A comparison of algebraic and semi-algebraic proof systems

Christoph Berkholz

Humboldt-Universität zu Berlin

22.10.2019
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) $(w, p) \in R \Rightarrow w \in L$
- (complete) for all $w \in L$ there exists $p \in \Sigma^*$ with $(w, p) \in R$
- (verifiable) $R$ is decidable in polynomial time

A proof system is $p$-bounded, if

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

Theorem ([Cook, Reckhow 1979])

There is a $p$-bounded proof system for UNSAT $\iff$ $\text{NP} = \text{co-NP}$. 

Definition

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

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

Theorem ([Cook, Reckhow 1979])

There is a p-bounded proof system for UNSAT $\iff$ 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 $|p| = \text{poly}(|w|)$
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 \(w \in L\) exists \(p \in \Sigma^*\) with \((w, p) \in R\)
- (verifiable) \(R\) is decidable in polynomial time

A proof system is p-bounded, if

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

Theorem ([Cook, Reckhow 1979])

There is a p-bounded proof system for UNSAT \( \iff \) \( NP = \text{co-NP} \).
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 \(|p| = \text{poly}(|w|)\)

Theorem ([Cook, Reckhow 1979])

There is a p-bounded proof system for UNSAT \( \iff \) 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 \( p' = \text{poly}(|p|) \).
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 $C$, $D$)

\[
\begin{array}{c}
C \lor x \\
D \lor \neg x \\
\hdashline
C \lor D
\end{array}
\]

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

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

$\leftrightarrow \phi$

Christoph Berkholz – A comparison of algebraic and semi-algebraic proof systems
Proof systems for UNSAT (= refutation systems for SAT)

Systems for proving the unsatisfiability of a CNF formula.

▶ Truth table

▶ Resolution (on clauses $C$, $D$)

\[
\frac{C \lor x \quad D \lor \neg x}{C \lor D}
\]

▶ Frege (Schoenfield’s system on formulas $\varphi, \psi, \eta$ over $\{\lor, \neg\}$):

\[
\begin{align*}
\varphi \lor \neg\varphi & \quad \varphi & \quad \varphi \lor \varphi & \quad \varphi \lor (\psi \lor \eta) & \quad \varphi \lor \psi & \quad \neg \psi \lor \eta \\
\varphi \lor \psi & \quad \varphi & \quad (\varphi \lor \psi) \lor \eta & \quad \varphi \lor \eta
\end{align*}
\]
Proof systems for UNSAT (= refutation systems for SAT)

Systems for proving the unsatisfiability of a CNF formula.

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

\[
\begin{array}{c}
C \lor x & D \lor \neg x \\
\hline
C \lor D
\end{array}
\]

- Frege (Schoenfield’s system on formulas $\varphi, \psi, \eta$ over \{\lor, \neg\}):

\[
\begin{array}{l}
\varphi \lor \neg \varphi \\
\varphi \lor \psi \\
\varphi \lor \varphi \\
\varphi \lor (\psi \lor \eta) \\
\varphi \lor \psi \\
\neg \psi \lor \eta \\
(\varphi \lor \psi) \lor \eta \\
\varphi \lor \eta
\end{array}
\]

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 $C$, $D$)

\[
\frac{C \lor x \quad D \lor \neg x}{C \lor D}
\]

- Frege (Schoenfield’s system on formulas $\varphi, \psi, \eta$ over $\{\lor, \neg\}$):

\[
\begin{align*}
\varphi \lor \neg \varphi & \quad \varphi \lor \psi & \quad \varphi \lor \varphi & \quad \varphi \lor (\psi \lor \eta) & \quad \varphi \lor \psi & \quad \neg \psi \lor \eta \\
(\varphi \lor \psi) \lor \eta & \quad \varphi \lor \eta
\end{align*}
\]

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

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

\[
x \leftrightarrow \varphi
\]
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:

\[
\begin{align*}
x_1 &= 0 \\ 1 - x_2 &= 0 \\ (1 - x_1)x_2(1 - x_3) &= 0
\end{align*}
\]

\[
\iff
\begin{align*}
\overline{x_1} \\ x_2 \\ x_1 \lor \overline{x_2} \lor x_3
\end{align*}
\]

for all clauses $C$: $f_C = 0 \iff C$

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

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

$\iff$

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 $q_j (x_j^2 - x_j)$.
- Refutations of degree $d$ can be found in time $n^{O(d)}$ by solving a system of linear equations.
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 $g_i, q_j, p$ 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 \( f_1(x_1, \ldots, x_n) = 0, \ldots, f_m(x_1, \ldots, x_n) = 0 \) of real polynomial equations has no 0/1-solution

\[ \iff \]

there are polynomials \( g_i, q_j, p \) such that

\[ \sum_{i=1}^{m} g_if_i + \sum_{j=1}^{n} q_j(x_j^2 - x_j) + p = -1, \]

