Michael Forbes
miforbes@csail.mit.edu
2014-11-04.1
jacob - guest lec

9/ G-10

Polynomial Identity Testing, Michael Forbes

outline: 1) overview
2) hitting sets ⇒ lower bounds
3) sums of powers of linear polynomials
- lower bounds
- identity testing
4) sums of powers of quad polynomials
- lower bounds
- identity testing

---

1) overview:

Q (polynomial identity testing (PIT)) given a polynomial $f(x_1,\dots,x_n)$, is $f \equiv 0$? ← deg d

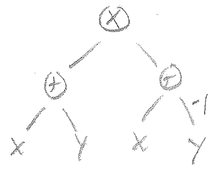
ie: $f(x_1,\dots,x_n) = \sum_{\bar a} c_{\bar a} \bar x^{\bar a}$ ← exponentially many monomials $\binom{n+d}{d}$

$\bar x^{\bar a} = \prod_i x_i^{a_i}$

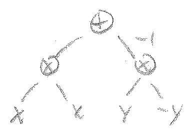
say "$f\equiv 0$" if $\forall \bar a, c_{\bar a} = 0$

not as a function, eg $x^2 - x$ is zero over $\mathbb{F}_2$ but $\not\equiv 0$ [algebraic computation is restricted in that it must compute polynomials formally, not as functions]

we give a polynomial $f(\bar x)$ by an algebraic circuit [implicit representation]



gives $(x+y)(x-y) = x^2 - y^2 =$



lem (Schwartz Zippel): $S \subseteq \mathbb{F}$, $\Pr_{\bar\alpha \in S^n}[f(\bar\alpha) = 0] \le \frac{d}{|S|}$, if $f \not\equiv 0$

⇓

randomized algo for PIT: given circuit C computing $f(\bar x)$
use C to evaluate $f(\bar\alpha)$ for $\bar\alpha \in S^n$, $|S| \approx 2d$ ← need $\mathbb{F}$ large enough
say "$f(\bar x) \not\equiv 0$" if get "$f(\bar\alpha) \neq 0$"

types of PIT: - black box: only use circuit C to evaluate $f(\bar x)$, [$f(\bar x)$ is in a black box]
- white box: can use circuit C in any way

long term goal: - efficient deterministic PIT algo for interesting models of restricted circuits
- hitting set: $\mathcal{H} \subseteq \mathbb{F}^n$, $f \equiv 0$ iff $f|_{\mathcal{H}} \equiv 0$, $\forall f$ computed by small circuits
≡ deterministic black box

for circuits of size s, exist $\mathcal{H}$ w/ $|\mathcal{H}| \le \text{poly}(s)$
construct explicit small $\mathcal{H}$?

Michael Forbes
miforbes@csail.mit.edu
2014-11-04.2
jakob green lec

Q: construct (any) hitting set?

Lem: $S \subseteq \mathbb{F}$, $|S| = d+1$. Then S^n is a $(d+1)^n$-size hitting set for n-var, degree $\leq d$ polys. [eg for such polys computed by small circuits]

Pf: $f(\bar{x})$ n var, deg $\leq d$

$$SZ \Rightarrow \Pr_{\bar{\alpha} \leftarrow S^n}[f(\bar{\alpha}) = 0] \leq \frac{d}{d+1} < 1 \quad \text{if } f \neq 0$$

$$\Rightarrow \exists\, \bar{\alpha} \in S^n \text{ st } f(\bar{\alpha}) \neq 0.$$ ☒

punchline: we have small hitting sets if n is small.

2) hitting sets $\Rightarrow$ lower bounds

Prop: let $\mathcal{C}_s = \{ f(\bar{x}) :$ f can be computed by circuit of size $s \}$ (n-var, degree d)

let $\mathcal{H}$ be a hitting set for $\mathcal{C}_s$

if $|\mathcal{H}| < \binom{n+d}{d}$ then can find an explicit $g(\bar{x})$ n var deg $\leq d$ st $g(\bar{x}) \notin \mathcal{C}_s$

in poly$(s, |\mathcal{H}|, n, d)$ time

ideally $|\mathcal{H}| = \text{poly}(s)$

getting $|\mathcal{H}| = \binom{n+d}{d}$ is not hard.

