Very limited time, can't dwell much on motivation or survey of results. Assume weighted NS&PC relevant and IF field $\mathbf{x} = (x_1, \ldots, x_n)$ focus on techniques

**Polynomial equations**

$$p_j(t) = 0 \quad j \in [m]$$

$$x_i^2 - x_i = 0 \quad i \in [n]$$

**Nullstellensatz** reputation

[Beame, Impagliazzo, Krajíček, Pitassi, Pudlák 1997]

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

$$\sum_j A_j p_j + \sum_i B_i (x_i^2 - x_i) = 1$$

Hilbert's Nullstellensatz: Reputation exists if 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.
Representations of CNF formulas

\[ F = \bigwedge_j C_j \quad C = a_1 \lor \ldots \lor a_n \]

Might be over any field, so additive translation \( a_1 + \ldots + a_n > 1 \)
doesn’t work

Multiplicative translation

\[ x_1 \lor \overline{x}_2 \lor x_3 \land (1-x_1) x_2 (1-x_3) = 0 \]

Actually, in algebraic setting more natural:

evaluate to true \( \Leftrightarrow \) vanish \( \iff \) equal to 0
So in this talk we will prefer

\[ x_1 \lor \overline{x}_2 \lor x_3 \land x_1 (1-x_2) x_3 = 0 \]

No big deal... [and drop “=0” from now on...]

How to prove lower bounds on degree?

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

1. \( D \) is linear
2. \( D(1) = 1 \)
3. \( D(A \cdot P_f) = 0 \)
4. \( D(x^2 A) = D(xA) \) [deg \( (A^2) \leq d-2 \)]

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

(*) has d-design \iff (**) has no NS-refutation of degree \leq d.

Note: Characterization!

Example: HOUSESITTING PRINCIPLE

Persons: \( I = \{0, 1, \ldots, n\} \)

Houses: \( J = \{1, 2, \ldots, n\} \)

Each person \( i \in I \) either

(a) stays at home or

(b) housesits for house \( j > i \) where

owner is not at home.

\[ P_i = x_{ii} + x_{ii+1} + \ldots + x_{in} - 1 \]

\[ a_{ij} = x_{ij} x_{ji} \]

(and as always \( x_{ij} + x_{ji} \))

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

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

But note that 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.]
Can also prove NS degree LBs by interpolation [Pudlak Szegedy '96]

Constant-degree NS vs polynomial-size monotone spanning programs

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

POLYNOMIAL CALCULUS

Polynomial calculus [Clegg, Edmonds, Impagliazzo '90]

Build up derivations 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 $x, \overline{x}$ for positive and negative friends

Derivative rules

\[
\begin{align*}
\frac{P_j}{x_i} & \quad \frac{x_i^2 - x_i}{x_i^2} & \quad \frac{x + \overline{x}}{-1} \\
\frac{A + B}{xA + \beta B} & \quad \frac{A}{xA}
\end{align*}
\]
Polynomial calculus resolution (PCR) is similar to other (semi)algebraic proof systems when size is measured, e.g., SOS.

Need better notation than tagging on "R"!?

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 multiplications.

Work in

$$F[x_1, \ldots, x_3]/\langle x_1^2 - x_1, \ldots, x_3^2 - x_3 \rangle$$

We will also do so. From now on all polynomials are considered as elements of $\mathbb{Z}$.

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 $d \Rightarrow$

$\exists$ PC(O(1)) refutation in size $n^{O(d)}$ [CE1996]

This bound is asymptotically tight (in the exponent) in the worst case [Arsi, Lauria, Nordström 96]
THEOREM [Impagliazzo, Rudlak, Yalal'99]

Let refutation size \( S \) (in PC ref) for \( \text{FO}(R) \)
\[ S = \exp \left( \Omega \left( \frac{(D-K)^2}{n} \right) \right) \]

then

so linear degree \( LB \geq \exp \text{size } LB \)

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

But:
- For resolution have well-developed
  machinery to prove width \( LB \)'s [BWS02]
- 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, Pirovani'02]
[Ben-Sasson, Impagliazzo'99/00]

Not so great if \( +1 = -1 \)

Tseitin \( \rightarrow \) Random 3-CNF (from 3-XOR)
Focus of rest of this talk:

- [Heckman, Razborov '03] (at least flexible)
- Characteristic-independent degree LB technique
- Constraint-variable incidence graph
- Random 3-cut

Constraint variable incidence graph

Used in [Galesi, Lauria '10a, '06]
[Miša, Nordstrom '14, 15]

This presentation based on [MN15] ECC TR15-078

Care only about degree - no variables after all

MONOMIAL \( m = \Pi_{i \in \mathcal{I}} x_i \)

TERM \( x^m \) \( m \) monomial \( x \in \mathbb{F} \)

(We will be a bit sloppy in distinguishing)

Ideal \( I = \langle P_1, \ldots, P_k \rangle \) smaller set of polynomials closed under addition and under multiplication by any polynomial

REZK: Always multilinear polynomials
Always mod out \( x_i^2 - x_i \)

Define \textit{ADMISSIBLE ORDERING} of monomials/terms

For simplicity concretely

- \( x_1 < x_2 < \ldots < x_m \)
- \( \deg(m_1) < \deg(m_2) \Rightarrow m_1 < m_2 \)
- For some degree, sort lexicographically
Leading term \( \text{LT}(P) = \text{largest term w.r.t.} \neq 0 \)

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

**FACT**: Any \( P \) can be written uniquely as

\[
P = Q + R, \quad Q \in I
\]

"\( P \) is reduced to \( R \) mod \( I \)" \( R(I)(P) = R \) [NOTATION]

**PC**: Computation in degree-bounded version of ideal = PSEUDO-REAL

Inspired by this, can define PSEUDO-REDUCTION operator \( R^* \) mapping multilinear polynomials to multilinear polynomials. Requirements:

1. \( R^* \) is linear
2. \( R^*(1) \neq 0 \)
3. \( R^*(p_i) = 0 \) for all input polynomials \( p_i \) \[ (*) \]
4. \( R^*(xt) = R^*(x) R^*(t) \) for terms \( t \) w/ \( \deg(t) < d \)

**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 P/I assignment, we could take \( R \) to be the real reduction operator mod this ideal.
(ii) For \( F \) over \( R \), pseudo-expectations as in SOS yield pseudo-reductions. (But "cheat" by mapping everything to \( R \), not \( \mathbb{R}[X] \)).

