MATHEMATICS OF COMPUTATION
Volume 87, Number 312, July 2018, Pages 2037–2045
http://dx.doi.org/10.1090/mcom/3284
Article electronically published on December 4, 2017

THE METHOD OF SHIFTED PARTIAL DERIVATIVES CANNOT SEPARATE THE PERMANENT FROM THE DETERMINANT

KLIM EFREMENKO, J. M. LANDSBERG, HAL SCHENCK, AND JERZY WEYMAN

ABSTRACT. The method of shifted partial derivatives introduced A. Gupta et al. [*Approaching the chasm at depth four*, IEEE Comp. Soc., 2013, pp. 65-73] and N. Kayal [*An exponential lower bound for the sum of powers of bounded degree polynomials*, ECCC 19, 2010, p. 81], was used to prove a super-polynomial lower bound on the size of depth four circuits needed to compute the permanent. We show that this method alone cannot prove that the padded permanent $\ell^{n-m}\mathrm{perm}_m$ cannot be realized inside the GL_{n^2}-orbit closure of the determinant $\det_n$ when $n > 2m^2 + 2m$. Our proof relies on several simple degenerations of the determinant polynomial, Macaulay's theorem, which gives a lower bound on the growth of an ideal, and a lower bound estimate from [*Approaching the chasm at depth four*, IEEE Comp. Soc., 2013, pp. 65-73] regarding the shifted partial derivatives of the determinant.

1. INTRODUCTION

Let $\mathfrak{S}_m$ denote the permutation group on m elements and let y^i_j be linear coordinates on $\mathbb{C}^{m^2}$. The permanent polynomial is

$$\mathrm{perm}_m(y^i_j) = \sum_{\sigma\in\mathfrak{S}_m} y^1_{\sigma(1)} \cdots y^m_{\sigma(m)}.$$

Valiant's famous conjecture **VP** $\neq$ **VNP** may be phrased as follows.

Conjecture 1.1 ([15]). *There does not exist a polynomial size circuit computing the permanent.*

Let $W = \mathbb{C}^N$ with linear coordinates $x_1, \ldots, x_N$, let W^* denote the dual vector space, let S^nW denote the space of degree-n homogeneous polynomials on W^*, and let $Sym(W) = \bigoplus_n S^nW$. Let $\mathrm{End}(W)$ denote the space of endomorphisms of W. An element $X \in \mathrm{End}(W)$ acts on S^nW by $P(y) \mapsto P(Xy) =: X^T \cdot P$. In particular, if $P \in S^nW$, $\mathrm{End}(W) \cdot P \subset S^nW$ is the set of homogeneous degree-n polynomials obtainable by linear specializations of the variables $x_1, \ldots, x_N$ in $P(x_1, \ldots, x_N)$.

Since the determinant $\det_n \in S^n\mathbb{C}^{n^2}$ is in **VP**, Conjecture 1.1 would imply the following conjecture.

Received by the editor September 7, 2016, and, in revised form, November 11, 2016, December 14, 2016, and February 22, 2017.

2010 *Mathematics Subject Classification.* Primary 68Q17, 13D02, 14L30, 20B30.

Key words and phrases. Computational complexity, free resolution, determinant, permanent.

The first author was supported in part by European Community Seventh Framework Programme (FP7/2007-2013) under grant agreement number 257575.

The second author was supported by NSF DMS-1405348.

The third author was supported by NSF DMS-1312071.

The fourth author was supported by NSF DMS-1400740.

