LECTURE 20

4/25/2012

Note Title 4/24/2012

Today:

lower bounds on circuit size

- [Baur-Strassen] via Bezout's Theorem
- [Smolensky] elementary

The Problem:

Multipoint (very special) Polynomial Evaluation:

$$(x_1, \ldots x_n) \longmapsto (x_1^r, x_2^r, \ldots x_n^r)$$

Bezout's Theorem - based Proof

Modelling the circuit

- Input variables : $x_1 \cdots x_n$
- Gate variables : $y_1 \cdots y_s$
- Constraints : degree two polynomials

$P_i(\bar{x}, \bar{y}) : y_i - y_j * y_k = 0$ etc.

Now fix the output variables

$$y_{s-n+1} = y_{s-n+2} = \cdots y_s = 1$$

Consider resulting equations

$$\{\tilde{P}_i = P_i \mid_{y_{s-n+1} = \cdots y_s = 1}\}$$

Claim: # solutions to $\{\tilde{P}_i\}_{i=1}^{s}$ is exactly r^n, if circuit is correct & $\mathbb{K}$ algebraically closed.

Proof:

- Given $(x_1 \dots x_n)$ all other values $(y_1 \dots y_s)$ determined uniquely
- $\{\#\ (x_1 \dots x_n)\} = r^n$

Bounding # solutions

Bezout's Theorem:

$f_1 \dots f_m$ poly's of degree $d_1 \dots d_m$

in n variables

$\Rightarrow$ # solutions is $\leq \prod_i d_i$

or infinite.

Claim: # solutions to $\{\tilde{p}_i\}_{i=1}^{s}$ is $\leq 2^s$

Proof: Immediate since $\deg(\tilde{p}_i) \leq 2$

Lower Bound: $2^s \geq r^n$

$\Rightarrow s \geq n \log r$

Aside on Bezout's Theorem

Classical Proof:

Look at

$$V(f_1 \dots f_m) = \{\text{set of common zeroes}\}.$$

Define:

$$\text{Deg}(V), \quad \text{Dim}(V)$$

- $\text{Dim}(V) = \operatorname{argmin}_k \{\exists \text{ codim } k \text{ affine subspace } A, \text{ s.t. } 0 < |V \cap A| < \infty\}$
- $\text{Deg}(V) = \max \{|V \cap A|\}$

A, $\text{codim}(A) = \dim(V)$

"Strong Bezout's Theorem"

Proof does not fit margin

- $\forall\ V_1, V_2$

$$\deg(V_1 \cap V_2) \leq \deg(V_1) \cdot \deg(V_2)$$

Prop: $V_i = \{\bar{a} \mid f_i(a) = 0\}$, $\deg(f_i) = d_i$

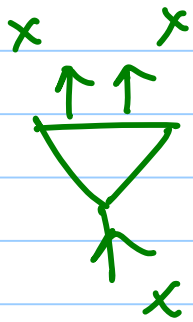
$\Rightarrow \deg(V_i) = d_i$

Strong Bezout + Prop $\Rightarrow$ Bezout.

[Smolensky]'s Proof:

- A "strange" intermediate model
- Force circuit to "duplicate" outputs explicitly.
  - All classical gates ⇒ fan-out = 1
  - Only gate with fan-out = 2 is "Duplicator"

$$d(x) = \{x, x\}$$



Key Lemma:

if Φ is a circuit with

- n input gates $x_1 \dots x_n$
- m outputs $y_1 \dots y_m$
- s duplicators duplicating poly's

$$d_1(x), \dots d_s(x)$$

then for every polynomial

$$T(x_1 \dots x_n, y_1 \dots y_m) \text{ with } \deg_{x_i}(T) \leq k$$

then $\exists \psi(x_1 \dots x_n, d_1 \dots d_s)$ s.t.

$$\deg_{x_i}(\psi) \leq k, \quad \deg_{d_i}(\psi) \leq 1,$$

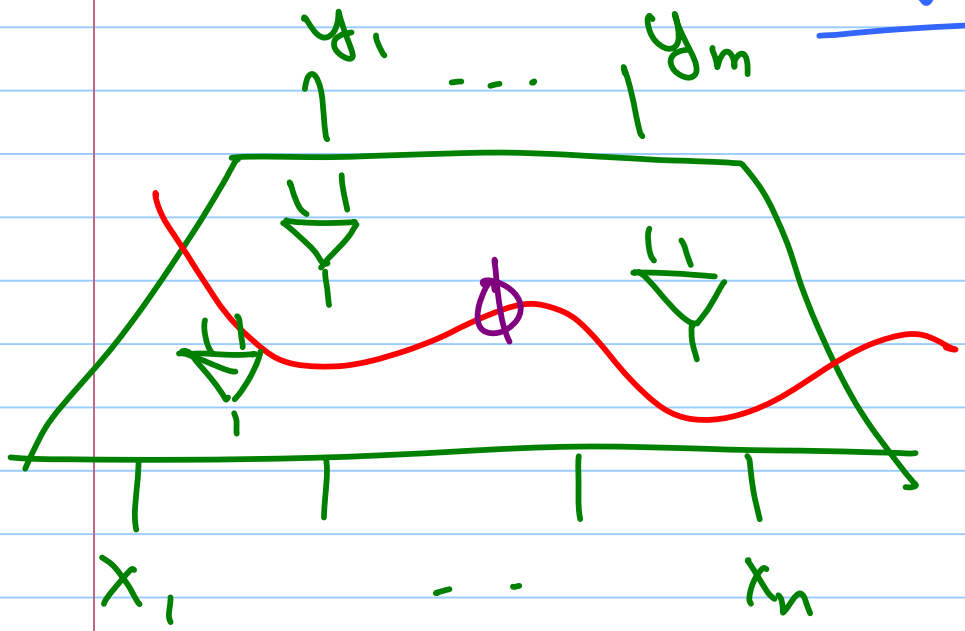
$$\psi(x_1 \dots x_n, d_1(\vec{x}), \dots d_s(\vec{x})) = T(x_1 \dots x_n, y_1(\vec{x}), \dots y_m(\vec{x}))$$

Lemma ⇒ Lower Bound

- Use $k = n-1$; $\#T = n^{2n}$
- $\#\psi = k^n \cdot 2^s$
- $\Rightarrow 2^s \geq n^n \Rightarrow s \geq n \log n$

Proof of Lemma :

Inductive Claim



Let $\sim$ be any partition with duplicators $d_1 \ldots d_\ell$ above partition & $x_1 \ldots x_n, y_1 \ldots y_t$ wires below partion.

Then $\exists \psi_\sim (\underbrace{x_1 \dots x_n, y_1 \dots y_m}\ \underbrace{d_1 \dots d_\ell})$

s.t. $\deg \le k$ $\deg \le 1$

s.t. $\psi_\sim(\quad) = T(x_1 \dots x_n, y_1(\bar{x}), \dots y_s(\bar{x}))$

- Claim true when $\sim$ is at the top
- Claim at bottom what we want.
- In between, can move $\sim$ down by one gate ... ☒