A comparison of algebraic and semi-algebraic proof systems

Christoph Berkholz

Humboldt-Universität zu Berlin

22.10.2019

Proof systems

Proof systems

A proof system for a language $L \subseteq \Sigma^*$ is a relation $R \subseteq \Sigma^* \times \Sigma^*$ between words $w \in L$ and proofs p such that:

- (correct) $(w, p) \in R \implies w \in L$
- (complete) for all $w \in L$ ex. $p \in \Sigma^*$ with $(w, p) \in R$
- (verifiable) R is decidable in polynomial time

Proof systems

A proof system for a language $L \subseteq \Sigma^*$ is a relation $R \subseteq \Sigma^* \times \Sigma^*$ between words $w \in L$ and proofs p such that:

- (correct) $(w, p) \in R \implies w \in L$
- (complete) for all $w \in L$ ex. $p \in \Sigma^*$ with $(w, p) \in R$
- (verifiable) R is decidable in polynomial time

A proof system is p-bounded, if

- for all $w \in L$ ex. $p \in \Sigma^*$ with $(w, p) \in R$ and $|p| = \text{poly}(|w|)$

Proof systems

A proof system for a language $L \subseteq \Sigma^*$ is a relation $R \subseteq \Sigma^* \times \Sigma^*$ between words $w \in L$ and proofs p such that:

- (correct) $(w, p) \in R \implies w \in L$
- (complete) for all $w \in L$ ex. $p \in \Sigma^*$ with $(w, p) \in R$
- (verifiable) R is decidable in polynomial time

A proof system is p-bounded, if

- for all $w \in L$ ex. $p \in \Sigma^*$ with $(w, p) \in R$ and $|p| = \text{poly}(|w|)$

Theorem ([Cook, Reckhow 1979])

There is a p-bounded proof system for UNSAT $\Leftrightarrow$ NP = co-NP.

Proof systems

A proof system for a language $L \subseteq \Sigma^*$ is a relation $R \subseteq \Sigma^* \times \Sigma^*$ between words $w \in L$ and proofs p such that:

- (correct) $(w, p) \in R \implies w \in L$
- (complete) for all $w \in L$ ex. $p \in \Sigma^*$ with $(w, p) \in R$
- (verifiable) R is decidable in polynomial time

A proof system is p-bounded, if

- for all $w \in L$ ex. $p \in \Sigma^*$ with $(w, p) \in R$ and $|p| = \mathrm{poly}(|w|)$

Theorem ([Cook, Reckhow 1979])

There is a p-bounded proof system for UNSAT $\Leftrightarrow$ NP = co-NP.

Definition

A proof system Q polynomially simulates R, if for every $(w, p) \in R$ there is $(w, p') \in Q$ such that $p' = \mathrm{poly}(|p|)$.

Proof systems for UNSAT (= refutation systems for SAT)

Systems for proving the unsatisfiability of a CNF formula.

- Truth table

Proof systems for UNSAT (= refutation systems for SAT)

Systems for proving the unsatisfiability of a CNF formula.

- Truth table
- Resolution (on clauses C, D)

$$\frac{C \vee x \quad D \vee \neg x}{C \vee D}$$

Proof systems for UNSAT (= refutation systems for SAT)

Systems for proving the unsatisfiability of a CNF formula.

- Truth table
- Resolution (on clauses C, D)

$$\frac{C \vee x \quad D \vee \neg x}{C \vee D}$$

- Frege (Schoenfield's system on formulas φ, ψ, η over $\{\vee, \neg\}$):

$$\frac{}{\varphi \vee \neg\varphi} \qquad \frac{\varphi}{\varphi \vee \psi} \qquad \frac{\varphi \vee \varphi}{\varphi} \qquad \frac{\varphi \vee (\psi \vee \eta)}{(\varphi \vee \psi) \vee \eta} \qquad \frac{\varphi \vee \psi \quad \neg\psi \vee \eta}{\varphi \vee \eta}$$

Proof systems for UNSAT (= refutation systems for SAT)

Systems for proving the unsatisfiability of a CNF formula.

- Truth table
- Resolution (on clauses C, D)

$$\frac{C \vee x \quad D \vee \neg x}{C \vee D}$$

- Frege (Schoenfield's system on formulas φ, ψ, η over $\{\vee, \neg\}$):

$$\frac{}{\varphi \vee \neg\varphi} \qquad \frac{\varphi}{\varphi \vee \psi} \qquad \frac{\varphi \vee \varphi}{\varphi} \qquad \frac{\varphi \vee (\psi \vee \eta)}{(\varphi \vee \psi) \vee \eta} \qquad \frac{\varphi \vee \psi \quad \neg\psi \vee \eta}{\varphi \vee \eta}$$

Any two complete Frege Systems polynomially simulate each other [Reckhow 1975]

Proof systems for UNSAT (= refutation systems for SAT)

Systems for proving the unsatisfiability of a CNF formula.

- Truth table
- Resolution (on clauses C, D)

$$\frac{C \vee x \quad D \vee \neg x}{C \vee D}$$

- Frege (Schoenfield's system on formulas φ, ψ, η over $\{\vee, \neg\}$):

$$\frac{}{\varphi \vee \neg\varphi} \qquad \frac{\varphi}{\varphi \vee \psi} \qquad \frac{\varphi \vee \varphi}{\varphi} \qquad \frac{\varphi \vee (\psi \vee \eta)}{(\varphi \vee \psi) \vee \eta} \qquad \frac{\varphi \vee \psi \quad \neg\psi \vee \eta}{\varphi \vee \eta}$$

  Any two complete Frege Systems polynomially simulate each other [Reckhow 1975]

- Extended Frege (additionally abbreviation by fresh variables x):

$$\frac{}{x \leftrightarrow \varphi}$$

Algebraic and semi-algebraic proof systems

Algebraic proof systems reason about polynomial equations over some field $\mathbb{F}$.

Algebraic and semi-algebraic proof systems

Algebraic proof systems reason about polynomial equations over some field $\mathbb{F}$.

Semi-algebraic proof systems reason about polynomial inequalities and equations over $\mathbb{R}$.

Algebraic and semi-algebraic proof systems

Algebraic proof systems reason about polynomial equations over some field $\mathbb{F}$.

Semi-algebraic proof systems reason about polynomial inequalities and equations over $\mathbb{R}$.

In this talk

- Systems of polynomial equations over $\mathbb{R}$.

Algebraic and semi-algebraic proof systems

Algebraic proof systems reason about polynomial equations over some field $\mathbb{F}$.

Semi-algebraic proof systems reason about polynomial inequalities and equations over $\mathbb{R}$.

In this talk

- Systems of polynomial equations over $\mathbb{R}$.
- Polynomials represented as a linear combination of monomials.

Algebraic and semi-algebraic proof systems

Algebraic proof systems reason about polynomial equations over some field $\mathbb{F}$.

Semi-algebraic proof systems reason about polynomial inequalities and equations over $\mathbb{R}$.

In this talk

- Systems of polynomial equations over $\mathbb{R}$.
- Polynomials represented as a linear combination of monomials.
- The Boolean axioms $x^2 = x$ are always present.

Systems of multivariate polynomial equations

We compare methods for solving systems of real polynomial equations over Boolean variables $x_1, \ldots, x_n$.

Generalises satisfiability for CNFs:

Systems of multivariate polynomial equations

We compare methods for solving systems of real polynomial equations over Boolean variables $x_1, \ldots, x_n$.

Generalises satisfiability for CNFs:

$$
\begin{aligned}
x_1 &= 0 &\quad \leftsquigarrow \quad& \overline{x_1} \\
1 - x_2 &= 0 &\quad \leftsquigarrow \quad& x_2 \\
(1 - x_1)x_2(1 - x_3) &= 0 &\quad \leftsquigarrow \quad& x_1 \vee \overline{x_2} \vee x_3
\end{aligned}
$$

$$
\begin{aligned}
\text{for all clauses } C: \quad f_C &= 0 &\quad \leftsquigarrow \quad& C \\
\text{for } i \in [n]: \quad x_i^2 - x_i &= 0 & &
\end{aligned}
$$

Nullstellensatz

A system $f_1(x_1, \dots, x_n) = 0, \dots, f_m(x_1, \dots, x_n) = 0$ of real polynomial equations has no 0/1-solution

$$\iff$$

there are polynomials g_i, q_j such that

$$\sum_{i=1}^{m} g_i f_i + \sum_{j=1}^{n} q_j(x_j^2 - x_j) \; = \; -1.$$

Nullstellensatz

A system $f_1(x_1, \ldots, x_n) = 0, \ \ldots, \ f_m(x_1, \ldots, x_n) = 0$ of real polynomial equations has no 0/1-solution

$$\iff$$

there are polynomials g_i, q_j such that

$$\sum_{i=1}^{m} g_i f_i + \sum_{j=1}^{n} q_j (x_j^2 - x_j) \ = \ -1.$$

- The degree of a Nullstellensatz refutation is maximum degree of $g_i f_i$ and $q_j(x_j^2 - x_j)$.

Nullstellensatz

A system $f_1(x_1, \ldots, x_n) = 0, \ \ldots, \ f_m(x_1, \ldots, x_n) = 0$ of real polynomial equations has no 0/1-solution

$$\Longleftrightarrow$$

there are polynomials g_i, q_j such that

$$\sum_{i=1}^{m} g_i f_i + \sum_{j=1}^{n} q_j(x_j^2 - x_j) \ = \ -1.$$

- The degree of a Nullstellensatz refutation is maximum degree of $g_i f_i$ and $q_j(x_j^2 - x_j)$.
- Refutations of degree d can be found in time $n^{O(d)}$ by solving a system of linear equations.

Sherali-Adams

A system $f_1(x_1, \dots, x_n) = 0, \dots, f_m(x_1, \dots, x_n) = 0$ of real polynomial equations has no 0/1-solution

$$\iff$$

there are polynomials g_i, q_j, p such that

$$\sum_{i=1}^{m} g_i f_i + \sum_{j=1}^{n} q_j(x_j^2 - x_j) + p \;=\; -1,$$

where $p = \sum_{A,B\subseteq[n]} a_{A,B} \cdot \left(\prod_{j\in A} x_j \prod_{j\in B}(1 - x_j)\right)$ with $a_{A,B} \geq 0$.

Sherali-Adams

A system $f_1(x_1, \dots, x_n) = 0, \dots, f_m(x_1, \dots, x_n) = 0$ of real polynomial equations has no 0/1-solution

$$\Longleftrightarrow$$

there are polynomials g_i, q_j, p such that

$$\sum_{i=1}^{m} g_i f_i + \sum_{j=1}^{n} q_j(x_j^2 - x_j) + p \;=\; -1,$$

where $p = \sum_{A,B \subseteq [n]} a_{A,B} \cdot \left(\prod_{j \in A} x_j \prod_{j \in B} (1 - x_j) \right)$ with $a_{A,B} \geq 0$.

- The degree of a Sherali-Adams refutation is maximum degree of $g_i f_i$, $q_j(x_j^2 - x_j)$ and p.
- Refutations of degree d can be found in time $n^{O(d)}$ by solving a linear programme.

Sum-of-squares

A system $f_1(x_1, \dots, x_n) = 0, \ \dots, \ f_m(x_1, \dots, x_n) = 0$ of real polynomial equations has no 0/1-solution

$$\Longleftrightarrow$$

there are polynomials g_i, q_j, p such that

$$\sum_{i=1}^{m} g_i f_i + \sum_{j=1}^{n} q_j (x_j^2 - x_j) + p \ = \ -1,$$

where $p = \sum_\ell (p_\ell)^2$ is a sum of squared polynomials.

Sum-of-squares

A system $f_1(x_1, \ldots, x_n) = 0$, ..., $f_m(x_1, \ldots, x_n) = 0$ of real polynomial equations has no 0/1-solution

$$\Longleftrightarrow$$

there are polynomials g_i, q_j, p such that

$$\sum_{i=1}^{m} g_i f_i + \sum_{j=1}^{n} q_j (x_j^2 - x_j) + p \; = \; -1,$$

where $p = \sum_\ell (p_\ell)^2$ is a sum of squared polynomials.

