**E0 309: Topics in Complexity Theory** **Spring 2015**

# Lecture 14: March 13, 2015

*Lecturer: Neeraj Kayal* *Scribe: Sumant Hegde*

## 14.1 A lower bound for the determinant

In lecture 12 we saw that the size of a diagonal depth three circuit computing a polynomial $f$ is lower bounded by $dim(Fspan(\partial^{=k}(f)))$ for any integer $k$. We also saw that if $f(x_1, \ldots, x_n) = x_1 \cdots x_n$ then $dim(Fspan(\partial^{=k}(f)))$ is $\binom{n}{k}$, which is maximum when $k = n/2$. Today we will analyze the value of $dim(Fspan(\partial^{=k}(f)))$, where $f = DET(X_{n\times n})$.

**Claim 14.1** *Let $f = DET(X_{n\times n})$. Then $dim(Fspan(\partial^{=k} f)) = \binom{n}{k}^2$.*

**Proof:** Any element in $\partial^{=k}(f)$ is a derivative $(\partial^k f)/(\partial x_{i_1 j_1} \ldots \partial x_{i_k j_k})$ for some $i_1, \ldots, j_k$. Now, $(\partial^k f)/(\partial x_{i_1 j_1} \ldots \partial x_{i_k j_k})$ is actually the minor obtained by removing exactly rows $i_1, \ldots, i_k$ and columns $j_1, \ldots, j_k$ from $X$. Thus $\partial^{=k}(f)$ is the set of all $(n-k) \times (n-k)$ minors of $X$.

Consider any two $(n-k) \times (n-k)$ minors $m_1, m_2$ of $X$. There must be some row (or column) $i$ of $X$ that is a "removed" row (column) w.r.t. $m_1$ but not w.r.t. $m_2$. It follows that every monomial in $m_1$ is devoid of variables of row (column) $i$ while every monomial in $m_2$ contains a variable of row (column) $i$. Therefore, the elements in $\partial^{=k}(f)$ are pairwise monomial-disjoint, and the dimension of $Fspan(\partial^{=k}(f))$ equals the number of elements in $\partial^{=k}(f)$. This number is $\binom{n}{k}^2$, the number of ways of choosing $k$ rows and $k$ columns independently from $X$. ■

$\binom{n}{k}^2$ is maximum when $k = n/2$. Thus we now have a size lower bound of $\binom{n}{n/2}^2 \approx (2^n/\sqrt{n})^2 = 2^{2n}/n$ for diagonal depth three circuits computing $DET(X_{n\times n})$.

## 14.2 A detour on binomial coefficients

If we plot a graph of $f(k) = \binom{n}{k}$ vs. $k$ for a fixed $n$, we see that $f(k)$ is maximum at $k = n/2$, and that $f(k)$ decreases rapidly as $|k - n/2|$ increases. When $f(k)$ is scaled by a factor of $1/2^n$, the graph resembles the binomial distribution $B(n, p)$ with $p = 1/2$. That is, if $X$ is the random variable with this distribution, then $Pr[X = k] = \binom{n}{k} p^k (1-p)^k = \binom{n}{k}/2^n$. The expected value is $E[X] = np = n/2$, variance is $var[X] = np(1-p) = n/4$ and standard deviation is $\sigma[X] = \sqrt{var[X]} = \sqrt{n}/2$. Thus we see that $X$ takes a value most likely in $[n/2 - \sqrt{n}/2,\ n/2 + \sqrt{n}/2]$, a small interval of length $\sqrt{n}$.

Now we consider an exercise which will be useful in future when discussing multilinear formula lower bounds.
**Question** Suppose we toss $n$ fair coins $t$ times ($t$ "batches"). For batch i, $1 \le i \le t$, let the vector $b_i = (b_{i,1}, \ldots, b_{i,n})$ represent the outcomes of $n$ coins, where $b_{i,j} \in \{-1, 1\}$. (Say -1 is tail and 1 is head.) Let

$$imbalance(b_i) = |\sum_{j=1}^{n} b_{i,j}|$$

Let $I = \sum_{i=1}^{t} imbalance(b_i)$. How is $I$ distributed?

**Hint** Consider $Pr[I = 0]$. For any $i$, $Pr[imbalance(b_i) = 0] = \binom{n}{n/2}/2^n \approx 1/\sqrt{2\pi n}$. Also, $imbalance(b_i)$ is always nonnegative. Therefore $Pr[I = 0] = Pr[\bigcap_{i=1}^{t} imbalance(b_i) = 0] \approx 1/\sqrt{2\pi n}^t$.

