

PROOF COMPLEXITY AS A COMPUTATIONAL LENSLECTURE 9: DEGREE LOWER BOUNDS FOR POLYNOMIAL CALCULUS

Fix field \mathbb{F} variables $\vec{x} = \{x_1, \dots, x_n\}$

Work in $\mathbb{F}[\vec{x}] / \{x_j^2 - x_j \mid j \in [n]\}$
so all polynomials multilinear

Also show in variables \bar{x}_j when convenient —
won't need them today

POLYNOMIAL CALCULUS DERIVATION from \mathcal{P}
polynomials $\pi = (p_1, p_2, \dots, p_k)$ such that

p_i is

INPUT POLYNOMIAL

$p_i \in \mathcal{P}$

BOOLEAN AXIOM $x_j^2 - x_j$ except we don't need
rule in multilinear setting

COMPLEMENTARITY AXIOM $x_j + \bar{x}_j = 1$

or derived from $p_j, p_k \in \mathcal{P}, j, k < i$ by

LINEAR COMBINATION

$$\frac{g}{\alpha g + \beta r} \quad \alpha, \beta \in \mathbb{F}$$

MULTIPLICATION

$$\frac{g}{m^q} \quad m \text{ monomial}$$

A POLYNOMIAL CALCULUS REFUTATION of set of polynomials \mathcal{P} is derivation from \mathcal{P} ending in $p_\ell = 1$

Size of \mathcal{P} $S(\mathcal{P}) = \# \text{monomials in representation of } \mathcal{P} \text{ as linear combination of monomials}$

$$S(\pi) = \sum_i S(p_i)$$

$\text{Deg}(\pi) = \max \text{ total degree of any polynomial } p_i$

THEM1 [Impagliazzo, Pudlák, & Sygal '99]

PCDD

$$\text{Spec}(P \perp \perp) = \exp\left(-2 \left(\frac{(\text{Deg}(P \perp \perp) - \text{Deg}(P))^2}{|\text{Vars}(P)|} \right)\right)$$

Focus on proving degree lower bounds

Build generalized constraint-variable incidence graph (CVIG)

sets of polynomials P over variables V

Partition $P = Q \cup \bigcup_{i=1}^m P_i$

Divide $V = \bigcup_{i=1}^n V_i$

(U,V)_Q-graph $\text{ol}(V) = \max_x |\{v_i \mid x \in v_i\}|$

Bipartite graph with

- left vertex set $U = \{P_1, P_2, \dots, P_m\}$
- right vertex set $V = \{V_1, \dots, V_n\}$
- Edge (P, V) if $\text{Vars}(P) \cap V \neq \emptyset$

The edge (P, V) is RESPECTFUL or PC if
satisficer wins following game on (P, V)

(1) Satisficer commits to $g: V \rightarrow \{\top, \perp\}$ such that if for $q \in Q$ it holds that $\text{Vars}(q) \cap V \neq \emptyset$, then g satisfies q

(2) Adversary plays α s.t. $\alpha(Q) = \top$

(3) Define $\alpha'(x)$ by

$$\alpha'(x) = \begin{cases} g(x) & \text{if } x \in V \\ \alpha(x) & \text{otherwise} \end{cases}$$

Satisficer wins if $\alpha'(P \cap Q) = \top$

Recall for $G = (\mathcal{U} \cup \mathcal{V}, E)$, $\mathcal{U}' \subseteq \mathcal{U}$

$$\partial(\mathcal{U}') = \{v \in \mathcal{V} : |\text{IN}(v) \cap \mathcal{U}'| = 1\}$$

BOUNDARY or UNIQUE NEIGHBOURS of \mathcal{U}'

PC BOUNDARY of \mathcal{U}' in $(\mathcal{U}, \mathcal{V})_Q$ -graph

$$\partial_Q^{\text{PC}}(\mathcal{U}') = \{v \in \mathcal{V} \mid v \in \partial(\mathcal{U}') \text{ and for } p_v \in \text{IN}(v) \cap \mathcal{U}' \quad (pv) \text{ is a PC edge}\}$$

$(\mathcal{U}, \mathcal{V})_Q$ -graph is (s, δ, ξ, Q) -PC EXPANDER

if $\forall \mathcal{U}' \subseteq \mathcal{U}, |\mathcal{U}'| \leq s$ it holds that

$$|\partial_Q^{\text{PC}}(\mathcal{U}')| = \delta |\mathcal{U}'| - \xi \quad \text{with overlap } \ell \text{ if } \text{ol}(\mathcal{U}') \leq \ell$$

THEOREM 2 [MN '24]

$$\text{Suppose } \forall p \in \mathcal{P} \quad |\text{Vars}(p)| \leq \frac{\delta s - 2\xi}{2\ell}$$

$(\mathcal{U}, \mathcal{V})_Q$ (s, δ, ξ, Q) -expander with overlap ℓ

$\forall \mathcal{U}', |\mathcal{U}'| \leq s \quad \mathcal{U}' \cup Q$ satisfiable.

