ADFOCS 2017

monotonicity

Amir Yehudayoff (Technion)

introduction

monotone polynomials

matrix product

$$XY$$

convolution

$$(x * y)_g = \sum_{h \in G} x_h y_{h^{-1}g}$$

permanent

$$perm_n(X) = \sum_{\pi \in S_n} \prod_{i \in [n]} X_{i,\pi(i)}$$

symmetric polynomials

$$S_{n,d}(X) = \sum_{T \subseteq [n] : |T| = d} \prod_{i \in T} x_i$$

monotone model

monotone polynomials have non-negative coefficients

monotone devices use only positive numbers

other models

monotonicity also appears in other models

$\star$ context-free grammars

$\star$ algorithms use the semi-ring $(+, \min)$

(tropical) algorithmic example

Bellman-Ford dynamic program (shortest s-t path)

$$f_{\ell+1}(v) = \min\{f_\ell(v)\} \cup \{f_\ell(u) + w_{u,v} : u \neq s\}$$

Floyd-Warshall dynamic program (all pairs shortest path)

$$f_{\ell+1}(v,u) = \min\{f_\ell(v,u), f_\ell(v,\ell+1) + f_\ell(\ell+1,u)\}$$

[BF] is incremental and [FW] is not

dynamic programs

[Jukna, Hrubes-Y]

there is an optimization problem over n elements

$$\min_{h \in H} \sum_{v \in V} x_{v,h(v)}$$

that can be solved in $poly(n)$ steps using a non-incremental dynamic program but every incremental dynamic program must use $n^{\Omega(\log n)}$ steps to solve

monotone complexities of a monotone polynomial?

[Schnorr]

the monotone circuit complexity of $n \times n$ matrix product is $\Theta(n^3)$

the monotone circuit complexity of convolution is $\Theta(n^2)$ over $\mathbb{Z}_n$

false for non-monotone [Strassen,...] & FFT

one negation suffices

[Valiant]

every circuit of size s over $\mathbb{R}$ can be written as the difference of two monotone circuits, each of which is of size $O(s)$

one negation can be powerful

[Valiant]

the perfect matching polynomial

$$p(x) = \sum_{M \subset E} \prod_{e \in M} x_e$$

where M is perfect matching of the triangle grid of length n

$\star$ p is monotone

$\star$ p has a circuit of size $poly(n)$ **[Kasteleyn]**

$\star$ every monotone circuit for p has size $exp(n)$

relations between monotone devices?

as before

all simulations preserve monotonicity, except reduction to depth 3

are they sharp?

formulas versus circuits/ABPs

[Shamir-Snir 79]

a monotone formula for $IMM_{n,n\times n}$ has size $n^{\Omega(\log n)}$

conclusion

Hyafil's simulation is sharp; every

$$ABP \underset{monotone}{\rightarrow} formula$$

must incur super-poly blowup

ABPs versus circuits

[Hrubes-Y 15]

there is an n-variate polynomial with monotone circuit complexity $poly(n)$ but monotone ABP complexity $n^{\Omega(\log n)}$

conclusion

VSBR can not be made more efficient for ABPs, without "violating monotonicity"

ABPs are much stronger than formulas (IMM) how to prove lower bounds?

outline of lower bounds proofs

weakness

combinatorics / counting

weakness of circuits

lemma

a monotone circuit of size s and pure degree r can be written as:

$$f = \sum_{i=1}^{s} h_i g_i$$

where for each i

$\star$ h_i, g_i are homogeneous and monotone

$\star$ $r/3 \leq deg(h_i) < 2r/3$ and $deg(g_i) = r - deg(h_i)$

weakness of circuits

lemma

a monotone circuit of size s and pure degree r can be written as:

$$f = \sum_{i=1}^{s} h_i g_i$$

where each $h_i g_i$ is a "balanced" product

comments:

⋆ f is hard if "far from a product set" $\frac{|mon(hg)|}{|mon(f)|} \ll 1$

⋆ importance of grading polynomials

⋆ can potentially prove non-monotone lower bounds

monotone LB for permanent

write

$$perm_n = \sum_{i=1}^{s} h_i g_i$$

with $h_i g_i$ balanced

monotone LB for permanent

write

$$perm_n = \sum_{i=1}^{s} h_i g_i$$

with $h_i g_i$ balanced

claim

if h, g are homogeneous, $mon(hg) \subset mon(perm)$ and $r = deg(h)$

$$\frac{|mon(hg)|}{|mon(f)|} \leq \frac{r!(n-r)!}{n!}$$

monotone LB for permanent

write

$$perm_n = \sum_{i=1}^{s} h_i g_i$$

with $h_i g_i$ balanced

claim

if h, g are homogeneous, $mon(hg) \subset mon(perm)$ and $r = deg(h)$

$$\frac{|mon(hg)|}{|mon(f)|} \leq \frac{r!(n-r)!}{n!}$$

$$\boxed{\mathbf{s \geq \binom{n}{n/3} = 2^{\Omega(n)}}}$$

weakness of formulas

lemma

a monotone formula of size s and pure degree r can be written as:

$$f = \sum_{i=1}^{s} g_{i,1} g_{i,2} \cdots g_{i,t}$$

with $t = \Omega(\log r)$ where monotonicity holds and for all $i, j < t$

$$(1/3)^j r \leq deg(g_{i,j}) \leq (2/3)^j r$$

monotone formula LB for IMM

write

$$f = (X^{(1)} X^{(2)} \cdots X^{(r)})_{1,1} = \sum_{i=1}^{s} g_i$$

where g_i is a product of length $t \approx \log r$

claim if $g = g_1 \cdots g_t$ as above and $mon(g) \subset mon(f)$

$$\frac{|mon(g)|}{|mon(f)|} \leq n^{-\Omega(t)}$$

monotone formula LB for IMM

write

$$f = (X^{(1)} X^{(2)} \cdots X^{(r)})_{1,1} = \sum_{i=1}^{s} g_i$$

where g_i is a product of length $t \approx \log r$

claim if $g = g_1 \cdots g_t$ as above and $mon(g) \subset mon(f)$

$$\frac{|mon(g)|}{|mon(f)|} \leq n^{-\Omega(t)}$$

sketch

i. there is partition of $[r]$ to $\{S_j\}$ so that $var(g_j) \subset \bigcup_{i \in S_j} X^{(i)}$

ii. $x^{(1)}_{1,1}$ can multiply $x^{(2)}_{1,k}$ but not $x^{(2)}_{2,k}$

iii. each product reduces number of monomials by $1/n$

weakness of ABPs

lemma

for all $k \leq r$ a monotone ABP of size s and degree r can be written as:

$$f = \sum_{i=1}^{s} h_i g_i$$

where for each i

⋆ h_i, g_i are homogeneous and monotone

⋆ $deg(h_i) = k$ and $deg(g_i) = r - k$

comment: weaker than circuits in that k is fixed

monotone circuits versus ABPs

[Hrubes-Y]

there is an n^2-variate degree-n polynomial f so that

$\star$ has $poly(n)$-size monotone circuit

(and $f = \sum_{i=1}^{n} h_i g_i$ with $deg(h_i) = n/2$)

$\star$ for some k if $f = \sum_{i=1}^{s} h_i g_i$ monotonically with $deg(h_i) = k$ then

$$s \geq n^{\Omega(\log n)}$$

detour: isoperimetry

definitions

let $G = (V, E)$ be an undirected graph

the size of the (edge) boundary of $A \subseteq V$ is

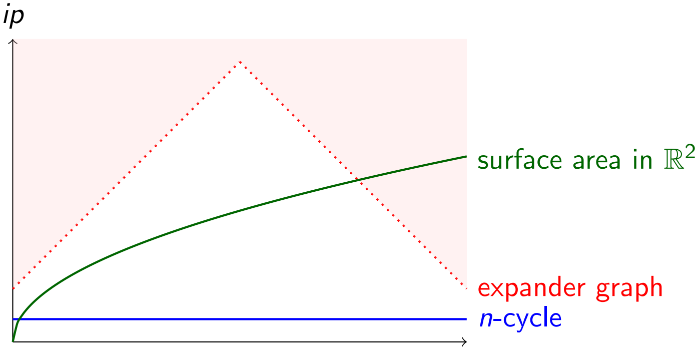
$$e(A) = |E(A, B)|$$

where $E(A, B) = \{\{a, b\} \in E : a \in A, b \in B\}$ and $B = V \setminus A$

the isoperimetric profile is

$$ip(k) = \min\{e(A) : |A| = k\}$$

pictorially



sensitive isoperimetric profiles

can $ip(k)$ be very sensitive to k?

sensitive isoperimetric profiles

can $ip(k)$ be very sensitive to k?

[Hrubes,Y] the full binary tree T_d of depth d

for each $0 < k < |V(T_d)|$

$$drop(k)/2 \leq ip(k) \leq 2drop(k)$$

where

$$drop(k) = |\{i : B_{i+1}(k) > B_i(k)\}|$$

and $B_0(k), B_1(k), \ldots$ is the binary representation of k

sensitive isoperimetric profiles

can $ip(k)$ be very sensitive to k?

