomials on either sides by monomials in $Z^{\leq \ell}$, we get the following.

$$Z^{\leq \ell} \cdot \left\{ P(\mathbf{e}, Z) \mid \mathbf{e} \in \{0, 1\}_{\leq k}^{|Y|} \right\} \subseteq \mathbb{F}\text{-span} \left\{ Z^{\leq \ell} \cdot \sigma_Y(\partial_Y^{\leq rk} P) \right\}.$$

Note that this inclusion continues to hold under multilinear projections.

$$\text{mult} \left(Z^{\leq \ell} \cdot \left\{ P(\mathbf{e}, Z) \mid \mathbf{e} \in \{0, 1\}_{\leq k}^{|Y|} \right\} \right) \subseteq \mathbb{F}\text{-span} \left\{ \text{mult} \left(Z^{\leq \ell} \cdot \sigma_Y(\partial_Y^{\leq rk} P) \right) \right\}.$$

Putting this together with Claim 6, we get the following.

$$\begin{aligned} \text{mSED}_{k, \ell}^{[Y, Z]}(P(Y, Z)) &= \dim \left(\text{Eval}_{\{0, 1\}}^{[Z]} \left\{ \text{mult} \left(Z^{\leq \ell} \cdot \left\{ P(\mathbf{e}, Z) \mid \mathbf{e} \in \{0, 1\}_{\leq k}^{|Y|} \right\} \right) \right\} \right) \\ &= \dim \left(\mathbb{F}\text{-span} \left\{ \text{mult} \left(Z^{\leq \ell} \cdot \left\{ P(\mathbf{e}, Z) \mid \mathbf{e} \in \{0, 1\}_{\leq k}^{|Y|} \right\} \right) \right\} \right) \\ &\leq \dim \left(\mathbb{F}\text{-span} \left\{ \text{mult} \left(Z^{\leq \ell} \cdot \sigma_Y(\partial_Y^{\leq rk} P) \right) \right\} \right) \\ &= \text{PSSPD}_{r, k, \ell}^{[Y, Z]}(P(Y, Z)). \end{aligned}$$

□

Complexity measure for the $\Sigma \wedge \Sigma \Pi$ circuits of low bottom support

Lemma 16. *Let m, k, ℓ and t be positive integers such that $\ell + kt < \frac{m}{2}$. Let Y and Z be disjoint sets of variables such that $|Z| = m$. Let $C(Y, Z)$ be a depth four $\Sigma \wedge \Sigma \Pi$ circuit of bottom support at most t with respect to variables from Z , and size s . Then, $\text{PSSPD}_{k, \ell}^{[Y, Z]}(C)$ is at most $s \cdot (k + 1) \cdot \binom{m}{\ell + kt} \cdot (\ell + kt)$.*

Proof. Let $C(Y, Z)$ be equal to the sum $T_1(Y, Z) + \dots + T_s(Y, Z)$ where $T_i(Y, Z) = (Q_i(Y, Z))^{e_i}$ ($i \in [s]$, $e_i \in \mathbb{Q}$ and $Q_i \in \mathbb{F}[Y \sqcup Z]$ is a polynomial each of whose monomials are supported on at most t many variables from Z). It is easy to verify that the measure of Projected Skew Partial derivatives is sub-additive and thus we get that

$$\text{PSSPD}_{k, \ell}^{[Y, Z]}(C(Y, Z)) \leq \sum_{i \in [s]} \text{PSSPD}_{k, \ell}^{[Y, Z]}(T_i(Y, Z)). \quad (1)$$

Let $T(Y, Z)$ be an arbitrary term in $\{T_1(Y, Z), \dots, T_s(Y, Z)\}$ such that $T = (Q(Y, Z))^e$ for some $Q(Y, Z)$ all of whose monomials are supported on at most t many variables from Z , and $e \in \mathbb{Q}$.

Case when $e \geq k$: We shall prove by induction on k that for any monomial $m \in \mathbb{F}[Y]$ of degree k ,

$$\partial_m^k(T(Y, Z)) \in \mathbb{F}\text{-span} \left\{ (Q(Y, Z))^{e-k} \cdot \{Z_{\{\leq kt\}}\} \cdot \mathbb{F}[Y] \right\}.$$

Base case when $k = 0$ is trivial as T is already in the required form $(Q(Y, Z))^e \cdot Z_{\{=0\}} \cdot 1$. Now assume the induction hypothesis for all $\partial_{m'}^{k'}$, ($k' \leq k - 1$). Let $m' = y_{i_1} \dots y_{i_{k-1}}$ be a monomial in $\mathbb{F}[Y]$ and $\partial_{m'}^{k-1}T$ be expressed as $(Q(Y, Z))^{e-(k-1)} \cdot g(Z) \cdot h(Y)$ where $g(Z)$ is a polynomial in $\mathbb{F}[Z]$ each of whose monomials are supported on at most $(k-1)t$ many variables, and $h(Y)$ is some arbitrary polynomial in $\mathbb{F}[Y]$. Further deriving $\partial_{m'}^{k-1}T$ with y_{i_k} , we get the following.

$$\begin{aligned} \frac{\partial (\partial_{m'}^{k-1}T)}{\partial y_{i_k}} &= (e - k + 1) \cdot (Q(Y, Z))^{e-(k-1)-1} \cdot \frac{\partial Q(Y, Z)}{\partial y_{i_k}} \cdot g(Z) \cdot h(Y) \\ &\quad + (Q(Y, Z))^{e-(k-1)-1} \cdot Q(Y, Z) \cdot g(Z) \cdot \frac{\partial h(Y)}{\partial y_{i_k}} \\ &= (Q(Y, Z))^{e-k} \cdot \left((e - k + 1) \cdot \frac{\partial Q(Y, Z)}{\partial y_{i_k}} \cdot h(Y) + Q(Y, Z) \cdot \frac{\partial h(Y)}{\partial y_{i_k}} \right) \cdot g(Z) \\ &\in \left\{ (Q(Y, Z))^{e-k} \cdot g(Z) \cdot Z_{\{\leq t\}} \cdot \mathbb{F}[Y] \right\} \\ &\subseteq \mathbb{F}\text{-span} \left\{ (Q(Y, Z))^{e-k} \cdot \{Z_{\{\leq kt\}}\} \cdot \mathbb{F}[Y] \right\}. \end{aligned}$$

The inclusion in the third line of the math block above follows from the fact that both the polynomial $Q(Y, Z)$ and its derivative $\frac{\partial Q(Y, Z)}{\partial y_{i_k}}$ can be expressed as $(\mathbb{F}[Y])$ -linear combinations of monomials in $Z_{\{\leq t\}}$, and the inclusion in the last line follows from the fact that $g(Z) \in \mathbb{F}[Z]$ is a polynomial each of whose monomials are supported on at most $(k-1)t$ many variables from Z . Thus,

$$\partial^{\leq k}T(Y, Z) \subseteq \mathbb{F}\text{-span} \left\{ \{(Q(Y, Z))^\alpha \mid \alpha \in [e - k, e]\} \cdot \{Z_{\{\leq kt\}}\} \cdot \mathbb{F}[Y] \right\}.$$

Applying the projection σ_Y , the shift Z^{ℓ} , and multilinear projection mult on both sides, we get that

$$\begin{aligned} \mathbb{F}\text{-span} \left\{ \text{mult} \left(Z^{\ell} \cdot \sigma_Y(\partial^{\leq k}T(Y, Z)) \right) \right\} &\subseteq \mathbb{F}\text{-span} \left\{ \text{mult} \left(\{(\sigma_Y(Q(Y, Z)))^\alpha \mid \alpha \in [e - k, e]\} \cdot \{Z_{\{\leq \ell+kt\}}\} \right) \right\} \\ &\subseteq \mathbb{F}\text{-span} \left\{ \text{mult} \left(\{(\sigma_Y(Q(Y, Z)))^\alpha \mid \alpha \in [e - k, e]\} \cdot Z_{\text{ML}}^{\leq \ell+kt} \right) \right\}. \end{aligned}$$

The last inclusion follows from Item 2 of Proposition 7. This implies that

$$\begin{aligned} \dim \left(\mathbb{F}\text{-span} \left\{ \text{mult} \left(Z^{\ell} \cdot \sigma_Y(\partial^{\leq k}T(Y, Z)) \right) \right\} \right) &\leq \dim \left(\text{mult} \left(\{(\sigma_Y(Q(Y, Z)))^\alpha \mid \alpha \in [e - k, e]\} \right) \right) \\ &\quad \cdot \dim(Z_{\text{ML}}^{\leq \ell+kt}). \end{aligned}$$

Here $\dim \left(\text{mult} \left(\{(\sigma_Y(Q(Y, Z)))^\alpha \mid \alpha \in [e - k, e]\} \right) \right)$ is at most $(k+1)$, and $\dim(Z_{\text{ML}}^{\leq \ell+kt})$ is at most $\binom{m}{\ell+kt} \cdot (\ell+kt)$ when $\ell+kt \leq \frac{m}{2}$. Thus, $\text{PSSPD}_{k,\ell}^{[Y,Z]}(T(Y, Z))$ is at most $(k+1) \cdot \binom{m}{\ell+kt} \cdot (\ell+kt)$ when $\ell+kt \leq \frac{m}{2}$.

