Lecture 18

Note Title 4/18/2012

4/18/2012

Today

Arithmetic Models of Computing

- Non-uniform Models
- Some connections
- toward lower bounds.

Problems:

I. $\phi : R^n \to R^m$

$\phi = (\phi_1 \ldots \phi_m)$, $\phi_i \in R[x_1 \ldots x_n]$

II. $\phi : R^n \times R^m \to R^l$

Given $x \in R^n$, find $y \in R^m$ s.t. $\phi(x,y) = \bar{0}$

Models of Computing

Algebraic Circuit / Straight-line Program:

SLP on $x_1 \dots x_n$

$V_1 \leftarrow$ ~~~

$V_2 \leftarrow$ ~~~

$\vdots$

$V_j \leftarrow A \diamond B$

$A, B \in \{x_1 \dots x_n, V_1 \dots V_{j-1}\} \cup R$

$\diamond \in \{+, \times, -, \div\}$

(1) Formula = every V_j appears in RHS at most once.

Complexity measures

- Size = # operations
- Depth = Longest chain
- Memory = $\max_i \{ \#\, v_j\text{'s defined before } i \text{ \& used after } i \}$

Valiant's Classes

$$VP = \{ \Phi = \{\Phi_n : R^n \to R\}_n \text{ s.t. } \deg \Phi_n \le \text{poly}(n) \}$$

$\forall n \; \exists$ Circuit of size poly(n) computing Φ_n $\}$

$$VNP = \{ \Phi = \{\Phi_n\}_n \; \exists \; \Psi = \{\Psi_n : R^n \times R^{k(n)} \to R\}$$

s.t. $\Phi_n(x) = \sum_{w \in \{0,1\}^{t(n)}} \Psi_n(x, w)$; $\Psi \in VP \}$

Main Results / Beliefs

① $\text{Det}_{n\times n}(M) \in VP$

② $\text{Perm}_{n\times n}(M) \in VNP$

$$\text{Perm}(M) = \sum_{T\subseteq[n]} (-1)^{n-|T|} \underbrace{\prod_{i=1}^{n} \sum_{j\in T} M_{ij}}_{\in VP}$$

$\in VNP$

Reducibility: $\phi(x_1 \ldots x_n) \leq_p \psi(y_1 \ldots y_m)$

if $\exists$ projection

$y_i \longleftarrow x_j$ or $c \in F$

[projective reductions]

③ $\text{Perm}_{n \times n}$ is VNP - complete !

④ $\text{Det}_{n \times n}$ is V-Quasi.P - complete.

Beliefs

Ⓐ $VP \neq VNP$

in fact

Ⓑ $VQP \neq VNP$

(so hope $\forall c$

$$\text{Perm}_n \not\in \text{Det}_m$$

for $m \leq 2^{(\log n)^c}$

Some Connections

I. Can get rid of divisions

Theorem: If ϕ is of deg r & can be computed by circuit of size s over $\{+, -, *, \div\}$ gates, then ϕ can be computed with $\text{poly}(r, s, n)$ gates over $\{+, -, *\}$

Proof uses Homogenization Lemma

Homogenization Lemma:

Ψ computed by size s circuit over $\{+, *, -\}$

$\Rightarrow \{\text{Hom}_0(\Psi), \ldots \text{Hom}_r(\Psi)\}$ computed by $O(r^2 s)$ sized circuit.

Proof of H.L :

By induction on gates of circuit.

- $\psi^{(1)} = \psi^{(2)} + \psi^{(3)}$

$\Rightarrow Hom_i(\psi^{(1)}) = Hom_i(\psi^{(2)}) + Hom_i(\psi^{(3)})$

- $\psi^{(1)} = \psi^{(2)} * \psi^{(3)}$

$\Rightarrow Hom_i(\psi^{(1)}) = \sum_{j \le i} Hom_j(\psi^{(2)}) \cdot Hom_{i-j}(\psi^{(3)})$

$\boxtimes$

Proof of Theorem :

Step 1: Compute numerators & denominators of every gate separately.