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 \( g_if_i, q_j(x_j^2 - x_j) \) and \( p. \)
- Refutations of degree \( d \) can be found in time \( n^{O(d)} \) by solving a linear programme.
Sum-of-squares

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

\( \iff \)

there are polynomials \( g_i, q_j, p \) 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 $f_1(x_1, \ldots, x_n) = 0, \ldots, f_m(x_1, \ldots, x_n) = 0$ of real polynomial equations has no 0/1-solution

$\iff$

there are polynomials $g_i$, $q_j$, $p$ 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
\[ \sum_i g_i f_i + \sum_j q_j (x_j^2 - x_j) + p = -1 \]

\[ \text{SDP} \quad \text{sum-of-squares} \]
\[ \text{LP} \quad \text{Sherali-Adams} \]
\[ \text{LinAlg} \quad \text{Nullstellensatz} \]
(Semi-)algebraic proof systems

Static systems
\[ \sum_i g_i f_i + \sum_j q_j (x_j^2 - x_j) + p = -1 \]

SDP  \hspace{1cm} \text{sum-of-squares}

LP  \hspace{1cm} \text{Sherali-Adams}

LinAlg  \hspace{1cm} \text{Nullstellensatz}
(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
\[ \frac{g=0}{ag+bf=0} \quad \frac{f=0}{ag+bf=0} \]

SDP \hspace{1cm} \text{sum-of-squares}

LP \hspace{1cm} \text{Sherali-Adams}

LinAlg \hspace{1cm} \text{Nullstellensatz}

 polynomial calculus

Gröbner
Polynomial calculus is a derivation system for polynomials.

\[
\begin{align*}
\overline{f_i} & \quad x_j^2 - x_j & \quad g & \quad f & \quad f \\
\frac{g}{ag + bf} & \quad x_jf
\end{align*}
\]

\(f_i = 0\) axiom; \(x_j\) variable; \(f, g, h\) polynomials; \(a, b \in \mathbb{R}\).
Polynomial calculus is a derivation system for polynomials.

\[ f_i \quad x_j^2 - x_j \quad g \frac{f}{ag + bf} \quad f \frac{f}{x_j f} \]

\( f_i = 0 \) 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.

\[ f_i \quad x_j^2 - x_j \quad g \quad \frac{f}{ag + bf} \quad \frac{f}{x_jf} \]

\(f_i = 0\) 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 is a derivation system for polynomials.

\[
\frac{f_i}{x_j^2 - x_j} \quad \frac{g}{ag + bf} \quad \frac{f}{x_j f}
\]

\[f_i = 0\] 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.

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

- 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: $\frac{C}{C \lor x}$, $\frac{C}{C \lor \overline{x}}$

Resolution: $\frac{C \lor x}{C}$, $\frac{C \lor \overline{x}}{C}$

(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: \( \frac{C}{C \lor x} \), \( \frac{C}{C \lor \overline{x}} \)

Resolution: \( \frac{C \lor x}{C} \), \( \frac{C \lor \overline{x}}{C} \)

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

Observation

Width-\(d\) resolution refutation \(\implies\) degree-\(d\) PC refutation.

Reminder: \( f_{x_1 \lor \overline{x}_2 \lor x_3} = (1 - x_1)x_2(1 - x_3) \)
Polynomial calculus simulates resolution

Resolution (slightly unusual version)

Weakening: $\frac{C}{C \lor x}$, $\frac{C}{C \lor \overline{x}}$

Resolution: $\frac{C \lor x}{C \lor \overline{x}}$

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

Observation

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

Reminder: $f_{x_1 \lor \overline{x}_2 \lor x_3} = (1 - x_1)x_2(1 - x_3)$

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

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

- Simulation of resolution rule by addition:

  $\frac{f_C \cdot x}{f_C \cdot (1 - x)}$
(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
\[ \frac{g=0}{ag+bf=0} \]
\[ \frac{f=0}{} \]

\( SDP \) sum-of-squares

\( LP \) Sherali-Adams

\( LinAlg \) Nullstellensatz

\( Gröbner \) polynomial calculus

\( Gröbner \) resolution
(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

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

**SDP** sum-of-squares

**LP** Sherali-Adams

**LinAlg** Nullstellensatz

**Gröbner** polynomial calculus

[BCIP02] \( P_g \)

resolution
(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

$$\begin{align*}
g &= 0 \\
f &= 0 \\
a g + b f &= 0
\end{align*}$$

$SDP$ sum-of-squares

$LP$ Sherali-Adams

$LinAlg$ Nullstellensatz

$SDP$ [IPS99] $\sum_{j=1}^n x_j = n + 1$

$LP$ polynomial calculus

$LinAlg$ [BCIP02] $P_G$

$Gröbner$ resolution

Christoph Berkholz – A comparison of algebraic and semi-algebraic proof systems
(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
\[ \begin{align*}
    g &= 0 \\
    f &= 0 \\
    ag + bf &= 0
\end{align*} \]

SDP
sum-of-squares

[IPS99] \[ \sum_{j=1}^n x_j = n + 1 \]

