symmetric computations

amir yehudayoff

Technion

algebraic complexity

field $\mathbb{F}$ ($char(\mathbb{F}) \neq 2$)
variables $X = \{x_1, \ldots, x_n\}$
polynomial $f \in \mathbb{F}[X]$

questions:
what is the circuit or formula size of f?
specifically, lower bounds?

study simpler/restricted models of computation
like monotone, multilinear, constant depth, ...

removing graph structure

theorem [Valiant]:
1. if f has a formula of size s then

$$f = det(M)$$

with M of size $\approx s$ and $M_{i,j} \in affine(X)$

2^*. if f has a circuit of size s then

$$f = perm(M)$$

with M of size $\approx s$ and $M_{i,j} \in affine(X)$

determinantal complexity

if f has a formula of size s then

$$f = det(M)$$

with M of size $s \times s$ and $M_{i,j} \in affine(X)$

Definition:

$$dc(f) = \min\{s : f = det(M)\}$$

an algebraic analog of formula size

GCT [Mulmuley]

an approach for investigating $dc(perm)$ based on symmetry

$V = lin_{\mathbb{F}}(X)$

$GL(V)$ acts on $V \Rightarrow GL(V)$ acts on $\mathbb{F}[X]$:

$$(hf)(x) = f(h^{-1}x)$$

the stabilizer[1] of f is

$$G_f = \{h : hf = f\}$$

idea: G_{perm} is far from G_{det} so $dc(perm)$ is large

again, simpler/restricted models of "computation"

[1] there is also a projective version

equivariance [Landsberg-Ressayre]

consider

$$f = det(M)$$

think of M as a device for computing f

question: does device respect symmetries of f?

every $h \in GL(V)$ acts on both sides of equality

$$hf = h\ det(M) = det(hM)$$

we can investigate what h does to M

equivariance

consider $f = det(M)$ with

$$M = A + B,\ \ A_{i,j} \in lin(X),\ \ B_{i,j} \in \mathbb{F}$$

let

$$G_M = \{g \in G_{det} : gA(V) = A(V),\ \ gB = B\}$$

"the part of symmetries of *det* that respects the device"

M is an <u>equivariant representation</u> of f

if for every $h \in G_f$ there is $g \in G_M$ so that $hM = gM$

h acts on M from "inside" while g from "outside"

$$edc(f) = \min\{s : f = det(M)\}$$

question: $edc(f) < \infty$?

statements

theorems [Landsberg-Ressayre]: over $\mathbb{C}$

1. $edc(perm_n) = \binom{2n}{n} - 1$ for $n \geq 3$
2. $edc\left(\sum_{i=1}^{n} x_i^2\right) = n + 1$

example: quadratics

let

$$q = \sum_{i=1}^{n} x_i^2$$

thus

$$G_q = \{h \in GL(V) : h^{-1} = h^T\}$$

example: quadratics

let

$$q = \sum_{i=1}^{n} x_i^2$$

thus

$$G_q = \{h \in GL(V) : h^{-1} = h^T\}$$

properties:

i. $dc_{\mathbb{C}}(q) \leq \frac{n}{2} + 1$ for n even

ii. $edc_{\mathbb{C}}(q) = n + 1$

iii. $dc_{\mathbb{R}}(q) = n + 1$

upper bound

claim: for

$$M = \begin{bmatrix} 0 & -x_1 & -x_2 & \dots & x_n \\ y_1 & 1 & 0 & \dots & 0 \\ y_2 & 0 & 1 & \dots & 0 \\ & & & \dots & \\ y_n & 0 & 0 & \dots & 1 \end{bmatrix} := \begin{bmatrix} 0 & -x \\ y & I \end{bmatrix}$$

we have

$$\sum_{i=1}^{n} x_i y_i = det(M)$$

upper bound on *edc*

know: $M = \begin{bmatrix} 0 & -x \\ x & I \end{bmatrix} \Rightarrow q = \sum_{i=1}^{n} x_i^2 = det(M)$

corollary: $edc(q) \leq n + 1$

upper bound on *edc*

know: $M = \begin{bmatrix} 0 & -x \\ x & I \end{bmatrix} \Rightarrow q = \sum_{i=1}^{n} x_i^2 = det(M)$

corollary: $edc(q) \leq n + 1$

proof: for $h \in G_q$, we have $h^{-1} = h^T$

$$hM = \begin{bmatrix} 0 & -(h^{-1})^T x \\ h^{-1}x & I \end{bmatrix}$$

and g defined by

$$M' \underset{g}{\mapsto} \begin{bmatrix} 1 & 0 \\ 0 & h^{-1} \end{bmatrix} M' \begin{bmatrix} 1 & 0 \\ 0 & (h^{-1})^T \end{bmatrix}$$

is so that $g \in G_{det}$ and $hM = gM$

real versus complex

know: $det\left(\begin{bmatrix} 0 & -x \\ y & I \end{bmatrix}\right) = \sum_{i=1}^{n} x_i y_i$

corollary:

1. $dc_{\mathbb{R}}(q) \leq edc_{\mathbb{R}}(q) \leq n+1$
2. $dc_{\mathbb{C}}(q) = \frac{n}{2} + 1$:

$$det\left(\begin{bmatrix} 0 & -x_1 - ix_2 & x_3 - ix_4 & \dots & x_{n-1} - ix_n \\ x_1 - ix_2 & 1 & 0 & \dots & 0 \\ x_3 - ix_4 & 0 & 1 & \dots & 0 \\ & & & \dots & \\ x_{n-1} + ix_n & 0 & 0 & \dots & 1 \end{bmatrix}\right)$$
$$= (x_1 + ix_2)(x_1 - ix_2) + \dots = q$$

real lower bound

claim: if $q = det(M)$ with M real and $s \times s$ then $s \geq n + 1$

real lower bound

claim: if $q = det(M)$ with M real and $s \times s$ then $s \geq n + 1$

idea:

real lower bound

claim: if $q = det(M)$ with M real and $s \times s$ then $s \geq n + 1$

idea:

a. q is degree 2 homogeneous and "smooth" & symmetries of *det*

$$\Rightarrow M = A + B \text{ with } B = diag(0, 1, 1, \ldots, 1)$$

real lower bound

claim: if $q = det(M)$ with M real and $s \times s$ then $s \geq n + 1$

idea:

a. q is degree 2 homogeneous and "smooth" & symmetries of *det*

$$\Rightarrow M = A + B \text{ with } B = diag(0, 1, 1, \ldots, 1)$$

b. first column of A must contain a copy of V;
otherwise can choose $v \neq 0$ so that first column of $A|_{x=v}$ is 0

$$0 \neq q(x) = det(A|_{x=v}) = 0$$

real lower bound

claim: if $q = det(M)$ with M real and $s \times s$ then $s \geq n+1$

idea:

a. q is degree 2 homogeneous and "smooth" & symmetries of *det*

$$\Rightarrow M = A + B \text{ with } B = diag(0, 1, 1, \ldots, 1)$$

b. first column of A must contain a copy of V;
otherwise can choose $v \neq 0$ so that first column of $A|_{x=v}$ is 0

$$0 \neq q(x) = det(A|_{x=v}) = 0$$

wrong over $\mathbb{C}$

complex lower bound

claim: if $q = det(M)$ with M equivariant and $s \times s$ then $s \geq n+1$

complex lower bound

claim: if $q = det(M)$ with M equivariant and $s \times s$ then $s \geq n+1$

idea:

deep structural properties of Lie groups

complex lower bound

claim: if $q = det(M)$ with M equivariant and $s \times s$ then $s \geq n+1$

idea:

deep structural properties of Lie groups

a. q is degree 2 homogeneous and "smooth" & symmetries of *det*

$$\Rightarrow M = A + B \text{ with } B = diag(0, 1, 1, \ldots, 1)$$

complex lower bound

claim: if $q = det(M)$ with M equivariant and $s \times s$ then $s \geq n+1$

idea:

deep structural properties of Lie groups

a. q is degree 2 homogeneous and "smooth" & symmetries of *det*

$$\Rightarrow M = A + B \text{ with } B = diag(0, 1, 1, \ldots, 1)$$

b. G_M which fixes B has a specific structure

complex lower bound

claim: if $q = det(M)$ with M equivariant and $s \times s$ then $s \geq n+1$

idea:

deep structural properties of Lie groups

a. q is degree 2 homogeneous and "smooth" & symmetries of *det*

$$\Rightarrow M = A + B \text{ with } B = diag(0, 1, 1, \ldots, 1)$$

b. G_M which fixes B has a specific structure

c. first column of A must contain a copy of V

summary

the algebraic language yields new types of “restricted models”

for equivariant representations, we can understand things (better)

also yields algorithms (“Ryser’s formula”)