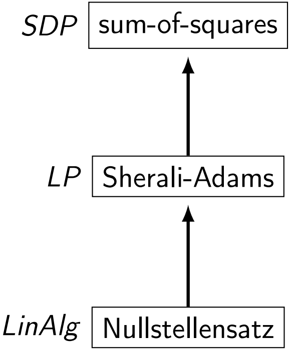
- The degree of a sum-of-squares refutation is maximum degree of $g_i f_i$, $q_j(x_j^2 - x_j)$ and p.
- Refutations of degree d can be found (in time $n^{O(d)}$)$^{*)}$ by solving a semidefinite programme.

$*$) if the bit-length of the coefficients is bounded by $n^{O(d)}$ (not always the case [RW17])

(Semi-)algebraic proof systems

Static systems

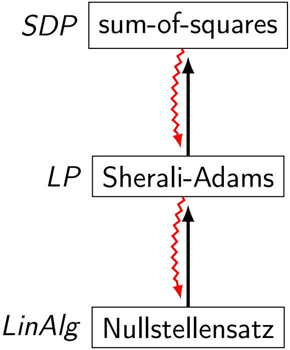
$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -1$



(Semi-)algebraic proof systems

Static systems

$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -1$



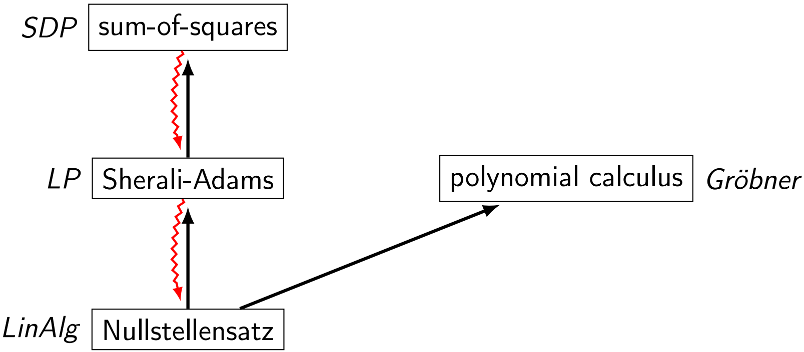
(Semi-)algebraic proof systems

Static systems

$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -1$

Derivation systems

$\frac{g=0 \qquad f=0}{ag+bf=0}$



Polynomial calculus

Polynomial calculus is a derivation system for polynomials.

$$\frac{}{f_i} \qquad \frac{}{x_j^2 - x_j} \qquad \frac{g \qquad f}{ag + bf} \qquad \frac{f}{x_j f}$$

$f_i = 0$ axiom; x_j variable; f, g, h polynomials; $a, b \in \mathbb{R}$.

Polynomial calculus

Polynomial calculus is a derivation system for polynomials.

$$\frac{}{f_i} \qquad \frac{}{x_j^2 - x_j} \qquad \frac{g \qquad f}{ag + bf} \qquad \frac{f}{x_j f}$$

$f_i = 0$ axiom; x_j variable; f, g, h polynomials; $a, b \in \mathbb{R}$.

- Goal: derive -1 (the contradiction $-1 = 0$).

Polynomial calculus

Polynomial calculus is a derivation system for polynomials.

$$\frac{}{f_i} \qquad \frac{}{x_j^2 - x_j} \qquad \frac{g \qquad f}{ag + bf} \qquad \frac{f}{x_j f}$$

$f_i = 0$ axiom; x_j variable; f, g, h polynomials; $a, b \in \mathbb{R}$.

- Goal: derive -1 (the contradiction $-1 = 0$).
- The degree is the maximum degree of every polynomial in the derivation.

Polynomial calculus

Polynomial calculus is a derivation system for polynomials.

$$\frac{}{f_i} \qquad \frac{}{x_j^2 - x_j} \qquad \frac{g \qquad f}{ag + bf} \qquad \frac{f}{x_j f}$$

$f_i = 0$ axiom; x_j variable; f, g, h polynomials; $a, b \in \mathbb{R}$.

- Goal: derive -1 (the contradiction $-1 = 0$).
- The degree is the maximum degree of every polynomial in the derivation.
- Refutations of degree d can be found in time $n^{O(d)}$ by a bounded degree variant of the Gröbner Basis Algorithm.

Polynomial calculus

Polynomial calculus is a derivation system for polynomials.

$$\frac{}{f_i} \qquad \frac{}{x_j^2 - x_j} \qquad \frac{g \qquad f}{ag + bf} \qquad \frac{f}{x_j f}$$

$f_i = 0$ axiom; x_j variable; f, g, h polynomials; $a, b \in \mathbb{R}$.

- Goal: derive -1 (the contradiction $-1 = 0$).
- The degree is the maximum degree of every polynomial in the derivation.
- Refutations of degree d can be found in time $n^{O(d)}$ by a bounded degree variant of the Gröbner Basis Algorithm.
- Extends Nullstellensatz: derive $\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j)$

Polynomial calculus simulates resolution

Resolution (slightly unusual version)

Weakening: $\dfrac{C}{C \vee x}, \quad \dfrac{C}{C \vee \overline{x}}$ Resolution: $\dfrac{C \vee x \qquad C \vee \overline{x}}{C}$

(translating to this special form increases width by at most one and length by a constant factor)

Polynomial calculus simulates resolution

Resolution (slightly unusual version)

Weakening: $\dfrac{C}{C \vee x}, \quad \dfrac{C}{C \vee \overline{x}}$ Resolution: $\dfrac{C \vee x \qquad C \vee \overline{x}}{C}$

(translating to this special form increases width by at most one and length by a constant factor)

Observation

Width-d resolution refutation $\Longrightarrow$ degree-d PC refutation.

Reminder: $f_{x_1 \vee \overline{x_2} \vee x_3} = (1 - x_1)x_2(1 - x_3)$

Polynomial calculus simulates resolution

Resolution (slightly unusual version)

Weakening: $\dfrac{C}{C \vee x}, \quad \dfrac{C}{C \vee \overline{x}}$ Resolution: $\dfrac{C \vee x \qquad C \vee \overline{x}}{C}$

(translating to this special form increases width by at most one and length by a constant factor)

Observation

Width-d resolution refutation $\Longrightarrow$ degree-d PC refutation.

Reminder: $f_{x_1 \vee \overline{x_2} \vee x_3} = (1 - x_1)x_2(1 - x_3)$

- Simulation of weakening by multiplication (and lin. comb.):

$$\frac{f_C}{f_C \cdot (1 - x)}, \quad \frac{f_C}{f_C \cdot x}$$

- Simulation of resolution rule by addition:

$$\frac{f_C \cdot x \qquad f_C \cdot (1 - x)}{f_C}$$

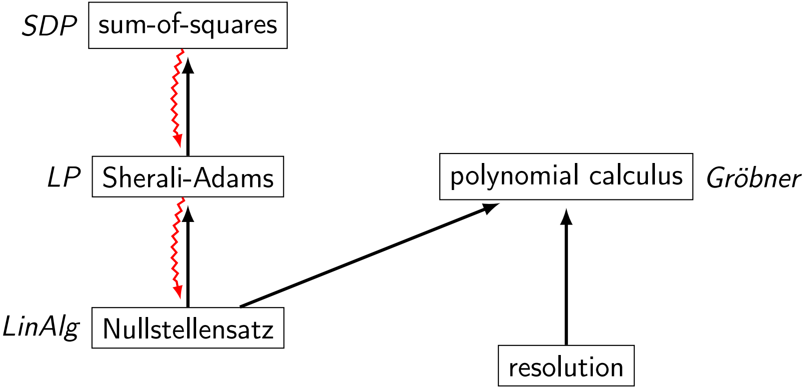
(Semi-)algebraic proof systems

Static systems

$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -1$

Derivation systems

$\frac{g=0 \qquad f=0}{ag+bf=0}$



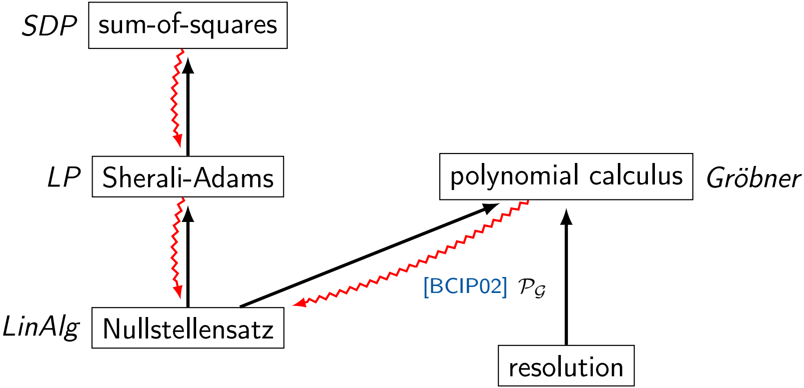
(Semi-)algebraic proof systems

Static systems

$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -1$

Derivation systems

$\frac{g=0 \qquad f=0}{ag+bf=0}$



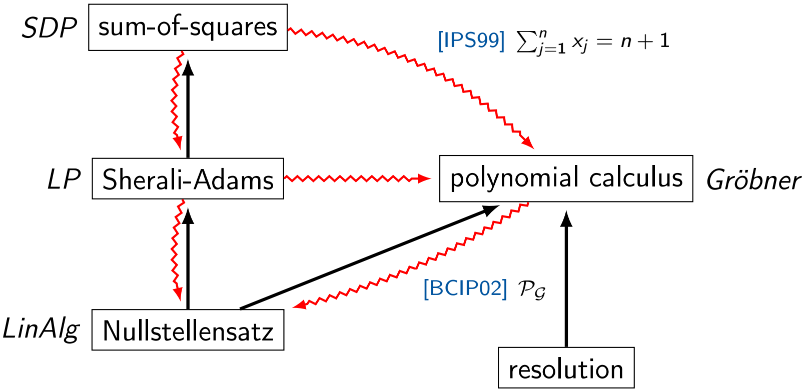
(Semi-)algebraic proof systems

Static systems

$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -1$

Derivation systems

$\frac{g=0 \qquad f=0}{ag+bf=0}$



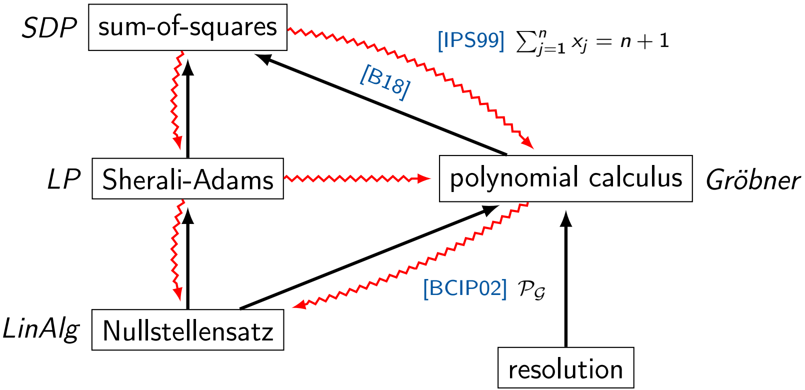
(Semi-)algebraic proof systems

Static systems

$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -1$

Derivation systems

$\frac{g=0 \qquad f=0}{ag+bf=0}$



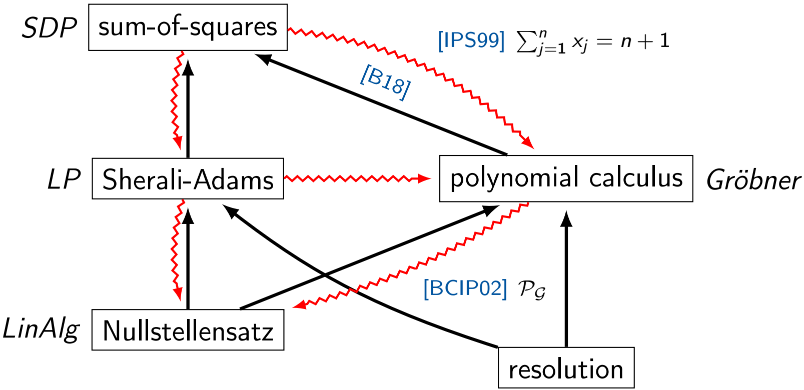
(Semi-)algebraic proof systems

Static systems

$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -1$

Derivation systems

$\frac{g=0 \qquad f=0}{ag+bf=0}$



Sherali-Adams simulates resolution

Theorem [DMR09]

If $\Gamma = \{C_1, \ldots, C_m\}$ has a resolution refutation of width d, then $\mathcal{F} = \{f_{C_1} = 0, \ldots, f_{C_m} = 0\}$ has a Sherali-Adams refutation of degree d.