## 14.3 A slightly generalized model for lower bound

Let $t$ be a positive integer. For a random $n$-variate degree $d$ polynomial $f$, we consider expressing $f$ as

$$f(x_1, \ldots, x_n) = Q_1^{e_1} + \cdots + Q_s^{e_s} \text{ where } deg(Q_i) \leq t, \tag{14.1}$$

and we try to lower bound $s$. Before further analysis we note that diagonal $\Sigma\Pi\Sigma$ circuits are a special case of this model (i.e. when $t = 1$).

Let $\mathbb{F}$ be a finite field. We will identify $\mathbb{F}$ with the size of $\mathbb{F}$.
Total number of $n$-variate degree $d$ polynomials ($f$'s) is $\mathbb{F}^{\binom{n+d}{d}}$.
Total number of $n$-variate degree $t$ polynomials ($Q_i$'s) is $\mathbb{F}^{\binom{n+t}{t}}$.
Maximum number of $f$'s that the $Q_i^{e_i}$'s as in equation 14.1 can cover is $(\mathbb{F}^{\binom{n+t}{t}})^s$. In order to cover all $f$'s, it is necessary that

$$\begin{aligned}(\mathbb{F}^{\binom{n+t}{t}})^s \geq& \mathbb{F}^{\binom{n+d}{d}} \\ s \geq& \binom{n+d}{d} / \binom{n+t}{t}\end{aligned}$$

Assume $n = d^2$ (as in determinant). Then

$$s \geq \binom{d^2+d}{d} / \binom{d^2+t}{t}$$

Using the fact that $\binom{n}{k} \approx e^{k\log(n/k)+k} \approx (en/k)^k$, we have

$$\begin{aligned}s \geq& (e(d^2+d)/d)^d / (e(d^2+t)/t)^t \\ \approx& (d^2)^{d-t} + \text{ lower order terms} \\ \approx& n^{d-t}.\end{aligned}$$

Thus, most polynomials require $n^{d-t} = n^{\sqrt{n}-t}$ sized circuits in this model. Naturally we now want to find (show) an explicit polynomial with "large" lower bound on the size in this model. The lower bound $n^{\omega(d/t)}$ is of great interest here: for $t \geq \log^2 d$, showing such a polynomial will resolve a fundamental question in the area of arithmetic complexity theory: "Is $\mathsf{VP} = \mathsf{VNP}$?".

**Definition 14.2** VP *is the class of (families of) polynomials $f(x_1, \ldots, x_n)$ whose degree is polynomial in $n$ and which can be computed efficiently, i.e., by (families of) arithmetic circuits of size polynomial in $n$.*

VNP is the class of polynomials $f(x_1, \ldots, x_n)$ such that given any monomial of $f$, its coefficient can be computed efficiently. Roughly, VP and VNP can be thought of as analogues of P and NP in boolean circuit complexity.

**Theorem 14.3 (Valiant,Agrawal-Vinay,Koiran,Fischer)** *If there exists an explicit polynomial $f(x_1, \ldots, x_n)$ of degree $d$ ($n \geq d^2$, say) such that for some $t \geq \log^2 d$ the number $s$ is roughly $n^{\omega(d/t)}$ then $\mathsf{VP} \neq \mathsf{VNP}$. i.e., this polynomial would not have a polynomial size circuit.*

A typical choice of $t$ is $t = \sqrt{d}$.
So far, we have been able to show the following.

**Theorem 14.4** *There is an explicit polynomial (in $\mathsf{VNP}$) $f(x_1, \ldots, x_n)$ of degree $d$ where $n = d^2$, such that for all $t$ the number of summands $s \geq n^{(1/4)(d/t)} = n^{\Omega(d/t)}$.*

It appears that the known proof techniques are not sufficient to prove the $n^{\omega(d/t)}$ lower bound.

# 14.4 Homogeneous Depth Three Circuits

A depth three circuit is homogeneous if every node in it computes a homogeneous polynomial. A degree $d$ polynomial $f(x_1, \ldots, x_n)$ is homogeneous if it is of the form

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{s} (l_{i_1} \cdots l_{i_d})$$

where each $l_{i_j}$ is a linear form, i.e. $l_{i_j} = \sum_{i=1}^{n} \alpha_i x_i$ ($\alpha_i$ is a field constant). Clearly homogeneous depth three circuits are a special form of depth three circuits model. We try to prove lower bounds in this model.

## 14.4.1 Partial Derivatives Measure

Let $f(x_1, \ldots, x_n)$ be a polynomial of degree $d$. We extend the notion of $\partial^{=k} f$ to define $\partial^* f$ as follows. Let $\partial^{=0} f = \{f\}$.

**Definition 14.5** $\partial^* f = \bigcup_{i=0}^{d} \partial^{=i} f$.

Now $dim(Fspan(\partial^* f))$ forms a complexity measure. This measure was introduced by Nisan and Wigderson[4].