LP
Sherali-Adams

polynomial calculus

Gröbner

LinAlg
Nullstellensatz

[BCIP02] \[ \mathcal{P}_g \]

resolution
(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
\[ g=0 \quad f=0 \quad ag+bf=0 \]

SDP
\text{sum-of-squares}

LP
\text{Sherali-Adams}

LinAlg
\text{Nullstellensatz}

\[ [\text{IPS99}] \sum_{j=1}^n x_j = n + 1 \]

\[ [\text{BCIP02}] \mathcal{P}_g \]

Gröbner
\text{resolution}
Sherali-Adams simulates resolution

**Theorem [DMR09]**

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

---

**Notation**

A Sherali-Adams proof of $f \geq 0$ from $F$ is the expression $\sum_i g_i f_i + \sum_j q_j (x_2^j - x^j) + p = f$, where $p = \sum_{A, B \subseteq [n]} a_{A, B} \cdot (\prod_{j \in A} x_j \prod_{j \in B} (1 - x^j))$ with $a_{A, B} \geq 0$. 

**Inductive lemma**

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

---

Christoph Berkholz – A comparison of algebraic and semi-algebraic proof systems 11
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 \( \Gamma \), 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: \[ C \vee x \quad C \vee \overline{x} \quad \frac{C}{C} \]
Sherali-Adams simulates resolution

Proof of the inductive lemma

Resolution rule: \( \frac{C \lor x}{C} \frac{C \lor \overline{x}}{C} \)

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

\[ \sum_i g''_i f_i + \sum_j q''_j (x_j^2 - x_j) + p'' = -(1 - x) \cdot f_C \]
Sherali-Adams simulates resolution
Proof of the inductive lemma

Resolution rule: \( \frac{C \lor x}{C} \frac{C \lor \overline{x}}{C} \)

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

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

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: \( \frac{C \lor x}{C} \frac{C \lor \overline{x}}{C} \)

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

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

adding these proofs yields:

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

Weakening rule: \( \frac{C}{C \lor x} \) or \( \frac{C}{C \lor \overline{x}} \)
Sherali-Adams simulates resolution

Proof of the inductive lemma

Resolution rule: \( \frac{C \lor x}{C \lor \overline{x}} \)

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

adding these proofs yields:

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

Weakening rule: \( \frac{C}{C \lor \overline{x}} \) or \( \frac{C}{C \lor x} \)

\[
\sum_i g_i f_i + \sum_j q_j (x_j^2 - x_j) + p = -f_C
\]
Sherali-Adams simulates resolution

Proof of the inductive lemma

Resolution rule: \( \frac{C \lor x \quad C \lor \neg x}{C} \)

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

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

adding these proofs yields:

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

Weakening rule: \( \frac{C}{C \lor \neg x} \) or \( \frac{C}{C \lor x} \)

\[ \sum_i g_i f_i + \sum_j q_j (x_j^2 - x_j) + p + (1 - x)f_C = -f_C + (1 - x)f_C \]
Sherali-Adams simulates resolution

Proof of the inductive lemma

Resolution rule: \[ \frac{C \lor x}{C} \]

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

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

Adding these proofs yields:

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

Weakening rule: \[ \frac{C}{C \lor x} \text{ or } \frac{C}{C \lor x} \]

\[ \sum_i g_i f_i + \sum_j q_j (x_j^2 - x_j) + p + (1 - x)f_C = -f_C + (1 - x)f_C = -xf_C \]
Sherali-Adams simulates resolution

Proof of the inductive lemma

Resolution rule: \( \frac{C \lor x}{C} \quad \frac{C \lor \overline{x}}{C} \)

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

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

adding these proofs yields:

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

Weakening rule: \( \frac{C}{C \lor x} \) or \( \frac{C}{C \lor \overline{x}} \)

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

\[
\sum_i g_i f_i + \sum_j q_j (x_j^2 - x_j) + p + xf_C = -f_C + xf_C = -(1 - x)f_C
\]
(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
\[ \frac{g=0}{ag+bf=0} \quad \frac{f=0}{ag+bf=0} \]

SDP
- sum-of-squares

LP
- Sherali-Adams

LinAlg
- Nullstellensatz

Gröbner
- polynomial calculus

[IPS99] \[ \sum_{j=1}^n x_j = n + 1 \]

[BCIP02] \[ P_G \]