Case when $e < k$: It is easy to see that Q^e and its partial derivatives of any order with respect to variables from Y can be expressed as a $(\mathbb{F}[Y])$ -linear combinations of monomials in $Z_{\{\leq kt\}}$. Thus,

$$\mathbb{F}\text{-span} \left\{ \text{mult} \left(Z^{\ell} \cdot \sigma_Y(\partial^{\leq k}T(Y, Z)) \right) \right\} \subseteq \mathbb{F}\text{-span} \left\{ \text{mult} \left(Z_{\{\leq \ell+kt\}} \right) \right\} \subseteq \mathbb{F}\text{-span} \left\{ Z_{\text{ML}}^{\leq \ell+kt} \right\}.$$

Thus, $\text{PSSPD}_{k,\ell}^{[Y,Z]}(T(Y, Z))$ in this case is at most $(\ell+kt) \cdot \binom{m}{\ell+kt}$ when $\ell+kt < \frac{m}{2}$.

Putting both of these cases together with Eq. (1) and the fact that $\ell + kt \leq \frac{m}{2}$, we get that

$$\begin{aligned} \text{PSSPD}_{k,\ell}^{[Y,Z]}(C(Y,Z)) &\leq \sum_{i \in [s]} \text{PSSPD}_{k,\ell}^{[Y,Z]}(T_i(Y,Z)) \leq s \cdot \max_{i \in [s]} \left\{ \text{PSSPD}_{k,\ell}^{[Y,Z]}(T_i(Y,Z)) \right\} \\ &\leq s \cdot (k+1) \cdot \binom{m}{\ell+kt} \cdot (\ell+kt). \end{aligned}$$

This completes the proof. \square

3 Hard Polynomial and Restrictions

In this section we recall the definition of the polynomial family and the set of deterministic and random restrictions imposed on the polynomial family, from [Chi20a].

3.1 Polynomial Family: Iterated Matrix Multiplication polynomial

Let $X^{(1)}, X^{(2)}, \dots, X^{(d)}$ be d generic $n \times n$ matrices defined over disjoint set of variables. For any $k \in [d]$, let $x_{i,j}^{(k)}$ be the variable in the matrix $X^{(k)}$ indexed by $(i, j) \in [n] \times [n]$. The Iterated Matrix Multiplication polynomial, denoted by the family $\{\text{IMM}_{n,d}\}$, is defined as follows.

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

3.2 Deterministic and Random Restrictions

Let k and α be parameters such that $d = (2\alpha + 3) \cdot k$. Let the d matrices be divided into k contiguous blocks of matrices B_1, B_2, \dots, B_k such that each block B_i contains $2\alpha + 3$ matrices. By suitable renaming, let us assume that each block B_i contains the following matrices.

$$X^{(i,L,\alpha+1)}, \dots, X^{(i,L,2)}, X^{(i,L,1)}, X^{(i)}, X^{(i,R,1)}, X^{(i,R,2)}, \dots, X^{(i,R,\alpha+1)}.$$

Let us first consider the following set of restrictions, first deterministic and then randomized.

Deterministic Restrictions

Let $V_0 : X \mapsto Y_0 \sqcup Z_0 \sqcup \{0, 1\}$ be a deterministic restriction of the variables X in to disjoint variable sets Y_0, Z_0 , and $\{0, 1\}$ as follows. For all $i \in [k]$,

- The variables in matrix in $X^{(i)}$ are each set to a distinct Y_0 variable. Henceforth, we shall refer to this as $Y^{(i)}$ matrix.
- The entries of the first row of matrix $X^{(i,L,\alpha+1)}$ are all set to 1 and the rest of the matrix to 0.
- The entries of the first column of matrix $X^{(i,R,\alpha+1)}$ are all set to 1 and the rest of the matrix to 0.
- The rest of the variables are all set to distinct Z_0 variables. Henceforth, for all $b \in \{L, R\}$ and $j \in [\alpha]$, we shall refer to the matrix $X^{(i,b,j)}$ as $Z^{(i,b,j)}$ matrix.

Random Restrictions

Let η and ε' be two fixed constants in $(0, 1)$. Let $V_1 : Y_0 \sqcup Z_0 \mapsto Y \sqcup Z \sqcup \{0, 1\}$ be a random restriction of the variables $Y_0 \sqcup Z_0$ as follows.

- Matrix $Z^{(i,L,1)}$: For every column, pick n^η distinct elements uniformly at random and keep these elements alive. Set the other entries in this matrix to zero.
- Matrix $Z^{(i,R,1)}$: For every row, pick n^η distinct elements uniformly at random and keep these elements alive. Set the other entries in this matrix to zero.
- Matrices $Z^{(i,L,j)}$ for all $j \in [2, \alpha - \varepsilon' \log n]$: For every column, pick 2 distinct elements uniformly at random and set all the other entries to zero.
- Matrices $Z^{(i,R,j)}$ for all $j \in [2, \alpha - \varepsilon' \log n]$: For every row, pick 2 distinct elements uniformly at random and set all the other entries to zero.
- Matrices $Z^{(i,L,j)}$ for all $j > \alpha - \varepsilon' \log n$: For every column, pick 1 element uniformly at random and set the other elements in that row to zero.
- Matrices $Z^{(i,R,j)}$ for all $j > \alpha - \varepsilon' \log n$: For every row, pick 1 element uniformly at random and set the other elements in that row to zero.

Let D be the distribution of all the restrictions $V : X \mapsto Y \sqcup Z \sqcup \{0, 1\}$ such that $V = V_1 \circ V_0$ where V_0 and V_1 are deterministic and random restrictions respectively, as described above. Let m be used to denote the number of Z variables left after the restriction and $m = 2kn(n^\eta + 2(\alpha - \varepsilon' \log n - 1) + \varepsilon' \log n) = O(n^{1+\eta}k)$ when $\alpha \leq O(n^\eta)$.

Effect of Restrictions on $\text{IMM}_{n,d}$

Let $g_{1,a}^{(i,L)}(Z)$ be the $(1, a)$ th entry in product of matrices $\prod_{j=0}^{\alpha} X^{(i,L,\alpha+1-j)}|_V$. Let $g_{b,1}^{(i,R)}(Z)$ be the $(b, 1)$ th entry in product of matrices $\prod_{j=1}^{\alpha+1} X^{(i,R,j)}|_V$. Let $g^{(i)}$ the $(1, 1)$ th entry in the product of all the matrices in the block B_i . Then we can express $g^{(i)}$ as follows.

$$g^{(i)}(Y, Z) = \sum_{a,b \in [n]} g_{1,a}^{(i,L)}(Z) \cdot y_{a,b}^{(i)} \cdot g_{b,1}^{(i,R)}(Z).$$

Let $P|_V(Y, Z)$ obtained by restricting $\text{IMM}_{n,d}(X)$ with the restriction $V \leftarrow D$. Thus,

$$P|_V(Y, Z) = \prod_{i=1}^k g^{(i)}(Y, Z).$$

To summarize, for some parameters α, k, η and m , $P|_V$ is polynomial in $\mathbb{F}[Y \sqcup Z]$ such that its degree is $d = (2\alpha + 3) \cdot k$, and has $m = O(n^{1+\eta}k)$ many Z variables. Here the definition of the polynomial $P|_V$ is heavily dependent on $V \leftarrow D$ and the choice of parameters α, k, ε' and η .