# of deg $\leq d$, n-var poly

ie $g(\bar{x})$ needs size $> s$ circuits [hard to prove!]

Pf. $\mathcal{H}$: $f \equiv 0$ iff $f|_{\mathcal{H}} \equiv 0$ $\forall f \in \mathcal{C}_s$

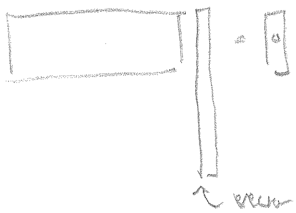
ie $f(\bar{x}) = \sum_{\bar{a}} c_{\bar{a}} x^{\bar{a}}$, $c_{\bar{a}} = 0\ \forall \bar{a}$

ie $f(\bar{\alpha}) = 0\ \forall \bar{\alpha} \in \mathcal{H}$

$$\sum_{\bar{a}} c_{\bar{a}} \underbrace{\bar{\alpha}^{\bar{a}}}_{\prod_i \alpha_i^{a_i}} = 0$$

is a homogeneous linear equation in the $c_{\bar{a}}$; $\bar{\alpha}$'s are constants

ie:



1 constraint for each $\bar{\alpha}$

vector of the $c_{\bar{a}}$'s, $\binom{n+d}{d}$ dim

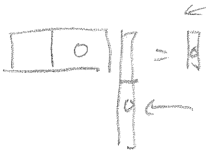
$\Rightarrow$ $|\mathcal{H}|$ constraints, $\binom{n+d}{d}$ constraints

$|\mathcal{H}| < \binom{n+d}{d} \overset{\text{lin alg}}{\Rightarrow}$ non zero solution

ie $g(\bar{x}) \neq 0$, $\forall \bar{\alpha} \in \mathcal{H}\ g(\bar{\alpha}) = 0$

$\Rightarrow g(\bar{x}) \notin \mathcal{C}_s$

computing $g(\bar{x})$: $\binom{n+d}{d}$ is too big



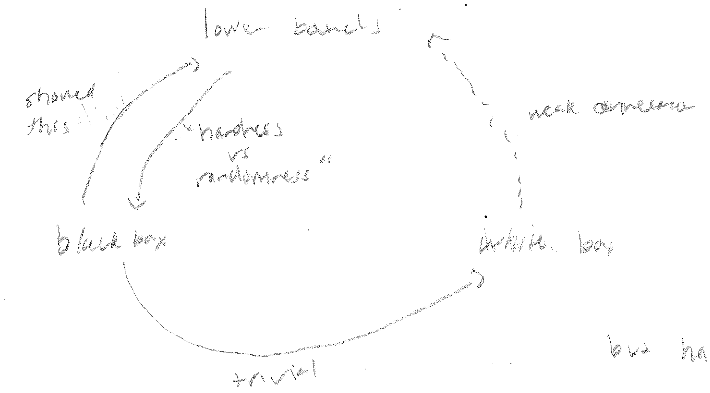
zero out

now poly$(|\mathcal{H}|)$-size linear system, so can solve.

☒

Michael Forbes
miforbes@csail.mit.edu
2014-11-04.3
jakob-guest-lec

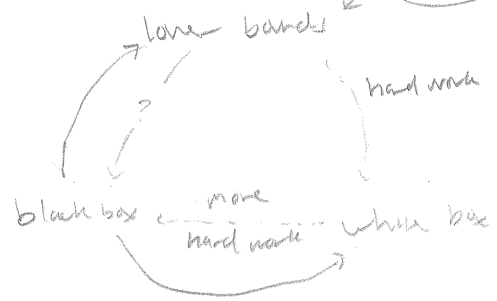
Circle of PIT of general circuits:



but have none of these!