Sherali-Adams simulates resolution

Theorem [DMR09]

If $\Gamma = \{C_1, \ldots, C_m\}$ has a resolution refutation of width d, then $\mathcal{F} = \{f_{C_1} = 0, \ldots, f_{C_m} = 0\}$ has a Sherali-Adams refutation of degree d.

Notation

A Sherali-Adams proof of $f \geq 0$ from $\mathcal{F}$ is the expression

$$\sum_i g_i f_i + \sum_j q_j (x_j^2 - x_j) + p = f.$$

where $p = \sum_{A,B \subseteq [n]} a_{A,B} \cdot \left(\prod_{j \in A} x_j \prod_{j \in B} (1 - x_j) \right)$ with $a_{A,B} \geq 0$.

Sherali-Adams simulates resolution

Theorem [DMR09]

If $\Gamma = \{C_1, \ldots, C_m\}$ has a resolution refutation of width d, then $\mathcal{F} = \{f_{C_1} = 0, \ldots, f_{C_m} = 0\}$ has a Sherali-Adams refutation of degree d.

Notation

A Sherali-Adams proof of $f \geq 0$ from $\mathcal{F}$ is the expression

$$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = f.$$

where $p = \sum_{A,B \subseteq [n]} a_{A,B} \cdot \left(\prod_{j \in A} x_j \prod_{j \in B}(1 - x_j)\right)$ with $a_{A,B} \geq 0$.

Inductive lemma

If C has a width-d resolution derivation from Γ,
then $-f_C \geq 0$ has a degree-d Sherali-Adams proof from $\mathcal{F}$.

Sherali-Adams simulates resolution

Proof of the inductive lemma

Resolution rule: $\dfrac{C \vee x \qquad C \vee \overline{x}}{C}$

Sherali-Adams simulates resolution

Proof of the inductive lemma

Resolution rule: $\frac{C \vee x \qquad C \vee \overline{x}}{C}$

$$\sum_i g_i' f_i + \sum_j q_j'(x_j^2 - x_j) + p' = -x \cdot f_C$$
$$\sum_i g_i'' f_i + \sum_j q_j''(x_j^2 - x_j) + p'' = -(1 - x) \cdot f_C$$

Sherali-Adams simulates resolution

Proof of the inductive lemma

Resolution rule: $\frac{C \vee x \qquad C \vee \overline{x}}{C}$

$$\sum_i g_i' f_i + \sum_j q_j'(x_j^2 - x_j) + p' = -x \cdot f_C$$

$$\sum_i g_i'' f_i + \sum_j q_j''(x_j^2 - x_j) + p'' = -(1 - x) \cdot f_C$$

adding these proofs yields:

$$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -f_C$$

Sherali-Adams simulates resolution

Proof of the inductive lemma

Resolution rule: $\frac{C \vee x \qquad C \vee \overline{x}}{C}$

$$\textstyle\sum_i g_i' f_i + \sum_j q_j'(x_j^2 - x_j) + p' = -x \cdot f_C$$

$$\textstyle\sum_i g_i'' f_i + \sum_j q_j''(x_j^2 - x_j) + p'' = -(1-x) \cdot f_C$$

adding these proofs yields:

$$\textstyle\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -f_C$$

Weakening rule: $\frac{C}{C \vee \overline{x}}$ or $\frac{C}{C \vee x}$

Sherali-Adams simulates resolution

Proof of the inductive lemma

Resolution rule: $\dfrac{C \vee x \qquad C \vee \overline{x}}{C}$

$$\sum_i g_i' f_i + \sum_j q_j'(x_j^2 - x_j) + p' = -x \cdot f_C$$

$$\sum_i g_i'' f_i + \sum_j q_j''(x_j^2 - x_j) + p'' = -(1 - x) \cdot f_C$$

adding these proofs yields:

$$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -f_C$$

Weakening rule: $\frac{C}{C \vee \overline{x}}$ or $\frac{C}{C \vee x}$

$$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p \qquad = -f_C$$

Sherali-Adams simulates resolution

Proof of the inductive lemma

Resolution rule: $\frac{C \vee x \qquad C \vee \overline{x}}{C}$

$$\sum_i g_i' f_i + \sum_j q_j'(x_j^2 - x_j) + p' = -x \cdot f_C$$

$$\sum_i g_i'' f_i + \sum_j q_j''(x_j^2 - x_j) + p'' = -(1 - x) \cdot f_C$$

adding these proofs yields:

$$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -f_C$$

Weakening rule: $\frac{C}{C \vee \overline{x}}$ or $\frac{C}{C \vee x}$

$$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p + (1 - x)f_C \quad = -f_C + (1 - x)f_C$$

Sherali-Adams simulates resolution

Proof of the inductive lemma

Resolution rule: $\frac{C \vee x \qquad C \vee \overline{x}}{C}$

$$\textstyle\sum_i g_i' f_i + \sum_j q_j'(x_j^2 - x_j) + p' = -x \cdot f_C$$
$$\textstyle\sum_i g_i'' f_i + \sum_j q_j''(x_j^2 - x_j) + p'' = -(1 - x) \cdot f_C$$

adding these proofs yields:

$$\textstyle\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -f_C$$

Weakening rule: $\frac{C}{C \vee \overline{x}}$ or $\frac{C}{C \vee x}$

$$\textstyle\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p + (1 - x)f_C \quad = -f_C + (1 - x)f_C = -xf_C$$

Sherali-Adams simulates resolution

Proof of the inductive lemma

Resolution rule: $\frac{C \vee x \qquad C \vee \overline{x}}{C}$

$$\sum_i g'_i f_i + \sum_j q'_j(x_j^2 - x_j) + p' = -x \cdot f_C$$
$$\sum_i g''_i f_i + \sum_j q''_j(x_j^2 - x_j) + p'' = -(1 - x) \cdot f_C$$

adding these proofs yields:

$$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -f_C$$

Weakening rule: $\frac{C}{C \vee \overline{x}}$ or $\frac{C}{C \vee x}$

$$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p + (1 - x)f_C \quad = -f_C + (1 - x)f_C = -xf_C$$
$$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p + xf_C \quad = -f_C + xf_C = -(1 - x)f_C$$

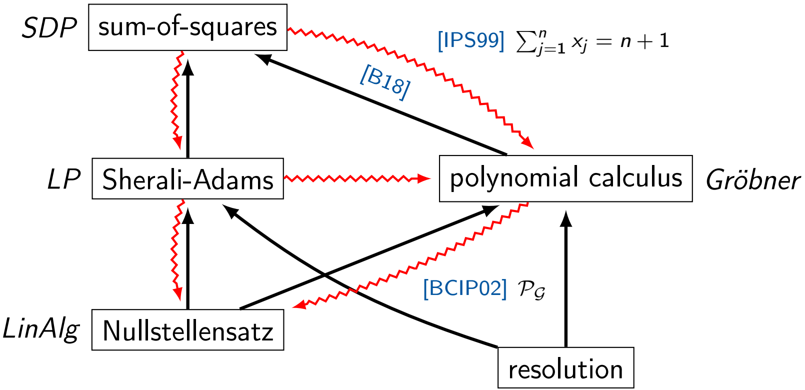
(Semi-)algebraic proof systems

Static systems

$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -1$

Derivation systems

$\frac{g=0 \qquad f=0}{ag+bf=0}$



Sum-of-squares simulates polynomial calculus

Theorem [B18]

If $F = \{ f_1 = 0, \ldots, f_m = 0 \}$ has a polynomial calculus refutation of degree d, then it has a sum-of-squares refutation of degree $2d$.

Notation

A sum-of-squares proof of $f \geq 0$ from F is the expression

$$\sum_i g_i f_i + \sum_j q_j (x_j^2 - x_j) + \sum_\ell (p_\ell)^2 = f .$$

Inductive lemma

If f has a degree-d polynomial calculus derivation from F, then $-f^2 \geq 0$ has a degree-$2d$ sum-of-squares proof from F.

Sum-of-squares simulates polynomial calculus

Proof of the inductive lemma

Inductive lemma

If f has a degree-d polynomial calculus derivation from F, then $-f^2 \geq 0$ has a degree-$2d$ sum-of-squares proof from F.

Proof.

Sum-of-squares simulates polynomial calculus

Proof of the inductive lemma

Inductive lemma

If f has a degree-d polynomial calculus derivation from F, then $-f^2 \geq 0$ has a degree-$2d$ sum-of-squares proof from F.

Proof.

Axioms $f = f_i$ and $f = x_j^2 - x_j$ multiplied by $-f$ to derive $-f^2$.

Sum-of-squares simulates polynomial calculus
Proof of the inductive lemma

Inductive lemma
If f has a degree-d polynomial calculus derivation from F,
then $-f^2 \geq 0$ has a degree-$2d$ sum-of-squares proof from F.

Proof.
Linear combination: $\frac{g \qquad h}{ag+bh}$ $\quad f = ag + bh \quad -f^2 = -(ag+bh)^2$

Sum-of-squares simulates polynomial calculus

Proof of the inductive lemma

Inductive lemma

If f has a degree-d polynomial calculus derivation from F, then $-f^2 \geq 0$ has a degree-$2d$ sum-of-squares proof from F.

Proof.

Linear combination: $\frac{g \qquad h}{ag+bh}$ $\quad f = ag + bh \quad -f^2 = -(ag+bh)^2$

$$\sum_i g_i' f_i + \sum_j q_j'(x_j^2 - x_j) + \sum_\ell (p_\ell')^2 = -g^2$$
$$\sum_i g_i'' f_i + \sum_j q_j''(x_j^2 - x_j) + \sum_\ell (p_\ell'')^2 = -h^2$$

Sum-of-squares simulates polynomial calculus

Proof of the inductive lemma

Inductive lemma

If f has a degree-d polynomial calculus derivation from F,
then $-f^2 \geq 0$ has a degree-$2d$ sum-of-squares proof from F.

Proof.

Linear combination: $\frac{g \qquad h}{ag+bh}$ $\quad f = ag + bh \quad -f^2 = -(ag+bh)^2$

$$2a^2\big(\textstyle\sum_i g_i' f_i + \sum_j q_j'(x_j^2 - x_j) + \sum_\ell (p_\ell')^2\big) = 2a^2(-g^2)$$
$$2b^2\big(\textstyle\sum_i g_i'' f_i + \sum_j q_j''(x_j^2 - x_j) + \sum_\ell (p_\ell'')^2\big) = 2b^2(-h^2)$$

Sum-of-squares simulates polynomial calculus

Proof of the inductive lemma

Inductive lemma

If f has a degree-d polynomial calculus derivation from F,
then $-f^2 \geq 0$ has a degree-$2d$ sum-of-squares proof from F.

Proof.

Linear combination: $\frac{g \qquad h}{ag+bh}$ $\quad f = ag + bh \quad -f^2 = -(ag+bh)^2$

$$\sum_i \hat{g}_i' f_i + \sum_j \hat{q}_j'(x_j^2 - x_j) + \sum_\ell (\hat{p}_\ell')^2 = -2(ag)^2$$
$$\sum_i \hat{g}_i'' f_i + \sum_j \hat{q}_j''(x_j^2 - x_j) + \sum_\ell (\hat{p}_\ell'')^2 = -2(bh)^2$$

Sum-of-squares simulates polynomial calculus

Proof of the inductive lemma

Inductive lemma

If f has a degree-d polynomial calculus derivation from F,
then $-f^2 \geq 0$ has a degree-$2d$ sum-of-squares proof from F.