Effect on random restrictions:

Lemma 17 (Lemma 8, [Chi20a]). *Let t be a parameter. Let C be any depth four circuit of size at most $s \leq n^{\frac{t}{2}}$ that computes $\text{IMM}_{n,d}$. Then with a probability of at least $1 - o(1)$, over $V \leftarrow D$ (where $V : X \mapsto Y \sqcup Z \sqcup \{0, 1\}$), $C|_V$ is a depth four circuit of bottom support at most t in Z variables that computes the polynomial $P|_V(Y, Z)$.*

3.3 Complexity of $P|_V$

Choice of parameters

We borrow the setting of the parameters involved directly from [Chi20a]⁸.

- $\varepsilon' = 0.34$,
- $\eta = 0.05$,
- $\varepsilon = \varepsilon' - \eta = 0.29$,
- $\tau = 0.08$,
- $\omega(\log n) \leq d \leq n^{0.01}$,
- $d = (2\alpha + 3)k$,
- $m = \Theta(n^{1+\eta k}) = \Theta(n^{1.05k})$,
- $\ell = \frac{m}{2}(1 - \Gamma)$,
- $(1 + \Gamma)^\alpha = 2n^\varepsilon$ such that $\Gamma = O_\varepsilon\left(\frac{\ln n}{\alpha}\right)$,

We shall now recall the following from [Chi20a].

Theorem 18 (Discussion above Theorem 17, [Chi20a]). *Let n be a large enough integer. Let $m, d, \ell, \alpha, k, \varepsilon$ and τ be as described above.*

$$\text{PSSPD}_{k,\ell}^{[Y,Z]}(P|_V) \geq \frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k} \cdot \binom{m-2\alpha k}{\ell}}{2^{O(k)} \cdot \left(\frac{\ell}{m-\ell}\right)^{2\alpha k(1-\tau)}}.$$

Note that for a N -variate polynomial $P(X, Y)$, the measure in [Chi20a] was defined to be equal to $\dim(\mathbb{F}\text{-span}\{\text{mult}_0(Z^{\leq \ell} \cdot \sigma_Y(\partial_Y^{\leq k} P))\})$ where $\text{mult}_0(P) = P \bmod \{x_i^2 \mid i \in [N]\}$ compared to the measure here which is equal to $\dim(\mathbb{F}\text{-span}\{\text{mult}(Z^{\leq \ell} \cdot \sigma_Y(\partial_Y^{\leq k} P))\})$ where $\text{mult}(P) = P \bmod \{x_i^2 - x_i \mid i \in [N]\}$. This change of definition would not affect the bound as the lower bound in [Chi20a] counts the leading monomials of support size and degree both equal to $d - k + \ell$, and $\sigma_Y(\partial^{\leq k} P|_V) = \emptyset$ for the polynomial $P|_V$ described above.

4 Functional Lower Bounds against restricted $\Sigma \wedge \Sigma \Pi$ Circuits

As mentioned in the proof overview, we first prove a lower bound against bounded bottom support depth four circuits and then escalate this lower bound to circuits without the restriction on bottom support.

Lemma 19. *Let n and d be large integers such that $\omega(\log^2 n) \leq d \leq n^{0.01}$. Let α, k, r and t be parameters such that $d = (2\alpha + 3)k$ and $r \leq \frac{\alpha}{200t}$. Any depth four $\Sigma \wedge \Sigma \Pi$ circuit of bounded individual degree r and bounded bottom fan-in at most t , computing a function equivalent to $P|_V(X_V)$ (for $V \leftarrow D$) on $\{0, 1\}^{|X_V|}$, must have size at least $n^{\Omega(k)}$.*

Proof. Let $C(Y, Z)$ be a $\Sigma \wedge \Sigma \Pi$ circuit of bounded individual degree r , bottom fan-in at most t and size s . Since the polynomial computed at the root of circuit $C(Y, Z)$ is functionally equivalent to $P|_V(Y, Z)$, we get that

$$\text{mSED}_{k,\ell}^{[Y,Z]}(P|_V(Y, Z)) = \text{mSED}_{k,\ell}^{[Y,Z]}(C(Y, Z)).$$

⁸In an attempt to have a clean up the notation in comparison to [Chi20a], we make the following notational changes – the parameter α here corresponds to k' in [Chi20a], the parameter k here corresponds to r' in [Chi20a]. Further the parameter $k = d - 3r' = 2k'r'$ in [Chi20a] translates to $2\alpha k$ here. The rest of the parameters $\varepsilon, \varepsilon', \eta$ and τ are the same in both the papers.

Further, from Corollary 13 and Corollary 15, the above equation can be extended to the following inequality.

$$\text{PSSPD}_{k,\ell}^{[Y,Z]}(\mathcal{P}|_{\mathcal{V}}(Y, Z)) \leq \text{mSED}_{k,\ell}^{[Y,Z]}(\mathcal{P}|_{\mathcal{V}}(Y, Z)) = \text{mSED}_{k,\ell}^{[Y,Z]}(C(Y, Z)) \leq \text{PSSPD}_{\tau k,\ell}^{[Y,Z]}(C(Y, Z)). \quad (2)$$

From Theorem 18, we have that

$$\text{PSSPD}_{k,\ell}^{[Y,Z]}(\mathcal{P}|_{\mathcal{V}}(Y, Z)) \geq \frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k} \cdot \binom{m-2\alpha k}{\ell}}{2^{O(k)} \cdot \left(\frac{\ell}{m-\ell}\right)^{2\alpha k(1-\tau)}} \quad (3)$$

and from Lemma 16, we have that

$$\text{PSSPD}_{\tau k,\ell}^{[Y,Z]}(C(Y, Z)) \leq s \cdot (kr + 1) \cdot \binom{m}{\ell + krt} \cdot (\ell + krt). \quad (4)$$

Putting Eq. (2), Eq. (3) and Eq. (4) together, we get the following.

$$\frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k} \cdot \binom{m-2\alpha k}{\ell}}{2^{O(k)} \cdot \left(\frac{\ell}{m-\ell}\right)^{2\alpha k(1-\tau)}} \leq s \cdot (kr + 1) \cdot \binom{m}{\ell + krt} \cdot (\ell + krt).$$

Thus,

$$\begin{aligned} s &\geq \frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k} \cdot \binom{m-2\alpha k}{\ell}}{2^{O(k)} \cdot \left(\frac{\ell}{m-\ell}\right)^{2\alpha k(1-\tau)}} \times \frac{1}{(kr + 1) \cdot \binom{m}{\ell + krt} \cdot (\ell + krt)} \\ &= \frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k}}{2^{O(k)}} \cdot \frac{(m - 2\alpha k)!}{\ell! \cdot (m - \ell - 2\alpha k)!} \cdot \frac{(\ell + krt)!(m - \ell - krt)!}{m!} \cdot \left(\frac{m - \ell}{\ell}\right)^{2\alpha k(1-\tau)} \\ &= \frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k}}{2^{O(k)}} \cdot \frac{(m - 2\alpha k)!}{m!} \cdot \frac{(m - \ell)!}{(m - \ell - 2\alpha k)!} \cdot \frac{(\ell + krt)!}{\ell!} \cdot \frac{(m - \ell - krt)!}{(m - \ell)!} \cdot \left(\frac{m - \ell}{\ell}\right)^{2\alpha k(1-\tau)} \\ &\approx \frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k}}{2^{O(k)}} \cdot \left(\frac{m - \ell}{m}\right)^{2\alpha k} \cdot \left(\frac{\ell}{m - \ell}\right)^{krt} \cdot \left(\frac{m - \ell}{\ell}\right)^{2\alpha k(1-\tau)} \\ &= \left(\frac{m - \ell}{\ell}\right)^{2\alpha k(1-\tau) - krt} \cdot \frac{1}{2^{O(k)}} \\ &= \left(\frac{1 + \Gamma}{1 - \Gamma}\right)^{2\alpha k(1-\tau) - krt} \cdot \frac{1}{2^{O(k)}} \\ &\geq ((1 + \Gamma)^2)^{2\alpha k(1-\tau) - krt} \cdot \frac{1}{2^{O(k)}} \\ &= ((1 + \Gamma)^\alpha)^{4k(1-\tau) - \frac{2krt}{\alpha}} \cdot \frac{1}{2^{O(k)}} \\ &\approx (2n^\varepsilon)^{4k(1-\tau) - \frac{2krt}{\alpha}} \cdot \frac{1}{2^{O(k)}} \\ &= \left(\Theta(1) \cdot n^{4\varepsilon(1-\tau) - 10^{-2}}\right)^k \\ &\geq n^{1.05k}. \end{aligned}$$