Circle for restricted models:

/maybe/ known



3) Sums of powers of linear polynomials

defn: a sum of power of linear polynomials ($\Sigma\wedge\Sigma$) is

$$f(\bar{x}) = \sum_{i=1}^{r} \underbrace{(\alpha_{i,0} + \alpha_{i,1}x_1 + \cdots + \alpha_{i,n}x_n)}_{\text{linear polynomial}}{}^{d_i}, \quad d_i \le d, \quad \alpha_{i,j} \in \mathbb{Q}$$

"size" $:= nrd$

ex: $(x+y)^2 - (x-y)^2 = 4xy \Rightarrow$ general powering circuits $\equiv$ general circuits

restriction to depth 3 is quite limiting, but nontrivial!

Lem: $$x_1 \cdots x_n = \frac{1}{n!} \sum_{S \subseteq [n]} (-1)^{n-|S|} \left(\sum_{i \in S} x_i\right)^n$$

size $n \cdot 2^n \cdot n$ $\Sigma\wedge\Sigma$

Cor: any n-var deg d poly has a $\exp(n,d)$-size $\Sigma\wedge\Sigma$ circuit

Q: explicit poly needing large $\Sigma\wedge\Sigma$ circuits?

Michael Forbes
mforbes@csail.mit.edu
2014-11-04.4
jakob guest lecture

3a) $\Sigma\wedge\Sigma$ lbs

Thm: $x_1 \cdots x_n$ needs $2^{\Omega(n)}$ size $\Sigma\wedge\Sigma$ circuits

strategy: complexity measure $\mu: \mathbb{Q}[\bar{x}] \to \mathbb{N}$

st: $\mu(x_1 \cdots x_n) \geq$ large

$\mu(f) \leq$ small, f has small $\Sigma\wedge\Sigma$ circuit

ie: $\mu(f+g) \leq \mu(f) + \mu(g)$

$\mu(\ell^d) \leq$ small if $\deg \ell \leq 1$

$\Rightarrow$ if $x_1 \cdots x_n = \sum_{i=1}^r \ell_i^{d_i}$

then $r \geq \dfrac{\mu(x_1 \cdots x_n)}{\mu(\ell^d)} \geq \dfrac{\text{large}}{\text{small}} = \text{large}$

fundamental measure: "size" of partial derivatives

ex: $f = (x_1 + \cdots + x_n)^d \Rightarrow$ only 1 partial derivative of each order!

$\partial_{x_i} f = d\,(x_1 + \cdots + x_n)^{d-1}$

$\partial_{x_i x_j} f = d(d-1)\,(x_1 + \cdots + x_n)^{d-2}$

$\vdots$

ex. $f(x,y) = (2x+y)^n$ ← chain rule: $\partial_x(f^d) = d \cdot f^{d} \cdot \partial_x f$

$\partial_x f = n \cdot 2(2x+y)^{n-1}$, $\partial_y = 2x+y$ ← 2 polys, but essentially the same

idea: measure size by linear algebra

ie $\mathbb{Q}[\bar{x}]^{\leq d}$ is a $\binom{n+d}{d}$-dimensional $\mathbb{Q}$-vec space

each differentiation maps $\mathbb{Q}[\bar{x}]^{\leq d}$ into itself

defn (partial derivative method): $\partial: \mathbb{Q}[\bar{x}]^{\leq d} \to 2^{(\mathbb{Q}[\bar{x}]^{\leq d})}$ ← power set

$\partial(f) = \{\partial_{\bar{x}^{\bar{a}}} f\}_{\bar{a}}$ ← set of all derivatives

$\partial_{\bar{x}^{\bar{a}}} = \dfrac{\partial^{a_1 + \cdots + a_n}}{\partial x_1^{a_1} \cdots \partial x_n^{a_n}}$

$|\partial(f)| := \dim_{\mathbb{Q}} \partial(f)$

ex: $f(x,y) = (2x+y)^2$, $\partial f = \{(2x+y)^2, 4(2x+y), 2(2x+y), 8, 4, 2\}$

← $\dim = 3 = 2+1$

ex: $f(x,y) = xy$, $\partial f = \{xy, x, y, 1\}$

← $\dim = 4 = 2^2$

[4 vs 3 not so big...]