At end $\phi = f \div g$

$g \not\equiv 0 \Rightarrow \exists\ \alpha_1 \ldots \alpha_n, \beta \neq 0$ s.t.

$$g(\alpha_1 \ldots \alpha_n) = \beta$$

w.l.o.g. $\alpha_1 \ldots \alpha_n = \bar{0}$ & $\beta = 1$

So $$\phi = \frac{f}{g} = \frac{f}{1-(1-g)}$$

$$= \sum_{i=0}^{d} f\,(1-g)^i$$

Note $(1-g)^i$ has terms of deg $\geq i$

$$\mathrm{Hom}_k(\phi) = \mathrm{Hom}_k\left(\sum_{i=0}^{k} f\,(1-g)^i\right)$$

$\uparrow\uparrow$

Can be computed in poly(r) size

∎

Memory vs. Depth

Depth $d \Rightarrow$ Memory ≤ 3 & Size $\leq 4^d$ [Ben-Or + Cleve]

Inductive Claim:

$\forall f$ of depth d,

can compute the map

$$(U, V, W) \longmapsto (U + f(\bar{x})V, V, W)$$

Base Case: $f(x) = x_i$ ... obvious

Induction: • $f = g + h$

4^{d-1} { $(U, V, W) \longmapsto (U + fV, V, W)$

4^{d-1} { $(U + fV, V, W) \longmapsto (U + (f+g)V, V, W)$

- $f = g * h$

$(U, V, W) \longmapsto (U + fV, V, W)$ good!

$(U + fV, V, W) \longmapsto (U + fV, V, W + gU + fgV)$

not good

$(U + f \cdot v, V, W + gU + fgv) \xrightarrow{-f \cdot v} (U, V, W + gU + fgv)$

$\xrightarrow{-gU} (U, V, W + fgV)$

⊠

Gives alternate, very intuitive proof that log-depth circuits have $O(1)$-width branching programs

[Barrington]

Some surprising connections

① if $\Phi : \mathbb{F}^n \to \mathbb{F}^m$ is "super-linear"

then so is

$$\hat{\Phi} : \mathbb{F}^n \times \mathbb{F}^m \to \mathbb{F} \quad \text{given by}$$

$$\hat{\Phi}(\bar{x}, y_1 \ldots y_m) = \sum_{i=1}^{m} \Phi_i(\bar{x}) \cdot y_i$$

[Baur-Strassen]

② Φ has size s, degree r

$\Rightarrow$ Φ has circuit of size $\text{poly}(s,r)$

& depth $\text{Polylog}(s,r)$

Partial Derivatives

$\frac{\partial f}{\partial x_i}$ 'as usual.

Theorem

[Baur-Strassen] $\phi(x_1 \ldots x_n)$ has size s ckt

$\Rightarrow \left(\frac{\partial \phi}{\partial x_1}, \ldots \frac{\partial \phi}{\partial x_n}\right)$ has size $O(s)$ ckt.

Proof: ① Can't afford to compute derivatives of all gates wrt all inputs.

② So will compute derivative of output wrt all gates.

so, we view circuit top-down rather than bottom-up.
= series of substitutions.

Initially

$$\phi(x_1 \ldots x_n, y_1 \ldots y_s) = y_s$$

Substitute

$$y_s \leftarrow y_{s-1} * y_{s-2}$$

$$\Leftarrow \phi(\quad) = y_{s-1} * y_{s-2}$$

$$\vdots$$

Initially: $\frac{\partial \phi}{\partial x_i} = 0$, $\frac{\partial \phi}{\partial y_i} = 0$ except $\frac{\partial \phi}{\partial y_s} = 1$

At intermediate stage

have $\phi(x_1 \ldots x_n, y_1 \ldots y_i) \leftarrow \frac{\partial \phi}{\partial x_i}, \frac{\partial \phi}{\partial y_i} \ldots$

$$y_i \leftarrow x_j + y_k$$

$$\frac{\partial \Phi(x_j, y_k, y_i(x_j, y_k))}{\partial x_j}$$

$$= \frac{\partial \Phi}{\partial x_j} + \frac{\partial \Phi}{\partial y_i} \cdot \frac{\partial y_i}{\partial x_j}$$

$$= 1 \quad \text{if} \quad y_i = x_j + y_k$$

$$= y_k \quad \text{if} \quad y_i = x_j * y_k$$

$$= \text{etc.}$$

Updates = $O(n)$ steps per gate!

Next Lecture: Depth reductions ...

(Notes for this lecture mostly from [Amirz Amir])