Conjecture 1.2 ([15]). *Let ℓ be a linear coordinate on $\mathbb{C}^1$ and consider any linear inclusion $\mathbb{C}^1 \oplus \mathbb{C}^{m^2} \to W = \mathbb{C}^{n^2}$ so, in particular, $\ell^{n-m}\operatorname{perm}_m \in S^nW$. Let $n(m)$ be a polynomial. Then for all sufficiently large m,*

$$[\ell^{n-m}\operatorname{perm}_m] \not\in \operatorname{End}(W) \cdot [\det_{n(m)}].$$

The polynomial $\ell^{n-m}\operatorname{perm}_m$ is called the *padded permanent.*

Instead of arbitrary circuits, by [1, 2, 8, 10, 14] one could try to prove Valiant's conjecture by restricting to depth-four circuits and proving a stronger lower bound: If $N(n)$ is a function whose growth is bounded by a polynomial and $\{P_n \in S^n\mathbb{C}^{N(n)}\}$ is a sequence of polynomials that can be computed by a circuit of size $s = s(n)$, then $\{P_n\}$ is computable by a homogeneous $\Sigma\Pi\Sigma\Pi$ circuit of size $2^{\Omega(\sqrt{n\log(ns)\log(N(n))})}$. So to prove **VP** $\neq$ **VNP**, it would be sufficient to show the permanent perm_m is not computable by a size $2^{\Omega(\sqrt{m\cdot poly(\log(m))})}$ homogeneous $\Sigma\Pi\Sigma\Pi$ circuit. The work of Gupta, Kamath, Kayal, and Saptharishi [7] generated considerable excitement, because it came tantalizingly close to proving Valiant's conjecture.

Any method of proof that separates **VP** from **VNP** would also have to separate the determinant from the permanent. We show that this cannot be done with the method of proof in [7], the *method of shifted partial derivatives.* This method builds upon the *method of partial derivatives* (see, e.g., [12]), which dates back to Sylvester [13].

1.1. The methods of partial and shifted partial derivatives.

The space S^kW^* may be interpreted as the space of homogeneous differential operators on $\operatorname{Sym}(W)$ of order k with constant coefficients. Given a homogeneous polynomial $P \in S^nW$, consider the linear map

$$\begin{aligned} P_{k,n-k} : S^kW^* &\to S^{n-k}W \\ D &\mapsto D(P). \end{aligned}$$

In coordinates the map is $\frac{\partial^k}{\partial x_{i_1}\cdots\partial x_{i_k}} \mapsto \frac{\partial^k P}{\partial x_{i_1}\cdots\partial x_{i_k}}$.

Given polynomials $P, Q \in S^nW$, and $k < n$, $P \in \operatorname{End}(W)\cdot Q$ implies that $\operatorname{rank}(P_{k,n-k}) \leq \operatorname{rank}(Q_{k,n-k})$. The method of partial derivatives is to find a k such that $\operatorname{rank}(P_{k,n-k}) > \operatorname{rank}(Q_{k,n-k})$ to prove $P \not\in \operatorname{End}(W)\cdot Q$.

Now consider $P_{k,n-k}\otimes \operatorname{Id}_{S^\tau W} : S^kW^*\otimes S^\tau W \to S^{n-k}W\otimes S^\tau W$ and project (multiply) the image to $S^{n-k+\tau}W$ to obtain a map

$$\begin{aligned} P_{(k,n-k)[\tau]} : S^kW^*\otimes S^\tau W &\to S^{n-k+\tau}W \\ D\otimes R &\mapsto D(P)R. \end{aligned}$$

Again $P \in \operatorname{End}(W)\cdot Q$ implies that $\operatorname{rank}(P_{(k,n-k)[\tau]}) \leq \operatorname{rank}(Q_{(k,n-k)[\tau]})$. The method of shifted partial derivatives is to find k, τ such that $\operatorname{rank}(P_{(k,n-k)[\tau]}) > \operatorname{rank}(Q_{(k,n-k)[\tau]})$ to prove $P \not\in \operatorname{End}(W)\cdot Q$.

Remark 1.3. Both these methods are *algebraic* in the sense that they actually prove $P \not\in \overline{\operatorname{End}(W)\cdot Q}$ where the overline denotes Zariski closure. Most known lower bound techniques for Valiant's conjecture are algebraic; see [6].

Remark 1.4. These methods may be viewed as special cases of the *Young flattenings* introduced in [11].

