

Algebraic Models of Computation and Interpolation for Algebraic Proof Systems (Pudlák, Sgall)

Sasha Redden and Mikey Baker

McGill University

April 9, 2026

Motivation

In class we used interpolant functions to find lower bounds on split CNF CP proof sizes.

Nullstellensatz (NS) is also an algebraic proof system so can we do something similar here?

Definitions

Labelled matrix: Matrix $\mathbf{A}$ with rows labelled by literals $\ell_i = x_i, 1 - x_i$. Given $\mathbf{A}$ and truth assignment $\vec{u}$, $\mathbf{A}(\vec{u})$ is the matrix consisting of only those rows of $\mathbf{A}$ labelled by literals that are true in assignment $\vec{u}$.

Labelled Matrix Example

$$\mathbf{A} = \begin{matrix} & x_1 & & \\ & 1-x_2 & & \\ & & x_3 & \end{matrix} \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \vec{u} = (1, 1, 0)$$

Then

$$\mathbf{A}(\vec{u}) = [1 \quad 1 \quad 1]$$

Definitions Cont.

Dependency program: Given $\mathbf{A}$, the value on assignment $\vec{u}$ is defined to be 1 if the rows of $\mathbf{A}(\vec{u})$ are linearly independent, and 0 otherwise.

Span program: Given $\mathbf{A}$, the value on assignment $\vec{u}$ is 1 if the vector $\vec{e}^T = (1, 0, \dots, 0)$ is a linear combination of the rows of $\mathbf{A}(\vec{u})$, and 0 otherwise.

Definitions Cont.

Polynomial program (of degree d): A set of polynomials in $K[y_1, \dots, y_m]$, where each polynomial is labelled by a literal (x_i or $1 - x_i$). Given assignment $\vec{u}$, the value of the PP is 1 if there exists a polynomial refutation of degree d from all those vectors that correspond to literal that are true under the assignment $\vec{u}$.

Monotone Polynomial: polynomial $p(\vec{x}, \vec{y})$ is monotone in $\vec{x}$ if it can be represented as $p'(\vec{x})p''(\vec{y})$, where p' is a monomial.

Known Lower Bound on DP Size

Theorem 3.1 (a known lower bound on mDP): Let $f = (x_1 \vee x_2) \wedge (x_3 \vee x_4) \wedge \cdots \wedge (x_{2n-1} \vee x_{2n})$. Then $mDP(f) \geq 2^n/n$ (for an arbitrary field.)

P-Simulation Interlude

Theorem 3.9 Polynomial programs of constant degree $d \geq 2$ over a finite field and boolean circuits mutually simulate each other. Monotone polynomial programs over a finite field simulate monotone circuits

So ... what? Since NS is a polynomial proof system, lower bounds on circuit size can be used to form lower bounds on proof size.

Question: How to correspond between an NS proof and a boolean circuit?

Statement of Main Result

Theorem 4.2 Suppose a set of polynomial equations of the form $p_s(\vec{x}, \vec{y}) = 0$, $q_t(\vec{x}, \vec{z}) = 0$ has a NS refutation of constant degree d . Then there exists a span program $\mathbf{C}$ with the property that if $\mathbf{C}$ accepts $\vec{u} \in \{0, 1\}^n$, then $p_s(\vec{x}, \vec{y}) = 0$ is not satisfiable, and if $\mathbf{C}$ does not accept, then $q_t(\vec{x}, \vec{z}) = 0$ is not satisfiable. The size of $\mathbf{C}$ is polynomial in the number of variables $\vec{x}, \vec{y}$. Moreover, if all $p_s(\vec{x}, \vec{y})$ are monotone in $\vec{x}$, then $\mathbf{C}$ is monotone.

Remember! $\mathbf{C}$ accepts $\vec{u}$ if $\vec{e} \in \text{span}(\mathbf{C}(\vec{u}))$

Part (I) of the proof

Suppose all p_s are o.t.f $x_i p'(\vec{y}) + p''(\vec{y})$, and further that $\forall i : x_i^2 - x_i = 0$. Now gather all the polynomials containing x_i :

$$x_i p'_{i,j} + p''_{i,j} \quad \forall j = 1, \dots, k_i$$

The columns of $\mathbf{C}$ are all of the monomials in $\vec{y}$ of $\deg \leq d$ so the size is polynomial in the number of variables.

Part (I) of the proof (continued)

The rows of $\mathbf{C}$ are coefficients of polynomials and come in three forms with corresponding labels:

Polynomial Form	Label
$r(\vec{y})p'_{i,j}(\vec{y}) + p''_{i,j}(\vec{y})$	x_i
$r(\vec{y})p''_{i,j}(\vec{y})$	$(1 - x_i)$
$r(\vec{y})p(\vec{y})$	1

This span program tests if for a given $\vec{u}$, there is a degree d NS refutation of $p_s(\vec{u}, \vec{y}) = 0$

Helpfully, if p_s are monotone then $\forall i, j : p''_{i,j} = 0$ so $\mathbf{C}$ is monotone.

Part (II) of the proof

For each variable x_i in each initial polynomial, introduce a new variable w_i . Then replace all polynomials $p_s(\vec{x}, \vec{y})$ with $p_s(\vec{w}, \vec{y})$, and for all x_i , add polynomials $x_i - w_i$.

Now consider the monotone case (i.e. all $p_s(\vec{x}, \vec{y})$ are monotone in $\vec{x}$), then $p_s(\vec{x}, \vec{y})$ has the form $x_{j_1} \dots x_{j_k} k p(\vec{y})$. Now if $k \geq 2$, replace $p_s(\vec{x}, \vec{y})$ with k polynomials

$$x_1(p(\vec{y}) + w_2 + \dots + w_k), x_2 w_2, \dots, x_k w_k$$

The new system of equations can derive the old using a degree at most one larger than the degree of the original polynomials.

Its Tight?!

Theorem 4.4 Let $\mathbf{A}$ be a span program of size m for inputs of size n . Then there are equations $p_s(\vec{x}, \vec{y}) = 0, q_t(\vec{x}, \vec{z}) = 0$ of degree 2 with $O(nm)$ variables which have a NS refutation proof of degree 3 and whose unique interpolant is the boolean function computed by $\mathbf{A}$.

This theorem is the converse to Theorem 4.2, showing that we cannot reduce the class of interpolating functions any further (every span program is a unique interpolant for some tautology provable by NS system.)

Open Problems: Lower bounds (I)

Monotone polynomial programs and polynomial calculus:

Lower bounds for monotone polynomial programs over finite field (for a suitable function) would also prove a lower bound for polynomial calculus by the interpolation theorem (Theorem 4.3)

Open Problems: Lower bounds (II)

Non-monotone span programs: Proving a superpolynomial lower bound on non-monotone span programs would also imply a lower bound on branching programs.

Open Problems: Lower bounds (III)

Better lower bounds for monotone span programs: No exponential lower bounds are known for monotone span programs, the best known is $n^{\Omega(\log n / \log \log n)}$.

Thank you for listening :D