Then

$$\text{Deg}(P \cup \perp) > \frac{\delta s - 2\xi}{2\ell}$$

COROLLARY 3 [MN '24]

$$\text{Suppose that } \forall p \in \mathcal{P} \quad |\text{Vars}(p)| \leq \frac{\delta s}{2\ell}$$

and $(\mathcal{U}, \mathcal{V})_Q$ -graph is $(s, \delta, 0, Q)$ -PC expander (i.e., $\xi = 0$)

Then

$$\text{Deg}(P \cup \perp) > \frac{\delta s}{2\ell}$$

How can we use this to prove lower bounds?

Build $(\mathcal{U}, V)_Q$ -graphs and show that they are PC expanders.

THEOREM 4 [Kabanikhin & Razborov '03]

Let F be a CNF formula such that the clause-variable incidence graph $G(F)$ is an (s, δ) -boundary expander for some $\delta > 0$. Then $\text{Deg}(F+1) > \delta s/2$.

COROLLARY 5

Random k -CNF formulas require polynomial calculus proofs of exponential size $\exp(-\Omega(n))$ asymptotically almost surely (and linear degree $\Omega(n)$)

for $k \geq 3$
 (with $\Theta(n)$ clauses over n variables)

Proof of Cor 5 The CVIG of such a random formula is a random k -left-regular bipartite graph, which is an excellent expander a.a.s.

Proof of Thm 4 Axion clauses/polynomials have $k = O(1)$ variables. Set $Q = \emptyset$, \mathcal{U} = singleton set of clauses, $V = \text{singleton sets of variables}$. All edges^(c, x) are PC good - can assign x to fix $c = 1$. \square

GRAPH ORDERING PRINCIPLE GOP(G)

"There exists a totally ordered set on n elements without a minimal element."

Variables $x_{u,v} = \text{"element } u \prec \text{element } v"$
 $u, v \in [n]$

Bounded-degree graph $G = (V, \bar{E})$ $V = [n]$

DEF Non-bipartite boundary expanders

Graph $G = (V, E)$ is an (δ, δ) -BOUNDARY

EXPANDER if $\forall V' \subseteq V$, $|V'| \leq \delta$, it holds that

$$|\partial(V')| \geq \delta |V'|, \text{ where}$$

$$\partial(V') = \{v \in V \mid V' : |N(v) \cap V'| = 1\}$$

$\bar{x}_{u,v} \vee \bar{x}_{v,w} \vee x_{u,w}$	$u, v, w \in V$ $u \neq v \neq w \neq u$	TRANSITIVITY
$\bar{x}_{u,v} \vee \bar{x}_{v,u}$	$u, v \in V$ $u \neq v$	ASYMMETRY
$x_{u,v} \vee x_{v,u}$	$u, v \in V$ $u \neq v$	TOTALITY
$\bigvee_{u \in N(v)} x_{u,v}$	$v \in V$	NON-MINIMALITY

" v is not minimal as witnessed by some neighbour u of v w.r.t. G "

For $G = K_n$, this formula is known as the LINEAR ORDERING PRINCIPLE FORMULA (or LEAST NUMBER PRINCIPLE FORMULA or GRAPH TATOLOGY)

THEOREM 6 [Galešić & Lauria '10]

For any non-bipartite (δ, δ) -boundary expander G it holds that $\boxed{\text{Deg}(GOP(G)) + 1} \geq \frac{\delta s}{4}$.

Remark 1 Result in Galešić-Lauria has slightly better constants — we optimize for simplicity of exposition (GL'10 gets lower bounds for 3-CNF
Here we need 5-CNF)

Remark 2 Random 5-regular graphs are $(\Omega(n), \delta > 0)$ -boundary expanders a.a.s. - calculation

Remark 3 Thm 6 yields 5-CNF formulas over $\Theta(n^2)$ variables with repetition degree $\Omega(n)$ [Stålmarck '96] showed that there are short resolution proofs. So these formulas demonstrate that size-width/degree claims in [IPS '99] and [BW '01] are essentially right. Might look at Stålmarck's resolution proof later in the course

Proof of Thm 6 Let Q consist of all transitivity, asymmetry, and totality axiom (enforcing that assignments are total orders)

Left vertex sets $U = \text{singleton sets with non-minimality axioms}$

Right vertex sets $V = \{V_v \mid v \in V\}$ where

$$V_v = \{x_{u,w} \mid u=v \text{ or } w=v\}$$

set of all variables that mention v .