From the perspective of algebraic geometry, the method of shifted partial derivatives compares growth of *Jacobian ideals*: For $P \in S^nW$, consider the ideal in $\mathrm{Sym}(W)$ generated by the partial derivatives of P of order k. Call this the *k-th Jacobian ideal* of P, and denote it by $\mathcal{I}^{P,k}$. It is generated in degree $n-k$. The method is comparing the dimensions of the Jacobian ideals in degree $n-k+\tau$, i.e., the *Hilbert functions* of the Jacobian ideals.

1.2. Statement of the result.

We prove that the method of shifted partial derivatives [9] cannot give better than a quadratic separation of the permanent from the determinant.

Theorem 1.5. *There exists a constant M such that for all $m > M$ and every $n > 2m^2 + 2m$, any τ and any $k < n$, we have*

$$\mathrm{rank}((\ell^{n-m}\,\mathrm{perm}_m)_{(k,n-k)[\tau]}) < \mathrm{rank}((\det_n)_{(k,n-k)[\tau]}).$$

Despite this, it may be possible that a more general Young flattening is able to prove, e.g., an $\omega(m^2)$ lower bound on n. This motivated the companion paper [3] where we study Jacobian ideals and their minimal free resolutions.

1.3. Overview of the proof.

The proof of Theorem 1.5 splits into four cases:

- (C1) Case $k \geq n - \frac{n}{m+1}$,
- (C2) Case $2m \leq k \leq n - 2m$,
- (C3) Case $k < 2m$ and $\tau > \frac{3}{2}n^2m$,
- (C4) Case $k < 2m$ and $\tau < \frac{n^3}{6m}$.

Note that C1, C2 overlap when $n > 2m^2 + 2m$ and C3, C4 overlap when $n > \frac{m^2}{4}$, so it suffices to take $n > 2m^2 + 2m$.

In the first case, the proof has nothing to do with the padded permanent or its derivatives; it is valid for any polynomial in $m^2 + 1$ variables. Cases C2 and C3 only use that we have a padded polynomial. In the case C4, the only property of the permanent that is used is an estimate on the size of the space of its partial derivatives. Case C1 is proved by showing that in this range the partials of the determinant can be degenerated into the space of *all* polynomials of degree $n-k$ in m^2+1 variables. Cases C2 and C3 use that when $k < n-m$, the Jacobian ideal of *any* padded polynomial $\ell^{n-m}P \in S^nW$ is contained in the ideal generated in degree $n-m-k$ by ℓ^{n-m-k}, which has slowest possible growth by Macaulay's theorem as explained below. Case C2 compares that ideal with the Jacobian ideal of the determinant; it is smaller in degree $n-k$ and therefore smaller in all higher degrees by Macaulay's theorem. Case C3 compares that ideal with an ideal with just two generators in degree $n-k$. Case C4 uses a lower bound for the determinant used in [7] and compares it with a very crude upper bound for the dimension of the space of shifted partial derivatives for the permanent.

If $\mathcal{I} \subset \mathrm{Sym}(W)$ is a ideal, we let $\mathcal{I}_d \subset S^dW$ denote its component in degree d.

We make repeated use of the estimate

$$\ln(q!) = q\ln(q) - q + \Theta(\ln(q)).[1] \tag{1}$$

We remind the reader that the space of partials of order k of $\det_n$ is spanned by the minors of size $n-k$ and the space of partials of order k of perm_m is spanned by the subpermanents of size $m-k$.

[1] Θ means that there exist positive constants c_1, c_2 such that $q\ln(q) - q + c_1\ln(q) \leq \ln(q!) \leq q\ln(q) - q + c_2\ln(q)$.

2. Macaulay's Theorem

We only use Corollary 2.4 from this section in the proof of Theorem 1.5.