In the above math block, in line 2 we absorb $(kr + 1) \cdot (\ell + krt)$ into $2^{O(k)}$, in line 4 we use Lemma 11 to get the approximations, in line 6 we use the fact that $m = \frac{\ell}{2}(1 - \Gamma)$, in line -3 we use the fact that $(1 + \Gamma)^\alpha \approx 2n^\varepsilon$, in line -2, we use the fact that r is at most $\frac{\alpha}{200t}$, and in the last line we use the fact that $\varepsilon = 0.29$ and $\tau = 0.08$. \square

Proof of Theorem 3

For a large integer n , let d be such that $\Omega(\log^2 n) \leq d \leq n^{0.01}$. Let t be a parameter that we shall soon fix. Let C be a $\Sigma\wedge\Sigma\Pi$ circuit of bounded individual degree at most r , and size $s \leq n^{\frac{1}{2}}$ that computes a polynomial $Q(X)$ that is functionally equivalent to $\text{IMM}_{n,d}(X)$ (over $\{0,1\}^{n^2d}$). Let α and k be parameters such that $d = (2\alpha + 3)k$. Recall that a restriction $V \leftarrow D$ fixes a subset of variables to values in $\{0,1\}$ and maps the rest to distinct Y and Z variables. For any such restriction $V \leftarrow D$, let $X_V = Y \sqcup Z$ be the set of variables in X that are not set to values in $\{0,1\}$ by V . From Lemma 17 we know that with a probability of at least $1 - o(1)$, the circuit C_V obtained by applying the restriction V to C is a $\Sigma\wedge\Sigma\Pi$ circuit of bounded individual degree at most r , size s and bottom support at most t . Let Q_V be the polynomial computed by C_V , over X_V variables. We shall now show that Q_V is functionally equivalent to $P|_V$ over $\{0,1\}^{|X_V|}$.

Let the set $S_V \subset \{0,1\}^{n^2d}$ be the subset of points such that for all $\mathbf{a} \in S_V$, if $x_i \in X \setminus X_V$ and V sets x_i to $b \in \{0,1\}$, then the value at the i 'th location of \mathbf{a} , $\mathbf{a}_i = b$. Since $Q(X)$ and $\text{IMM}_{n,d}(X)$ are functionally equivalent over all of $\{0,1\}^{n^2d}$, they are functionally equivalent over S_V as well. Thus, $Q_V(\mathbf{a}|_{X_V}) = Q(\mathbf{a}) = \text{IMM}(\mathbf{a}) = P|_V(\mathbf{a}|_{X_V})$ for all $\mathbf{a} \in S_V$. Here $\mathbf{a}|_{X_V} \in \{0,1\}^{|X_V|}$ corresponds to projection of $\mathbf{a} \in \{0,1\}^{n^2d}$ to locations corresponding to the variables in X_V .

This implies that $Q_V(X_V)$ and $P|_V(X_V)$ are functionally equivalent over $\{0,1\}^{|X_V|}$ and thus, there is a $\Sigma\wedge\Sigma\Pi$ circuit of bounded individual degree at most r , size $s \leq n^{\frac{1}{2}}$ and bottom support at most t that functionally computes $P|_V(Y, Z)$. On the other hand if r is at most $\frac{\alpha}{200t}$ then from Lemma 19 we know that any $\Sigma\wedge\Sigma\Pi$ circuit of bounded individual degree at most r and bottom support at most t that functionally computes $P|_V$ must have size $n^{\Omega(k)}$. Putting these together by fixing the value of t to $3k$ we get that s must at least be $n^{\Omega(k)}$. Since r is at most $\frac{\alpha}{200t}$, under this substitution of t , this value computes to $\frac{1}{200 \cdot 3k} \cdot \left(\frac{d}{2k} - \frac{3}{2}\right) = \frac{d}{1200k^2} - \frac{1}{400k}$. \square

5 Syntactic circuit lower bounds against $\Sigma\wedge\Sigma\Pi$ circuits

We shall again prove a lower bound against circuits of low bottom support and then escalate this bound to circuits without any restriction on bottom support.

Lemma 20. *Let n and d be large integers such that $\omega(\log^2 n) \leq d \leq n^{0.01}$. Let α and k be parameters such that $d = (2\alpha + 3)k$. Any depth four $\Sigma\wedge\Sigma\Pi$ circuit of bounded bottom fan-in at most $t = \frac{\alpha}{200}$, syntactically computing $P|_V(X_V)$ (for $V \leftarrow D$) must have size at least $n^{1.05k}$.*

Proof. Let $C(Y, Z)$ be a $\Sigma\wedge\Sigma\Pi$ circuit of bounded individual degree r , bottom fan-in at most t and size s . Since the polynomial computed at the root of circuit C is functionally equivalent to $P|_V(Y, Z)$, we get that

$$\text{PSSPD}_{k,\ell}^{[Y,Z]}(P|_V(Y, Z)) \leq \text{PSSPD}_{k,\ell}^{[Y,Z]}(C(Y, Z)). \quad (5)$$

From Theorem 18, we have

$$\text{PSSPD}_{k,\ell}^{[Y,Z]}(P|_V(Y, Z)) \geq \frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k} \cdot \binom{m-2\alpha k}{\ell}}{2^{O(k)} \cdot \left(\frac{\ell}{m-\ell}\right)^{2\alpha k(1-\tau)}} \quad (6)$$

and from Lemma 16, we have that

$$\text{PSSPD}_{r,k,\ell}^{[Y,Z]}(C(Y, Z)) \leq s \cdot (k+1) \cdot \binom{m}{\ell + kt} \cdot (\ell + kt). \quad (7)$$

Putting Eq. (5), Eq. (6) and Eq. (7) together, we get the following.

$$s \cdot (k+1) \cdot \binom{m}{\ell+kt} \cdot (\ell+kt) \geq \frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k} \cdot \binom{m-2\alpha k}{\ell}}{2^{\mathcal{O}(k)} \cdot \left(\frac{\ell}{m-\ell}\right)^{2\alpha k(1-\tau)}}.$$

Thus,

$$\begin{aligned} s &\geq \frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k} \cdot \binom{m-2\alpha k}{\ell}}{2^{\mathcal{O}(k)} \cdot \left(\frac{\ell}{m-\ell}\right)^{2\alpha k(1-\tau)}} \times \frac{1}{(k+1) \cdot \binom{m}{\ell+kt} \cdot (\ell+kt)} \\ &= \frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k}}{2^{\mathcal{O}(k)}} \cdot \frac{(m-2\alpha k)!}{\ell! \cdot (m-\ell-2\alpha k)!} \cdot \frac{(\ell+kt)!(m-\ell-kt)!}{m!} \cdot \left(\frac{m-\ell}{\ell}\right)^{2\alpha k(1-\tau)} \\ &= \frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k}}{2^{\mathcal{O}(k)}} \cdot \frac{(m-2\alpha k)!}{m!} \cdot \frac{(m-\ell)!}{(m-\ell-2\alpha k)!} \cdot \frac{(\ell+kt)!}{\ell!} \cdot \frac{(m-\ell-kt)!}{(m-\ell)!} \cdot \left(\frac{m-\ell}{\ell}\right)^{2\alpha k(1-\tau)} \\ &\approx \frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k}}{2^{\mathcal{O}(k)}} \cdot \left(\frac{m-\ell}{m}\right)^{2\alpha k} \cdot \left(\frac{\ell}{m-\ell}\right)^{kt} \cdot \left(\frac{m-\ell}{\ell}\right)^{2\alpha k(1-\tau)} \\ &= \left(\frac{m-\ell}{\ell}\right)^{2\alpha k(1-\tau)-kt} \cdot \frac{1}{2^{\mathcal{O}(k)}} \\ &= \left(\frac{1+\Gamma}{1-\Gamma}\right)^{2\alpha k(1-\tau)-kt} \cdot \frac{1}{2^{\mathcal{O}(k)}} \\ &\geq ((1+\Gamma)^2)^{2\alpha k(1-\tau)-kt} \cdot \frac{1}{2^{\mathcal{O}(k)}} \\ &= ((1+\Gamma)^\alpha)^{4k(1-\tau)-\frac{2kt}{\alpha}} \cdot \frac{1}{2^{\mathcal{O}(k)}} \\ &\approx (2n^\varepsilon)^{4k(1-\tau)-\frac{2kt}{\alpha}} \cdot \frac{1}{2^{\mathcal{O}(k)}} \\ &= \left(\Theta(1) \cdot n^{4\varepsilon(1-\tau)-10^{-2}}\right)^k \\ &\geq n^{1.05k}. \end{aligned}$$