Michael Forbes
miforbes@csail.mit.edu
2014-11-04.5
jakob guest lecture

<u>lem</u>: $|\partial(f+g)| \le |\partial(f)| + |\partial(g)|$

<u>Pf</u>: linearity: $\partial_{\bar{x}^{\bar{a}}}(f+g) = \partial_{\bar{x}^{\bar{a}}}(f) + \partial_{\bar{x}^{\bar{a}}}(g)$

thus $\partial(f+g) \subseteq \text{span}\{\partial(f), \partial(g)\}$ $\square$

<u>lem</u>: $\ell(\bar{x})$ deg ≤ 1, $|\partial(\ell^d)| \le d+1$

<u>Pf</u>: $\ell(\bar{x})^d = (\alpha_0 + \alpha_1 x_1 + \cdots + \alpha_n x_n)^d$ scalar

$\partial_{x_i}(\ell(\bar{x})^d) = d\alpha_i(\alpha_0 + \alpha_1 x_1 \cdots + \alpha_n x_n)^{d-1} \in \text{span}\ \ell(\bar{x})^{d-1}$

$\partial_{x_i x_j}(\ell(\bar{x})^d) = d(d-1)\alpha_i\alpha_j(\alpha_0 + \alpha_1 x_1 + \cdots \alpha_n x_n)^{d-2} \in \text{span}\ \ell(\bar{x})^{d-2}$

so $\partial(\ell^d) \in \text{span}(\ell(\bar{x})^d, \ell(\bar{x})^{d-1}, \ldots, \ell(\bar{x}), 1)$

<u>lem</u>: $|\partial(x_1 \cdots x_n)| = 2^n$

<u>Pf</u>: $\partial(x_1 \cdots x_n) = \{\prod_{i\in S} x_i\}_{S\subseteq[n]}$

$\uparrow$ all linearly indep

<u>eg</u>: $\partial_{x_i} \prod_{j\in S} x_j = \begin{cases} 0 & i \notin S \\ \prod_{j\in S\setminus\{i\}} x_j & i \in S \end{cases}$

<u>Thm</u>: $x_1 \cdots x_n$ needs $2^{\Omega(n)}$ size $\Sigma\wedge\Sigma$

<u>Pf</u> $f(\bar{x}) = \sum_{i=1}^{r} \ell_i(\bar{x})^{d_i} \Rightarrow |\partial(f)| \le \sum_i |\partial(\ell_i^{d_i})|$

$\le \sum_i (d_i+1)$

$\le r(d+1) \lesssim \text{size} = dnr$

so if $f(\bar{x}) = x_1 \cdots x_n$, need $r \ge 2^n/d+1$ $\square$

this "closes" the lower bounds question

but <u>not</u> identity testing: no hardness vs randomness → explicit

<u>Thm</u>: given f, size s $\Sigma\wedge\Sigma$, can decide whether "$f \equiv 0$" in poly(s) steps

↪ white box, deterministic

<u>Thm</u>: there are explicit $\text{poly}(s)^{\lg s}$-size hitting sets for size-s $\Sigma\wedge\Sigma$ circuits ← today

<u>Thm</u>: " $\text{poly}(s)^{\lg\lg s}$ "

↑ best, despite simplicity of $\Sigma\wedge\Sigma$

<u>Pf</u>: <u>idea</u>: "scale down" — lower bound

"squeeze more" from lower bound

Michael Forbes
miforbes@csail.mit.edu
2014-11-04.6
jakob-guest lecture

ie say $f(\bar{x}) = \sum_{i \le r} l_i(\bar{x})^{d_i}$, $d_i \le d$, what do we know?

if $r \ll 2^n$ then $f \ne x_1 \cdots x_n$

scale down: $f \ne x_{i_1} \cdots x_{i_k}$, $i_1 < \cdots < i_k$ for $k \gg \lg r$

so $\Sigma\wedge\Sigma$ size can "only" compute $\log(s)$-size monomials

ex $(x_1 + \cdots + x_n)^n = n!\, x_1 \cdots x_n + \cdots + x_1^n + \cdots$

large monomial! — only involves 1 var

[want to say this doesn't degrade under summation]

Main Prop: $f \ne 0$ size s $\Sigma\wedge\Sigma$, $f = \sum_{\bar{a}} c_{\bar{a}} \bar{x}^{\bar{a}}$