Theorem 2.1 (Macaulay, see, e.g., [5])**.** *Let $\mathcal{I} \subset \mathrm{Sym}(\mathbb{C}^N)$ be a homogeneous ideal, and let d be a natural number. Write*

$$\dim S^d\mathbb{C}^N/\mathcal{I}_d = \binom{a_d}{d} + \binom{a_{d-1}}{d-1} + \cdots + \binom{a_\delta}{\delta} \tag{2}$$

with $a_d > a_{d-1} > \cdots > a_\delta$ (such an expression exists and is unique). Then

$$\dim \mathcal{I}_{d+\tau} \geq \binom{N+d+\tau-1}{d+\tau} - \left[\binom{a_d+\tau}{d+\tau} + \binom{a_{d-1}+\tau}{d+\tau-1} + \cdots + \binom{a_\delta+\tau}{\delta+\tau}\right]. \tag{3}$$

Remark 2.2. Gotzman [4] showed that if $\mathcal{I}$ is generated in degree at most d, then equality is achieved for all τ in (3) if equality holds for $\tau = 1$. Ideals satisfying this minimal growth exist, for example, *lex-segment ideals* satisfy this property; see [5].

Remark 2.3. Usually Macaulay's theorem is stated in terms of the coordinate ring $\mathbb{C}[X] := \mathrm{Sym}(W)/\mathcal{I}$ of the variety (scheme) $X \subset W^*$ that is the zero set of $\mathcal{I}$, namely

$$\dim \mathbb{C}[X]_{d+\tau} \leq \binom{a_d+\tau}{d+\tau} + \binom{a_{d-1}+\tau}{d+\tau-1} + \cdots + \binom{a_\delta+\tau}{\delta+\tau}.$$

Corollary 2.4. *Let $\mathcal{I}$ be an ideal such that* $\dim \mathcal{I}_d \geq \dim S^{d-q}\mathbb{C}^N = \binom{N+d-q-1}{d-q}$ *for some $q < d$. Then* $\dim \mathcal{I}_{d+\tau} \geq \dim S^{d-q+\tau}\mathbb{C}^N = \binom{N+\tau+d-q-1}{\tau+d-q}$.

Proof. First use the identity

$$\binom{a+b}{b} = \sum_{j=1}^{q} \binom{a+b-j}{b-j+1} + \binom{a+b-q}{b-q} \tag{4}$$

with $a = N-1$, $b = d$. Write this as

$$\binom{N-1+d}{d} = Q_d + \binom{N-1+d-q}{d-q}.$$

Set

$$Q_{d+\tau} := \sum_{j=1}^{q} \binom{N-1+d+\tau-j}{d+\tau-j+1}.$$

By Macaulay's theorem, any ideal $\mathcal{I}$ with

$$\dim \mathcal{I}_d \geq \binom{N-1+d-q}{d-q}$$

must satisfy

$$\dim \mathcal{I}_{d+\tau} \geq \binom{N-1+d+\tau}{d+\tau} - Q_{d+\tau} = \binom{N-1+d-q+\tau}{d-q+\tau}. \qquad \square$$

We will use Corollary 2.4 with $N = n^2$, $d = n-k$, and $d-q = m$.

3. Case C1

Our assumption is $(m+1)(n-k) \leq n$. It will be sufficient to show that some $R \in \operatorname{End}(W) \cdot \det_n$ satisfies $\operatorname{rank}((\ell^{n-m} \operatorname{perm}_m)_{(k,n-k)[\tau]}) < \operatorname{rank}(R_{k,n-k[\tau]})$. Block the matrix $x = (x^s_u) \in \mathbb{C}^{n^2}$, with $1 \leq s, u \leq n$, as a union of $n-k$ blocks of size $m \times m$ in the upper-left corner plus the remainder. By our assumption we will have at least $n-k$ blocks on the diagonal. Set each diagonal block to the matrix (y^i_j), with $1 \leq i, j \leq m$, (there are $n-k$ such blocks), fill the remainder of the diagonal with ℓ (there are at least $n-k$ such terms), and fill the remainder of the matrix with zeros.

Formally: At place i, j put $y^{i \mod m}_{j \mod m}$ for $|i-j| \leq m-1$ for $i, j \leq m \cdot (n-k)$ and $i - \lfloor \frac{j-1}{m} \rfloor m \leq m$ and for $i, j > m \cdot (n-k)$ put ℓ at place $i = j$. Put zeroes elsewhere.