Proof.

Linear combination: $\frac{g \qquad h}{ag+bh}$ $\quad f = ag + bh \quad -f^2 = -(ag+bh)^2$

$$\sum_i \hat{g}_i' f_i + \sum_j \hat{q}_j'(x_j^2 - x_j) + \sum_\ell (\hat{p}_\ell')^2 = -2(ag)^2$$

$$\sum_i \hat{g}_i'' f_i + \sum_j \hat{q}_j''(x_j^2 - x_j) + \sum_\ell (\hat{p}_\ell'')^2 = -2(bh)^2$$

$$(ag - bh)^2 = (ag)^2 - 2ag\,bh + (bh)^2$$

Sum-of-squares simulates polynomial calculus

Proof of the inductive lemma

Inductive lemma

If f has a degree-d polynomial calculus derivation from F,
then $-f^2 \geq 0$ has a degree-$2d$ sum-of-squares proof from F.

Proof.

Linear combination: $\frac{g \qquad h}{ag+bh}$ $\quad f = ag + bh \quad -f^2 = -(ag+bh)^2$

$$\sum_i \hat{g}_i' f_i + \sum_j \hat{q}_j'(x_j^2 - x_j) + \sum_\ell (\hat{p}_\ell')^2 = -2(ag)^2$$

$$\sum_i \hat{g}_i'' f_i + \sum_j \hat{q}_j''(x_j^2 - x_j) + \sum_\ell (\hat{p}_\ell'')^2 = -2(bh)^2$$

$$(ag - bh)^2 = (ag)^2 - 2ag\,bh + (bh)^2$$

adding these sos proofs yields:

Sum-of-squares simulates polynomial calculus

Proof of the inductive lemma

Inductive lemma

If f has a degree-d polynomial calculus derivation from F,
then $-f^2 \geq 0$ has a degree-$2d$ sum-of-squares proof from F.

Proof.

Linear combination: $\frac{g \qquad h}{ag+bh}$ $\quad f = ag + bh \quad -f^2 = -(ag+bh)^2$

$$\sum_i \hat{g}'_i f_i + \sum_j \hat{q}'_j (x_j^2 - x_j) + \sum_\ell (\hat{p}'_\ell)^2 = -2(ag)^2$$
$$\sum_i \hat{g}''_i f_i + \sum_j \hat{q}''_j (x_j^2 - x_j) + \sum_\ell (\hat{p}''_\ell)^2 = -2(bh)^2$$
$$(ag - bh)^2 = (ag)^2 - 2ag\,bh + (bh)^2$$

adding these sos proofs yields:

$$\sum_i g_i f_i + \sum_j q_j (x_j^2 - x_j) + \sum_\ell (p_\ell)^2 = -(ag)^2 - 2ag\,bh - (bh)^2$$

Sum-of-squares simulates polynomial calculus

Proof of the inductive lemma

Inductive lemma

If f has a degree-d polynomial calculus derivation from F, then $-f^2 \geq 0$ has a degree-$2d$ sum-of-squares proof from F.

Proof.

Linear combination: $\frac{g \qquad h}{ag+bh}$ $\quad f = ag + bh \quad -f^2 = -(ag+bh)^2$

$$\begin{aligned}
\textstyle\sum_i \hat{g}_i' f_i + \sum_j \hat{q}_j'(x_j^2 - x_j) + \sum_\ell (\hat{p}_\ell')^2 &= -2(ag)^2 \\
\textstyle\sum_i \hat{g}_i'' f_i + \sum_j \hat{q}_j''(x_j^2 - x_j) + \sum_\ell (\hat{p}_\ell'')^2 &= -2(bh)^2 \\
(ag - bh)^2 &= (ag)^2 - 2ag\,bh + (bh)^2
\end{aligned}$$

adding these sos proofs yields:

$$\begin{aligned}
\textstyle\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + \sum_\ell (p_\ell)^2 &= -(ag)^2 - 2ag\,bh - (bh)^2 \\
&= -(ag+bh)^2 = -f^2
\end{aligned}$$

Sum-of-squares simulates polynomial calculus

Inductive lemma

If f has a degree-d polynomial calculus derivation from F, then $-f^2 \geq 0$ has a degree-$2d$ sum-of-squares proof from F.

Proof.

Multiplication: $\frac{g}{x_s g}$ $\qquad f = x_s g \qquad -f^2 = -x_s^2 g^2$

Sum-of-squares simulates polynomial calculus

Inductive lemma

If f has a degree-d polynomial calculus derivation from F,
then $-f^2 \geq 0$ has a degree-$2d$ sum-of-squares proof from F.

Proof.

Multiplication: $\frac{g}{x_s g}$ $\qquad f = x_s g \qquad -f^2 = -x_s^2 g^2$

$$\sum_i g_i' f_i + \sum_j q_j'(x_j^2 - x_j) + \sum_\ell (p_\ell')^2 = -g^2$$

Sum-of-squares simulates polynomial calculus

Inductive lemma

If f has a degree-d polynomial calculus derivation from F,
then $-f^2 \geq 0$ has a degree-$2d$ sum-of-squares proof from F.

Proof.

Multiplication: $\frac{g}{x_s g}$ $\qquad f = x_s g \qquad -f^2 = -x_s^2 g^2$

$$\sum_i g_i' f_i + \sum_j q_j'(x_j^2 - x_j) + \sum_\ell (p_\ell')^2 = -g^2$$

$$(g - x_s g)^2 = g^2 - 2x_s g^2 + x_s^2 g^2$$

Sum-of-squares simulates polynomial calculus

Inductive lemma

If f has a degree-d polynomial calculus derivation from F,
then $-f^2 \geq 0$ has a degree-$2d$ sum-of-squares proof from F.

Proof.
Multiplication: $\frac{g}{x_s g}$ $\qquad f = x_s g \qquad -f^2 = -x_s^2 g^2$

$$\begin{aligned}
\textstyle\sum_i g_i' f_i + \sum_j q_j'(x_j^2 - x_j) + \sum_\ell (p_\ell')^2 &= -g^2 \\
(g - x_s g)^2 &= g^2 - 2x_s g^2 + x_s^2 g^2 \\
-2g^2(x_s^2 - x_s) &= \quad + 2x_s g^2 - 2x_s^2 g^2
\end{aligned}$$

Sum-of-squares simulates polynomial calculus

Inductive lemma

If f has a degree-d polynomial calculus derivation from F,
then $-f^2 \geq 0$ has a degree-$2d$ sum-of-squares proof from F.

Proof.

Multiplication: $\frac{g}{x_s g}$ $\qquad f = x_s g \qquad -f^2 = -x_s^2 g^2$

$$
\begin{aligned}
\textstyle\sum_i g_i' f_i + \sum_j q_j'(x_j^2 - x_j) + \sum_\ell (p_\ell')^2 &= -g^2 \\
(g - x_s g)^2 &= g^2 - 2x_s g^2 + x_s^2 g^2 \\
-2g^2(x_s^2 - x_s) &= \quad + 2x_s g^2 - 2x_s^2 g^2
\end{aligned}
$$

adding these sos proofs yields:

Sum-of-squares simulates polynomial calculus

Inductive lemma

If f has a degree-d polynomial calculus derivation from F,
then $-f^2 \geq 0$ has a degree-$2d$ sum-of-squares proof from F.

Proof.

Multiplication: $\frac{g}{x_s g}$ $\qquad f = x_s g \qquad -f^2 = -x_s^2 g^2$

$$\begin{aligned}
\textstyle\sum_i g_i' f_i + \sum_j q_j'(x_j^2 - x_j) + \sum_\ell (p_\ell')^2 &= -g^2 \\
(g - x_s g)^2 &= g^2 - 2x_s g^2 + x_s^2 g^2 \\
-2g^2(x_s^2 - x_s) &= \quad +2x_s g^2 - 2x_s^2 g^2
\end{aligned}$$

adding these sos proofs yields:

$$\begin{aligned}
\textstyle\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + \sum_\ell (p_\ell)^2 &= -x_s^2 g^2 \\
&= -f^2
\end{aligned}$$

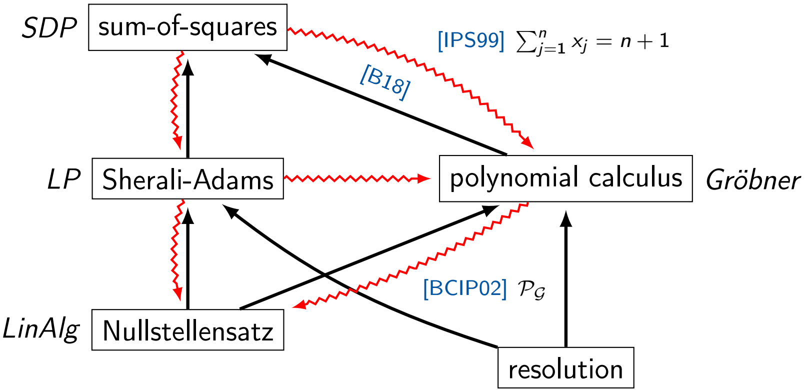
(Semi-)algebraic proof systems

Static systems

$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -1$

Derivation systems

$\frac{g=0 \quad f=0}{ag+bf=0}$



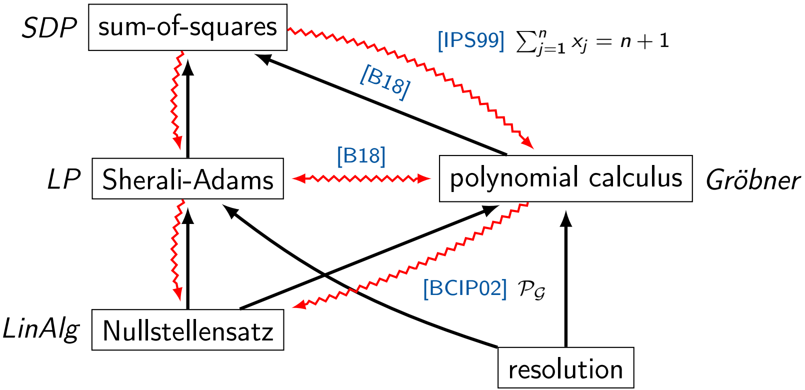
(Semi-)algebraic proof systems

Static systems

$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -1$

Derivation systems

$\frac{g=0 \qquad f=0}{ag+bf=0}$



Lower bounds for static systems

To prove a degree-d lower bound define a d-evaluation $D : \mathbb{R}^{\leq d}[x_1, \ldots, x_n] \to \mathbb{R}$ satisfying the following:

Lower bounds for static systems

To prove a degree-d lower bound define a d-evaluation $D : \mathbb{R}^{\leq d}[x_1, \ldots, x_n] \to \mathbb{R}$ satisfying the following:

- D is linear: $D(af + bg) = aD(f) + bD(g)$ for all $f, g \in \mathbb{R}[x_1, \ldots, x_n]$; $D(1) = 1$

Lower bounds for static systems

To prove a degree-d lower bound define a d-evaluation $D : \mathbb{R}^{\leq d}[x_1, \ldots, x_n] \to \mathbb{R}$ satisfying the following:

- D is linear: $D(af + bg) = aD(f) + bD(g)$ for all $f, g \in \mathbb{R}[x_1, \ldots, x_n]$; $D(1) = 1$
- D is multi-linear: $D(\prod_j x_j^{d_j}) = D(\prod_j x_j)$

Lower bounds for static systems

To prove a degree-d lower bound define a d-evaluation $D : \mathbb{R}^{\leq d}[x_1, \ldots, x_n] \to \mathbb{R}$ satisfying the following:

- D is linear: $D(af + bg) = aD(f) + bD(g)$ for all $f, g \in \mathbb{R}[x_1, \ldots, x_n]$; $D(1) = 1$
- D is multi-linear: $D(\prod_j x_j^{d_j}) = D(\prod_j x_j)$
- $D(g \cdot f_i) = 0$ for every axiom $f_i \in \mathcal{F}$ and $g \in \mathbb{R}[x_1, \ldots, x_n]$ with $\deg(g) \leq d - \deg(f_i)$

