Nullstellensatz Proof Systems

Paul Beame
University of Washington
Seattle, WA 98195
Hilbert’s Nullstellensatz

Given multivariate polynomials
\[ Q_1(\bar{x}), \ldots, Q_m(\bar{x}) \in k[x_1, \ldots, x_n] \]
there is no solution to
\[
\begin{align*}
Q_1(\bar{x}) &= 0 \\
\vdots &= \vdots \\
Q_m(\bar{x}) &= 0
\end{align*}
\]
over any extension field of \( k \)
\[ \Leftrightarrow \exists \ P_1(\bar{x}), \ldots, P_m(\bar{x}) \in k[x_1, \ldots, x_n] \]
such that \( \sum_{i=1}^{m} P_i(\bar{x}) \cdot Q_i(\bar{x}) \equiv 1 \)

\( P_1, \ldots, P_m \) are Nullstellensatz refutation of (*)

The degree of the refutation
\[ = \max \text{ degree of } P_i \]

Note: Adding \( x_1^p - x_1, \ldots, x_n^p - x_n \) to the \( Q_i \)'s makes this work for solutions in \( k = GF(p) \).
Nullstellensatz proof systems over $GF(2)$

Refutation systems for Boolean formulas. Introduced in (Beame, Krajíček, Impagliazzo, Pitassi, Pudlák1994).

**Basic Approach:** Given formula $A$, convert $\neg A$ into low degree family of polynomial equations $\{Q_i(\bar{x}) = 0\}_i$ over $GF(2)$, possibly including more variables than in original formula. A proof of $A$ is a family of polynomials $\{P_i\}_i$ over $GF(2)$ such that

$$\sum_i P_i \cdot Q_i \equiv 1 \pmod{\mathcal{I}}$$

where $\mathcal{I}$ is the ideal generated by all $x_j^2 - x_j$, i.e. all exponents are reduced to 1.
Proof systems distinguished by choice of method of converting $\neg A$ to family of low degree polynomials.

For a good proof system, the size to represent the family should be polynomial in the size of $\neg A$.

Suppose $\vec{x} = \{x_1, \ldots, x_n\}$. Given a bound $d$ on the degrees of the $P_i$’s, there are only

$$\sum_{i=0}^{d} \binom{n}{i} = O(n^d)$$

multilinear monomials of degree $\leq d$.

$\Rightarrow$ $P_i$’s may be found by linear algebra in time $n^{O(d)}$, i.e. in polynomial time in # of bits to represent the proof.

$\Rightarrow$ degree $d$ is key size parameter of a proof.
Some conversion methods:

1. (a) Convert $\neg A$ to a 3-CNF formula $A'$ by adding new variables for each subformula of $A$. (as in conversion to apply Resolution.)
   (b) Create variable $x_i$ for each propositional variable $p_i$ in $A'$.
   (c) Add degree-3 equation for each clause in $A'$:

      e.g. $C = (p_1 \lor \overline{p}_2 \lor p_3)$ becomes
        $$(x_1 - 1) \cdot x_2 \cdot (x_3 - 1) = 0.$$ 

2. (a) Convert to CNF but allow long clauses.
   (b) Convert propositional variables $p_i$ to $x_i$ and add new variables $r_{i,j}$ for each occurrence of $p_i$ in clause $C_j$.
   (c) For clause $C_j = (p_1 \lor \overline{p}_2 \lor p_3 \lor \overline{p}_4)$ for example create equation

      $$r_{1,j}x_1 + r_{2,j}(1-x_2) + r_{3,j}x_3 + r_{4,j}(1-x_4) - 1 = 0.$$ 

3. Direct conversion sometimes natural.
**Open Question:** Can Nullstellensatz proof systems efficiently simulate Resolution? Bounded-depth Frege? with Mod$_2$?

**Note:**
(1) Certain reasoning involving mod 2 counting is easy, e.g. natural conversion of Count$_2$ has trivial degree 1 Nullstellensatz proofs.
(2) ’efficiently’ means quasi-polynomial time rather than polynomial size. Since Ind$_n$ expressing induction up to $n$ requires degree $\log_2 n$, $\log^{O(1)} n$ degree bound seems best possible.

**Open Question:** What is largest degree required for an $n$-variable Nullstellensatz refutation over $GF(2)$?

Best known is $\Omega(n^{1/2})$ from (Edmonds 1995). Will give $\Omega(n^{1/4})$ lower bound for refutations of natural conversion of $\neg PHP$ from (Beame, Cook, Edmonds, Impagliazzo, Pitassi 1995).
\( \neg PHP_n^{n+1} \) as an unsatisfiable family of polynomial equations

\( n(n+1) \) variables \( x_{ij}, \ i \in [1, n+1], \ j \in [1, n] \).

For each \( i \in [1, n+1] \):

\[
\sum_{j=1}^{n} x_{ij} - 1 = 0
\]

For each \( i \in [1, n+1], \ j \neq j' \in [1, n] \):

\[
x_{ij} \cdot x_{ij'} = 0
\]

For each \( i \neq i' \in [1, n+1], \ j \in [1, n] \):

\[
x_{ij} \cdot x_{i'j} = 0
\]
Observations:

For $i = 1, \ldots, n$, let

$$Q_i(\vec{x}) = \sum_{j=1}^{n} x_{ij} - 1.$$ 

Other polynomials are simply monomials
⇒ they can be easily cancelled in any equation and their coefficients don’t dominate the degree of any refutation of $\neg PHP^1_n$.