Let R be the restriction of the determinant to this subspace. Then the space of partials of R of degree $n-k$, $R_{k,n-k}(S^k \mathbb{C}^{n^2 *}) \subset S^{n-k} \mathbb{C}^{n^2}$ contains a space isomorphic to $S^{n-k} \mathbb{C}^{m^2+1}$, and $\mathcal{I}^{\ell^{n-m} \operatorname{perm}_m, k}_{n-k} \subset S^{n-k} \mathbb{C}^{m^2+1}$, yielding the desired inequality.

Example 3.1. Let $m = 2$, $n = 6$, $k = 4$. The matrix is

$$\begin{pmatrix} y^1_1 & y^1_2 & & & & \\ y^2_1 & y^2_2 & & & & \\ & & y^1_1 & y^1_2 & & \\ & & y^2_1 & y^2_2 & & \\ & & & & \ell & \\ & & & & & \ell \end{pmatrix}.$$

Note that any monomial of degree $n-k$ in ℓ and the y^i_j arises as the image of a differential operator because we may obtain any y^i_j from each of the $n-k$ blocks by choosing a monomial appearing in the determinant of that block that contains y^i_j and differentiating in the x directions of the $m-1$ slots of the monomial that do not correspond to y^i_j. One also differentiates the diagonal terms below the blocks of y's the number of times complementary to the degree of ℓ in the monomial. For example, the polynomial $(y^1_1)^2$ is the image of $\frac{\partial^4}{\partial x^2_2 \partial x^4_4 \partial x^5_5 \partial x^6_6}$ and the polynomial $y^1_2 y^2_2$ is the image of $\frac{\partial^4}{\partial x^2_1 \partial x^3_3 \partial x^5_5 \partial x^6_6}$.

4. Case C2

As long as $k < n-m$, $\mathcal{I}^{\ell^{n-m} \operatorname{perm}_m, k}_{n-k} \subset \ell^{n-m-k} \cdot S^m W$, so

$$\dim \mathcal{I}^{\ell^{n-m} \operatorname{perm}_m, k}_{n-k+\tau} \leq \binom{n^2+m+\tau-1}{m+\tau}. \tag{5}$$

By Corollary 2.4, it will be sufficient to show that

$$\dim \mathcal{I}^{\det_n, k}_{n-k} = \binom{n}{k}^2 \geq \dim S^m W = \binom{n^2+m-1}{m}. \tag{6}$$

In the range $2m \leq k \leq n-2m$, the quantity $\binom{n}{k}$ is minimized at $k = 2m$ and $k = n-2m$, so it is enough to show that

$$\binom{n}{2m}^2 \geq \binom{n^2+m-1}{m}. \tag{7}$$

Using (1)

$$\begin{aligned}\ln\binom{n}{2m}^2 &= 2[n\ln(n) - 2m\ln(2m) - (n-2m)\ln(n-2m)] - \Theta(\ln(n))\\ &= 2[n\ln(\frac{n}{n-2m}) + 2m\ln(\frac{n-2m}{2m})] - \Theta(\ln(n))\\ &\leq 4m + m\ln[(\frac{n}{2m}-1)^4] - \Theta(\ln(n)),\end{aligned}$$

where to obtain the last line we used $(1-\frac{2m}{n})^n > e^{-2m}e^{\Theta(\frac{m^2}{n})}$, and

$$\begin{aligned}\ln\binom{n^2+m-1}{m} &= (n^2+m-1)\ln(n^2+m-1) - m\ln(m)\\ &\quad - (n^2-1)\ln(n^2-1) - \Theta(\ln(n))\\ &= (n^2-1)\ln(\frac{n^2+m-1}{n^2-1}) + m\ln(\frac{n^2+m-1}{m}) - \Theta(\ln(n))\\ &= m\ln(\frac{n^2}{m} - \frac{m-1}{m}) + m - \Theta(\ln(n)).\end{aligned}$$

So (7) will hold when $(\frac{n}{2m}-1)^4 > (\frac{n^2}{m} - \frac{m-1}{m})$ which holds for all sufficiently large m when $n > m^2$.

