LOWER BOUND TECHNIQUES FOR NS AND PC

Very limited time, so can't dwell much on motivation or survey of results. Assume we agree NS & PC relevant and focus on techniques

$\mathbb{F}$ field $\vec{x} = (x_1, \ldots, x_n)$

Polynomial equations

$$\boxed{\begin{array}{lll} P_j(\vec{x}) = 0 & & j \in [m] \\ x_i^2 - x_i = 0 & & i \in [n] \end{array}} \quad (*)$$

NULLSTELLENSATZ refutation

[Beame, Impagliazzo, Krajíček, Pitassi, Pudlák '95]

Polynomials $A_j, B_i \in \mathbb{F}[\vec{x}]$ s.t.

$$\boxed{\sum_j A_j P_j + \sum_i B_i (x_i^2 - x_i) = 1}$$

Hilbert's Nullstellensatz: Refutation exists iff no solution to $(*)$

Measures

Degree: $\max\{\deg(A_j P_j), \deg(B_i (x_i^2 - x_i))\}$

Size # monomials when all polynomials expanded out

Other representations? Next talk on ideal proof systems.

Refutations of CNF formulas

$F = \bigwedge_j C_j \quad , \quad C = a_1 \vee \dots \vee a_w$

Might be over any field, so additive translation $a_1 + \dots + a_w \geq 1$ doesn't work

Multiplicative translation

$$\boxed{x_1 \vee \overline{x_2} \vee x_3 \rightsquigarrow (1-x_1)\, x_2\, (1-x_3) = 0}$$

Actually, in algebraic setting more natural:

$\boxed{\text{evaluate to true} \Leftrightarrow \text{vanish} \Leftrightarrow \text{equal to } 0}$

So in this talk we will sometimes prefer

$$x_1 \vee \overline{x_2} \vee x_3 \rightsquigarrow \boxed{x_1\,(1-x_2)\, x_3 = 0}$$

No big deal... [and drop "$=0$" from now...]

How to prove lower bounds on degree?

A $\boxed{d\text{-DESIGN}}$ for $*$ is a map D from polynomials of degree $\leq d$ to $\mathbb{F}$ such that

D (1) D is linear $\quad D(\alpha A + \beta B) = \alpha D(A) + \beta D(B)$, $\quad \alpha, \beta \in \mathbb{F}$

D (2) $D(1) = 1$

D (3) $D(A \cdot P_j) = 0 \qquad [\deg(AP_j) \leq d]$

D (4) $D(x^2 A) = D(xA) \qquad [\deg(A) \leq d-2]$

clearly spelled out in [Buss '96] but known before then.

THEOREM

(*) has d-design $\Leftrightarrow$ (*) has no NS-refutation of degree $\leq d$

Note: Characterization!

Example: $\boxed{\text{HOUSESITTING PRINCIPLE}}$

Persons $I = \{0, 1, \ldots, n\}$

Houses $J = \{1, 2, \ldots, n\}$

Each person $i \in I$ either

a) stays at home i or

b) housesits for house $j > i$ where owner is not at home

$P_i = x_{i,i} + x_{i,i+1} + \ldots + x_{i,n} - 1$

$Q_{i,j} = x_{i,j} \, x_{j,j}$

(and, as always $x_{i,j}^2 - x_{i,j}$)

THEOREM [Buss '96, CEI '96 for GF(2)]

Housesitting principle requires NS degree $n+1$ in any field (or ring).

But note than in natural CNF encoding easily solved by resolution (unit propagation Person n has to be in house n, which reduces to housesitting principle over $n-1$ houses)

[Will soon define PC – not hard to see housesitting can be done in constant degree.]