Lower bounds for static systems

To prove a degree-d lower bound define a d-evaluation $D : \mathbb{R}^{\leq d}[x_1, \ldots, x_n] \to \mathbb{R}$ satisfying the following:

- D is linear: $D(af + bg) = aD(f) + bD(g)$ for all $f, g \in \mathbb{R}[x_1, \ldots, x_n]$; $D(1) = 1$
- D is multi-linear: $D(\prod_j x_j^{d_j}) = D(\prod_j x_j)$
- $D(g \cdot f_i) = 0$ for every axiom $f_i \in \mathcal{F}$ and $g \in \mathbb{R}[x_1, \ldots, x_n]$ with $\deg(g) \leq d - \deg(f_i)$
- $D(p) \geq 0$ for non-neg. p, $\deg(p) \leq d$. (Sherali-Adams/SOS)

Lower bounds for static systems

To prove a degree-d lower bound define a d-evaluation $D : \mathbb{R}^{\leq d}[x_1, \ldots, x_n] \to \mathbb{R}$ satisfying the following:

- D is linear: $D(af + bg) = aD(f) + bD(g)$ for all $f, g \in \mathbb{R}[x_1, \ldots, x_n]$; $D(1) = 1$
- D is multi-linear: $D(\prod_j x_j^{d_j}) = D(\prod_j x_j)$
- $D(g \cdot f_i) = 0$ for every axiom $f_i \in \mathcal{F}$ and $g \in \mathbb{R}[x_1, \ldots, x_n]$ with $\deg(g) \leq d - \deg(f_i)$
- $D(p) \geq 0$ for non-neg. p, $\deg(p) \leq d$. (Sherali-Adams/SOS)

$$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -1$$

Lower bounds for static systems

To prove a degree-d lower bound define a d-evaluation $D : \mathbb{R}^{\leq d}[x_1, \ldots, x_n] \to \mathbb{R}$ satisfying the following:

- D is linear: $D(af + bg) = aD(f) + bD(g)$ for all $f, g \in \mathbb{R}[x_1, \ldots, x_n]$; $D(1) = 1$
- D is multi-linear: $D(\prod_j x_j^{d_j}) = D(\prod_j x_j)$
- $D(g \cdot f_i) = 0$ for every axiom $f_i \in \mathcal{F}$ and $g \in \mathbb{R}[x_1, \ldots, x_n]$ with $\deg(g) \leq d - \deg(f_i)$
- $D(p) \geq 0$ for non-neg. p, $\deg(p) \leq d$. (Sherali-Adams/SOS)

$$D\Big(\sum_i g_i f_i + \sum_j q_j (x_j^2 - x_j) + p \Big) = D\Big(-1 \Big)$$

Lower bounds for static systems

To prove a degree-d lower bound define a d-evaluation $D : \mathbb{R}^{\leq d}[x_1, \ldots, x_n] \to \mathbb{R}$ satisfying the following:

- D is linear: $D(af + bg) = aD(f) + bD(g)$ for all $f, g \in \mathbb{R}[x_1, \ldots, x_n]$; $D(1) = 1$
- D is multi-linear: $D(\prod_j x_j^{d_j}) = D(\prod_j x_j)$
- $D(g \cdot f_i) = 0$ for every axiom $f_i \in \mathcal{F}$ and $g \in \mathbb{R}[x_1, \ldots, x_n]$ with $\deg(g) \leq d - \deg(f_i)$
- $D(p) \geq 0$ for non-neg. p, $\deg(p) \leq d$. (Sherali-Adams/SOS)

$$\sum_i D\Big(g_i f_i\Big) + \sum_j D\Big(q_j(x_j^2 - x_j)\Big) + D\Big(p\Big) = D\Big(-1\Big)$$

Lower bounds for static systems

To prove a degree-d lower bound define a d-evaluation $D : \mathbb{R}^{\leq d}[x_1, \ldots, x_n] \to \mathbb{R}$ satisfying the following:

- D is linear: $D(af + bg) = aD(f) + bD(g)$ for all $f, g \in \mathbb{R}[x_1, \ldots, x_n]$; $D(1) = 1$
- D is multi-linear: $D(\prod_j x_j^{d_j}) = D(\prod_j x_j)$
- $D(g \cdot f_i) = 0$ for every axiom $f_i \in \mathcal{F}$ and $g \in \mathbb{R}[x_1, \ldots, x_n]$ with $\deg(g) \leq d - \deg(f_i)$
- $D(p) \geq 0$ for non-neg. p, $\deg(p) \leq d$. (Sherali-Adams/SOS)

$$\sum_i \underbrace{D\Big(g_i f_i\Big)}_{=0} + \sum_j \underbrace{D\Big(q_j(x_j^2 - x_j)\Big)}_{=0} + \underbrace{D\Big(p\Big)}_{\geq 0} = \underbrace{D\Big(-1\Big)}_{=-1}$$

Lower bounds for static systems

To prove a degree-d lower bound define a d-evaluation $D : \mathbb{R}^{\leq d}[x_1, \ldots, x_n] \to \mathbb{R}$ satisfying the following:

- D is linear: $D(af + bg) = aD(f) + bD(g)$ for all $f, g \in \mathbb{R}[x_1, \ldots, x_n]$; $D(1) = 1$
- D is multi-linear: $D(\prod_j x_j^{d_j}) = D(\prod_j x_j)$
- $D(g \cdot f_i) = 0$ for every axiom $f_i \in \mathcal{F}$ and $g \in \mathbb{R}[x_1, \ldots, x_n]$ with $\deg(g) \leq d - \deg(f_i)$
- $D(p) \geq 0$ for non-neg. p, $\deg(p) \leq d$. (Sherali-Adams/SOS)

$$\sum_i \underbrace{D\Big(g_i f_i\Big)}_{=0} + \sum_j \underbrace{D\Big(q_j(x_j^2 - x_j)\Big)}_{=0} + \underbrace{D\Big(p\Big)}_{\geq 0} = \underbrace{D\Big(-1\Big)}_{=-1}$$

Suffices to define D on multi-linear monomials $\prod_{i \in I} x_i$.

Nullstellensatz does not simulate resolution & PC

Theorem [BCIP02]

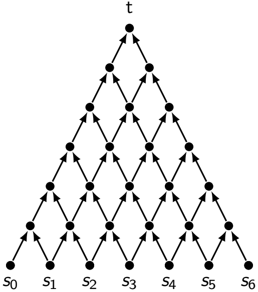
There are 3-CNF formulas that have a resolution refutation of width 3, but no Nullstellensatz refutations of degree $o(n/\log n)$.

Nullstellensatz does not simulate resolution & PC

Theorem [BCIP02]

There are 3-CNF formulas that have a resolution refutation of width 3, but no Nullstellensatz refutations of degree $o(n/\log n)$.

- Pebbling contradiction $\mathcal{F}_{\mathcal{G}}$:



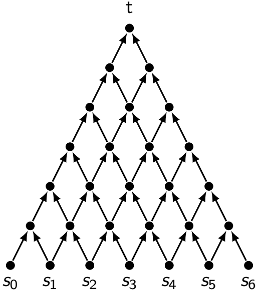
Nullstellensatz does not simulate resolution & PC

Theorem [BCIP02]

There are 3-CNF formulas that have a resolution refutation of width 3, but no Nullstellensatz refutations of degree $o(n/\log n)$.

- Pebbling contradiction $\mathcal{F}_{\mathcal{G}}$:

  $x_{s_i} = 1 \qquad (x_{s_i})$



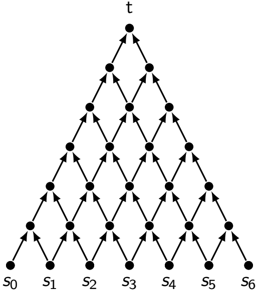
Nullstellensatz does not simulate resolution & PC

Theorem [BCIP02]

There are 3-CNF formulas that have a resolution refutation of width 3, but no Nullstellensatz refutations of degree $o(n/\log n)$.

- Pebbling contradiction $\mathcal{F}_{\mathcal{G}}$:

$$x_{s_i} = 1 \qquad (x_{s_i})$$
$$x_t = 0 \qquad (\overline{x_t})$$



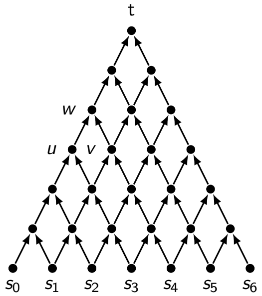
Nullstellensatz does not simulate resolution & PC

Theorem [BCIP02]

There are 3-CNF formulas that have a resolution refutation of width 3, but no Nullstellensatz refutations of degree $o(n/\log n)$.

- Pebbling contradiction $\mathcal{F}_{\mathcal{G}}$:

$$\begin{aligned} x_{s_i} &= 1 & & (x_{s_i}) \\ x_t &= 0 & & (\overline{x_t}) \\ x_u x_v &= x_u x_v x_w & & (x_u \wedge x_v \rightarrow x_w) \end{aligned}$$



Nullstellensatz does not simulate resolution & PC

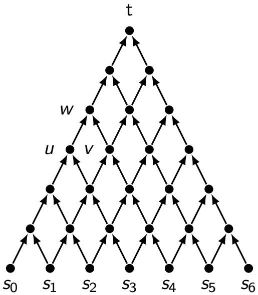
Theorem [BCIP02]

There are 3-CNF formulas that have a resolution refutation of width 3, but no Nullstellensatz refutations of degree $o(n/\log n)$.

- Pebbling contradiction $\mathcal{F}_{\mathcal{G}}$:

$$\begin{aligned} x_{s_i} &= 1 && (x_{s_i}) \\ x_t &= 0 && (\overline{x_t}) \\ x_u x_v &= x_u x_v x_w && (x_u \wedge x_v \rightarrow x_w) \end{aligned}$$

- Resolution refutation of width 3



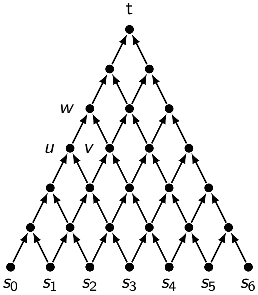
Nullstellensatz does not simulate resolution & PC

Theorem [BCIP02]

There are 3-CNF formulas that have a resolution refutation of width 3, but no Nullstellensatz refutations of degree $o(n/\log n)$.

- Pebbling contradiction $\mathcal{F}_{\mathcal{G}}$:

$$
\begin{array}{rll}
x_{s_i} &= 1 & (x_{s_i}) \\
x_t &= 0 & (\overline{x_t}) \\
x_u x_v &= x_u x_v x_w & (x_u \wedge x_v \rightarrow x_w)
\end{array}
$$



- Resolution refutation of width 3
- $\Rightarrow$ degree 3 in Sherali-Adams / PC

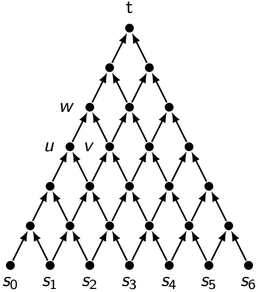
Nullstellensatz does not simulate resolution & PC

Theorem [BCIP02]

There are 3-CNF formulas that have a resolution refutation of width 3, but no Nullstellensatz refutations of degree $o(n/\log n)$.

- Pebbling contradiction $\mathcal{F}_{\mathcal{G}}$:

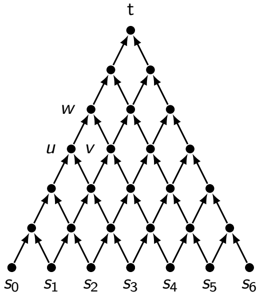
$$
\begin{array}{rcl}
x_{s_i} = 1 & \qquad & (x_{s_i}) \\
x_t = 0 & \qquad & (\overline{x_t}) \\
x_u x_v = x_u x_v x_w & \qquad & (x_u \wedge x_v \rightarrow x_w)
\end{array}
$$



- Resolution refutation of width 3
- $\Rightarrow$ degree 3 in Sherali-Adams / PC
- Nullstellensatz degree $\Omega(n/\log n)$

Nullstellensatz does not simulate resolution & PC

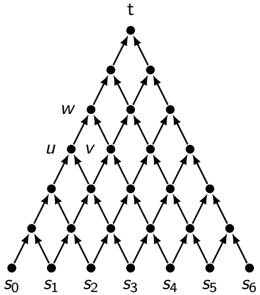
The black pebble game is a one-player game on directed acyclic graphs.