5. Case C3

Here we simply degenerate $\det_n$ to $R = \ell_1^n + \ell_2^n$ by e.g., setting all diagonal elements to ℓ_1, all the subdiagonal and $(1,n)$-entry to ℓ_2 and setting all other elements of the matrix to zero. Then $\mathcal{I}^{R,k}_{n-k} = \operatorname{span}\{\ell_1^{n-k}, \ell_2^{n-k}\}$. In degree $n-k+\tau$, this ideal consists of all polynomials of the form $\ell_1^{n-k}Q_1 + \ell_2^{n-k}Q_2$ with $Q_1, Q_2 \in S^\tau\mathbb{C}^{n^2}$, which has dimension $2\dim S^\tau\mathbb{C}^{n^2} - \dim S^{\tau-(n-k)}\mathbb{C}^{n^2}$ because the polynomials of the form $\ell_1^{n-k}\ell_2^{n-k}Q_3$ with $Q_3 \in S^{\tau-(n-k)}\mathbb{C}^{n^2}$ appear in both terms. By this discussion, or simply because this is a complete intersection ideal, we have

$$\dim\mathcal{I}^{R,k}_{n-k+\tau} = 2\binom{n^2+\tau-1}{\tau} - \binom{n^2+\tau-(n-k)-1}{\tau-(n-k)}. \tag{8}$$

We again use the estimate (5) from Case C2, so we need to show that

$$2\binom{n^2+\tau-1}{\tau} - \binom{n^2+\tau+m-1}{\tau+m} - \binom{n^2+\tau-(n-k)-1}{\tau-(n-k)} > 0.$$

Divide by $\binom{n^2+\tau-1}{\tau}$. We need

$$2 > \Pi_{j=1}^m \frac{n^2+\tau+m-j}{\tau+m-j} + \Pi_{j=1}^{n-k}\frac{\tau-j}{n^2+\tau-j} \tag{9}$$

$$= \Pi_{j=1}^m(1+\frac{n^2}{\tau+m-j}) + \Pi_{j=1}^{n-k}(1-\frac{n^2}{n^2+\tau-j}). \tag{10}$$

The second line is less than

$$(1+\frac{n^2}{\tau})^m + (1-\frac{n^2}{n^2+\tau-1})^{n-k}. \tag{11}$$

We analyze (11) as a function of τ. Write $\tau = n^2 m\delta$, for some function $\delta = \delta(n,m)$. Then (11) is bounded above by

$$e^{\frac{1}{\delta}} + e^{\frac{2}{\delta} - \frac{n}{m\delta}}.$$

The second term goes to zero for large m, so we only need the first term to be < 2: take $\delta \geq \frac{3}{2}$.

6. Case C4

We use a lower bound on $\mathcal{I}^{\det_n,k}_{n-k+\tau}$ from [7]: Given a polynomial f given in coordinates, its *leading monomial* in some monomial order, is the monomial in its expression that is highest in the order. If an ideal is generated by $f_1,\dots,f_q$ in degree $n-k$, then in degree $n-k+\tau$, its dimension is at least the number of monomials in degree $n-k+\tau$ that contain a leading monomial from one of the f_j.

If we order the variables in $\mathbb{C}^{n^2}$ by $x^1_1 > x^1_2 > \cdots > x^1_n > x^2_1 > \cdots > x^n_n$, then the leading monomial of any minor is the product of the elements on the principal diagonal. Even estimating just the number of these monomials is difficult, so in [7] they restrict further to only look at leading monomials of size $(n-k)$ minors among the variables on the diagonal and super-diagonal: $\{x^1_1,\dots,x^n_n, x^1_2, x^2_3,\dots,x^{n-1}_n\}$. Among these, they compute that the number of leading monomials of degree $n-k$ is $\binom{n+k}{2k}$. Then they show that in degree $n-k+\tau$ the dimension of this ideal is bounded below by $\binom{n+k}{2k}\binom{n^2+\tau-2k}{\tau}$, so we conclude

$$\dim \mathcal{I}^{\det_n,k}_{n-k+\tau} \geq \binom{n+k}{2k}\binom{n^2+\tau-2k}{\tau}. \tag{12}$$