Every variable $x_{u,w}$ occurs in V_u and V_w , so overlap = 2.

We claim that all edges (P_v, V_w) are PC-good.
 $w \in \{v\} \cup N(v)$

If $w \in N(v)$, then let

$$f_w(x_{w,u}) = T \quad \text{for all } u \text{ such that } x_{u,w} \text{ or } x_{w,u} \text{ are in } V_w$$

$$f_w(x_{u,w}) = \perp$$

i.e., f_w sets w to be locally smallest element.

$$P_v = \left\{ \bigvee_{u \in N(v)} x_{u,v} \right\} \text{ is satisfied.}$$

For Q , asymmetry and totality axioms are either untouched or satisfied, since if g assigns $x_{u,w}$ it also assigns $x_{w,u}$ and exactly one of the variables is true and the other false.

$$\overline{x}_{a,b} \vee \overline{x}_{b,c} \vee x_{a,c}$$

For transitivity if $g(x_{a,c}) = T$, then we're OK and if $g(x_{a,c}) = \perp$ then $c=w$ and we also have $g(x_{b,c}) = \perp$

Similarly, if $g(x_{a,b}) = T$ then $\overline{g(x_{a,c})} = T$

If $g(x_{b,c}) = T$ then $b=w$ and $g(x_{a,b}) = \perp$

\Rightarrow Consider vertex set $V' \subseteq V(G)$. By discussion above, we have

$$\mathcal{I}_Q(V_{v' \in V'} \{P_{v'}\}) \supseteq \{V_w \mid w \in \partial(V')\}$$

In $(2l, V)_Q$ -graph, so the $(2l, V)_Q$ -graph has at least as good expansion parameters. We get

$$\text{Deg}(GOP(G) + \perp) > \frac{\delta_s}{2l} = \frac{\delta_s}{\gamma} \quad \boxed{\checkmark}$$

If $w=v$ then let

$$g_v(x_{v,u}) = \perp$$

$$g_v(x_{u,v}) = T$$

i.e., g_v sets v to locally largest element
Exactly same argument shows that Q is OK

GRAPH PIGEONHOLE PRINCIPLE FORMULAS

PCD VIII

$$G = (U \cup V, E) \quad \text{Pigeon } u \text{ can fly to holes } N(u)$$

$$\forall_{v \in N(u)} x_{u,v} \quad u \in U \quad \text{PIGEON AXIOMS}$$

$$\bar{x}_{u,v} \vee \bar{x}_{u',v} \quad v \in V \quad u, u' \in N(v) \quad u \neq u' \quad \text{HOLE AXIOMS}$$

$$\bar{x}_{u,v} \vee \bar{x}_{u,v'} \quad u \in U \quad v \neq v' \in N(u) \quad \text{FUNCTIONALITY AXIOMS}$$

$$\forall_{v \in N(v)} x_{u,v} \quad v \in V \quad \text{ONTO AXIOMS}$$

Standard pigeonhole principle formulas
for graph $K_{n+1, n}$. Get formula over G
by restriction

$$g_G(x_{u,v}) = \begin{cases} 0 & \text{if } (u,v) \notin E \\ * & \text{otherwise} \end{cases}$$

So lower bounds for graph PHP formulas imply
lower bounds for standard PHP formulas

Let $\text{Onto-PHP}(G)$ contain pigeon, hole, and onto axioms
 $\neg \vdash \text{FPHP}(G) - \vdash \neg \text{pigeon, hole, and functionality axioms}$

THEOREM 7 (Essentially [AR'03])

Let $G = (U \cup V, E)$ be an (s, δ) -boundary expander
without isolated vertices in V . Then

$$\text{Deg}(\text{Onto-PHP}(G) \vdash \perp) > \frac{s\delta}{2}.$$

Proof sketch Let $Q =$ onto & hole axioms

Let $\mathcal{U} =$ singleton sets with pigeon axioms.

Let $V_v = \{x_{u,v} \mid u \in N(v)\}$, i.e., variables are partitioned w.r.t. holes. All edges are PC-good, and the $(\mathcal{U}, V)_Q$ -graph is isomorphic to G . (Note, though, that pigeons might be sent to several holes to satisfy onto axioms in Q .) □

This does not work for FPHP(G), if we try to substitute functionality axioms for onto axioms in Q .