$\Rightarrow \exists\, \bar{a}$, $c_{\bar{a}} \ne 0$ so $\bar{x}^{\bar{a}}$ involves $\le \log(s)$ variables

in fact: $\bar{a}$ is the lexicographically first nonzero monomial [robust form of lower bound]

defn: the lexicographic ordering on monomials $\prec$ is [dictionary order]

$\bar{x}^{\bar{a}} \prec \bar{x}^{\bar{b}}$ iff $a_1 \cdots a_n$ is lexicographically before $b_1 \cdots b_n$

$\bar{a}, \bar{b} \in \mathbb{N}^n$ ie $\bar{b} - \bar{a}$ has its first nonzero coordinate positive

$x_1 > \cdots > x_n$

ex: $x > y > z$: $x > y^{10} > z^{100}$

$x^{10} > yz > z^{100}$

ex: $(x_1 + \cdots + x_n)^n = x_1^n +$ lower order $+ \cdots + x_n^n$

first — last

Thm: explicit hitting set $\mathcal{H}$ for size s $\Sigma\wedge\Sigma$, $|\mathcal{H}| = \mathrm{poly}(s)^{\lg s}$

Pf: 1) guess the $\lg s$ variables in leading monomial $\longrightarrow \binom{n}{\lg s}$ choices

2) zero out other variables $\longleftarrow$ preserves nonzeroness

$\Rightarrow$ get nonzero deg $\le d$ poly in $\lg s$ vars

3) use brute force hitting set on remaining $\log(s)$-vars $\longrightarrow (d+1)^{\lg s}$ choices

$\le (nd)$

formally: $S \subseteq \mathbb{F}$ w/ $|S| = d+1$, $0 \in S$ $\overset{\mathrm{SZ}}{\Rightarrow} S^k$ is hit set for deg $\le d$, k-var poly

$\mathcal{H} := \{ \bar{\alpha} : \bar{\alpha} \in S^n,\ \bar{\alpha}$ has $\le \lg s$ nonzero values $\}$

$|\mathcal{H}| \le \binom{n}{\lg s}(d+1)^{\lg s}$, is hitting set

∎

Lem: 1) '$\prec$' is a total order on monomials

2) $1 = \bar{x}^{\bar{0}} \prec \bar{x}^{\bar{a}}$

3) $\bar{x}^{\bar{a}} \prec \bar{x}^{\bar{b}} \Rightarrow \bar{x}^{\bar{a}+\bar{c}} \prec \bar{x}^{\bar{b}+\bar{c}}$

Pf: 1) by defn

2) $\bar{a} - \bar{0} = \bar{a} \Rightarrow$ first nonzero coord positive

3) if first nonzero coord of $\bar{b} - \bar{a}$ is positive, so is $(\bar{b}+\bar{c}) - (\bar{a}+\bar{c})$

Michael Forbes
miforbes@csail.mit.edu
2014-11-04.7
jakob-guest lecture

Lem. $\bar{x}^{\bar{a}} < \bar{x}^{\bar{b}}$. Suppose $\partial_{\bar{x}^{\bar{c}}}(\bar{x}^{\bar{a}}), \partial_{\bar{x}^{\bar{c}}}(\bar{x}^{\bar{b}}) \neq 0$,

then $\partial_{\bar{x}^{\bar{c}}}(\bar{x}^{\bar{a}}) < \partial_{\bar{x}^{\bar{c}}}(\bar{x}^{\bar{b}})$

Pf. $\partial_{\bar{x}^{\bar{c}}}(\bar{x}^{\bar{a}}) = \text{const} \cdot \bar{x}^{\bar{a}-\bar{c}}$, nonzero $\Rightarrow \bar{a} \geq \bar{c}$

$\partial_{\bar{x}^{\bar{c}}}(\bar{x}^{\bar{b}}) = \text{const}' \cdot \bar{x}^{\bar{b}-\bar{c}}$ $\qquad \bar{b} \geq \bar{c}$

$\bar{x}^{\bar{a}} < \bar{x}^{\bar{b}} \Rightarrow \bar{x}^{\bar{a}-\bar{c}} < \bar{x}^{\bar{b}-\bar{c}}$