**Lemma 14.6** *Subadditivity: $dim(Fspan(\partial^*(f+g))) \leq dim(Fspan(\partial^* f)) + dim(Fspan(\partial^* g))$*
*Submultiplicativity: $dim(Fspan(\partial^*(f \cdot g))) \leq dim(Fspan(\partial^* f)) \cdot dim(Fspan(\partial^* g))$*

**Proof:** Subadditivity: This can be proved along the lines of lemma 12.11 of lecture 12.
Submultiplicativity: Let $m$ and $n$ be dimensions of $Fspan(\partial^* f)$ and $Fspan(\partial^* g)$ respectively. Let $f_1, \ldots, f_m$ and $g_1, \ldots, g_m$ be basis vectors (polynomials) of the vector spaces respectively.

Any polynomial $h$ in $Fspan(\partial^*(fg))$ is a linear combination of polynomials from $\partial^*(fg)$. That is, $h = \sum_{i=1}^{k} h_i$ such that $h_i \in \partial^*(fg)$. Now each $h_i$ is of the form $\partial^{d_i}(fg)/(\partial x_{i_1} \partial x_{i_2} \ldots \partial x_{i_{d_i}})$ where $0 \leq d_i \leq d$. Applying product rule repeatedly, we eventually get $h_i$ as a sum of products, where each product is of the form $f'g'$

such that $f' \in \partial^*(f)$ and $g' \in \partial^*(g)$. Since $f'$ can be expressed in the form $\sum_{i=1}^{m} \beta_i f_i$ and $g'$ in the form $\sum_{i=1}^{n} \gamma_i g_i$, the product $f'g'$ can be expressed in the form $\sum_{i=1}^{m}\sum_{j=1}^{n} \delta_{ij} f_i g_j$. ($\alpha_i, \beta_i, \gamma_i, \delta_i$ are field constants.) In fact every $f'g'$ in the expanded form of $h_i$ can be written as a linear combination of polynomials $f_1g_1, \ldots, f_m g_n$. Finally, $h$ being the sum of all $h_i$'s, can itself be written as a sum of linear combination of aforementioned polynomials. This proves that all polynomials in $Fspan(\partial^*(f \cdot g))$ are linear combinations of at most $mn$ polynomials. ■

### 14.4.2 Homogeneous $\Sigma\Pi\Sigma$ circuit lower bound for determinant

**Claim 14.7** *Any homogeneous $\Sigma\Pi\Sigma$ circuit computing $DET(X_{n\times n})$ must have size $2^{\Omega(n)}$.*

**Proof:** We use counting argument. $Fspan(\partial^*(DET_n))$ has all the minors of $X_{n\times n}$. The number of $k \times k$ minors is $\binom{n}{k}^2$ as we saw in claim 14.1. Therefore the total number of minors is $\binom{n}{0}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n} \approx 2^{2n}/\sqrt{2\pi 2n}$. This is equal to the dimension of $Fspan(\partial^*(DET_n))$ as all the minors are pairwise monomial disjoint.
Any homogeneous $\Sigma\Pi\Sigma$ circuit computing $DET_n$ is of the form

$$C = \sum_{i=1}^{s} (l_{i_1} \cdots l_{i_n})$$

where $l_{i_j}$'s are linear forms.
We claim that $dim(Fspan(\partial^* l_{i_j})) \leq 2$ for every $l_{i_j}$. To see why, we first observe that $\partial^{=1} l_{i_j}$ contains only constants, while $\partial^{=0} l_{i_j}$ contains only $l_{i_j}$, a linear polynomial. The proof follows since $\partial^* l_{i_j} = \partial^{=0} l_{i_j} \cup \partial^{=1} l_{i_j}$. From submultiplicativity (lemma 14.6), the product $l_{i_j} \cdots l_{i_n}$ contributes at most $2^n$ to the dimension. From subadditivity, $dim(Fspan(\partial^* C)) \leq s \cdot 2^n$.
Since $C = DET_n$, it follows that

$$\begin{aligned} 2^{2n}/\sqrt{2\pi 2n} &\leq s \cdot 2^n \\ s &\geq 2^n/\sqrt{2\pi 2n} \\ s &= 2^{\Omega(n)} \end{aligned}$$

■

## 14.5 References


[1] Amir Shpilka, Amir Yehudayoff, Arithmetic Circuits: A survey of recent results and open questions, 2010.

[2] M. Agrawal, V. Vinay, Arithmetic Circuits: A chasm at depth four. *FOCS 2008*

[3] P. Koiran, Arithmetic Circuits: The chasm at depth four gets wider. *CoRR, abs/1006.4700, 2010*

[4] Noam Nisan, Avi Wigderson Lower Bounds on Arithmetic Circuits via Partial Derivatives. *Computational Complexity, 1996*