IV

Can also prove NS degree LBs by interpolation [Pudlák Sgall '96]

$\Downarrow$ Constant-degree NS $\rightsquigarrow$ polynomial-size monotone spanning programs

Interesting recent work in other direction: Lift NS lower bounds to monotone spanning program lower bounds (using composition with gadgets)

$\boxed{\text{POLYNOMIAL CALCULUS}}$

Polynomial calculus [Clegg, Edmonds, Impagliazzo '96]
Build up derivation of 1 (=0) dynamically

Annoying issue when working with CNFs: Wide clauses with "wrong sign" blow up exponentially

[Alekhnovich, Ben-Sasson, Razborov, Wigderson '02]
Formal variables $x, \bar{x}$ for positive and negative literals

Derivation rules

$$\frac{}{P_j} \qquad \frac{}{x_i^2 - x_i} \qquad \frac{}{x + \bar{x} - 1}$$

$$\frac{A \quad B}{\alpha A + \beta B} \qquad \frac{A}{x A}$$

V

"Polynomial calculus (with) resolution" (PCR)

Similar issue with other (semi) algebraic proof systems when size is measured, e.g., SOS

Need better notation than tagging on "R" !?

Measures

Degree (no difference between PC & PCR)
Size (potentially big difference)
Length = # derivation steps

Often applications of $x_i^2 - x_i$ folded into implicit multilinearization of multiplication

Work in

$$\boxed{\mathbb{F}[x_1, \ldots, x_n] / \langle x_1^2 - x_1, \ldots, x_n^2 - x_n \rangle}$$

We will also do so. From now on all polynomials MULTILINEAR

In this setting, any unsatisfiable k-CNF formula is refutable in PC in linear length

So size is a better measure to focus on...

CONNECTIONS BETWEEN DEGREE & SIZE

$\exists$ PC(R) refutation in degree d $\Longrightarrow$
$\exists$ PC(R) refutation in size $n^{O(d)}$ [CEI '96]

This bound is asymptotically tight (in the exponent) in the worst case [Atserias, Lauria, Nordström '16]

THEOREM [Impagliazzo, Pudlák, Sgall '99] VI

Let refutation size S (in PC or) PCR
— " — degree D
Initial degree K
variables n Then

$$\boxed{S = \exp\left(\Omega\left(\frac{(D-K)^2}{n}\right)\right)}$$

so linear degree LB $\Rightarrow$ exp size LB

Same bound as in [Ben-Sasson, Wigderson '01]
Can run exactly same proof

But:

- For resolution have well-developed machinery to prove width LBs [BW01] PLUS OTHER METHODS!
- For PC quite challenging to prove degree lower bounds (AND NOT MUCH ELSE)

For fields of char $\neq 2$, can make affine transformation to ± 1 "Fourier basis"

Convenient for proving degree LB if input is (CNF encoding, possibly) of XORs

[Buss, Grigoriev, Impagliazzo, Pitassi '01]
[Ben-Sasson Impagliazzo '99 / '10]

Not so great if $+1 = -1$ ...

Tseitin
Random 3-CNF (from 3-XOR)

Focus of rest of this talk:

[Alekhnovich, Razborov '03] (or at least flexible)

Characteristic-independent degree LB technique

- Constraint-variable incidence graph
- plus expansion
- plus extra structural properties

Random 3-CNF
PHP

Used in [Galesi, Lauria '10a, '10b] Ordering Automatizability

[Mikša, Nordström '14, '15] FPHP

This presentation based on [MN15] ECCC TR15-078

Care only about degree — no $\bar{x}$ variables after all

$\boxed{\text{MONOMIAL } m = \prod_{i \in S} x_i}$

$\boxed{\text{TERM } \alpha \cdot m}$ m monomial $\alpha \in \mathbb{F}$

(We will be a bit sloppy in distinguishing)

$\boxed{\text{Ideal } I = \langle P_1, \ldots, P_\ell \rangle}$ smallest set of polynomials closed under addition and under multiplication by any polynomial

RECALL: Always multilinear polynomials
Always mod out $x_i^2 - x_i$

Define $\boxed{\text{ADMISSIBLE ORDERING}}$ of monomials/terms

For simplicity concretely

- $x_1 \prec x_2 \prec \ldots \prec x_n$
- $\deg(m_1) < \deg(m_2) \Rightarrow m_1 \prec m_2$
- For same degree, sort lexicographically