[BCIP02] \[ \mathcal{P}_G \]
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 $F$. 
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: $\frac{g}{ag+bh} + h \cdot f = ag + bh \quad -f^2 = -(ag + bh)^2$
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: \( \frac{g}{ag+bh} \cdot \frac{h}{f} = ag + bh \) \(-f^2 = -(ag + bh)^2\)

\[ \sum_i g'_i f_i + \sum_j q'_j (x_j^2 - x_j) + \sum_\ell (p'_\ell)^2 = -g^2 \]
\[ \sum_i g''_i f_i + \sum_j q''_j (x_j^2 - x_j) + \sum_\ell (p''_\ell)^2 = -h^2 \]
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:** \( \frac{g}{ag+bh} h \)

\[
f = ag + bh \quad -f^2 = -(ag + bh)^2
\]

\[
2a^2 \left( \sum_i g'_i f_i + \sum_j q'_j(x^2_j - x_j) + \sum_{\ell}(p'_\ell)^2 \right) = 2a^2 (-g^2)
\]

\[
2b^2 \left( \sum_i g''_i f_i + \sum_j q''_j(x^2_j - x_j) + \sum_{\ell}(p''_{\ell})^2 \right) = 2b^2 (-h^2)
\]
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: \( \frac{g}{ag+bh} h \)
\[ f = ag + bh \quad -f^2 = -(ag + bh)^2 \]

\[
\sum_i \hat{g}_i f_i + \sum_j \hat{q}_j' (x_j^2 - x_j) + \sum_{\ell} (\hat{p}_{\ell}')^2 = -2(ag)^2 \\
\sum_i \hat{g}_i'' f_i + \sum_j \hat{q}_j'' (x_j^2 - x_j) + \sum_{\ell} (\hat{p}_{\ell}'')^2 = -2(bh)^2 
\]
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-2$d$ sum-of-squares proof from $F$.

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

\[
\sum_i \hat{g}_i' f_i + \sum_j \hat{q}_j' (x_j^2 - x_j) + \sum_{\ell} (\hat{p}_\ell')^2 = -2(ag)^2 \\
\sum_i \hat{g}_i'' f_i + \sum_j \hat{q}_j'' (x_j^2 - x_j) + \sum_{\ell} (\hat{p}_\ell'')^2 = -2(bh)^2 \\
(ag - bh)^2 = (ag)^2 - 2agbh + (bh)^2
\]
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: \( \frac{g}{ag+bh} \ f = ag + bh \quad -f^2 = -(ag + bh)^2 \)

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

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

\[
(ag - bh)^2 = (ag)^2 - 2agbh + (bh)^2
\]

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: 
\[
\frac{g}{ag+bh} = f = ag + bh
\]
\[-f^2 = -(ag + bh)^2
\]

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

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

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

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

\[
(ag - bh)^2 = (ag)^2 - 2agbh + (bh)^2
\]

Adding these sos proofs yields:

\[
\sum_i g_i f_i + \sum_j q_j(x_j^2 - x_j) + \sum_{\ell} (p_\ell)^2 = -(ag)^2 - 2agbh - (bh)^2
\]

\[
= -(ag + bh)^2 = -f^2
\]
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: $\frac{g}{x_sg} \quad f = x_sg \quad -f^2 = -x_s^2g^2$
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:** \( \frac{g}{x_sg} \quad f = x_sg \quad -f^2 = -x_s^2g^2 \)

\[
\sum_i g_i'f_i + \sum_j q_j'(x_j^2 - x_j) + \sum_{\ell} (p'_\ell)^2 = -g^2
\]
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: $\frac{g}{x_s g} f = x_s g$ \quad $-f^2 = -x_s^2 g^2$

\[\sum_i g'_i f_i + \sum_j q'_j (x_j^2 - x_j) + \sum_\ell (p'_\ell)^2 = -g^2\]
\[(g - x_s g)^2 = g^2 - 2x_s g^2 + x_s^2 g^2\]
Inductive lemma
If $f$ has a degree-$d$ polynomial calculus derivation from $F$, then $-f^2 \geq 0$ has a degree-2$d$ sum-of-squares proof from $F$.

Proof.
Multiplication: \[ \frac{g}{x_s g} f = x_s g \quad -f^2 = -x_s^2 g^2 \]

\[ \sum_i g'_i f_i + \sum_j q'_j (x_j^2 - x_j) + \sum_\ell (p'_\ell)^2 = -g^2 \]

\[ (g - x_s g)^2 = g^2 - 2x_s g^2 + x_s^2 g^2 \]

\[ -2g^2 (x_s^2 - x_s) = + 2x_s g^2 - 2x_s^2 g^2 \]
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: \( \frac{g}{x_sg} \quad f = x_sg \quad -f^2 = -x_s^2g^2 \)

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

\[
(g - x_sg)^2 = g^2 - 2x_sg^2 + x_s^2g^2
\]

\[
- 2g^2(x_s^2 - x_s) = + 2x_s^2g^2 - 2x_s^2g^2
\]

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: \( \frac{g}{x_sg} \)
\[ f = x_sg \quad -f^2 = -x_s^2g^2 \]

\[ \sum_i g_i'f_i + \sum_j q_j'(x_j^2 - x_j) + \sum_\ell (p_\ell')^2 = -g^2 \]
\[ (g - x_sg)^2 = g^2 - 2x_sg^2 + x_s^2g^2 \]
\[ -2g^2(x_s^2 - x_s) = + 2x_sg^2 - 2x_s^2g^2 \]

adding these sos proofs yields:
\[ \sum_i g_if_i + \sum_j q_j(x_j^2 - x_j) + \sum_\ell (p_\ell)^2 = -x_s^2g^2 \]
\[ = -f^2 \]
(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
\[ g = 0 \quad \frac{f = 0}{ag + bf = 0} \]