We compare this with the very crude estimate

$$\dim \mathcal{I}^{\ell^{n-m}\operatorname{perm}_m,k}_{n-k+\tau} \leq \sum_{j=0}^{k}\binom{m}{j}^2\binom{n^2+\tau-1}{\tau},$$

where $\sum_{j=0}^{k}\binom{m}{j}^2$ is the dimension of the space of partials of order k of $\ell^{n-m}\operatorname{perm}_m$, and the $\binom{n^2+\tau-1}{\tau}$ is what one would have if there were no syzygies (relations among the products).

We have

$$\begin{aligned}\ln\binom{n+k}{2k} &= n\ln\frac{n+k}{n-k} + k\ln\frac{n^2-k^2}{4k^2} + \Theta(\ln(n)) \\ &= k\ln\frac{n^2-k^2}{4k^2} + \Theta(\ln(n)),\end{aligned} \tag{13}$$

$$\begin{aligned}\ln\frac{\binom{n^2+\tau-2k}{\tau}}{\binom{n^2+\tau-1}{\tau}} &= n^2\ln\frac{(n^2+\tau-2k)(n^2-1)}{(n^2-2k)(n^2+\tau-1)} + \tau\ln\frac{n^2+\tau-2k}{n^2+\tau-1} \\ &\quad + 2k\ln\frac{n^2-2k}{n^2+\tau-2k} + \Theta(\ln(n)) \\ &= -2k\ln(\frac{\tau}{n^2}+1) + \Theta(\ln(n)),\end{aligned} \tag{14}$$

where the second lines of expressions (13), (14) hold because $k < 2m$. We split this into two subcases: $k \geq \frac{m}{2}$ and $k < \frac{m}{2}$.

6.1. **Subcase $k \geq \frac{m}{2}$.** In this case we have $\sum_{j=0}^{k} \binom{m}{j}^2 < \binom{2m}{m}$. We show the ratio

$$\frac{\binom{n+k}{2k}\binom{n^2+\tau-2k}{\tau}}{\binom{2m}{m}\binom{n^2+\tau-1}{\tau}} \tag{15}$$

is greater than one. Now

$$\begin{aligned} \ln\binom{2m}{m} &= m\ln 4 + \Theta(\ln(m)) \\ &= k\ln(4^{\frac{m}{k}}) + \Theta(\ln(m)). \end{aligned} \tag{16}$$

If

$$k\ln\left(\frac{n^2-k^2}{4k^2}\frac{1}{(\frac{\tau}{n^2}+1)^2}\frac{1}{4^{\frac{m}{k}}}\right) \pm \Theta(\ln(n))$$

is positive, then (15) is greater than one. This will occur if

$$\frac{n^2-k^2}{4k^2}\frac{1}{(\frac{\tau}{n^2}+1)^2}\frac{1}{4^{\frac{m}{k}}} > 1,$$

i.e., if

$$\tau < n^2(\frac{\sqrt{n^2-k^2}}{2k4^{\frac{m}{2k}}} - 1).$$

Write this as

$$\tau < n^2(\frac{n}{2\epsilon m 4^{\frac{1}{2\epsilon}}} - 1). \tag{17}$$

The worst case is $\epsilon = 2$ where it suffices to take $\tau < \frac{n^3}{6m}$.

6.2. **Subcase $k < \frac{m}{2}$.** Here we use that $\sum_{j=0}^{k} \binom{m}{j}^2 < k\binom{m}{k}^2$ and a similar argument gives that it suffices to have

$$\tau < n^2(\frac{\sqrt{n^2-k^2}}{2k}\frac{1}{\sqrt{\frac{m}{k}}-1} - 1).$$

The smallest upper bound for τ occurs when $k = \frac{m}{2}$, where the estimate easily holds when $\tau < \frac{n^3}{6m}$.