How to build pseudo-reduction?
Use true reductions modulo ideals, one ideal \( I_t \) per term \( t \).

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

Extend by linearity: \( R^*(p) = \sum_{t \in p} R^*(t) \).

Show that if chosen so that \( R^*(I_t - R^*I_t) \) 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 hardwire example setup from [MN/15] (following and developing [AR/05]).
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 overlap every variable $x_i$ only in few $V_j$. For now, think partition).

Take some polynomials and put in a filter 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

- $P_1, \ldots, P_m$ on left
- $V_1, \ldots, V_n$ on right
- Edge if variable occurs in polynomial $P_j$ in $V_i$.

Assume $|\text{Vars}(P_j)|$ bounded (true, e.g. for $k$-CNF).

Assume that $G$ is an $(\varepsilon, \delta)$-bounded expander: All sets $U \subseteq \Omega, |U| \leq \varepsilon$ have $|\Theta(U)| \geq \delta |U|$ unique neighbors on right-hand side.

(We will also need other conditions on graph, but let us ignore this for now and start doing the proof.)
For term \( t \), look at its neighbourhood \( N(t) \) in \( V \) (all neighbours \( V_i \) if \( t \) would have been left vertex).

Lying flatly, let the support of \( t \) (kept) be largest \( U' \subseteq U \) of size \( \leq s \) such that \( tU' \subseteq N(t) \) plus all \( G \).

Intuition (vague and potentially not true):

- Polynomials in \( U' \) could have been involved in defining polynomials \( t \) in low-degree, because variables in \( N(U') \setminus \delta U' \) could have cancelled.

- But using \( P \in U \setminus U' \) would have left unique-neighbour variables that could not have cancelled.

And we want for free anyway.

How to prove properties of pseudo-reduction?

\( R(1) \) linearity by definition.

\( R(2) \) \( \text{Supp}(1) = \emptyset \) by expansion. \( N(1) = \emptyset \). \( R(2) \) (1) = 1 since \( \emptyset \) is satisfied.

\( R(3) \) \( \mathbf{R^*}(P; j) = 0 \) already interesting case.

What we would like:

Reduce modulo \( \langle N(N(P; j)) \rangle \cdot p_j \rightarrow 0 \).

Want "\( p_j \) reduced modulo ideal containing \( p_j \)."
But \( R^*(P) = \sum_{t \in P} R^{<\text{supp}(t)>}(t) \)

with reduction modulo different ideals.

Idea: Take \( S = \cup \text{supp}(t) \cup \text{supp}(\text{vars}(P)) \)

Show that \( \forall t \in P \) in fact

\[
R^*(t) = R^{<\text{supp}(t)>}(t) = R^{<S>}(t)
\]

Then

\[
R^*(P) = \sum_{t \in P} R^{<S>}(t) = R^{<S>}(P) = 0
\]

Since \( P \subseteq \text{supp}(\text{vars}(P)) \) clearly holds.

But why would this be true?! Let us tackle special case

If \( t \) is irreducible mod \( <\text{supp}(t)> \), then \( t \) irreducible mod \( <\text{supp}(t), P_j> \)

Suppose not. Then

\[
t = S' + Q' + A_j P_j
\]

\[
S' \in <\text{supp}(t)> \quad Q' = <A_i>
\]

But \( \exists v_i \) s.t. \( \forall i; \text{vars}(P_j) \neq \emptyset, \forall i; \text{vars}(t) = \emptyset \) otherwise \( P_j \) would have been in the support. For some reason \( \text{vars}(S') \cap V_i = \emptyset \)
Suppose we could find assignment $f$ to $V_1$ s.t.

- $f(P_1) = 0$
- For all $P_{i+1}, \ldots, P_m \in \mathcal{A}_1$, either $f(P_{i+1}) = 0$ or $P_{i+1}$ left untouched.

Then $t = s_1 + q''$, $q'' \in \langle \mathcal{A} \rangle$
so $t$ was reducible mod $\langle \text{Supp}(s) \rangle$
after all.

Generalizing this, get $R_3 \& R_4$
provided that all edges $P_j - V_i$ in $G$
satisfy condition (f)

Other variants [CAR03]

Graph still expands
No condition on edges
But no $P_i$ has low-degree implications
(i.e. $P_i$ have high immunity)

Different but related $R^*$ operator works
Similar argument.

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

Takes characteristic into account
Open problems

1. PC degree LB for 3-colouring
   known worst-case [Laurent-Nederpalm '17]
   Want average-case like for resolution in
   [Beame, Callahan, Mitchell, Moore '05]

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

3. PC size lower bounds for PHP\(^m\),
   \(m \gg n\) (degree + 1PS99 fails for \(m \geq n^2\))

4. \(\text{Oto-} \text{FPHP}^m\) 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 [Arsentic, Dalmau '08]
   Can we prove monomial space \(\geq\) degree? At least when [AR03] framework establishes
   degree LB?

6. Feasible interpolation for PC? [4 Pillars]

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