SDP: sum-of-squares

LP: Sherali-Adams

LinAlg: Nullstellensatz

SDP \rightarrow SDP

LP \rightarrow LP

LinAlg \rightarrow LinAlg

SDP \rightarrow LP

LP \rightarrow LinAlg

nullstellensatz

linalg

resolution

[BCIP02] \[ P_G \]

[IPS99] \[ \sum_{j=1}^n x_j = n + 1 \]

[B18]
(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
\[ \frac{g=0}{ag+bf=0} \]

\[ \sum_{j=1}^n x_j = n + 1 \]

\[ \mathcal{P}_g \]

\[ \text{resolution} \]
Lower bounds for static systems

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

1. **Linearity:**
   \[
   D(af + bg) = aD(f) + bD(g)
   \]
   for all \(f, g \in \mathbb{R}[x_1, \ldots, x_n]\).

2. **Multilinearity:**
   \[
   D(\prod_j x_j^{d_j}) = D(\prod_j x_j)
   \]
   \(D(\prod_j x_j^{d_j})\) is a monomial in \(x_1, \ldots, x_n\).

3. **Homogeneity:**
   \[
   D(g \cdot f_i) = 0
   \]
   for every axiom \(f_i \in F\) and \(g \in \mathbb{R}[x_1, \ldots, x_n]\) with \(\deg(g) \leq d - \deg(f_i)\).

4. **Positivity:**
   \[
   D(p) \geq 0
   \]
   for non-negative \(p\), \(\deg(p) \leq d\). (Sherali-Adams/SOS)
Lower bounds for static systems

To prove a degree-$d$ lower bound define a $d$-evaluation $D : \mathbb{R}^{\leq d}[x_1, \ldots, x_n] \rightarrow \mathbb{R}$ 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 $D : \mathbb{R}^{\leq d}[x_1, \ldots, x_n] \rightarrow \mathbb{R}$ 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: $D(\prod_j x_j^{d_j}) = D(\prod_j x_j)$

$\triangleright$ $D$ 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 $f_i \in F$ and $g \in \mathbb{R}[x_1, \ldots, x_n]$ with $\deg(g) \leq d - \deg(f_i)$

$D(p) \geq 0$ for non-negative $p$, $\deg(p) \leq d$. (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)
Lower bounds for static systems

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

\[
D\left(\sum_i g_i f_i + \sum_j q_j (x_j^2 - x_j) + p\right) = D\left(-1\right)
\]
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)

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

$$\sum_i D\left(g_i f_i\right) + \sum_j D\left(q_j(x_j^2 - x_j)\right) + D\left(p\right) \geq 0 \geq D\left(-1\right)$$
Lower bounds for static systems

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

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

\[
\sum_i D(g_i f_i) + \sum_j D\left(q_j(x_j^2 - x_j)\right) + D\left(p\right) = D\left(-1\right)
\]

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

Christoph Berkholz – A comparison of algebraic and semi-algebraic proof systems 18
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 $\mathcal{F}_G$: 

![Pebbling diagram]
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 $\mathcal{F}_G$:
  \[x_{s_i} = 1 \quad (x_{s_i})\]
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 $\mathcal{F}_G$:
  
  \[
  x_{s_i} = 1 \quad (x_{s_i}) \\
  x_t = 0 \quad (\overline{x}_t)
  \]
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 $F_G$:
  \[
  x_{s_i} = 1 \quad (x_{s_i}) \\
  x_t = 0 \quad (\overline{x_t}) \\
  x_u x_v = x_u x_v x_w \quad (x_u \land x_v \rightarrow x_w)
  \]
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 $F_G$:
  
  \[
  \begin{align*}
  x_{s_i} &= 1 & (x_{s_i}) \\
  x_t &= 0 & (\overline{x_t}) \\
  x_u x_v &= x_u x_v x_w & (x_u \land x_v \rightarrow x_w)
  \end{align*}
  \]

- 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 $\mathcal{F}_G$:**
  
  $\begin{align*}
x_{s_i} &= 1 \\
x_t &= 0 \\
x_u x_v &= x_u x_v x_w \quad (x_u \land x_v \rightarrow x_w)
  \end{align*}$

- **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 $\mathcal{F}_G$:
  \[
  x_{s_i} = 1 \quad \text{(}x_{s_i}\text{)}
  \\
  x_t = 0 \quad \text{(}\overline{x}_t\text{)}
  \\
  x_u x_v = x_u x_v x_w \quad \text{(}x_u \land x_v \rightarrow x_w\text{)}
  
  - 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.
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
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.

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

**Theorem** \[\text{PTC77}\]

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

Fix $d = Peb(G) - 1$.