Main lemma. $|\partial(f)| \geq |\partial(LM(f))|$

where $LM(f)$ is the *leading monomial* of f

so if $\overset{\shortparallel}{c_{\bar{a}}\bar{x}^{\bar{a}}}$ then $f = c_{\bar{a}}\bar{x}^{\bar{a}} +$ lower terms

Main lemma $\Rightarrow$ main prop. f size s $\Sigma\Lambda\Sigma$ $\Rightarrow$ $\underset{\text{VI}}{|\partial(f)|} \leq s$

if $LM(f)$ involves k vars $\underset{\text{as before}}{\Rightarrow}$ $|\partial(LM(f))| \geq 2^k$

$\Rightarrow$ leading monomial involves $\leq \log|s|$ variables

Pf of Main lemma: let's do $|\partial(f)| \geq 2^k$, $k = $ # vars in $LM(f)$

ex: $f = xy +$ lower, $LM(f) = xy$

$\partial_x = y +$ lower

$\partial_y = x +$ lower

$\partial_{xy} = 1 +$ lower

$\partial_z = 0 +$ lower

Clm. $f = c_{\bar{a}}\bar{x}^{\bar{a}} +$ lower

if $\partial_{\bar{x}^{\bar{c}}}(\underset{\uparrow \text{iff } \bar{a} \geq \bar{c}}{\bar{x}^{\bar{a}}}) \neq 0 \Rightarrow \partial_{\bar{x}^{\bar{c}}}(\bar{x}^{\bar{a}})$ is leading monomial of $\partial_{\bar{x}^{\bar{c}}}(f)$

Pf. $\bar{x}^{\bar{a}} > \bar{x}^{\bar{b}}$

$\underset{\neq 0}{\partial_{\bar{x}^{\bar{c}}}(\bar{x}^{\bar{a}})}$ vs $\partial_{\bar{x}^{\bar{c}}}(\bar{x}^{\bar{b}})$ trivial $\partial_{\bar{x}^{\bar{c}}}(\bar{x}^{\bar{b}}) = 0$ nontrivial $\neq 0$

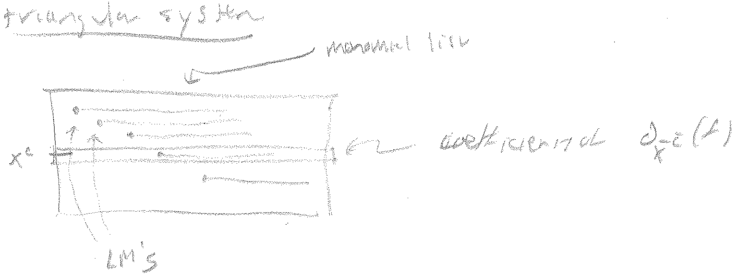
say $f = c_{\bar{a}}\bar{x}^{\bar{a}} +$ lower

consider $\{\partial_{\bar{x}^{\bar{c}}}(f) : 0 \leq \bar{c} \leq \bar{a}\}$ $\leftarrow$ $\geq 2^k$ such $\bar{c}$, if $\bar{x}^{\bar{a}}$ involves k vars

Clm: all polys in $\nearrow$ are linearly indep

Pf. $LM(\partial_{\bar{x}^{\bar{c}}}(f)) = \bar{x}^{\bar{a}-\bar{c}}$ $\leftarrow$ distinct for distinct $\bar{x}^{\bar{c}}$

so get *triangular system*



linear algebra $\Rightarrow$ polys are lin indep $\qquad \boxtimes$

Michael Forbes
miforbes@csail.mit.edu
2014-11-04.8
Jakob-visit

Recap: - defined $\Sigma\wedge\Sigma$ - $x_1 \cdots x_n$ has size 2^n $\Sigma\wedge\Sigma$
- define $|\partial(f)|$ ← complexity measure
- $|\partial(x_1 \cdots x_n)| \geq 2^n$
$|\partial(\text{size } s\ \Sigma\wedge\Sigma)| \leq s$ } ⇒ need 2^n size $\Sigma\wedge\Sigma$ for $x_1 \cdots x_n$
- "scale down" and "get more" from lower bound
ie: f size s $\Sigma\wedge\Sigma$ ⇒ $LM(f)$ involves $\leq \lg(s)$ variables
- use structural results to get hitting set