[Hrubes,Y] the full binary tree T_d of depth d

for each $0 < k < |V(T_d)|$

$$drop(k)/2 \leq ip(k) \leq 2drop(k)$$

where

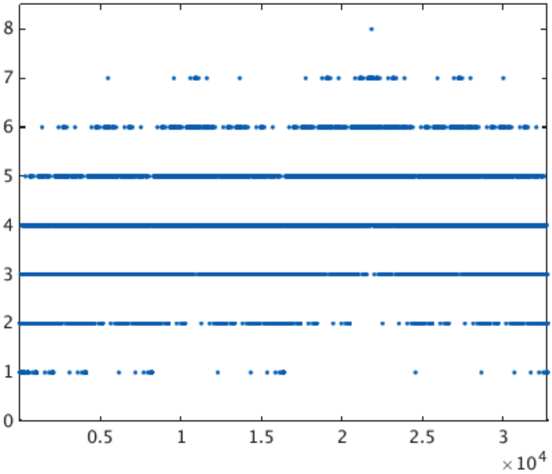
$$drop(k) = |\{i : B_{i+1}(k) > B_i(k)\}|$$

and $B_0(k), B_1(k), \ldots$ is the binary representation of k

i. *ip* of infinite binary tree studied by [Bharadwaj, Chandran, Das]

ii. have more accurate estimates on *ip* but no “explicit” formula

pictorially



graph of $drop(k) \approx ip_{T_{15}}(k)$

summary

for the full binary tree T_d

1. *ip* constantly fluctuates between 1 and $\Omega(d)$
2. for σ_d that has binary representation $(1, 0, 1, 0, 1, 0, \ldots)$

$$ip(\sigma_d) = \frac{d}{2} - \Theta(\log(d))$$

$\sigma_d \approx \frac{2}{3}|V(T_d)|$

sharpness of

$$\textit{circuits} \underset{\textit{monotone}}{\longrightarrow} \textit{ABPs}$$

theorem:

the n-variate tree polynomial $\tau = \tau_n$ has

1. monotone circuit-size $\leq poly(n)$
2. monotone ABP-size is $\geq n^{\Omega(\log n)}$

$\mathcal{T}$

fix d, m and let $V = V(T_d)$

a function $\gamma : V \to \mathbb{Z}_m$ is called legal if for every vertex v which is not a leaf and its two children v_1, v_2, we have

$$\gamma(v) = \gamma(v_1) + \gamma(v_2)$$

if γ is legal then its value on leaves determines it

τ

fix d, m and let $V = V(T_d)$

a function $\gamma : V \to \mathbb{Z}_m$ is called legal if for every vertex v which is not a leaf and its two children v_1, v_2, we have

$$\gamma(v) = \gamma(v_1) + \gamma(v_2)$$

if γ is legal then its value on leaves determines it

the tree polynomial

$$\tau(x) = \sum_{\gamma \in \text{legal}} \prod_{v \in V} x_{v,\gamma(v)}$$

τ

boundary lemma: if $mon(hg) \subset mon(\tau)$ and

$$A = \{v : x_{v,*} \in h\} \text{ and } B = \{v : x_{v,*} \in g\}$$

then

$$A \cap B = \emptyset$$

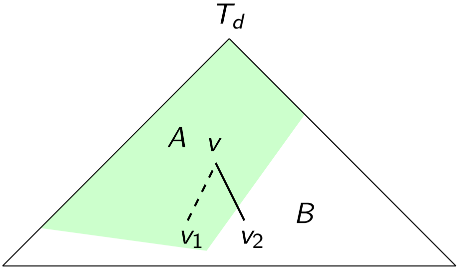
and

$$\frac{|mon(hg)|}{|mon(\tau)|} \leq m^{-|E(A,B)|/4}$$

boundary lemma: if $mon(hg) \subset mon(\tau)$ and $A = \{v : x_{v,*} \in h\}$ and $B = \{v : x_{v,*} \in g\}$ then

$$\frac{|mon(hg)|}{|mon(\tau)|} \leq m^{-|E(A,B)|/4}$$

intuition: each edge in boundary reduces number of options by factor of m since $\gamma(v) = \gamma(v_1) + \gamma(v_2)$



the tree polynomial

theorem: for $m = 2^d = n$

1. monotone circuit-size of τ is $\leq O(m^3 2^d) = poly(n)$
2. monotone ABP-size of τ is $\geq m^{\Omega(d)} = n^{\Omega(\log n)}$

the tree polynomial

theorem: for $m = 2^d = n$

1. monotone circuit-size of τ is $\leq O(m^3 2^d) = poly(n)$
2. monotone ABP-size of τ is $\geq m^{\Omega(d)} = n^{\Omega(\log n)}$

proof

1. tree $\Rightarrow$ simple induction
2. structure of ABPs & boundary lemma & $ip(\sigma_d) = \Omega(d)$

summary

monotone computations are naive (?)

still, non-trivial algorithms

appear in various contexts

demonstrate interesting phenomena

combinatorial arguments