$A \subseteq V(G)$ is reachable, if the player can reach a position in the black $d$-pebble game where all $a \in A$ are pebbled.

$D(\prod_{a \in A} x_a) :=
\begin{cases} 
1 & \text{if } A \text{ is reachable}, \\
0 & \text{otherwise}.
\end{cases}$
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** $\text{Peb}(G)$ 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 $\text{Peb}(G)$ is the minimum number of pebbles needed to place a pebble on the sink $t$.

**Theorem [PTC77]**

There are graphs $G$ on $n$ vertices with $\text{Peb}(G) = \Omega(n/\log n)$. 
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 $\text{Peb}(G)$ is the minimum number of pebbles needed to place a pebble on the sink $t$.

**Theorem [PTC77]**

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

Fix $d = \text{Peb}(G) - 1$. 
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** $\text{Peb}(G)$ is the minimum number of pebbles needed to place a pebble on the sink $t$.

**Theorem [PTC77]**

There are graphs $G$ on $n$ vertices with $\text{Peb}(G) = \Omega\left(\frac{n}{\log n}\right)$.

Fix $d = \text{Peb}(G) - 1$. $A \subseteq V(G)$ 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 \( \text{Peb}(G) \) is the minimum number of pebbles needed to place a pebble on the sink \( t \).

**Theorem [PTC77]**

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

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

\[
D\left(\prod_{a \in A} x_a\right) := \begin{cases} 
1 & \text{if } A \text{ is reachable,} \\
0 & \text{otherwise.}
\end{cases}
\]
Nullstellensatz does not simulate resolution & PC

\[ D\left( \prod_{a \in A} x_a \right) := \begin{cases} 1 & \text{if } A \text{ is reachable,} \\ 0 & \text{otherwise.} \end{cases} \]
Nullstellensatz does not simulate resolution & PC

\[ D\left(\prod_{a \in A} x_a\right) := \begin{cases} 
1 & \text{if } A \text{ is reachable}, \\
0 & \text{otherwise}.
\end{cases} \]

It remains to check \( D\left((\prod_{a \in A} x_a) \cdot f_i\right) = 0 \) for all axioms \( f_i = 0 \) and \( |A| \leq d - \deg(f_i) \):
Nullstellensatz does not simulate resolution & PC

\[ D \left( \prod_{a \in A} x_a \right) := \begin{cases} 1 & \text{if } A \text{ is reachable}, \\ 0 & \text{otherwise}. \end{cases} \]

It remains to check \[ D \left( (\prod_{a \in A} x_a) \cdot f_i \right) = 0 \] for all axioms \( f_i = 0 \) and \( |A| \leq d - \deg(f_i) \):

\[ x_s = 1 \quad \rightsquigarrow \quad D \left( \prod_{a \in A \cup \{s\}} x_a \right) = D \left( \prod_{a \in A} x_a \right) \]
Nullstellensatz does not simulate resolution & PC

\[ D\left( \prod_{a \in A} x_a \right) := \begin{cases} 1 & \text{if } A \text{ is reachable}, \\ 0 & \text{otherwise}. \end{cases} \]

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

\[
\begin{align*}
x_s &= 1 & \sim\Rightarrow & \quad D\left( \prod_{a \in A \cup \{s\}} x_a \right) = D\left( \prod_{a \in A} x_a \right) \\
x_t &= 0 & \sim\Rightarrow & \quad D\left( \prod_{a \in A \cup \{t\}} x_a \right) = 0
\end{align*}
\]
Nullstellensatz does not simulate resolution & PC

\[ D\left( \prod_{a \in A} x_a \right) := \begin{cases} 
1 & \text{if } A \text{ is reachable}, \\
0 & \text{otherwise}.
\end{cases} \]

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

\[
\begin{align*}
    x_s &= 1 & \leadsto & & D\left( \prod_{a \in A \cup \{s\}} x_a \right) = D\left( \prod_{a \in A} x_a \right) \\
    x_t &= 0 & \leadsto & & D\left( \prod_{a \in A \cup \{t\}} x_a \right) = 0 \\
    x_u x_v &= x_u x_v x_w & \leadsto & & D\left( \prod_{a \in A \cup \{u,v\}} x_a \right) = D\left( \prod_{a \in A \cup \{u,v,w\}} x_a \right)
\end{align*}
\]
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 $F_G[+_k]$ to $F_G$: 
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 $F_G[+k]$ to $F_G$:

- 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 $F_{G}[+k]$ to $F_{G}$:

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

We get:

- there is a degree-3 refutation of $F_{G}[+k]$ in polynomial calculus (by substituting everything in the refutation of $F_{G}$)
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 $F_{G[+k]}$ to $F_G$:
- replace every variable $x_v$ by $x_v^{(1)} + \cdots + x_v^{(k)}$

We get:
- there is a degree-3 refutation of $F_{G[+k]}$ in polynomial calculus (by substituting everything in the refutation of $F_G$)
- Sherali-Adams requires degree $\min(\text{Peb}(G), k/2)$:
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 $\mathcal{F}_G[+k]$ to $\mathcal{F}_G$:

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

We get:

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

$$D(x) := \begin{cases} 
(\frac{1}{k})^{|A|} & \text{if } x = \prod_{a \in A} x_a^{(\ell_a)} \text{ and } A \text{ is reachable}, \\
0 & \text{otherwise}.
\end{cases}$$
Sherali-Adams does not simulate polynomial calculus

\[ D(x) := \begin{cases} 
(\frac{1}{k})^{|A|} & \text{if } x = \prod_{a \in A} x_a^{(\ell_a)} \text{ and } A \text{ is reachable,} \\
0 & \text{otherwise.} 
\end{cases} \]
Sherali-Adams does not simulate polynomial calculus

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

Checking \( D(g,f_i) = 0 \) is essentially the same as before.
Sherali-Adams does not simulate polynomial calculus

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

Checking \( D(g_i) = 0 \) 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

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

Checking \( D(g; f_i) = 0 \) 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

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

Checking \( D(g; f_i) = 0 \) 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

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

Checking \( D(g; f_i) = 0 \) 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 \( D(\prod_{(v, \ell) \in I} x_v^{(\ell)}) = 0 \), then \( D(p) = 0 \).
- Otherwise:

\[
D(p) = (\frac{1}{k})^{|I|} + \sum_{\emptyset \neq K \subseteq J} (-1)^{|K|} D(\prod_{(v, \ell) \in K \cup I} x_v, \ell) \\
\geq (\frac{1}{k})^{|I|} (1 - \sum_{z=1}^{|J|} (\frac{|J|}{z}) (\frac{1}{k})^z) 
\]
Sherali-Adams does not simulate polynomial calculus

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

Checking \( D(g;f_i) = 0 \) is essentially the same as before.

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

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

\[
D(p) = \left(\frac{1}{k}\right)^{|I|} + \sum_{\emptyset \neq K \subseteq J} (-1)^{|K|} D\left( \prod_{(v,\ell) \in K \cup I} x_{v,\ell} \right) \\
\geq \left(\frac{1}{k}\right)^{|I|} \left( 1 - \sum_{z=1}^{|J|} \binom{|J|}{z} \left(\frac{1}{k}\right)^z \right) \\
> 0 \text{ if } |J| \leq k/2
\]
(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
\[ \frac{g=0}{ag+bf=0} \]
\[ \frac{f=0}{ag+bf=0} \]

\[ \sum_{j=1}^n x_j = n + 1 \]

SDP \hspace{1cm} \text{sum-of-squares}

LP \hspace{1cm} \text{Sherali-Adams}

LinAlg \hspace{1cm} \text{Nullstellensatz}

Gröbner

polynomial calculus

resolution

[IPS99] \[ \sum_{j=1}^n x_j = n + 1 \]

[B18] \[ g=0, f=0 \]

[BCIP02] \[ P_G \]
Proof size

All simulations do also hold with respect to proof size:

- SOS polynomially simulates PC.

For simulating resolution we encode clauses using twin variables $x, x\neg$:

$$x \lor y \lor z \Rightarrow x\neg y\neg z = 0$$

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 of work to do:

Observation: Every pebbling contradiction $P_G$ has a Nullstellensatz refutation of polynomial size (and large degree).
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 $x, \overline{x}$:

$$x \lor y \lor z \Rightarrow x \land \overline{y} \land \overline{z} = 0$$ $$x + x \overline{y} = 0$$

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 of work to do:

Observation: Every pebbling contradiction $P_G$ has a Nullstellensatz refutation of polynomial size (and large degree).
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 $x$, $\overline{x}$:
  - $x \lor y \lor \overline{z} \leadsto x \overline{x} y \overline{z} = 0$
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 $x, \overline{x}$:
  - $x \lor y \lor \overline{z} \leadsto x \overline{y} \overline{z} = 0$
  - additional axioms $x + x \overline{x} = 0$
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 $x, x^\perp$:
  - $x \lor y \lor \overline{z} \leadsto x^\perp y^\perp z = 0$
  - additional axioms $x + x^\perp = 0$
  - This is necessary because encoding $\bigvee_{i \in \left[ n \right]} x_i$ as $\prod_{i \in \left[ n \right]} (1 - x_i)$ 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 $x, x^\sim$:
  - $x \lor y \lor z \leadsto x^\sim y^\sim z = 0$
  - additional axioms $x + x^\sim = 0$
  - 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 $x, \overline{x}$:
  - $x \lor y \lor \overline{z} \iff x \land \overline{y} \land \overline{z} = 0$
  - additional axioms $x + x \overline{x} = 0$
  - 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 $P_G$ 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 $P = \text{Nullstellensatz, Sherali-Adams, or sum-of-squares.}$
Proof size