In the above math block, in line 2 we absorb $(k+1) \cdot (\ell+kt)$ into $2^{\mathcal{O}(k)}$, in line 4 we use Lemma 11 to get the approximations, in line 6 we use the fact that $m = \frac{\ell}{2}(1-\Gamma)$, in line -3 we use the fact that $(1+\Gamma)^\alpha \approx 2n^\varepsilon$, in line -2 we use the fact that t is at most $\frac{\alpha}{200}$, and in the last line we use the fact that $\varepsilon = 0.29$ and $\tau = 0.08$. \square

Proof of Theorem 4

Let t be a parameter such that $t \geq 3k$ and $t \leq \frac{\alpha}{200}$. Let α and k be such that $d = (2\alpha + 3) \cdot k$. Let C be a $\Sigma \wedge \Sigma \Pi$ circuit of size at most $n^{\frac{1}{2}}$ computing the $\text{IMM}_{n,d}$ polynomial. From Lemma 17, we get that with a probability of at least $(1 - o(1))$ over $V \leftarrow D$, $C|_V$ is a $\Sigma \wedge \Sigma \Pi$ circuit of bottom support at most t . Note that $C|_V$ is of size at most $n^{\frac{1}{2}}$. From Lemma 20, $C|_V$ must have size at least $n^{1.05k}$. From our choice of parameters, $1.05k$ is at most $\frac{1}{2}$. We choose the parameters α and k to be in the order of $\Theta(\sqrt{d})$ such that $\alpha \geq 600k$. Thus, any $\Sigma \wedge \Sigma \Pi$ circuit computing $\text{IMM}_{n,d}$ must have size at least $n^{1.05k} = n^{\Omega(\sqrt{d})}$. \square

6 Functional lower bounds against restricted $\Sigma\Pi\Sigma\Pi$ circuits

Analogous to Lemma 16, we can also prove a bound on $\text{PSSPD}_{k,\ell}^{[Y,Z]}(C)$ where C is a $\Sigma\Pi\Sigma\Pi$ circuit of bounded formal degree and bounded bottom support.

Lemma 21. *Let n, k, r, ℓ and t be positive integers such that $\ell + kt < \frac{m}{2}$. Let $C(Y, Z)$ be a depth four circuit of formal degree at most d , bottom support at most t with respect to Z variables, and size s . Then, $\text{PSSPD}_{k,\ell}^{[Y,Z]}(C)$ is at most $s \cdot \binom{\frac{2d}{t}+1}{k} \cdot \binom{m}{\ell+kt} \cdot (\ell + kt)$.*

We shall again prove a lower bound on circuits of bounded bottom support and then escalate it to the model of interest.

Proof of Theorem 5

Let α and k be parameters such that $d = (2\alpha + 3)k$. Let t be a parameter that we shall soon fix so that it satisfies the criteria that $t \geq 0.1k$ and $r \leq \frac{\alpha}{200t}$. For a large integer n , let d be such that $\Omega(\log^2 n) \leq d \leq n^{0.01}$. Let C be a $\Sigma\Pi\Sigma\Pi$ circuit of bounded formal degree d , bounded individual degree at most r , and size $s \leq n^{\frac{1}{2}}$ that computes a polynomial $Q(X)$ that is functionally equivalent to $\text{IMM}_{n,d}(X)$ (over $\{0, 1\}^{n^{2d}}$).

From Lemma 17 we know that with a probability of at least $1 - o(1)$, the circuit C_V obtained by applying the restriction V to C is a $\Sigma\Pi\Sigma\Pi$ circuit of bounded formal degree d , bounded individual degree at most r , size s and bottom support at most t . Using the same arguments as those in Theorem 3, we get that C_V also functionally computes $P|_V(Y, Z)$. Thus,

$$\text{mSED}_{k,\ell}^{[Y,Z]}(P|_V(Y, Z)) = \text{mSED}_{k,\ell}^{[Y,Z]}(C_V(Y, Z)).$$

Further, from Corollary 13 and Corollary 15, the above equation can be extended to the following inequality.

$$\text{PSSPD}_{k,\ell}^{[Y,Z]}(P|_V(Y, Z)) \leq \text{mSED}_{k,\ell}^{[Y,Z]}(P|_V(Y, Z)) = \text{mSED}_{k,\ell}^{[Y,Z]}(C_V(Y, Z)) \leq \text{PSSPD}_{r,k,\ell}^{[Y,Z]}(C_V(Y, Z)). \quad (8)$$

From Theorem 18, we have that

$$\text{PSSPD}_{k,\ell}^{[Y,Z]}(P|_V(Y, Z)) \geq \frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k} \cdot \binom{m-2\alpha k}{\ell}}{2^{O(k)} \cdot \left(\frac{\ell}{m-\ell}\right)^{2\alpha k(1-\tau)}} \quad (9)$$

and from Lemma 21, we have that

$$\text{PSSPD}_{r,k,\ell}^{[Y,Z]}(C_V(Y, Z)) \leq s \cdot \binom{\frac{2d}{t}+1}{kr} \cdot \binom{m}{\ell+kr} \cdot (\ell + kr). \quad (10)$$

Putting Eq. (8), Eq. (9) and Eq. (10) together, we get the following.

$$\frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k} \cdot \binom{m-2\alpha k}{\ell}}{2^{O(k)} \cdot \left(\frac{\ell}{m-\ell}\right)^{2\alpha k(1-\tau)}} \leq s \cdot \binom{\frac{2d}{t}+1}{kr} \cdot \binom{m}{\ell+kr} \cdot (\ell + kr).$$

Thus,

$$s \geq \frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k} \cdot \binom{m-2\alpha k}{\ell}}{2^{O(k)} \cdot \left(\frac{\ell}{m-\ell}\right)^{2\alpha k(1-\tau)}} \times \frac{1}{\binom{\frac{2d}{t}+1}{kr} \cdot \binom{m}{\ell+kr} \cdot (\ell + kr)}$$

$$\begin{aligned}
&= \frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k}}{2^{\mathcal{O}(k)} \cdot \binom{\frac{2d}{t}+1}{kr}} \cdot \frac{(m-2\alpha k)!}{\ell! \cdot (m-\ell-2\alpha k)!} \cdot \frac{(\ell+krt)!(m-\ell-krt)!}{m!} \cdot \left(\frac{m-\ell}{\ell}\right)^{2\alpha k(1-\tau)} \\
&= \frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k}}{2^{\mathcal{O}(k)} \cdot \binom{\frac{2d}{t}+1}{kr}} \cdot \frac{(m-2\alpha k)!}{m!} \cdot \frac{(m-\ell)!}{(m-\ell-2\alpha k)!} \cdot \frac{(\ell+krt)!}{\ell!} \cdot \frac{(m-\ell-krt)!}{(m-\ell)!} \cdot \left(\frac{m-\ell}{\ell}\right)^{2\alpha k(1-\tau)} \\
&\approx \frac{\left(\frac{m}{m-\ell}\right)^{2\alpha k}}{2^{\mathcal{O}(k)} \cdot \binom{\frac{2d}{t}+1}{kr}} \cdot \left(\frac{m-\ell}{m}\right)^{2\alpha k} \cdot \left(\frac{\ell}{m-\ell}\right)^{krt} \cdot \left(\frac{m-\ell}{\ell}\right)^{2\alpha k(1-\tau)} \\
&= \left(\frac{m-\ell}{\ell}\right)^{2\alpha k(1-\tau)-krt} \cdot \frac{1}{2^{\mathcal{O}(k)} \cdot \binom{\frac{2d}{t}+1}{kr}} \\
&= \left(\frac{1+\Gamma}{1-\Gamma}\right)^{2\alpha k(1-\tau)-krt} \cdot \frac{1}{2^{\mathcal{O}(k)} \cdot \binom{\frac{2d}{t}+1}{kr}} \\
&\geq ((1+\Gamma)^2)^{2\alpha k(1-\tau)-krt} \cdot \frac{1}{2^{\mathcal{O}(k)}} \\
&= ((1+\Gamma)\alpha)^{4k(1-\tau)-\frac{2krt}{\alpha}} \cdot \frac{1}{2^{\mathcal{O}(k)} \cdot \binom{\frac{2d}{t}+1}{kr}} \\
&\approx (2n^\varepsilon)^{4k(1-\tau)-\frac{2krt}{\alpha}} \cdot \frac{1}{2^{\mathcal{O}(k)} \cdot \binom{\frac{2d}{t}+1}{kr}} \\
&\geq \left(\Theta(1) \cdot n^{4\varepsilon(1-\tau)-10^{-2}}\right)^k \left(\frac{krt}{e(2d+t)}\right)^{kr} \\
&\geq n^{1.05k} \cdot \left(\frac{krt}{6d}\right)^{kr}
\end{aligned}$$