4) sums of powers of quad. polynomials
we studied $\sum_{i=1}^{s} \ell_i(\bar{x})^{d_i}$ where $\deg(\ell_i) \leq 1$ $(\Sigma\wedge\Sigma)$
Q: what if $\deg(\ell_i) \leq 2$? ie $\Sigma\wedge\Sigma\Pi^2$ ← fanin 2

scenarios:
1) $\Sigma\wedge\Sigma\Pi^2$ size s ⇒ $\Sigma\wedge\Sigma$ size poly(s) [I vote II]
$\boxed{2)}$ some f small $\Sigma\wedge\Sigma\Pi^2$ w/ f needs large $\Sigma\wedge\Sigma$

~~More scenarios: 1) $x_1 \cdots x_n$ has small $\Sigma\wedge\Sigma\Pi^2$ circuit~~
~~$\boxed{2)}$ $x_1 \cdots x_n$ needs large $\Sigma\wedge\Sigma\Pi^2$ circuits~~ ← only 2012!

Prop: $f := (x_1^2 + \cdots + x_n^2)^n$
a) f has small $\Sigma\wedge\Sigma\Pi^2$
b) f needs $2^{\Omega(n)}$ $\Sigma\wedge\Sigma$

Pf: (a) by defn
(b) want $|\partial(f)| \geq 2^n$
$f(x,y) = (x^2+y^2)^2$ $\quad 1$
$\partial_x = 2 \cdot 2x(x^2+y^2)$ $\quad x$
$\partial_y = 2 \cdot 2y(x^2+y^2)$ $\quad y$
$\partial_{xy} = 8xy$ $\quad xy$

Claim: $S \subseteq [n]$ $\partial_{\prod_{i\in S} x_i} (x_1^2 + \cdots + x_n^2)^n = \text{const} \cdot \prod_{i\in S} x_i (x_1^2 + \cdots + x_n^2)^{n-|S|}$

Pf induction:
$S = \emptyset$: just $(x_1^2 + \cdots + x_n^2)^n$
$S \to S \cup \{j\}$: $\partial_{x_j} \underbrace{\prod_{i\in S} x_i}_{\text{indep of } x_j} (x_1^2 + \cdots + x_n^2)^{n-|S|}$
$= 2(n-|S|) \cdot \prod_{i \in S\cup\{j\}} x_i (x_1^2 + \cdots + x_n^2)^{n-|S|-1}$

Michael Forbes
miforbes@csail.mit.edu
2014-11-04.9
jakob-lec-

Polynomial Identity testing, Michael Forbes

<u>outline</u>: 1) review

2) identity testing of sums of powers of linear polys

3) sums of powers of quadratic poly (?)

1) review

<u>Q</u> (polynomial identity testing): given a polynomial $f(x_1 \ldots x_n)$, is $f \equiv 0$?

$$\begin{tikzcd} & \text{lower bounds} \arrow[dl, squiggly] & \\ \text{white box} \arrow[rr, squiggly] & & \text{black box} \arrow[ul, "\text{saw this}"'] \end{tikzcd}$$

<u>defn</u>: sums of powers of linear forms ($\Sigma\wedge\Sigma$)

$$f(\bar{x}) = \sum_{i=1}^{s} l_i(\bar{x})^{d_i}, \quad \deg l_i \le 1, \ d_i \le d$$

<u>Prop</u>: $x_1 \cdots x_n$ has 2^n size $\Sigma\wedge\Sigma$

<u>Thm</u>: $x_1 \cdots x_n$ needs $2^{\Omega(n)}$ size $\Sigma\wedge\Sigma$

<u>defn</u>: $\underline{\partial} : \mathbb{Q}[\bar{x}] \to 2^{\mathbb{Q}[\bar{x}]}$

$$f \longmapsto \{\partial_{\bar{x}^{\bar{a}}} f\}_{\bar{a}}$$

$$\|\underline{\partial} f\| := \dim_{\mathbb{Q}} (\underline{\partial} f) \quad \longleftarrow \text{dimension of partial derivatives}$$

we saw:
- $\|\underline{\partial}\, x_1 \cdots x_n\| \ge 2^n$
- $\|\underline{\partial}\, l^d\| \le d+1$
- $\|\cdot\|$ is subadditive

