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

Lecture 11: Mar 2, 2015

Lecturer: Neeraj Kayal *Scribe: Saravanan K*

11.1 $\sum \bigwedge \sum$ Circuits

Consider a special class of depth-3 circuits, where the bottom layer consists of addition gates of unbounded fan-in, first layer consists of exponentiation gates (it performs the operation of product gate whose input edges are from a single node) and the root node is an addition gate. We call this family of circuits, the $\sum \bigwedge \sum$ circuits.

We can map this to polynomials of the form

$$f(\mathbf{x}) = \alpha_1.l_1^{e_1}(\mathbf{x}) + \alpha_2.l_2^{e_2}(\mathbf{x}) + \cdots + \alpha_s.l_s^{e_s}(\mathbf{x}) \tag{11.1}$$

where $\mathbf{x}$ is a n-tuple $(x_1, x_2, \cdots, x_n)$ of variables over the field $\mathbb{F}$, $l_1(\mathbf{x}), l_2(\mathbf{x}), \cdots, l_s(\mathbf{x})$ are linear polynomials (that is of degree equal to 1) and α_1, α_2, $\cdots$, α_s are scalars.

It has been proved by W.J.Ellison[1] that any polynomial of degree d can be expressed in the form (11.1), where $e_i \leq d$ and $e_i \in \mathbb{Z}_+$, for all $1 \leq i \leq s$. Hence we state the theorem,

Theorem 11.1 *Let $f(\boldsymbol{x})$ be a n-variate polynomial of degree $d \geq 1$, where $\boldsymbol{x}$ is a n-tuple of variables over the field $\mathbb{F}$. Then $f(\boldsymbol{x})$ can be expressed as,*

$$f(\boldsymbol{x}) = \alpha_1 l_1^{e_1}(\boldsymbol{x}) + \alpha_2 l_2^{e_2}(\boldsymbol{x}) + \cdots + \alpha_s l_s^{e_s}(\boldsymbol{x})$$

where $e_i \in \mathbb{Z}_+$ and $e_i \leq d$, for all $1 \leq i \leq s$,
$l_1, l_2, l_3, \cdots, l_s$ are polynomials in $\boldsymbol{x}$ of degree 1 and α_1, α_2, $\cdots$, α_s are scalars.

Before proving the theorem let us look at a simple example to get some idea.

Example : Consider the polynomial $f(x_1) = x_1^2 + x_1$. Our goal is to express $f(x_1)$ in the form (11.1). Indeed it is sufficient to prove that there exist scalars $\alpha_1, \alpha_2, \alpha_3$ such that $f(x_1)$ can be expressed as,

$$f(x_1) = x_1^2 + x_1 = \alpha_1(x_1 + 0)^2 + \alpha_2(x_1 + 1)^2 + \alpha_3(x_1 + 2)^2 \tag{11.2}$$

Now, let us find the values of $\alpha_1, \alpha_2, \alpha_3$. By equating coefficients of x_1^2, x_1 and the constant term we get,

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= 1 \\ 2\alpha_2 + 4\alpha_3 &= 1 \\ \alpha_2 + 4\alpha_3 &= 0 \end{aligned}$$

Solving the above equations we get, $\alpha_1 = 1/4$, $\alpha_2 = 1$, $\alpha_3 = -1/4$. Therefore we can express $f(x_1)$ as

$$f(x_1) = x_1^2 + x_1 = (1/4)x_1^2 + (1)(x_1 + 1)^2 - (1/4)(x_1 + 2)^2 \tag{11.3}$$

In the proof we generalize the example for uni-variate polynomials of degree $d \geq 1$.

Lemma 11.2 *Let M be any given matrix over the field $\mathbb{F}$ and M' be a matrix obtained by multiplying some rows (or some columns) of M by a non-zero scalar. Then rank of M is equal to the rank of M'*

Proof of Theorem 11.1 :

Case 1 : $n = 1$

Consider the uni-variate polynomial

$$f(x_1) = c_0 + c_1 \cdot x_1 + c_2 \cdot x_1^2 + \cdots + c_d \cdot x_1^d \tag{11.4}$$

of degree d, where $x_1 \in \mathbb{F}$ is the formal variable and $c_0, c_1, \cdots, c_d$ are coefficients over the field $\mathbb{F}$.