Leading term $\boxed{LT(P)}$ = largest term wrt $<$

Term t $\boxed{\text{REDUCIBLE}}$ modulo ideal I if $\exists$ $Q \in I$ s.t. $LT(Q) = t$; otherwise $\boxed{\text{IRREDUCIBLE}}$

FACT Any P can be written uniquely as

$$P = Q + R, \quad Q \in I$$

R lin comb of irreducible terms

"P is reduced to R mod I" $\boxed{R_I(P) = R}$ NOTATION

PC: computations in degree-bounded version of ideal — $\boxed{\text{PSEUDO-IDEAL}}$

Inspired by this, can define $\boxed{d\text{-PSEUDO-REDUCTION}}$ operator R^* mapping multilinear polynomials to multilinear polynomials. Requirements:

R(1) R^* is linear

R(2) $R^*(1) \neq 0$

R(3) $R^*(P_j) = 0$ for all input polynomials in $(*)$

R(4) $R^*(xt) = R^*(x R^*(t))$ for terms t with $\deg(t) < d$

LEMMA [Razborov '98]
If $(*)$ has d-pseudo-reduction operator, then degree-d PC cannot refute $(*)$.

Proof sketch: For any Q derived, show inductively that $R^*(Q) = 0$.
But $R^*(1) \neq 0$.

Not a characterization [as far as I know]

Observations:

(i) If set of polynomials did have satisfying 0/1 assignment, we could take R to be the real reduction operator mod this ideal.

(ii) For PC over $\mathbb{R}$, pseudo-expectations as in SOS yield pseudo-reductions (but "cheat" by mapping everything to $\mathbb{R}$, not $\mathbb{R}[\vec{x}]$)

How to build pseudo-reduction?

Use true reductions modulo ideals, one ideal I_t per term t

Define $\boxed{R^*(t) = R_{I_t}(t)}$

Extend by linearity $R^*(P) = \sum_{t \in P} R^*(t)$

Show that I_t chosen so that R(1) - R(4) work out $= \sum_{t \in P} R_{I_t}(t)$

How to choose ideals for terms?

This is where the magic is...

And where technical developments are needed.

[Or maybe we need other, new tools?]

Will try to handwave example set-up from [MN15] (following and developing [AR03])

X

Given polynomials $P_1, \ldots, P_m$ over $x_1, \ldots, x_n$

Divide variables into groups V_j
(doesn't have to be partition, but should have bounded overlaps every variable x_i only in few V_j. For now, think partition)

Take some polynomials $P_{\ell+1}, \ldots, P_m$ and put in set Q filtering which truth value assignments we are interested in (e.g. for PHP axioms making sure that we get partial matchings)

Build bipartite graph G with
- $P_1, \ldots, P_\ell$ on left
- $V_1, \ldots, V_N$ on right
- Edge if variable in V_i occurs in polynomial P_j

Assume $|Vars(P_i)|$ bounded (true, e.g., for k-CNF)

Assume that $G = (\mathcal{U} \cup \mathcal{V}, E)$ is an (s, δ)-BOUNDARY EXPANDER: All sets $\mathcal{U}' \subseteq \mathcal{U}$, $|\mathcal{U}'| \le s$ have $|\partial \mathcal{U}'| \ge \delta |\mathcal{U}'|$ unique neighbours on right-hand side UNIQUE NEIGHBOURS

(We will also need other conditions on graph, but let us ignore this for now and start doing the proof)

For term t, look an "neighbourhood" (fake)
$N(t)$ in V (all neighbouring V_i if t would have been left vertex)

Lying blatantly, let the $\boxed{\text{SUPPORT}}$ of t $Supp(t)$
be largest $\mathcal{U}' \subseteq \mathcal{U}$ of size $\leq s$
such that $\boxed{\partial \mathcal{U}' \subseteq N(t)}$ plus all of Q

Intuition (vague and probably not true):

- Polynomials in $\mathcal{U}'$ could have been involved in deriving polynomial t in low-degree, because variables ~~xxxxx~~ in $N(\mathcal{U}') \setminus \partial\mathcal{U}'$ could have cancelled
- But using $P \in \mathcal{U} \setminus \mathcal{U}'$ would have left unique-neighbour variables that could not have cancelled.
- And Q we give for free anyway.