Nullstellensatz does not simulate resolution & PC

The black pebble game is a one-player game on directed acyclic graphs. In each round the player can

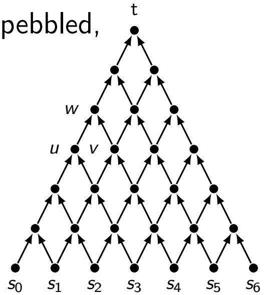
- place a pebble on a source s_i,



Nullstellensatz does not simulate resolution & PC

The black pebble game is a one-player game on directed acyclic graphs. In each round the player can

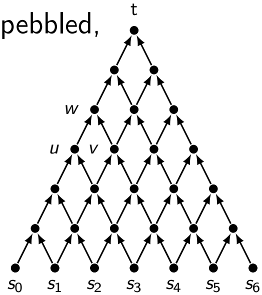
- place a pebble on a source s_i,
- place a pebble on w if $N^-(w) = \{u, v\}$ are pebbled,



Nullstellensatz does not simulate resolution & PC

The black pebble game is a one-player game on directed acyclic graphs. In each round the player can

- place a pebble on a source s_i,
- place a pebble on w if $N^-(w) = \{u, v\}$ are pebbled,
- remove a pebble.

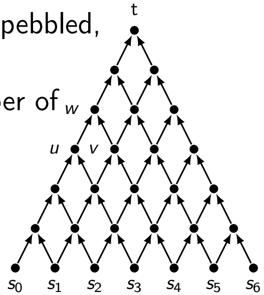


Nullstellensatz does not simulate resolution & PC

The black pebble game is a one-player game on directed acyclic graphs. In each round the player can

- place a pebble on a source s_i,
- place a pebble on w if $N^-(w) = \{u, v\}$ are pebbled,
- remove a pebble.

The pebbling prize $\mathrm{Peb}(\mathcal{G})$ is the minimum number of pebbles needed to place a pebble on the sink t.

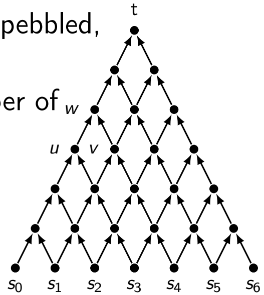


Nullstellensatz does not simulate resolution & PC

The black pebble game is a one-player game on directed acyclic graphs. In each round the player can

- place a pebble on a source s_i,
- place a pebble on w if $N^-(w) = \{u, v\}$ are pebbled,
- remove a pebble.

The pebbling prize $\mathrm{Peb}(\mathcal{G})$ is the minimum number of pebbles needed to place a pebble on the sink t.



Theorem [PTC77]

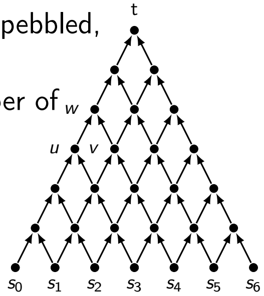
There are graphs $\mathcal{G}$ on n vertices with $\mathrm{Peb}(\mathcal{G}) = \Omega(n/\log n)$.

Nullstellensatz does not simulate resolution & PC

The black pebble game is a one-player game on directed acyclic graphs. In each round the player can

- place a pebble on a source s_i,
- place a pebble on w if $N^-(w) = \{u, v\}$ are pebbled,
- remove a pebble.

The pebbling prize $\mathrm{Peb}(\mathcal{G})$ is the minimum number of pebbles needed to place a pebble on the sink t.



Theorem [PTC77]

There are graphs $\mathcal{G}$ on n vertices with $\mathrm{Peb}(\mathcal{G}) = \Omega(n/\log n)$.

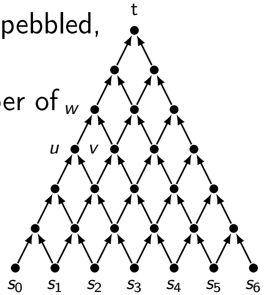
Fix $d = \mathrm{Peb}(\mathcal{G}) - 1$.

Nullstellensatz does not simulate resolution & PC

The black pebble game is a one-player game on directed acyclic graphs. In each round the player can

- place a pebble on a source s_i,
- place a pebble on w if $N^-(w) = \{u, v\}$ are pebbled,
- remove a pebble.

The pebbling prize $\mathrm{Peb}(\mathcal{G})$ is the minimum number of pebbles needed to place a pebble on the sink t.



Theorem [PTC77]

There are graphs $\mathcal{G}$ on n vertices with $\mathrm{Peb}(\mathcal{G}) = \Omega(n/\log n)$.

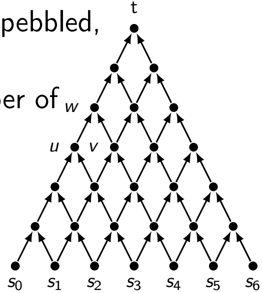
Fix $d = \mathrm{Peb}(\mathcal{G}) - 1$. $A \subseteq V(G)$ is reachable, if the player can reach a position in the black d-pebble game where all $a \in A$ are pebbled.

Nullstellensatz does not simulate resolution & PC

The black pebble game is a one-player game on directed acyclic graphs. In each round the player can

- place a pebble on a source s_i,
- place a pebble on w if $N^-(w) = \{u, v\}$ are pebbled,
- remove a pebble.

The pebbling prize $\mathrm{Peb}(\mathcal{G})$ is the minimum number of pebbles needed to place a pebble on the sink t.



Theorem [PTC77]

There are graphs $\mathcal{G}$ on n vertices with $\mathrm{Peb}(\mathcal{G}) = \Omega(n/\log n)$.

Fix $d = \mathrm{Peb}(\mathcal{G}) - 1$. $A \subseteq V(G)$ is reachable, if the player can reach a position in the black d-pebble game where all $a \in A$ are pebbled.

$$D\Big(\prod\nolimits_{a \in A} x_a\Big) := \begin{cases} 1 \text{ if } A \text{ is reachable,} \\ 0 \text{ otherwise.} \end{cases}$$

Nullstellensatz does not simulate resolution & PC

$$D\Big(\prod_{a\in A} x_a\Big) := \begin{cases} 1 \text{ if } A \text{ is reachable,} \\ 0 \text{ otherwise.} \end{cases}$$

Nullstellensatz does not simulate resolution & PC

$$D\Big(\prod_{a\in A} x_a\Big) := \begin{cases} 1 \text{ if } A \text{ is reachable,} \\ 0 \text{ otherwise.} \end{cases}$$

It remains to check $D\Big((\prod_{a\in A} x_a) \cdot f_i\Big) = 0$ for all axioms $f_i = 0$ and $|A| \le d - \deg(f_i)$:

Nullstellensatz does not simulate resolution & PC

$$D\Big(\prod_{a\in A} x_a\Big) := \begin{cases} 1 \text{ if } A \text{ is reachable,} \\ 0 \text{ otherwise.} \end{cases}$$

It remains to check $D\Big((\prod_{a\in A} x_a)\cdot f_i\Big) = 0$ for all axioms $f_i = 0$ and $|A| \le d - \deg(f_i)$:

$$x_s = 1 \qquad \rightsquigarrow \qquad D\Big(\prod_{a\in A\cup\{s\}} x_a\Big) = D\Big(\prod_{a\in A} x_a\Big)$$

Nullstellensatz does not simulate resolution & PC

$$D\Big(\prod_{a\in A} x_a\Big) := \begin{cases} 1 \text{ if } A \text{ is reachable,} \\ 0 \text{ otherwise.} \end{cases}$$

It remains to check $D\Big((\prod_{a\in A} x_a)\cdot f_i\Big) = 0$ for all axioms $f_i = 0$ and $|A| \le d - \deg(f_i)$:

$$x_s = 1 \qquad \rightsquigarrow \qquad D\Big(\prod_{a\in A\cup\{s\}} x_a\Big) = D\Big(\prod_{a\in A} x_a\Big)$$

$$x_t = 0 \qquad \rightsquigarrow \qquad D\Big(\prod_{a\in A\cup\{t\}} x_a\Big) = 0$$

Nullstellensatz does not simulate resolution & PC

$$D\Big(\prod_{a\in A} x_a\Big) := \begin{cases} 1 \text{ if } A \text{ is reachable,} \\ 0 \text{ otherwise.} \end{cases}$$

It remains to check $D\Big((\prod_{a\in A} x_a)\cdot f_i\Big) = 0$ for all axioms $f_i = 0$ and $|A| \le d - \deg(f_i)$:

$$\begin{aligned}
x_s = 1 \quad &\rightsquigarrow \quad D\Big(\prod_{a\in A\cup\{s\}} x_a\Big) = D\Big(\prod_{a\in A} x_a\Big) \\
x_t = 0 \quad &\rightsquigarrow \quad D\Big(\prod_{a\in A\cup\{t\}} x_a\Big) = 0 \\
x_u x_v = x_u x_v x_w \quad &\rightsquigarrow \quad D\Big(\prod_{a\in A\cup\{u,v\}} x_a\Big) = D\Big(\prod_{a\in A\cup\{u,v,w\}} x_a\Big)
\end{aligned}$$

□

Sherali-Adams does not simulate polynomial calculus

Theorem [B18]

There is a system F that has a polynomial calculus refutation of degree 3, but no Sherali-Adams refutation of degree $o(\sqrt{n}/\log n)$.

Sherali-Adams does not simulate polynomial calculus

Theorem [B18]

There is a system F that has a polynomial calculus refutation of degree 3, but no Sherali-Adams refutation of degree $o(\sqrt{n}/\log n)$.

Proof. Apply substitution $\mathcal{F}_{\mathcal{G}}[+_k]$ to $\mathcal{F}_{\mathcal{G}}$:

Sherali-Adams does not simulate polynomial calculus

Theorem [B18]

There is a system F that has a polynomial calculus refutation of degree 3, but no Sherali-Adams refutation of degree $o(\sqrt{n}/\log n)$.

Proof. Apply substitution $\mathcal{F}_{\mathcal{G}}[+_k]$ to $\mathcal{F}_{\mathcal{G}}$:

- replace every variable x_v by $x_v^{(1)} + \cdots + x_v^{(k)}$

Sherali-Adams does not simulate polynomial calculus

Theorem [B18]

There is a system F that has a polynomial calculus refutation of degree 3, but no Sherali-Adams refutation of degree $o(\sqrt{n}/\log n)$.

Proof. Apply substitution $\mathcal{F}_{\mathcal{G}}[+_k]$ to $\mathcal{F}_{\mathcal{G}}$:

- replace every variable x_v by $x_v^{(1)} + \cdots + x_v^{(k)}$

We get:

- there is a degree-3 refutation of $\mathcal{F}_{\mathcal{G}}[+_k]$ in polynomial calculus (by substituting everything in the refutation of $\mathcal{F}_{\mathcal{G}}$)

Sherali-Adams does not simulate polynomial calculus

Theorem [B18]

There is a system F that has a polynomial calculus refutation of degree 3, but no Sherali-Adams refutation of degree $o(\sqrt{n}/\log n)$.

Proof. Apply substitution $\mathcal{F}_\mathcal{G}[+_k]$ to $\mathcal{F}_\mathcal{G}$:

- replace every variable x_v by $x_v^{(1)} + \cdots + x_v^{(k)}$

We get:

- there is a degree-3 refutation of $\mathcal{F}_\mathcal{G}[+_k]$ in polynomial calculus (by substituting everything in the refutation of $\mathcal{F}_\mathcal{G}$)
- Sherali-Adams requires degree $\min(\mathrm{Peb}(\mathcal{G}), k/2)$:

Sherali-Adams does not simulate polynomial calculus

Theorem [B18]

There is a system F that has a polynomial calculus refutation of degree 3, but no Sherali-Adams refutation of degree $o(\sqrt{n}/\log n)$.