For edge (P_u, V_v) , need to set $x_{u,v} = T$

But $(\bar{x}_{u,v} \vee \bar{x}_{u,v'}) \wedge_{x_{u,v}} = \bar{x}_{u,v'} —$ clause touched but not satisfied

THEOREM 8 [MN '24]

Let $G = (\mathcal{U} \cup \mathcal{V}, E)$ be a bipartite (s, δ) -expander with left degree $\leq d$. Then

$$\text{Deg } (\text{FPHP}(G) + 1) > \frac{\delta s}{2d}$$

Proof Construct $(\mathcal{U}, V)_Q$ -graph as follows.

$Q =$ hole & functionality axioms

$\mathcal{U} =$ singleton sets with pigeon axioms

$V = \{V_v \mid v \in V\}$ where

$$V_v = \{x_{u,v} \mid u' \in N(v) \text{ and } v' \in N(u')\}$$

i.e. - start with hole v

- go to all pigeons u' that can fly to v

- consider all holes v' such pigeons u' can fly to

PCDX

Overlap is $\leq d$, since $x_{u,v}$ can only appear in sets $V_{v'}$ such that $v' \in N(u)$, and $|N(u)| \leq \text{left degree } d$.

G and $(2l, V)_Q$ is same graph

If $(u, v) \in E(G)$, then clearly 3 edge $P_u \leftrightarrow V_v$

Suppose (P_u, V_v) is edge in $(2l, V)_Q$

Then by construction $u \in N(v)$, so $(u, v) \in E(G)$.

Finally, we claim that all edges are PC good.

Consider $P_u = \{V_{w \in N(u)} x_{u,w}\}$ and V_v s.t.

$v \in N(u)$, i.e., (P_u, V_v) is edge. Choose

$$g_{uv}(x_{u',v'}) = \begin{cases} T & \text{if } u'=u \text{ & } v'=v \\ \perp & \text{otherwise} \end{cases}$$

$\forall_{w \in N(u)} x_{u,w}$ is satisfied

Hole axioms for v satisfied, since $g(x_{u',v}) = \perp$

All other hole axioms untouched or satisfied, since all other variables in V_v set to \perp .

Functionality axioms for u satisfied,

since $g(x_{u,v'}) = \perp$

All other functionality axioms either untouched or satisfied, since all other variables in V_v set to \perp .

Same graph and all edges good \Rightarrow same expansion

Overlap $l \leq d$ yields degree lower bound

$$\delta s / (2d)$$

✓

COROLLARY 9 [MN'24]

PCD XI

$$S_{\text{PCR}}(FPHP_n^{n+1} \uparrow \perp) = \exp(-\Omega(n))$$

Proof Apply restriction to $K_{n+1,n}$ to get, say, 5-left-regular $(\Omega(n), \delta > 0)$ -boundary expander G .

Theorem 8 \Rightarrow degree lower bound $\Omega(n)$ for $FPHP(G)$

[IPS'99] \Rightarrow exponential size lower bound for $FPHP(G)$

Since $FPHP_n^{n+1} \upharpoonright_{\mathcal{G}} = FPHP(G)$ and restrictions preserve reputations, means that same lower bound applies for $FPHP_n^{n+1}$ \square

Some questions

Results for resolution
in [BTS'07]

- ① Can we get PC lower bounds for graph coloring?
Yes, future lecture
- ② What about clique or vertex cover?
- ③ PC lower bounds for Ramsey theory problems?
- ④ Degree lower bounds for dense linear orders
formulas

Resolution
[Atserias, Dalmau '08]

Resolution results
 [Carlucci, Gallo, Lauria '16]
 [Lauria, Pudlák, Rödl, Thapen '17]
 [Pudlák '12]

- ⑤ PC size lower bounds for weak pigeonhole principle (WPHP) formulas with $\geq n^2$ pigeons

Understood for resolution Raz & Razborov
Also for graph-WPHP [de Rezende, Nederim, Risk, Sokolov '25]

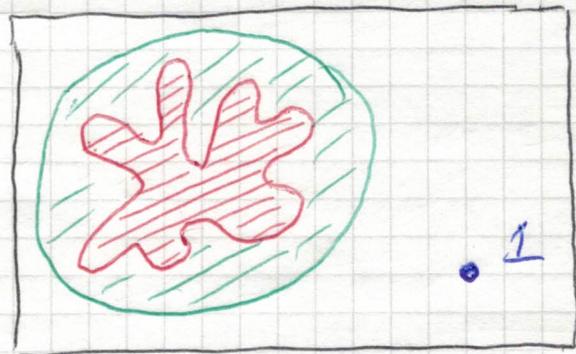
The lower bound method we have presented works regardless of the field. What about lower bounds that depend on the field?