In order to prove this case, it is sufficient to prove that there exist $\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_d$ such that,

$$f(x_1) = \alpha_0(x_1 + 0)^d + \alpha_1(x_1 + 1)^d + \alpha_2(x_1 + 2)^d + \cdots + \alpha_d(x_1 + d)^d \tag{11.5}$$

From (11.4) and (11.5) we get,

$$c_0 + c_1 \cdot x_1 + c_2 \cdot x_1^2 + \cdots + c_d \cdot x_1^d = \alpha_0(x_1 + 0)^d + \alpha_1(x_1 + 1)^d + \alpha_2(x_1 + 2)^d + \cdots + \alpha_d(x_1 + d)^d$$

Equating the coefficients of $x_1^d, x_1^{d-1}, \cdots x_1$ and the constant term on both sides we get equations,

$$\begin{aligned}
\alpha_0 + \alpha_1 + \alpha_2 + \cdots + \alpha_d &= c_d \\
0 + 1\binom{d}{d-1} + 2\binom{d}{d-1} + \cdots + d\binom{d}{d-1} &= c_{d-1} \\
0 + 1^2\binom{d}{d-2} + 2^2\binom{d}{d-2} + \cdots + d^2\binom{d}{d-2} &= c_{d-2} \\
&\vdots \\
0 + 1^d\binom{d}{0} + 2^d\binom{d}{0} + \cdots + d^d\binom{d}{0} &= c_0
\end{aligned}$$

In matrix notation we write,

$$A.\mathbf{x} = \mathbf{c}$$

where,

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1\binom{d}{d-1} & 2\binom{d}{d-1} & 3\binom{d}{d-1} & \cdots & d\binom{d}{d-1} \\ 0 & 1^2\binom{d}{d-2} & 2^2\binom{d}{d-2} & 3^2\binom{d}{d-2} & \cdots & d^2\binom{d}{d-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1^d\binom{d}{0} & 2^d\binom{d}{0} & 3^d\binom{d}{0} & \cdots & d^d\binom{d}{0} \end{bmatrix}_{(d+1)\times(d+1)}, \quad \mathbf{x} = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_d \end{bmatrix}_{(d+1)\times 1} \quad \text{and} \quad \mathbf{c} = \begin{bmatrix} c_d \\ c_{d-1} \\ \vdots \\ c_1 \\ c_0 \end{bmatrix}_{(d+1)\times 1}$$

If inverse of A exists, then we can solve the vector x by computing $x = A^{-1}c$.

Let $A^{'}$ be a matrix obtained by multiplying i^{th} row of A by $\frac{1}{\binom{d}{d-i+1}}$, for all $1 \leq i \leq d+1$. Now,

$$A^{'} = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & 3 & \cdots & d \\ 0 & 1^2 & 2^2 & 3^2 & \cdots & d^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1^d & 2^d & 3^d & \cdots & d^d \end{bmatrix}_{(d+1)\times(d+1)},$$

We can see that $A^{'}$ is a Vandermonde matrix whose determinant is non-zero. This implies rank of $A^{'} = d+1$. Since $\frac{1}{\binom{d}{d-i+1}}$ is non-zero for all $1 \leq i \leq d+1$, by using *lemma* 11.2 we get,

$$\text{rank of } A = \text{rank of } A^{'} = d+1$$

Since A has full rank, inverse of A exists. Thus we compute the vector $\mathbf{x}$ by

$$\mathbf{x} = A^{-1}c$$

Hence we conclude *case* 1 by stating: there exist scalars $\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_d$ such that $f(x_1)$ can be expressed in the form

$$f(x_1) = \alpha_0(x_1+0)^d + \alpha_1(x_1+1)^d + \alpha_2(x_1+2)^d + \cdots + \alpha_d(x_1+d)^d$$

Case 2 : $n = 2$

Consider a bi-variate polynomial $f(x_1, x_2)$. We need to prove that $f(x_1, x_2)$ can be expressed as the sum of powers of linear forms. It is indeed sufficient to prove that any monomial can be expressed in the sum of powers of linear forms (Because, sum of all the monomial expressions yield the same form).

That is, our proof suffices when we prove that any monomial of the form $x_1^{\beta_1}x_2^{\beta_2}$ can be expressed as

$$x_1^{\beta_1}x_2^{\beta_2} = \alpha_0(x_1+0.x_2)^{d_m} + \alpha_1(x_1+1.x_2)^{d_m} + \alpha_2(x_1+2x_2)^{d_m} + \cdots + \alpha_{d_m}(x_1+d_m.x_2)^{d_m}$$

where $d_m = \beta_1 + \beta_2 \leq d$ is the degree of the monomial and $\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{d_m}$ are some scalars.