Proof. Apply substitution $\mathcal{F}_{\mathcal{G}}[+_k]$ to $\mathcal{F}_{\mathcal{G}}$:

- replace every variable x_v by $x_v^{(1)} + \cdots + x_v^{(k)}$

We get:

- there is a degree-3 refutation of $\mathcal{F}_{\mathcal{G}}[+_k]$ in polynomial calculus (by substituting everything in the refutation of $\mathcal{F}_{\mathcal{G}}$)
- Sherali-Adams requires degree $\min(\mathrm{Peb}(\mathcal{G}), k/2)$:

$$D\Big(\mathbf{x}\Big) := \begin{cases} \left(\frac{1}{k}\right)^{|A|} & \text{if } \mathbf{x} = \prod_{a \in A} x_a^{(\ell_a)} \text{ and } A \text{ is reachable,} \\ 0 & \text{otherwise.} \end{cases}$$

Sherali-Adams does not simulate polynomial calculus

$$D(\mathsf{x}) := \begin{cases} \left(\frac{1}{k}\right)^{|A|} & \text{if } \mathsf{x} = \prod_{a \in A} x_a^{(\ell_a)} \text{ and } A \text{ is reachable,} \\ 0 & \text{otherwise.} \end{cases}$$

Sherali-Adams does not simulate polynomial calculus

$$D(\mathbf{x}) := \begin{cases} \left(\frac{1}{k}\right)^{|A|} & \text{if } \mathbf{x} = \prod_{a \in A} x_a^{(\ell_a)} \text{ and } A \text{ is reachable,} \\ 0 & \text{otherwise.} \end{cases}$$

Checking $D(g_i f_i) = 0$ is essentially the same as before.

Sherali-Adams does not simulate polynomial calculus

$$D(\mathbf{x}) := \begin{cases} \left(\frac{1}{k}\right)^{|A|} & \text{if } \mathbf{x} = \prod_{a \in A} x_a^{(\ell_a)} \text{ and } A \text{ is reachable,} \\ 0 & \text{otherwise.} \end{cases}$$

Checking $D(g_i f_i) = 0$ is essentially the same as before.

Remains: $D(p) \geq 0$ for $p = \prod_{(v,\ell)\in I} x_v^{(\ell)} \prod_{(v,\ell)\in J} (1 - x_v^{(\ell)})$

Sherali-Adams does not simulate polynomial calculus

$$D(\mathbf{x}) := \begin{cases} \left(\frac{1}{k}\right)^{|A|} & \text{if } \mathbf{x} = \prod_{a \in A} x_a^{(\ell_a)} \text{ and } A \text{ is reachable,} \\ 0 & \text{otherwise.} \end{cases}$$

Checking $D(g_i f_i) = 0$ is essentially the same as before.
Remains: $D(p) \geq 0$ for $p = \prod_{(v,\ell) \in I} x_v^{(\ell)} \prod_{(v,\ell) \in J} (1 - x_v^{(\ell)})$

- If $D\left(\prod_{(v,\ell) \in I} x_v^{(\ell)}\right) = 0$, then $D(p) = 0$.

Sherali-Adams does not simulate polynomial calculus

$$D(\mathbf{x}) := \begin{cases} \left(\frac{1}{k}\right)^{|A|} & \text{if } \mathbf{x} = \prod_{a \in A} x_a^{(\ell_a)} \text{ and } A \text{ is reachable,} \\ 0 & \text{otherwise.} \end{cases}$$

Checking $D(g_i f_i) = 0$ is essentially the same as before.
Remains: $D(p) \geq 0$ for $p = \prod_{(v,\ell) \in I} x_v^{(\ell)} \prod_{(v,\ell) \in J} (1 - x_v^{(\ell)})$

- If $D\left(\prod_{(v,\ell) \in I} x_v^{(\ell)}\right) = 0$, then $D(p) = 0$.
- Otherwise:
  $$D(p) = \left(\frac{1}{k}\right)^{|I|} + \sum_{\emptyset \neq K \subseteq J} (-1)^{|K|} D\left(\prod_{(v,\ell) \in K \cup I} x_{v,\ell}\right)$$

Sherali-Adams does not simulate polynomial calculus

$$D(\mathbf{x}) := \begin{cases} \left(\frac{1}{k}\right)^{|A|} & \text{if } \mathbf{x} = \prod_{a \in A} x_a^{(\ell_a)} \text{ and } A \text{ is reachable,} \\ 0 & \text{otherwise.} \end{cases}$$

Checking $D(g_i f_i) = 0$ is essentially the same as before.
Remains: $D(p) \geq 0$ for $p = \prod_{(v,\ell) \in I} x_v^{(\ell)} \prod_{(v,\ell) \in J} (1 - x_v^{(\ell)})$

- If $D\left(\prod_{(v,\ell) \in I} x_v^{(\ell)}\right) = 0$, then $D(p) = 0$.
- Otherwise:

$$\begin{aligned} D(p) &= \left(\tfrac{1}{k}\right)^{|I|} + \sum_{\emptyset \neq K \subseteq J} (-1)^{|K|} D\left(\prod_{(v,\ell) \in K \cup I} x_{v,\ell}\right) \\ &\geq \left(\tfrac{1}{k}\right)^{|I|} \left(1 - \sum_{z=1}^{|J|} \binom{|J|}{z} \left(\tfrac{1}{k}\right)^{z}\right) \end{aligned}$$

Sherali-Adams does not simulate polynomial calculus

$$D(\mathbf{x}) := \begin{cases} \left(\frac{1}{k}\right)^{|A|} & \text{if } \mathbf{x} = \prod_{a \in A} x_a^{(\ell_a)} \text{ and } A \text{ is reachable,} \\ 0 & \text{otherwise.} \end{cases}$$

Checking $D(g_i f_i) = 0$ is essentially the same as before.
Remains: $D(p) \geq 0$ for $p = \prod_{(v,\ell) \in I} x_v^{(\ell)} \prod_{(v,\ell) \in J} (1 - x_v^{(\ell)})$

- If $D\left(\prod_{(v,\ell) \in I} x_v^{(\ell)}\right) = 0$, then $D(p) = 0$.
- Otherwise:

$$\begin{aligned} D(p) &= \left(\tfrac{1}{k}\right)^{|I|} + \sum_{\emptyset \neq K \subseteq J} (-1)^{|K|} D\left(\prod_{(v,\ell) \in K \cup I} x_{v,\ell}\right) \\ &\geq \left(\tfrac{1}{k}\right)^{|I|} \left(1 - \sum_{z=1}^{|J|} \binom{|J|}{z} \left(\tfrac{1}{k}\right)^{z}\right) \\ &> 0 \quad \text{if } |J| \leq k/2 \end{aligned}$$

$\square$

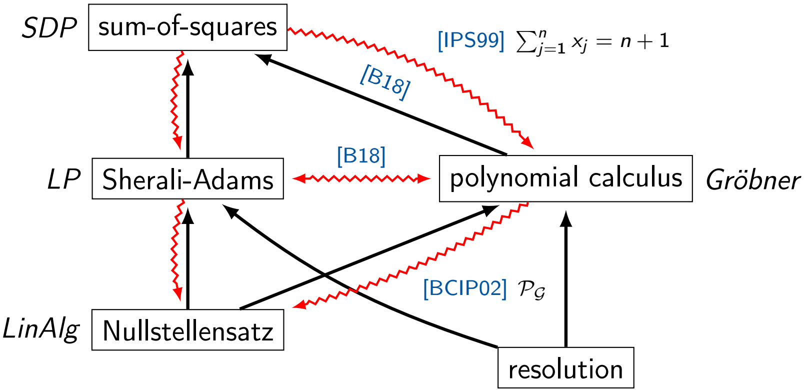
(Semi-)algebraic proof systems

Static systems

$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -1$

Derivation systems

$\frac{g=0 \qquad f=0}{ag+bf=0}$



Proof size

All simulations do also hold with respect to proof size:

- SOS polynomially simulates PC.

Proof size

All simulations do also hold with respect to proof size:

- SOS polynomially simulates PC.
- Sherali-Adams / PC polynomially simulate resolution*.

Proof size

All simulations do also hold with respect to proof size:

- SOS polynomially simulates PC.
- Sherali-Adams / PC polynomially simulate resolution*.
- $*$) For simulating resolution we encode clauses using twin variables x, $x^{\neg}$:

Proof size

All simulations do also hold with respect to proof size:

- SOS polynomially simulates PC.
- Sherali-Adams / PC polynomially simulate resolution*.
- $*$) For simulating resolution we encode clauses using twin variables x, $x^\neg$:
  - $x \vee y \vee \overline{z} \quad \rightsquigarrow \quad x^\neg\, y^\neg\, z = 0$

Proof size

All simulations do also hold with respect to proof size:

- SOS polynomially simulates PC.
- Sherali-Adams / PC polynomially simulate resolution*.
- *) For simulating resolution we encode clauses using twin variables x, $x^{\neg}$:
  - $x \vee y \vee \overline{z} \quad \rightsquigarrow \quad x^{\neg} y^{\neg} z = 0$
  - additional axioms $x + x^{\neg} = 0$

Proof size

All simulations do also hold with respect to proof size:

- SOS polynomially simulates PC.
- Sherali-Adams / PC polynomially simulate resolution*.
- $*$) For simulating resolution we encode clauses using twin variables x, $x^\neg$:
  - $x \vee y \vee \overline{z} \quad \rightsquigarrow \quad x^\neg\, y^\neg\, z = 0$
  - additional axioms $x + x^\neg = 0$
  - This is necessary because encoding $\bigvee_{i \in [n]} x_i$ as $\prod_{i \in [n]}(1 - x_i)$ has size 2^n!

Proof size

All simulations do also hold with respect to proof size:

- SOS polynomially simulates PC.
- Sherali-Adams / PC polynomially simulate resolution*.
- *) For simulating resolution we encode clauses using twin variables x, $x^{\neg}$:
  - $x \vee y \vee \overline{z} \quad \rightsquigarrow \quad x^{\neg} y^{\neg} z = 0$
  - additional axioms $x + x^{\neg} = 0$
  - This is necessary because encoding $\bigvee_{i \in [n]} x_i$ as $\prod_{i \in [n]} (1 - x_i)$ has size 2^n!

All separations do also hold with respect to size, but there is a bit work to do:

Proof size

All simulations do also hold with respect to proof size:

- SOS polynomially simulates PC.
- Sherali-Adams / PC polynomially simulate resolution*.
- *) For simulating resolution we encode clauses using twin variables x, $x^{\neg}$:
  - $x \vee y \vee \overline{z} \quad \rightsquigarrow \quad x^{\neg} y^{\neg} z = 0$
  - additional axioms $x + x^{\neg} = 0$
  - This is necessary because encoding $\bigvee_{i \in [n]} x_i$ as $\prod_{i \in [n]} (1 - x_i)$ has size 2^n!

All separations do also hold with respect to size, but there is a bit work to do:

Observation

Every pebbling contradiction $\mathcal{P}_{\mathcal{G}}$ has a Nullstellensatz refutation of polynomial size (and large degree).

Proof size

Solution: use substitution of x by $x^0 + x^1$!

Proof size

Solution: use substitution of x by $x^0 + x^1$!

- Static proof systems have to "multiply out" large substituted monomials:

Proof size

Solution: use substitution of x by $x^0 + x^1$!

- Static proof systems have to "multiply out" large substituted monomials:

Lemma

Let P = Nullstellensatz, Sherali-Adams, or sum-of-squares.

Proof size

Solution: use substitution of x by $x^0 + x^1$!