Also,

$$x_{ik} Q_i = x_{ik}^2 - x_{ik} + \sum_{j \neq k} x_{ik} \cdot x_{ij}$$

⇒ $x_{ik}^2 - x_{ik}$ is a degree 1 combination of these equations so no need to add it.
⇒ can work modulo the ideal generated by these polynomials
⇒ wlog all monomials are partial matchings
**Thm:** Any degree $d$ Nullstellensatz refutation of $-PHP^{{n+1}}_n$ over $GF(2)$ must have $\binom{d+2}{2} > n$.

**Proof:** Suppose

$$\sum_{i} P_i(\bar{x}) \cdot Q_i(\bar{x}) = 1 \quad (\ast)$$

and each $P_i$ has degree $\leq d$. Let

$$P_i(x) = \sum_{|\pi| \leq d} \alpha_i^\pi \cdot x_\pi$$

where

$$x_\pi = \prod_{\{j,k\} \in \pi} x_{jk}.$$ 

Equate coefficients of monomials on the two sides of $(\ast)$ to obtain system of linear equations in $\alpha_i^\pi$ for $|\pi| \leq d$.

Equations will have a solution if and only if $(\ast)$ has a solution of degree $\leq d$.

Can further ignore $\alpha_i^\pi$ for $i$ matched by $\pi$ since it has no effect on $(\ast)$. 

9
\(-P_n^{n+1}\) equations and their 'dual'

Write \(i \in \pi\) if vertex \(i\) is matched by \(\pi\),
If \(i \in \pi\) use \(\pi - i\) to denote \(\pi\) with the edge in \(\pi\) touching \(i\) removed.

Let \(E_\pi\) denote coefficient of \(x_\pi\) on left of (\(*\)).

\[
E_\emptyset = 1 : \quad \sum_{i=1}^{n+1} \alpha_\emptyset^i = 1
\]
\[
E_\pi = 0 : \quad \sum_{i \in \pi} \alpha_{\pi-i}^i - \sum_{i \notin \pi} \alpha_\pi^i = 0 \quad 0 \leq |\pi| \leq d + 1
\]

No solution exists if 'dual' has a solution in \(\beta_\pi, |\pi| \leq d + 1\):

\[
E_\emptyset = \sum_{0 < |\pi| \leq d+1} \beta_\pi \cdot E_\pi
\]

Obtain dual equations for each variable \(\alpha_\pi^i\):

\[
\beta_\pi = \sum_{j \notin \pi} \beta_{\pi \cup \{i,j\}}
\]

Claim: Dual solution for exists if \(\left(\frac{d+2}{2}\right) \leq n\).
Uniquely describe solution in $\beta_\pi$ by giving
\[ \{ \pi \mid \beta_\pi = 1 \} \]

**Def:** Let $\mathcal{M}$ be a set of matchings so that all $\pi \in \mathcal{M}$ match $i \in [1, n + 1]$. Define
\[ \mathcal{M} - i = \bigoplus_{\pi \in \mathcal{M}} \{ \pi - i \} \]
where $\bigoplus$ operates like $\cup$ except that it only includes elements that appear in an odd number of its arguments.
Let $dom(M) = \{ i \in [1, N + s] \mid i \in M \}$ be the projection of $M$ onto the first co-ordinate.

**Def:** A $d + 1$-solution to the dual is a set $\mathcal{M}$ of matchings s.t. each $\pi \in \mathcal{M}$ has $|\pi| \leq d + 1$ and
(a) The empty matching $\pi = \emptyset$ is in $\mathcal{M}$,
(b) The sets $\mathcal{M}_S = \{ \pi \in \mathcal{M} \mid dom(\pi) = S \}$ for $S \subset [1, n + 1], |S| \leq d + 1$, satisfy
\[ \mathcal{M}_{S - \{i\}} = \mathcal{M}_S - i. \]
**Def:** Let \([n]^{(k)} \subset [n]^k\) be set of \(k\)-tuples from \([1, n]\) with no repeated elements. For any set \(S \subset [1, n + 1]\), define set of matchings \(\mathcal{M}_S\) by giving a set \(\mathcal{V}_S \subseteq [n]^{(|S|)}\) where each tuple in \(\mathcal{V}_S\) lists the mates of elements of \(S\) in order.

**Example:** For \(S = \{a, b, c\}, \ a < b < c\), \(\mathcal{M}_S\) might be

\[
\begin{bmatrix}
  a & 1 & 3 & 3 & 5 & 2 \\
  b & 2 & 1 & 1 & 4 & 4 \\
  c & 3 & 2 & 4 & 1 & 1 \\
\end{bmatrix}
\]

and \(\mathcal{V}_S\) is the set of columns right of the bar.

We’ll design a solution so that \(\mathcal{V}_S\) only depends on \(k = |S|\). Call this \(\mathcal{V}_k\).
Define

\[ V_0 = () \]
\[ V_1 = (1) \]
\[ V_2 = \begin{pmatrix} 2 & 1 & 2 \\ 1 & 3 & 3 \end{pmatrix} \]
\[ V_3 = \begin{pmatrix} 4 & 4 & 4 & 2 & 1 & 2 & 2 & 1 & 2 & 4 & 4 & 1 & 4 \\ 2 & 1 & 2 & 5 & 5 & 5 & 1 & 3 & 3 & 5 & 1 & 5 & 5 \\ 1 & 3 & 3 & 1 & 3 & 3 & 6 & 6 & 6 & 1 & 6 & 6 & 6 \end{pmatrix} \]

and so on.

Number of elements needed for \( V_k \) is \( \binom{k+1}{2} \).

Define \( V - j \) as analog of \( \mathcal{M}_S - i \).

**Claim:** For every \( j \leq k \), \( V_k - j = V_{k-1} \).

**Cor:** For any \( i \in S \), \( \mathcal{M}_S - i = \mathcal{M}_{S-\{i\}} \)

\( \Box \)