Equating the coefficients of $x_1^{d_m}x_2^0$, $x_1^{(d_m-1)}x_2^1$, $x_1^{(d_m-2)}x_2^2 \cdots\cdots x_1^0x_2^{d_m}$ on both sides we get equations,

$$\begin{aligned}
\alpha_0 + \alpha_1 + \alpha_2 + \cdots + \alpha_{d_m} &= 0 \\
0 + 1\binom{d_m}{d_m-1}\alpha_1 + 2\binom{d_m}{d_m-1}\alpha_2 + \cdots + d\binom{d_m}{d_m-1}\alpha_{d_m} &= 0 \\
0 + 1^2\binom{d_m}{d_m-2}\alpha_1 + 2^2\binom{d_m}{d_m-2}\alpha_2 + \cdots + d^2\binom{d_m}{d_m-2}\alpha_{d_m} &= 0 \\
&\vdots \\
0 + 1^{\beta_2}\binom{d_m}{d_m-\beta_2}\alpha_1 + 2^{\beta_2}\binom{d_m}{d_m-\beta_2}\alpha_2 + \cdots + d_m^{\beta_2}\binom{d_m}{d_m-\beta_2}\alpha_{d_m} &= 1 \\
&\vdots \\
0 + 1^{d_m}\binom{d_m}{0}\alpha_1 + 2^{d_m}\binom{d_m}{0}\alpha_2 + \cdots + d_m^{d_m}\binom{d_m}{0}\alpha_{d_m} &= 0
\end{aligned}$$

In matrix notation we write,

$$A.\mathbf{x} = \mathbf{c}$$

where,

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1\binom{d_m}{d_m-1} & 2\binom{d_m}{d_m-1} & 3\binom{d_m}{d_m-1} & \cdots & d_m\binom{d_m}{d_m-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 1^{\beta_2}\binom{d_m}{d_m-\beta_2} & 2^{\beta_2}\binom{d_m}{d_m-\beta_2} & 3^{\beta_2}\binom{d_m}{d_m-\beta_2} & \cdots & {d_m}^{\beta_2}\binom{d_m}{d_m-\beta_2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 1^{d_m}\binom{d_m}{0} & 2^{d_m}\binom{d_m}{0} & 3^{d_m}\binom{d_m}{0} & \cdots & d^{d_m}\binom{d_m}{0} \end{bmatrix}_{(d_m+1)\times(d_m+1)},$$

$$\mathbf{x} = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \vdots \\ \vdots \\ \alpha_d \end{bmatrix}_{(d_m+1)\times 1} \quad and \quad \mathbf{c} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}_{(d_m+1)\times 1}$$

By a similar argument like in *case* 1, we find that inverse of A exists. Hence we compute the vector $\mathbf{x}$ by $\mathbf{x} = A^{-1}\mathbf{c}$.

Thus there exist scalars $\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{d_m}$ such that any d_m-degree monomial of the form $x_1^{\beta_1}x_2^{\beta_2}$ can be expressed as

$$x_1^{\beta_1}x_2^{\beta_2} = \alpha_0(x_1 + 0.x_2)^{d_m} + \alpha_1(x_1 + 1.x_2)^{d_m} + \alpha_2(x_1 + 2.x_2)^{d_m} + \cdots + \alpha_{d_m}(x_1 + d_m.x_2)^{d_m}$$

That is,

$$x_1^{\beta_1}x_2^{\beta_2} = \alpha_0 l_{11}^{d_m} + \alpha_1 l_{12}^{d_m} + \alpha_2 l_{13}^{d_m} + \cdots + \alpha_{d_m} l_{1s_1}^{d_m} \tag{11.6}$$

where, $l_{11}, l_{12}, l_{13}, \cdots, l_{1s_1}$ are linear forms in variables x_1, x_2 and s_1 is some positive integer.

Case 3 : $n \geq 3$

Now we extend the proof for 3-variate polynomials. The monomials of a 3-variate polynomial can be expressed as $x_1^{\beta_1}x_2^{\beta_2}x_3^{\beta_3}$. Using (11.6) we express $x_1^{\beta_1}x_2^{\beta_2}x_3^{\beta_3}$ as

$$x_1^{\beta_1}x_2^{\beta_2}x_3^{\beta_3} = \alpha_0 l_{11}^{d_m}x_3^{\beta_3} + \alpha_1 l_{12}^{d_m}x_3^{\beta_3} + \alpha_2 l_{13}^{d_m}x_3^{\beta_3} + \cdots + \alpha_{d_m} l_{1s_1}^{d_m}x_3^{\beta_3}$$