In the above math block, in line 2 we absorb $(\ell+krt)$ into $2^{\mathcal{O}(k)}$, in line 4 we use Lemma 11 to get the approximations, in line 6 we use the fact that $m = \frac{\ell}{2}(1-\Gamma)$, in line -3 we use the fact that $(1+\Gamma)^\alpha \approx 2n^\varepsilon$, in line -2, we use the fact that r is at most $\frac{\alpha}{200t}$, $\binom{n}{k} \leq \left(\frac{en}{k}\right)^k$ and in the last line we use the fact that $\varepsilon = 0.29$ and $\tau = 0.08$.

We shall now fix the values of k and t such that $t = k = \sqrt{\frac{d}{600r}}$. The above expression simplifies further to $s \geq \left(\frac{n^{1.05}}{(3600)^r}\right)^k$. If r is at most $\frac{\log n}{12} \leq \frac{\log n}{\log 3600}$, we get that $s \geq n^{0.05k}$. This setting of parameters also satisfies the criteria that $s \leq n^{\frac{t}{2}}$ and $r \leq \frac{\alpha}{200t}$. Under this substitution,

$$r \leq \frac{\alpha}{200t} = \frac{1}{200k} \cdot \left(\frac{d}{2k} - \frac{1}{3}\right) \leq \frac{d}{401k^2} \leq \frac{600r}{401}.$$

□

7 Acknowledgments

The author is grateful to Nikhil Balaji, Mrinal Kumar, Noga Ron-Zewi, Nithin Saurabh, and Nithin Varma for helpful discussions. The author thanks Nikhil Balaji for telling him more about the Boolean complexity of Iterated Matrix Multiplication. The author thanks Ramprasad Satharishi for patiently presenting the results in [FKS16] while the author visited Tel Aviv University in 2016, hosted by Amir Shpilka.

References

- [AG94] Eric Allender and Vivek Gore. A uniform circuit lower bound for the permanent. *SIAM J. Comput.*, 23(5):1026–1049, 1994. URL: <https://doi.org/10.1137/S0097539792233907>, doi:10.1137/S0097539792233907. 2
- [AKSS95] Vikraman Arvind, Johannes Köbler, Uwe Schöning, and Rainer Schuler. If NP has polynomial-size circuits, then MA=AM. *Theor. Comput. Sci.*, 137(2):279–282, 1995. URL: [https://doi.org/10.1016/0304-3975\(95\)91133-B](https://doi.org/10.1016/0304-3975(95)91133-B), doi:10.1016/0304-3975(95)91133-B. 1
- [AV08] Manindra Agrawal and V. Vinay. Arithmetic circuits: A chasm at depth four. In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pages 67–75. IEEE Computer Society, 2008. URL: <https://doi.org/10.1109/FOCS.2008.32>, doi:10.1109/FOCS.2008.32. 2
- [BS83] Walter Baur and Volker Strassen. The complexity of partial derivatives. *Theor. Comput. Sci.*, 22:317–330, 1983. URL: [https://doi.org/10.1016/0304-3975\(83\)90110-X](https://doi.org/10.1016/0304-3975(83)90110-X). 2
- [BT94] Richard Beigel and Jun Tarui. On ACC. *Comput. Complex.*, 4:350–366, 1994. URL: <https://doi.org/10.1007/BF01263423>, doi:10.1007/BF01263423. 2
- [Bür00] Peter Bürgisser. Cook’s versus valiant’s hypothesis. *Theoretical Computer Science*, 235(1):71 – 88, 2000. URL: <http://www.sciencedirect.com/science/article/pii/S0304397599001838>, doi:[https://doi.org/10.1016/S0304-3975\(99\)00183-8](https://doi.org/10.1016/S0304-3975(99)00183-8). 1, 3
- [CELS18] Suryajith Chillara, Christian Engels, Nutan Limaye, and Srikanth Srinivasan. A near-optimal depth-hierarchy theorem for small-depth multilinear circuits. In Mikkel Thorup, editor, *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*, pages 934–945. IEEE Computer Society, 2018. URL: <https://doi.org/10.1109/FOCS.2018.00092>, doi:10.1109/FOCS.2018.00092. 2
- [Chi20a] Suryajith Chillara. New exponential size lower bounds against depth four circuits of bounded individual degree. *Electronic Colloquium on Computational Complexity (ECCC)*, 27:33, 2020. URL: <https://eccc.weizmann.ac.il/report/2020/033>. 2, 3, 5, 6, 11, 12, 13
- [Chi20b] Suryajith Chillara. On Computing Multilinear Polynomials Using Multi-r-ic Depth Four Circuits. In Christophe Paul and Markus Bläser, editors, *37th International Symposium on Theoretical Aspects of Computer Science (STACS 2020)*, volume 154 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 47:1–47:16, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. URL: <https://drops.dagstuhl.de/opus/volltexte/2020/11908>, doi:10.4230/LIPIcs.STACS.2020.47. 2, 3, 5, 6
- [CLS19] Suryajith Chillara, Nutan Limaye, and Srikanth Srinivasan. Small-depth multilinear formula lower bounds for iterated matrix multiplication with applications. *SIAM J. Comput.*, 48(1):70–92, 2019. URL: <https://doi.org/10.1137/18M1191567>. 2
- [CM19] Suryajith Chillara and Partha Mukhopadhyay. Depth-4 lower bounds, determinantal complexity: A unified approach. *computational complexity*, May 2019. URL: <https://doi.org/10.1007/s00037-019-00185-4>, doi:10.1007/s00037-019-00185-4. 2
- [Fis94] Ismor Fischer. Sums of like powers of multivariate linear forms. *Mathematics Magazine*, 67(1):59–61, 1994. URL: <https://doi.org/10.1080/0025570X.1994.11996185>, doi:10.1080/0025570X.1994.11996185. 4

- [FKS16] Michael A. Forbes, Mrinal Kumar, and Ramprasad Saptharishi. Functional lower bounds for arithmetic circuits and connections to boolean circuit complexity. In Ran Raz, editor, *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*, volume 50 of *LIPICs*, pages 33:1–33:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016. URL: <https://doi.org/10.4230/LIPICs.CCC.2016.33>, doi:10.4230/LIPICs.CCC.2016.33. 2, 3, 4, 5, 6, 8, 9, 18
- [FLMS15] Hervé Fournier, Nutan Limaye, Guillaume Malod, and Srikanth Srinivasan. Lower bounds for depth-4 formulas computing iterated matrix multiplication. *SIAM J. Comput.*, 44(5):1173–1201, 2015. URL: <https://doi.org/10.1137/140990280>. 2
- [GKKS14] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Approaching the chasm at depth four. *Journal of the ACM (JACM)*, 61(6):33, 2014. URL: <https://doi.org/10.1145/2629541>. 2, 7
- [GKKS16] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Arithmetic circuits: A chasm at depth 3. *SIAM Journal of Computing*, 45(3):1064–1079, 2016. URL: <https://doi.org/10.1137/140957123>, doi:10.1137/140957123. 4
- [GR00] Dima Grigoriev and Alexander A. Razborov. Exponential lower bounds for depth 3 arithmetic circuits in algebras of functions over finite fields. *Appl. Algebra Eng. Commun. Comput.*, 10(6):465–487, 2000. URL: <https://doi.org/10.1007/s002009900021>, doi:10.1007/s002009900021. 2
- [GST20] Nikhil Gupta, Chandan Saha, and Bhargav Thankey. A super-quadratic lower bound for depth four arithmetic circuits. In Shubhangi Saraf, editor, *35th Computational Complexity Conference, CCC 2020, July 28-31, 2020, Saarbrücken, Germany (Virtual Conference)*, volume 169 of *LIPICs*, pages 23:1–23:31. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. URL: <https://doi.org/10.4230/LIPICs.CCC.2020.23>, doi:10.4230/LIPICs.CCC.2020.23. 2
- [KL80] Richard M. Karp and Richard J. Lipton. Some connections between nonuniform and uniform complexity classes. In *Proceedings of the Twelfth Annual ACM Symposium on Theory of Computing, STOC '80*, page 302–309, New York, NY, USA, 1980. Association for Computing Machinery. URL: <https://doi.org/10.1145/800141.804678>, doi:10.1145/800141.804678. 1
- [KLSS14] Neeraj Kayal, Nutan Limaye, Chandan Saha, and Srikanth Srinivasan. Super-polynomial lower bounds for depth-4 homogeneous arithmetic formulas. In David B. Shmoys, editor, *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 119–127. ACM, 2014. URL: <https://doi.org/10.1145/2591796.2591823>, doi:10.1145/2591796.2591823. 2, 6
- [KLSS17] Neeraj Kayal, Nutan Limaye, Chandan Saha, and Srikanth Srinivasan. An exponential lower bound for homogeneous depth four arithmetic formulas. *SIAM J. Comput.*, 46(1):307–335, 2017. URL: <https://doi.org/10.1137/151002423>, doi:10.1137/151002423. 2, 6
- [KS14] Mrinal Kumar and Shubhangi Saraf. Superpolynomial lower bounds for general homogeneous depth 4 arithmetic circuits. In Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias, editors, *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part I*, volume 8572 of *Lecture Notes in Computer Science*, pages 751–762. Springer, 2014. URL: https://doi.org/10.1007/978-3-642-39979-5_50. 2, 6