How to prove properties of pseudo-reduction?

R(1) Linearity by definition

R(2) $Supp(1) = \emptyset$ by expansion ($N(1) = \emptyset$). $R_{\langle Q \rangle}(1) = 1$ since Q satisfiable

R(3) $\boxed{R^*(P_j) = 0}$ already interesting case

What we would like:

Reduce modulo $\langle N(N(P_j)) \rangle \ni P_j \rightsquigarrow 0$

Want "P_j reduced modulo ideal containing P_j"

But $R^*(P) = \sum_{t \in P} R_{\langle Supp(t)\rangle}(t)$

with reduction modulo different ideals!

Idea: Take $S = \cancel{\bigcup_{t\in P} Supp(t)}$ $Supp(Vars(P))$

Show that $\forall t \in P$ in fact

$$\boxed{R^*(t) = R_{\langle Supp(t)\rangle}(t) = R_{\langle S\rangle}(t)}$$

Then $R^*(P) = \sum_{t \in P} R_{\langle S\rangle}(t)$

$$= R_{\langle S\rangle}(P) = 0$$

since $P \in Supp(Vars(P))$ clearly holds.

BUT WHY WOULD THIS BE TRUE?! Let us sketch

Special case

$$\boxed{\begin{array}{l}\text{If } t \text{ is irreducible mod } \langle Supp(t)\rangle \\ \text{then } t \text{ irreducible mod } \langle Supp(t), P_j\rangle\end{array}}$$

some P_j outside of support of t

Suppose not. Then

$t = S' + Q' + A_j P_j$

$S' \in \langle Supp(t)\rangle \quad Q' = \langle Q\rangle$

But $\exists V_i$ s.t. $V_i \cap Vars(P_j) \neq \emptyset$, $V_i \cap Vars(t) = \emptyset$

Otherwise P_j would have been in the support. For same reason $Vars(S') \cap V_i = \emptyset$

Suppose we could find assignment ρ to V_i' s.t.

- $\rho(P_j') = 0$
- For all $P_{\ell+1}, \ldots, P_m \in Q$, either $\rho(P_\ell') = 0$ or P_ℓ' left untouched.

(+)

Then $t = S' + Q''$ $\quad Q'' \in \langle Q \rangle$
so t was reducible mod $\langle Supp(t) \rangle$ after all. ∎

Generalizing this, get R③ & R④ provided that all edges $P_j - V_i$ in G satisfy condition (+)

This is [MN15]
Works for any field
(when it works)

Other variant [AR03]

- Graph still expander
- No condition on edges
- But no P_i has low-degree implications (i.e. P_i have $\boxed{\text{HIGH IMMUNITY}}$)

Takes characteristic into account

Different but related R^*-operator works

Similar argument.

Open problems

1. PC degree LB for 3-colouring
Known worst-case [Lauria-Nordström '17]
Want average-case like for resolution in
[Beame, Culberson, Mitchell, Moore '05]

2. PC size lower bound for k-clique
[not even known for general resolution]

3. PC size lower bounds for PHP^m_n,
$m \gg n$ (degree + IPS99 fails for $m \geq n^2$)

4. Onto-FPHP^m_n is easy for $m = n+1$
in any field. What about $\mathbb{F}_p$ when
$(m-n) \equiv 0 \pmod{p}$? IS THIS KNOWN?

5. For resolution we know for k-CNFs
clause space $\geq$ width [Atserias, Dalmau '08]
Can we prove $\boxed{\text{monomial space} \geq \text{degree}}$?
At least when [AR03]-framework establishes
degree LB?

6. Feasible interpolation for PC? [Cf Pudlák]

7. Tseitin / k-XOR lower bounds break if we allow
affine transformation of input + PC.
Prove lower bounds robust against such
preprocessing step?