Every monomial in the above expression can be viewed as a $2-variate$ monomial in l_i, x_3 , for all $1 \leq i \leq s_1$. By again using (11.6) we get,

$$x_1^{\beta_1}x_2^{\beta_2}x_3^{\beta_3} = \alpha_0 l_{21}^{d_m} + \alpha_1 l_{22}^{d_m} + \alpha_2 l_{23}^{d_m} + \cdots + \alpha_{d_m} l_{2s_2}^{d_m}$$

where, $l_{21}, l_{22}, l_{23}, \cdots, l_{2s_2}$ are linear forms in variables l_1,x_3, which is indeed linear forms in x_1, x_2, x_3 and s_2 is some positive integer.

We see that, by induction we can extend the above argument for n-variate polynomials. Hence we conclude the proof by stating: any n-variate d-degree polynomial $f(\mathbf{x})$ can be expressed as

$$f(\mathbf{x}) = \alpha_1.l_1^{e_1}(\mathbf{x}) + \alpha_2.l_2^{e_2}(\mathbf{x}) + \cdots + \alpha_s.l_s^{e_s}(\mathbf{x})$$

where the powers $e_i \leq d$, for all $1 \leq i \leq s$.

11.1.1 Fisher's formula :

I.Fisher[4] proved that we can express the monomial $x_1x_2\cdots x_n$ as

$$x_1x_2\cdots x_n = \frac{1}{2^{(n-1)}n!} \cdot \sum_{e_2=\{0,1\},\cdots,e_n=\{0,1\}} (-1)^{e_2+\cdots+e_n} \cdot (x_1 + (-1)^{e_2}x_2 + \cdots + (-1)^{e_n}x_n)^n$$

Here the number of summands is $s = 2^{n-1}$.

S.B.Gashkov and *E.T.Shavgulidze* [5] proved that Fisher's formula is optimal. That is, the above monomial can never be expressed as a sum of n^{th} powers of linear forms, for $s < 2^{n-1}$.

11.2 Lower Bounds on $\sum\bigwedge\sum$ circuits

When we convert the exponentiation gates $\bigwedge$ to product gates $\prod$ of fan-in 2, we require $\log e_i$ number of product gates for every monomial in the expression of $f(\mathbf{x})$. Assuming the addition gates have unbounded fan-in, we get the size of the circuit as

$$size = \sum_{i=1}^{s} \log e_i$$

where s is the number of summands.

In the last lecture we have seen that, d-degree n-variate random polynomials cannot be computed by a circuit of size $(1/2)\sqrt{\binom{n+d}{d}}$ with high probability. Therefore, for a random polynomial

$$\begin{aligned}
&\sum_{i=1}^{s} \log e_i \geq (1/2)\sqrt{\binom{n+d}{d}} \\
\implies\ & s\log d \geq (1/2)(n^d)^{1/2} \quad \text{(Since } e_i \text{ is at most } d\text{)} \\
\implies\ & s \geq \frac{n^{d/2}}{2\log d}
\end{aligned}$$

In the next lecture we will improve this bound on the number of summands s required for a random n-variate polynomial of degree d. That is, we will show that $s \geq \frac{1}{n+1}\binom{n+d}{d}$ (using a dimension argument). On the upper bound front, it is known that a random n-variate, degree-d polynomial can be expressed as a sum of at most $\lceil \binom{n+d}{n}\frac{n}{n+1} + 1 \rceil$ many d^{th} powers of linear polynomials [6].

References

[1] W.J. Ellison, A waring's problem for homogeneous forms, *Proceedings of the Cambridge Philosophical Society*, 65:663-672, 1969

[2] Neeraj Kayal, An exponential lower bound for the sum of powers of bounded degree polynomials, *Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 81*, 2012

[3] Xi Chen, Neeraj Kayal, Avi Wigderson, Partial Derivatives in Arithmetic Complexity and beyond, *Foundations and Trends in Theoretical Computer Science: Vol. 6: No. 1–2, pp 1-138*, 2012

[4] I. Fisher, Sums of Like Powers of Multivariate Linear Forms, *Mathematics Magazine, 67(1)*, 1994

[5] S.B. Gashkov and E.T. Shavgulidze, Representation of Monomials as a Sum of Powers of Linear forms, *Moscow University Mathematics Bulletin*, 2014

[6] J. Alexander and A. Hirchowitz, Polynomial interpolation in several variables, *Journal of Algebraic Geometry*, 1995