- doi.org/10.1007/978-3-662-43948-7_62, doi:10.1007/978-3-662-43948-7_62. 2, 6
- [KS15] Mrinal Kumar and Shubhangi Saraf. The limits of depth reduction for arithmetic formulas: It’s all about the top fan-in. *SIAM J. Comput.*, 44(6):1601–1625, 2015. URL: <https://doi.org/10.1137/140999220>, doi:10.1137/140999220. 2
- [KS17a] Neeraj Kayal and Chandan Saha. Multi-k-ic depth three circuit lower bound. *Theory Comput. Syst.*, 61(4):1237–1251, 2017. URL: <https://doi.org/10.1007/s00224-016-9742-9>, doi:10.1007/s00224-016-9742-9. 3
- [KS17b] Mrinal Kumar and Shubhangi Saraf. On the power of homogeneous depth 4 arithmetic circuits. *SIAM J. Comput.*, 46(1):336–387, 2017. URL: <https://doi.org/10.1137/140999335>, doi:10.1137/140999335. 2, 6
- [KSS14] Neeraj Kayal, Chandan Saha, and Ramprasad Saptharishi. A super-polynomial lower bound for regular arithmetic formulas. In David B. Shmoys, editor, *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 146–153. ACM, 2014. URL: <https://doi.org/10.1145/2591796.2591847>, doi:10.1145/2591796.2591847. 2
- [KST18] Neeraj Kayal, Chandan Saha, and Sébastien Tavenas. On the size of homogeneous and of depth-four formulas with low individual degree. *Theory of Computing*, 14(16):1–46, 2018. URL: <http://www.theoryofcomputing.org/articles/v014a016>, doi:10.4086/toc.2018.v014a016. 2, 3, 6
- [LST21] Nutan Limaye, Srikanth Srinivasan, and Sébastien Tavenas. Superpolynomial lower bounds against low-depth algebraic circuits. *Electron. Colloquium Comput. Complex.*, 28:81, 2021. URL: <https://ecc.weizmann.ac.il/report/2021/081>. 2
- [MW20] Cody D. Murray and R. Ryan Williams. Circuit lower bounds for nondeterministic quasipolytime from a new easy witness lemma. *SIAM J. Comput.*, 49(5), 2020. URL: <https://doi.org/10.1137/18M1195887>, doi:10.1137/18M1195887. 2
- [NW97] Noam Nisan and Avi Wigderson. Lower bounds on arithmetic circuits via partial derivatives. *Computational Complexity*, 6(3):217–234, 1997. doi:10.1007/BF01294256. 2
- [Raz04] Ran Raz. Multilinear-NC² \neq multilinear-NC¹. In *proceedings of Foundations of Computer Science (FOCS)*, pages 344–351, 2004. URL: <https://doi.org/10.1109/FOCS.2004.42>, doi:10.1109/FOCS.2004.42. 2
- [Raz06] Ran Raz. Separation of multilinear circuit and formula size. *Theory of Computing*, 2(1):121–135, 2006. doi:10.4086/toc.2006.v002a006. 2
- [Raz10] Ran Raz. Elusive functions and lower bounds for arithmetic circuits. *Theory Comput.*, 6(1):135–177, 2010. URL: <https://doi.org/10.4086/toc.2010.v006a007>, doi:10.4086/toc.2010.v006a007. 2
- [RY08] Ran Raz and Amir Yehudayoff. Balancing syntactically multilinear arithmetic circuits. *Computational Complexity*, 17(4):515–535, 2008. doi:10.1007/s00037-008-0254-0. 2
- [RY09] Ran Raz and Amir Yehudayoff. Lower bounds and separations for constant depth multilinear circuits. *Computational Complexity*, 18(2):171–207, 2009. doi:10.1007/s00037-009-0270-8. 2

- [Rys63] Herbert John Ryser. *Combinatorial mathematics*, volume 14. American Mathematical Soc., 1963. URL: <https://www.jstor.org/stable/10.4169/j.ctt5hh8v6>. 4
- [Sap19] Ramprasad Satharishi. A survey of lower bounds in arithmetic circuit complexity version 8.0.4. Github survey, 2019. URL: <https://github.com/dasarpmar/lowerbounds-survey/releases/>. 2
- [SS97] Victor Shoup and Roman Smolensky. Lower bounds for polynomial evaluation and interpolation problems. *Computational Complexity*, 6(4):301–311, 1997. URL: <https://doi.org/10.1007/BF01270384>, doi:10.1007/BF01270384. 2
- [SY10] Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Found. Trends Theor. Comput. Sci.*, 5(3-4):207–388, 2010. URL: <https://doi.org/10.1561/04000000039>, doi:10.1561/04000000039. 2
- [Val79] Leslie G. Valiant. Completeness classes in algebra. In Michael J. Fischer, Richard A. DeMillo, Nancy A. Lynch, Walter A. Burkhard, and Alfred V. Aho, editors, *Proceedings of the 11th Annual ACM Symposium on Theory of Computing, April 30 - May 2, 1979, Atlanta, Georgia, USA*, pages 249–261. ACM, 1979. URL: <https://doi.org/10.1145/800135.804419>, doi:10.1145/800135.804419. 1
- [Val92] Leslie G. Valiant. *Why is Boolean Complexity Theory so Difficult?*, page 84–94. London Mathematical Society Lecture Note Series. Cambridge University Press, 1992. doi:10.1017/CB09780511526633.008. 1
- [Vin91] V. Vinay. Counting auxiliary pushdown automata and semi-unbounded arithmetic circuits. In *Proceedings of the Sixth Annual Structure in Complexity Theory Conference, Chicago, Illinois, USA, June 30 - July 3, 1991*, pages 270–284. IEEE Computer Society, 1991. URL: <https://doi.org/10.1109/SCT.1991.160269>, doi:10.1109/SCT.1991.160269. 3
- [Wil14] Ryan Williams. Nonuniform ACC circuit lower bounds. *J. ACM*, 61(1):2:1–2:32, 2014. URL: <https://doi.org/10.1145/2559903>, doi:10.1145/2559903. 2

A Proof of Lemma 21

Let C be expressed as sum of terms $T_1 + T_2 + \dots + T_s$ where each T_i is a product of polynomials $Q_{i1} \cdot \dots \cdot Q_{iD}$. W.L.O.G we can assume that all but one of the polynomials $Q_{i,j}$'s have a degree of at least $\frac{t}{2}$. If not, pick two polynomials of degree strictly smaller than $\frac{t}{2}$ and merge them. Repeat this process until all but one of the factors have degree at least $\frac{t}{2}$. Note that for all $i \in [s]$, the formal degree of T_i is at most the formal degree of C , and syntactic degree of the term T_i is at most the formal degree of T_i . From the afore mentioned arguments, for all $i \in [s]$ syntactic degree of T_i is at least $(D - 1) \cdot \frac{t}{2}$ and formal degree of T_i is at most d . Thus, D is at most $\frac{2d}{t} + 1$.