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

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

**Lemma**
Let $P = \text{Nullstellensatz}$, 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 $F$ has degree at least $d$, then every $P$-refutation of $F[+2]$ 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 $P = \text{Nullstellensatz, Sherali-Adams, or sum-of-squares}$. If every $P$-refutation of $F$ has degree at least $d$, then every $P$-refutation of $F[+2]$ 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 $F$ has degree at least $d$, then every $P$-refutation of $F[+2]$ 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 $F$ 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
\[ \frac{g=0}{ag+bf=0} \frac{f=0}{\sum_j x_j = n + 1} \]

SDP \quad \text{sum-of-squares}

LP \quad \text{Sherali-Adams}

LinAlg \quad \text{Nullstellensatz}

SDP \quad \text{Gröbner}

LP \quad \text{resolution}

LinAlg \quad \text{polynomial calculus}

[BCIP02] \quad \mathcal{P}_g

[IPS99] \quad \sum_{j=1}^n x_j = n + 1

[B18]
(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
\[ \begin{align*}
  g &= 0 \\
  f &= 0 \\
  \frac{ag + bf}{0} &= 0
\end{align*} \]

- **SDP**
  - sum-of-squares

- **LP**
  - Sherali-Adams

- **LinAlg**
  - Nullstellensatz

- **Positivstellensatz calculus**

- **Gröbner**

- **Polynomial calculus**

- **Resolution**

References:
- [IPS99] \[ \sum_{j=1}^n x_j = n + 1 \]
- [B18] \[ \sum_{j=1}^n x_j = n + 1 \]
- [BCIP02] \[ \mathcal{P}_G \]
(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
\[ \frac{g=0}{ag+bf=0} \]

SDP: sum-of-squares
LP: Sherali-Adams
LinAlg: Nullstellensatz

Positivstellensatz calculus
\[ \sum_{j=1}^{n} x_j = n + 1 \]

SDP \rightarrow LP \rightarrow LinAlg

[B18]

[IPS99]

[B18]

[BCIP02] \( P_G \)

resolution

\( \sum_{j}^{n} \)
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

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

where $p$, $p_l$ 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

\[
f - p - \sum_{I \subseteq [s]} p_I \prod_{\ell \in I} h_\ell \quad \text{from } \mathcal{F}.
\]
Positivstellensatz vs. Positivstellensatz calculus

Theorem [B18]

Positivstellensatz $\equiv$ Positivstellensatz calculus on Boolean systems.

Proof. $(F, H)$ 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 $F = \implies (\text{ind. lemma})$ there is a degree-2 $d$ SOS proof

$$\sum_{m_i = 1} g_i f_i + \sum_{n_j = 1} q_j (x_j^2 - x_j) + p' = -(-1 - p - \sum_{I \subseteq [s]} p_I \prod_{\ell \in I} h_\ell)^2.$$

$\implies$ this is a Positivstellensatz refutation of $(F, H)$.

Interestingly, on non-Boolean systems this is not the case:

$F_{ts}^n = \{ y x_1 = 1, x_2 \neq x_3, \ldots, x_{2n-2} = x_n, x_n = 0 \}$

Theorem [GV01] (without $x_2 = x_3$ axioms):

$\blacktriangleright F_{ts}^n$ has Positivstellensatz calculus refutations of degree $O(n)$.

$\blacktriangleright F_{ts}^n$ requires Positivstellensatz refutations of degree $2 \Omega(n)$. 
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 ≡ Positivstellensatz calculus on Boolean systems.

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

\[\iff -1 - p - \sum_{I \subseteq [s]} p_I \prod_{\ell \in I} h_\ell \text{ has a PC derivation from } \mathcal{F}\]

\[\implies \text{(ind. lemma) there is a degree-2} d \text{ SOS proof}\]

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

\[\sum_{i=1}^m g_if_i + \sum_{j=1}^n q_j(x_j^2 - x_j) + p' = -(-1 - p - \sum_{I \subseteq [s]} p_I \prod_{\ell \in I} h_\ell)^2.\]

\(\implies\) this is a Positivstellensatz refutation of \((\mathcal{F}, \mathcal{H})\). \(\Box\)

Interestingly, on non-Boolean systems this is not the case:

\(\mathcal{F}_{ts}^n := \{yx_1 = 1, x_1^2 = x_2, x_2^2 = x_3, \ldots, x_{n-1}^2 = x_n, x_n = 0\}\)

Theorem [GV01]

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

\(\mathcal{F}_{ts}^n\) has Positivstellensatz calculus refutations of degree \(O(n)\).

\(\mathcal{F}_{ts}^n\) 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
\[ \begin{align*}
  g &= 0 \\
  f &= 0 \\
  ag + bf &= 0
\end{align*} \]

SDP
sum-of-squares

LP
Sherali-Adams

LinAlg
Nullstellensatz

Positivstellensatz calculus

Polynomial calculus

Gröbner

resolution

[IPS99] \[ \sum_{j=1}^n x_j = n + 1 \]

[B18] \[ \mathcal{P}_G \]

[BCIP02] Christoph Berkholz – A comparison of algebraic and semi-algebraic proof systems