- Static proof systems have to "multiply out" large substituted monomials:

Lemma

Let P = Nullstellensatz, Sherali-Adams, or sum-of-squares.
If every P-refutation of $\mathcal{F}$ has degree at least d, then every P-refutation of $\mathcal{F}[+_2]$ has degree at least d and size $\Omega(2^d)$.

Proof size

Solution: use substitution of x by $x^0 + x^1$!

- Static proof systems have to "multiply out" large substituted monomials:

Lemma
Let P = Nullstellensatz, Sherali-Adams, or sum-of-squares.
If every P-refutation of $\mathcal{F}$ has degree at least d, then every P-refutation of $\mathcal{F}[+_2]$ has degree at least d and size $\Omega(2^d)$.

Proof. For every x uniformly at random set either x^0 or x^1 to 0.

Proof size

Solution: use substitution of x by $x^0 + x^1$!

- Static proof systems have to "multiply out" large substituted monomials:

Lemma

Let P = Nullstellensatz, Sherali-Adams, or sum-of-squares.
If every P-refutation of $\mathcal{F}$ has degree at least d, then every P-refutation of $\mathcal{F}[+_2]$ has degree at least d and size $\Omega(2^d)$.

Proof. For every x uniformly at random set either x^0 or x^1 to 0.
If there are at most 2^{d-1} multi-linear monomials of degree $\geq d$,

Proof size

Solution: use substitution of x by $x^0 + x^1$!

- Static proof systems have to "multiply out" large substituted monomials:

Lemma
Let P = Nullstellensatz, Sherali-Adams, or sum-of-squares.
If every P-refutation of $\mathcal{F}$ has degree at least d, then every P-refutation of $\mathcal{F}[+_2]$ has degree at least d and size $\Omega(2^d)$.

Proof. For every x uniformly at random set either x^0 or x^1 to 0.
If there are at most 2^{d-1} multi-linear monomials of degree $\geq d$, they all vanish with non-zero probability,

Proof size

Solution: use substitution of x by $x^0 + x^1$!

- Static proof systems have to "multiply out" large substituted monomials:

Lemma

Let P = Nullstellensatz, Sherali-Adams, or sum-of-squares.
If every P-refutation of $\mathcal{F}$ has degree at least d, then every P-refutation of $\mathcal{F}[+_2]$ has degree at least d and size $\Omega(2^d)$.

Proof. For every x uniformly at random set either x^0 or x^1 to 0.
If there are at most 2^{d-1} multi-linear monomials of degree $\geq d$, they all vanish with non-zero probability,
leading to a P-refutation of $\mathcal{F}$ of degree $< d$. $\square$

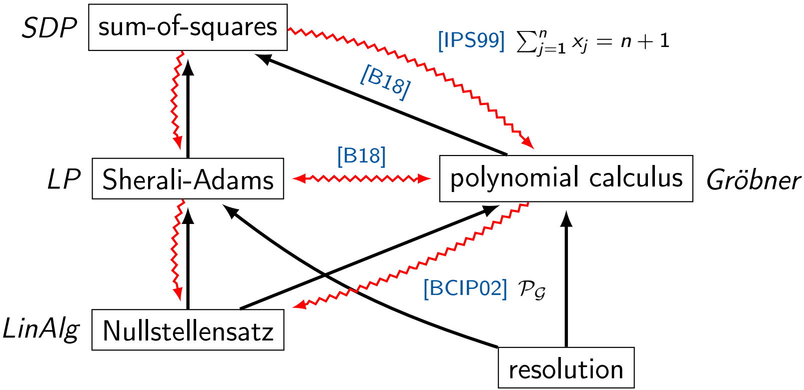
(Semi-)algebraic proof systems

Static systems

$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -1$

Derivation systems

$\frac{g=0 \qquad f=0}{ag+bf=0}$



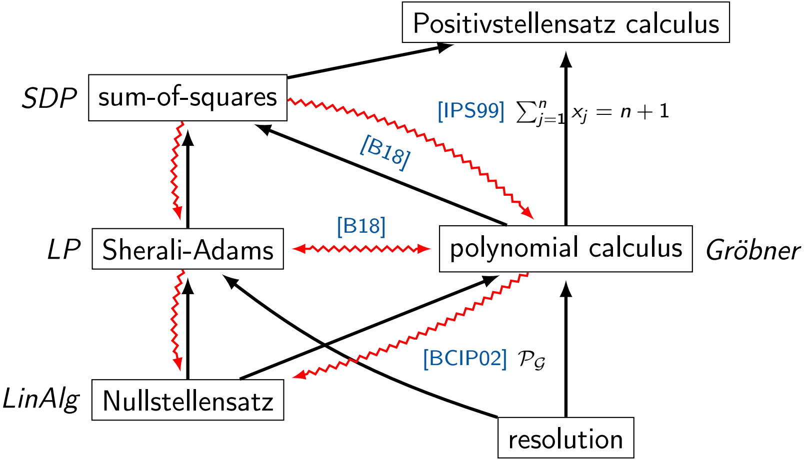
(Semi-)algebraic proof systems

Static systems

$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -1$

Derivation systems

$\frac{g=0 \quad f=0}{ag+bf=0}$



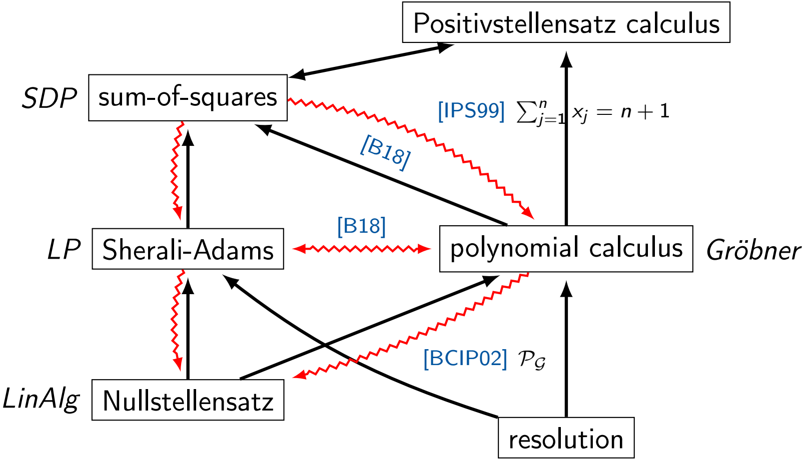
(Semi-)algebraic proof systems

Static systems

$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -1$

Derivation systems

$\dfrac{g=0 \qquad f=0}{ag+bf=0}$



Positivstellensatz and Positivstellensatz calculus

Let $\mathcal{F} = \{f_1 = 0, \ldots, f_m = 0\}$ and $\mathcal{H} = \{h_1 \geq 0, \ldots, h_s \geq 0\}$.

Positivstellensatz and Positivstellensatz calculus

Let $\mathcal{F} = \{f_1 = 0, \ldots, f_m = 0\}$ and $\mathcal{H} = \{h_1 \geq 0, \ldots, h_s \geq 0\}$.

A Positivstellensatz proof of $f \geq 0$ from $(\mathcal{F}, \mathcal{H})$ is

$$\sum_{i=1}^{m} g_i f_i + \sum_{j=1}^{n} q_j(x_j^2 - x_j) + p + \sum_{I \subseteq [s]} p_I \prod_{\ell \in I} h_\ell = f,$$

where p, p_I are sums-of-squares.

Positivstellensatz and Positivstellensatz calculus

Let $\mathcal{F} = \{f_1 = 0, \ldots, f_m = 0\}$ and $\mathcal{H} = \{h_1 \geq 0, \ldots, h_s \geq 0\}$.

A Positivstellensatz proof of $f \geq 0$ from $(\mathcal{F}, \mathcal{H})$ is

$$\sum_{i=1}^{m} g_i f_i + \sum_{j=1}^{n} q_j (x_j^2 - x_j) + p + \sum_{I \subseteq [s]} p_I \prod_{\ell \in I} h_\ell = f,$$

where p, p_I are sums-of-squares.

A Positivstellensatz calculus proof of $f \geq 0$ from $(\mathcal{F}, \mathcal{H})$ is a polynomial calculus proof of

$$f - p - \sum_{I \subseteq [s]} p_I \prod_{\ell \in I} h_\ell \qquad \text{from } \mathcal{F}.$$

Positivstellensatz vs. Positivstellensatz calculus

Theorem [B18]

Positivstellensatz $\equiv$ Positivstellensatz calculus on Boolean systems.

Proof. $(\mathcal{F}, \mathcal{H})$ has a Positivstellensatz calculus refutation

Positivstellensatz vs. Positivstellensatz calculus

Theorem [B18]

Positivstellensatz $\equiv$ Positivstellensatz calculus on Boolean systems.

Proof. $(\mathcal{F}, \mathcal{H})$ has a Positivstellensatz calculus refutation
$\iff -1 - p - \sum_{I \subseteq [s]} p_I \prod_{\ell \in I} h_\ell$ has a PC derivation from $\mathcal{F}$

Positivstellensatz vs. Positivstellensatz calculus

Theorem [B18]

Positivstellensatz $\equiv$ Positivstellensatz calculus on Boolean systems.

Proof. $(\mathcal{F}, \mathcal{H})$ has a Positivstellensatz calculus refutation
$\iff -1 - p - \sum_{I \subseteq [s]} p_I \prod_{\ell \in I} h_\ell$ has a PC derivation from $\mathcal{F}$
$\implies$ (ind. lemma) there is a degree-$2d$ SOS proof
$\sum_{i=1}^m g_i f_i + \sum_{j=1}^n q_j (x_j^2 - x_j) + p' = -(-1 - p - \sum_{I \subseteq [s]} p_I \prod_{\ell \in I} h_\ell)^2.$

Positivstellensatz vs. Positivstellensatz calculus

Theorem [B18]

Positivstellensatz $\equiv$ Positivstellensatz calculus on Boolean systems.

Proof. $(\mathcal{F}, \mathcal{H})$ has a Positivstellensatz calculus refutation
$\iff -1 - p - \sum_{I \subseteq [s]} p_I \prod_{\ell \in I} h_\ell$ has a PC derivation from $\mathcal{F}$
$\implies$ (ind. lemma) there is a degree-$2d$ SOS proof
$\sum_{i=1}^m g_i f_i + \sum_{j=1}^n q_j(x_j^2 - x_j) + p' = -(-1 - p - \sum_{I \subseteq [s]} p_I \prod_{\ell \in I} h_\ell)^2$.
$\implies$ this is a Positivstellensatz refutation of $(\mathcal{F}, \mathcal{H})$. $\square$

Positivstellensatz vs. Positivstellensatz calculus

Theorem [B18]

Positivstellensatz $\equiv$ Positivstellensatz calculus on Boolean systems.

Proof. $(\mathcal{F}, \mathcal{H})$ has a Positivstellensatz calculus refutation
$\iff -1 - p - \sum_{I \subseteq [s]} p_I \prod_{\ell \in I} h_\ell$ has a PC derivation from $\mathcal{F}$
$\implies$ (ind. lemma) there is a degree-$2d$ SOS proof
$\sum_{i=1}^m g_i f_i + \sum_{j=1}^n q_j(x_j^2 - x_j) + p' = -(-1 - p - \sum_{I \subseteq [s]} p_I \prod_{\ell \in I} h_\ell)^2$.
$\implies$ this is a Positivstellensatz refutation of $(\mathcal{F}, \mathcal{H})$. $\square$

Interestingly, on non-Boolean systems this is not the case:
$\mathcal{F}_n^{\text{ts}} := \{yx_1 = 1,\ x_1^2 = x_2,\ x_2^2 = x_3,\ \ldots,\ x_{n-1}^2 = x_n,\ x_n = 0\}$

Theorem [GV01]

(without $x^2 - x = 0$ axioms:)

- $\mathcal{F}_n^{\text{ts}}$ has Positivstellensatz calculus refutations of degree $O(n)$.
- $\mathcal{F}_n^{\text{ts}}$ requires Positivstellensatz refutations of degree $2^{\Omega(n)}$.

(Semi-)algebraic proof systems

Static systems

$\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + p = -1$

Derivation systems

$\frac{g=0 \qquad f=0}{ag+bf=0}$