From the sub-additivity of measure, we know that

$$\text{PSSPD}_{k,\ell}^{[Y,Z]}(C) \leq \sum_{i=1}^s \text{PSSPD}_{k,\ell}^{[Y,Z]}(T_i). \quad (11)$$

Let $T = Q_1 \cdot \dots \cdot Q_D$ be an arbitrary term in $\{T_1, \dots, T_s\}$. We shall henceforth obtain a bound on $\text{PSSPD}_{k,\ell}^{[Y,Z]}(T)$ and then put it together with Eq. (11) to get the desired result.

We will first show by induction on k the following for the set of k th order partial derivatives of T with respect to degree k monomials over variables from Y .

$$\partial_{\bar{Y}}^k T \subseteq \mathbb{F}\text{-span} \left(\left\{ \bigcup_{S \in \binom{[D]}{D-k}} \left\{ \left(\prod_{i \in S} Q_i(Y, Z) \right) \cdot Z_{\{\leq kt\}} \cdot \mathbb{F}[Y] \right\} \right\} \right).$$

The base case of induction for $k = 0$ is trivial as T is already in the required form. Let us assume the induction hypothesis for all derivatives of order $< k$. That is, $\partial_{\bar{Y}}^{k-1} T$ can be expressed as a linear combination of terms of the form

$$h(Y, Z) = \left(\prod_{i \in S} Q_i(Y, Z) \right) \cdot h_1(Z) \cdot h_2(Y).$$

where S is a set of size $D - (k - 1)$, $h_1(Z)$ is a *structured* polynomial in $\mathbb{F}[Z]$ such that $h_1(Z)$ can be expressed as a linear combination of multilinear monomials of support at most $(k - 1)t$, and $h_2(Y)$ is some polynomial in $\mathbb{F}[Y]$.

For some $u \in [Y]$ and some fixed i_0 in S ,

$$\begin{aligned} \frac{\partial h(Y, Z)}{\partial y_u} &= \left(\sum_{j \in S} \left(\prod_{\substack{i \in S \\ i \neq j}} Q_i(Y, Z) \right) \cdot \frac{\partial Q_j(Y, Z)}{\partial y_u} \cdot h_1(Z) \cdot h_2(Y) \right) \\ &\quad + \frac{\prod_{i \in S} Q_i}{Q_{i_0}} \cdot Q_{i_0}(Y, Z) \cdot h_1(Z) \cdot \frac{\partial h_2(Y)}{\partial y_u} \end{aligned}$$

where the first summand on the right hand side of the above equation lies in the subspace $\mathbb{F}\text{-span} \left\{ \left(\prod_{\substack{i \in S \\ i \neq j}} Q_i(Y, Z) \right) \cdot \frac{\partial Q_j(Y, Z)}{\partial y_u} \cdot h_1(Z) \cdot \mathbb{F}[Y] : j \in [S] \right\}$ and the second summand in the same equation, lies in the subspace $\mathbb{F}\text{-span} \left\{ \frac{\prod_{i \in S} Q_i}{Q_{i_0}} \cdot Q_{i_0}(Y, Z) \cdot h_1(Z) \cdot \mathbb{F}[Y] \right\}$.

Note that $\frac{\partial Q_j(Y, Z)}{\partial y_u}$ and Q_{i_0} are polynomials such that every monomial in these depends on at most t many variables from Z . Thus,

$$\frac{\partial h(Y, Z)}{\partial y_u} \in \mathbb{F}\text{-span} \left\{ \bigcup_{T \in \binom{[S]}{S-1}} \left\{ \left(\prod_{i \in T} Q_i(Y, Z) \right) \cdot Z_{\{\leq t\}} \cdot h_1(Z) \cdot \mathbb{F}[Y] \right\} \right\}.$$

In the above expression, the contribution from the variables from Y , to the monomials in $\frac{\partial Q_j(Y, Z)}{\partial y_u}$ and Q_{i_0} gets absorbed into $\mathbb{F}[Y]$ factor.

Recall the fact that $h_1(Z)$ is a linear combination of monomials of support at most $(k - 1)t$. Thus, we get that,

$$\frac{\partial h(Y, Z)}{\partial y_u} \in \mathbb{F}\text{-span} \left\{ \bigcup_{T \in \binom{[D]}{D-k}} \left\{ \left(\prod_{i \in T} Q_i(Y, Z) \right) \cdot Z_{\{\leq kt\}} \cdot \mathbb{F}[Y] \right\} \right\}.$$

From the discussion above we know that any polynomial in $\partial_{\bar{Y}}^k(T)$ can be expressed as a linear combination of polynomials of the form $\frac{\partial h}{\partial y_u}$. Further, every polynomial of the form $\frac{\partial h}{\partial y_u}$ belongs to the set

$$W = \mathbb{F}\text{-span} \left\{ \bigcup_{T \in \binom{[D]}{D-k}} \left\{ \left(\prod_{i \in T} Q_i(Y, Z) \right) \cdot Z_{\{\leq kt\}} \cdot \mathbb{F}[Y] \right\} \right\}.$$

Thus, we get that $\partial_{\bar{Y}}^k T$ is a subset of W . This completes the inductive argument.

From the aforementioned discussion, we can now derive the following expressions.

$$\sigma_Y(\partial_{\bar{Y}}^k T) \subseteq \mathbb{F}\text{-span} \left\{ \bigcup_{S \in \binom{[D]}{D-k}} \left\{ \left(\prod_{i \in S} \sigma_Y(Q_i) \right) \cdot Z_{\{\leq kt\}} \right\} \right\}.$$

It is easy to see that this inclusion holds under shift by monomials of degree at most ℓ over variables from Z .

$$Z^{\leq \ell} \cdot \sigma_Y(\partial_{\bar{Y}}^k T) \subseteq \mathbb{F}\text{-span} \left\{ \bigcup_{S \in \binom{[D]}{D-k}} \left\{ \left(\prod_{i \in S} \sigma_Y(Q_i) \right) \cdot Z_{\{\leq \ell+kt\}} \right\} \right\}.$$

By taking a multilinear projection of the elements on both sides, we get that

$$\begin{aligned} \mathbb{F}\text{-span} \left\{ \text{mult} \left(Z^{\leq \ell} \cdot \sigma_Y(\partial_{\bar{Y}}^k T) \right) \right\} &\subseteq \mathbb{F}\text{-span} \left\{ \bigcup_{S \in \binom{[D]}{D-k}} \left\{ \text{mult} \left(\left(\prod_{i \in S} \sigma_Y(Q_i) \right) \cdot Z_{\{\leq \ell+kt\}} \right) \right\} \right\} \\ &\subseteq \mathbb{F}\text{-span} \left\{ \bigcup_{S \in \binom{[D]}{D-k}} \left\{ \left(\text{mult} \left(\prod_{i \in S} \sigma_Y(Q_i) \right) \right) \cdot Z_{ML}^{\leq kt+\ell} \right\} \right\}. \end{aligned}$$

Thus we get that $\dim(\mathbb{F}\text{-span} \{ \text{mult}(Z^{\leq \ell} \cdot \sigma_Y(\partial_{\bar{Y}}^k T)) \})$ is at most

$$\begin{aligned} &\dim \left(\mathbb{F}\text{-span} \left\{ \bigcup_{S \in \binom{[D]}{D-k}} \left\{ \left(\text{mult} \left(\prod_{i \in S} \sigma_Y(Q_i) \right) \right) \cdot Z_{ML}^{\leq kt+\ell} \right\} \right\} \right) \\ &\leq \dim \left(\mathbb{F}\text{-span} \left\{ \bigcup_{S \in \binom{[D]}{D-k}} \left\{ \text{mult} \left(\prod_{i \in S} \sigma_Y(Q_i) \right) \right\} \right\} \right) \cdot \dim(\mathbb{F}\text{-span} \{ Z_{ML}^{\leq kt+\ell} \}) \\ &\leq \binom{D}{D-k} \cdot \sum_{i=0}^{kt+\ell} \binom{m}{i} \\ &\leq \binom{D}{k} \cdot \binom{m}{\ell+kt} \cdot (\ell+kt) \qquad \qquad \qquad (\text{Since } \ell+kt < m/2). \end{aligned}$$