- (6) [Alekhnovich & Razborov '03] have a version of their method that depends on the field. Can it be combined with generalized CVGs and filtering sets \mathcal{Q} ?
- (7) What about Ono-FPHP formulas in fields \mathbb{F} of characteristic p with $n + p^d$ pigeons and n holes? Upper & lower bounds for Nullstellensatz in [Beame & Riss '98]
Nothing known for PC
- (8) What about perfect matching on sparse non-bipartite graphs G with $|V(G)|$ odd?
 [Austin & Risse '22] Degree lower bound $\Omega\left(\frac{n}{\log n}\right)$ for random d -regular graphs.
 Issues: (a) d has to be very large
 (b) log factor loss
 Proof by reduction to Tseitin formulas.
 Direct argument would be desirable

PROOF STRATEGY FOR DEGREE LOWER BOUNDS

Give our approximation of what can be derived in degree D by defining operator R such that if p derivable from P in degree $\leq D$, then $R(p) = 0$.

Then show $R(I) \neq 0$



desirable in degree D
 $\{ p \mid R(p) = 0 \}$

LEMMA 10 [Kazborov '98]

Let P set of multilinear polynomials, DENT

Suppose \exists linear operator R on multilinear polynomials over $\text{Vars}(P)$ of degree $\leq D$ such that

(1) $R(f) = 0$ for all axioms $f \in P$

(2) For every term t with $\text{Deg}(t) < D$ and every variable x it holds that $R(xt) = R(x)R(t)$

(3) $R(I) \neq 0$

Then $\text{Deg}_{pc}(P \vdash I) > D$

(or $> D/2$ if we want to play it safe)

Proof By forward induction over derivation Π . Change multiplication rule to only multiply one variable at a time.

$$\begin{array}{ll} \text{VARIABLE} & P \\ \text{MULTIPLICATION} & xp \end{array}$$

Modified multiplication rule

Will prove degree lower bound in this setting. Strictly speaking, maybe lose factor 2 for monomial multiplication at get degree LB $\geq D/2$

Or work slightly harder on property (2)

PCD XIV

to get it for monomial multiplication. Might be possible.
Will not worry about this

~~~~~ DETOUR ~~~~

What is the issue?

Could have  $p = \sum_i x_i m_i$

Multiply by  $t$  to get  $tp = \sum_i x_i tm_i$

Could have high-degree terms  $tm_1$  &  $tm_2$  that cancel

But maybe we don't have cancellation if have to multiply by  $x \in \text{Vars}(t)$  one at a time

Variable multiplication can only double the degree

$p$  has degree  $D_1 \geq \max\{\deg(m_1), \deg(m_2)\}$   
 $tp$  has degree  $D_2 \geq \deg(t)$

$\forall i \quad \deg(tm_i) \leq D_1 + D_2 \leq 2 \max\{D_1, D_2\}$

By induction over  $\pi = (p_1, p_2, \dots, p_k)$

$$R(p_i) = 0$$

Base case:  $p_i \in P$   $R(p_i) = 0$  by property (1)

Inductive step  $p_i$  derived by  $\frac{q}{\alpha q + \beta r}$

$$\begin{aligned} R(\alpha q + \beta r) &= \alpha R(q) + \beta R(r) \quad [\text{by linearity}] \\ &= \alpha \cdot 0 + \beta \cdot 0 \quad [\text{by IH}] \\ &= 0 \end{aligned}$$

$P_i$  denoted by  $\frac{P}{xp}$

PCD XV

$$P = \sum_i t_i \quad \text{for terms } t_i = x_i \cdot m_i$$

$$\begin{aligned} R(xp) &= R(x \sum_i t_i) \\ &= R(\sum_i xt_i) \quad [\text{linearity}] \\ &= \sum_i R(xt_i) \\ &= \sum_i R(xR(t_i)) \quad [\text{property (2)}] \\ &= \sum_i R(x \cdot 0) \quad [\text{linearity}] \\ &= 0 \end{aligned}$$

So if such operator  $R$  exists, all polynomials  $P$  derivable in degree  $\leq D_{\text{one}} + 1$   $\square$

How to construct such an  $R$ ?

$R$  looks a lot like reduction modulo polynomial ideal  $I$

Ideal  $\langle P \rangle$  generated by <sup>input</sup>  $P$  satisfy (1) and (2)

But not (3), since  $P$  is unsatisfiable iff  $1 \in \langle P \rangle$

Solution Reduce different polynomials modulo different subsets of polynomials of  $P$  that are satisfiable. Piece together so that it looks like real polynomial ideal in degree  $\leq D$