$\Rightarrow$ gives theorem

so we "understand" $\Sigma\wedge\Sigma$ lbs

<u>Clm</u>: $\{\prod_{i \in S} x_i (x_1^2 + \cdots + x_n^2)^{n-|S|}\}_{S \subseteq [n]}$ are lin indep

<u>Pf</u>: deg $\uparrow$ is $|S| + 2(n-|S|) = 2n - |S|$

so only compare for fixed $|S|$, but $\{\prod_{i \in S} x_i\}_{S \in \binom{[n]}{k}}$

are lin indep, so mult by

$(x_1^2 + \cdots + x_n^2)^{n'}$ remains so $\square$

Thus $f = (x_1^2 + \cdots + x_n^2)^n$, $\underline{\partial}(f) \supseteq \{\partial_{\prod_{i \in S} x_i} f\}_{S \subseteq [n]}$

$\uparrow$ 2^n lin indep poly

<u>thus</u>: $\Sigma\wedge\Sigma\Pi^2$ is exponentially more powerful than $\Sigma\wedge\Sigma$!

Chaim Farber
Mito-base CSAIL, MIT edu
2014-11-09 10
jacob-wall

more generally: 1) $x_1 \cdots x_n$ has small $\Sigma\Lambda\Sigma\Pi^2$ ~~gate~~
2) $x_1 \cdots x_n$ needs large $\Sigma\Lambda\Sigma\Pi^2$ || vote

Qm: $x_1 \cdots x_n$ has $2^{n/d}$ size $\Sigma\Lambda\Sigma\Pi^d$

Pf. use ~~2^{size}~~ $2^{n/d}$ size $\Sigma\Lambda\Sigma$ to get $y_1 \cdots y_{n/d}$
then substitute $y_1 = x_1 \cdots x_d$
$y_2 = x_{d+1} \cdots x_{2d}$
$\vdots$
$y_{n/d} = x \ldots x_n$

Thm: $x_1 \cdots x_n$ needs $2^{\Omega(n/d)}$ size $\Sigma\Lambda\Sigma\Pi^d$
only in 2012!

Thm: the leading monomial of size s $\Sigma\Lambda\Sigma\Pi^d$ involves $\leq O(d \lg s)$ variables
$\Rightarrow$ hitting sets of size $\mathrm{poly}(s)^{d \lg s}$ for $\Sigma\Lambda\Sigma\Pi^d$
2015!

intuition: consider $\partial^{\leq k, \mathrm{ml}}$ = operator of order $\leq k$ multilinear derivatives

a) $\partial^{\leq k, \mathrm{ml}} x_1 \cdots x_n = \{ \prod_{i \in S} x_i \}_{S \in \binom{[n]}{n-k}}$

b) $\partial^{\leq k, \mathrm{ml}} (x_1^2 + \cdots x_n^2)^n = \{ \prod_{i \in S} x_i \, (x_1^2 + \cdots + x_n^2)^{n-k} \}_{S \in \binom{[n]}{k}}$

both sets are of same size
but (a) is deg $n-k$ ← high
(b) is deg k, up to global $(x_1^2 + \cdots + x_n^2)^{n-k}$ ← low
"1 dimensional"

key property of deg: low deg · low deg = low-deg

new measure: $\underline{\bar{x}^{=l}}\, \underline{\partial^{=k}}(f) = \{ \bar{x}^{\bar{a}} \partial_{\bar{x}^{\bar{b}}}(f) : \deg \bar{x}^{\bar{a}} \leq l, \deg \bar{x}^{\bar{b}} \leq k \}$

"shifted partial derivatives"

lots of exciting recent work on this measure

& proving the $2^{n/d}$ lb not too hard, but another time