Acknowledgments

Efremenko, Landsberg and Weyman thank the Simons Institute for the Theory of Computing, UC Berkeley, for providing a wonderful environment during the fall 2014 program, *Algorithms and Complexity in Algebraic Geometry*, to work on this article. The authors also thank the anonymous referee of a previous version for pointing out a gap in our argument.

References

[1] M. Agrawal and V. Vinay, *Arithmetic circuits: A chasm at depth four*, In Proc. 49th IEEE Symposium on Foundations of Computer Science (2008), 67–75.

[2] R. P. Brent, *The parallel evaluation of general arithmetic expressions*, J. Assoc. Comput. Mach. **21** (1974), 201–206, DOI 10.1145/321812.321815. MR0660280

[3] K. Efremenko, J. M. Landsberg, H. Schenck, and J. Weyman, *On minimal free resolutions of sub-permanents and other ideals arising in complexity theory*, preprint (2016). To appear in J. Algebra.

[4] G. Gotzmann, *Eine Bedingung für die Flachheit und das Hilbertpolynom eines graduierten Ringes* (German), Math. Z. **158** (1978), no. 1, 61–70, DOI 10.1007/BF01214566. MR0480478

[5] M. L. Green, *Generic initial ideals*, Six lectures on commutative algebra (Bellaterra, 1996), Progr. Math., vol. 166, Birkhäuser, Basel, 1998, pp. 119–186. MR1648665

[6] J. A. Grochow, *Unifying known lower bounds via geometric complexity theory*, Comput. Complexity **24** (2015), no. 2, 393–475, DOI 10.1007/s00037-015-0103-x. MR3349809

[7] A. Gupta, P. Kamath, N. Kayal, and R. Saptharishi, *Approaching the chasm at depth four*, 2013 IEEE Conference on Computational Complexity—CCC 2013, IEEE Computer Soc., Los Alamitos, CA, 2013, pp. 65–73, DOI 10.1109/CCC.2013.16. MR3306975

[8] A. Gupta, P. Kamath, N. Kayal, and R. Saptharishi, *Arithmetic circuits: A chasm at depth three*, Electronic Colloquium on Computational Complexity (ECCC) **20** (2013), p. 26.

[9] N. Kayal, *An exponential lower bound for the sum of powers of bounded degree polynomials*, Electronic Colloquium on Computational Complexity (ECCC) **19** (2012), p. 81.

[10] P. Koiran, *Arithmetic circuits: the chasm at depth four gets wider*, Theoret. Comput. Sci. **448** (2012), 56–65, DOI 10.1016/j.tcs.2012.03.041. MR2943969

[11] J. M. Landsberg and G. Ottaviani, *Equations for secant varieties of Veronese and other varieties*, Ann. Mat. Pura Appl. (4) **192** (2013), no. 4, 569–606, DOI 10.1007/s10231-011-0238-6. MR3081636

[12] N. Nisan and A. Wigderson, *Lower bounds on arithmetic circuits via partial derivatives*, Comput. Complexity **6** (1996/97), no. 3, 217–234, DOI 10.1007/BF01294256. MR1486927

[13] J. J. Sylvester, *On the principles of the calculus of forms*, Cambridge and Dublin Mathematical Journal (1852), 52–97.

[14] S. Tavenas, *Improved bounds for reduction to depth 4 and depth 3*, Inform. and Comput. **240** (2015), 2–11, DOI 10.1016/j.ic.2014.09.004. MR3303254

[15] L. G. Valiant, *Completeness classes in algebra*, Conference Record of the Eleventh Annual ACM Symposium on Theory of Computing (Atlanta, GA, 1979), ACM, New York, 1979, pp. 249–261. MR564634

Computer Science Department, Ben-Gurion University, Beer-Sheva, 84105 Israel
E-mail address: klimefrem@gmail.com

Department of Mathematics, Texas A&M University, College Station, Texas 77843
E-mail address: jml@math.tamu.edu

Department of Mathematics, Iowa State University, Ames, Iowa 50011
E-mail address: hschenck@iastate.edu

Department of Mathematics, University of Connecticut, Storrs, Connecticut 06269
E-mail address: jerzy.weyman@gmail.com