SELECTED TOPICS ON SEMI-ALGEBRAIC PROOF COMPLEXITY

$$\frac{1}{2}X^2 + \frac{1}{2}Y^2 - XY = \frac{1}{2}(X-Y)^2$$

Albert Atserias
Universitat Politècnica de Catalunya
Barcelona

Subsets of $\{0,1\}^n$ defined by polynomial inequalities

Variables:

$$X_1, \ldots, X_n \text{ and } \overline{X}_1, \ldots, \overline{X}_n$$

Polynomial inequalities (coefficients in $\mathbb{R}$):

$$P_1 \geq 0, \ldots, P_m \geq 0$$

Axioms:

$$X_i \geq 0 \qquad X_i^2 - X_i = 0$$
$$1 - X_i \geq 0 \qquad 1 - X_i - \overline{X}_i = 0$$

Obviously positive polynomials

Squares:

$$Q^2$$

Non-negative juntas (nn-juntas):

$$\sum_{\substack{I,J\subseteq K\\ I\cap J=\emptyset}} a_{I,J} \prod_{i\in I} X_i \prod_{j\in J} \overline{X}_j$$

where $K \subseteq [n]$ and $a_{I,J} \geq 0$ for all $I, J \subseteq K$ with $I \cap J = \emptyset$.

Obviously positive polynomials

Squares:

$$Q^2$$

Non-negative juntas (nn-juntas):

$$\sum_{\substack{I,J \subseteq K \\ I \cap J = \emptyset}} a_{I,J} \prod_{i \in I} X_i \prod_{j \in J} \overline{X}_j$$

where $K \subseteq [n]$ and $a_{I,J} \geq 0$ for all $I, J \subseteq K$ with $I \cap J = \emptyset$.

Sums of such things:

sos: "sums of squares"
sosonnj: "sums of squares or nn-juntas"

Inferences

given

$$P_1 \geq 0, \ldots, P_m \geq 0$$

and

$Q_0, Q_1, \ldots, Q_m$ that are sums of squares or nn-juntas
with
$$Q_0 + P_1 Q_1 + \cdots + P_m Q_m = P$$

infer

$$P \geq 0.$$

degree of the inference:

$$\max\{\deg(Q_0), \deg(P_i Q_i) : i = 1, \ldots, m\}$$

Proof systems for this talk

LS: twin variables, Boolean axioms, and sums of nn-juntas only.

LS$^+$: twin variables, Boolean axioms, and sosonnj.

Proof systems for this talk

LS: twin variables, Boolean axioms, and sums of nn-juntas only.
LS$^+$: twin variables, Boolean axioms, and sosonnj.

Proofs:

$$P_1 \geq 0, \ldots, P_t \geq 0$$

where each $P_i \geq 0$ is

a) an axiom, or
b) a given inequality, or
c) is derived by an inference.

Proof systems for this talk

LS: twin variables, Boolean axioms, and sums of nn-juntas only.
LS$^+$: twin variables, Boolean axioms, and sosonnj.

Proofs:

$$P_1 \geq 0, \ldots, P_t \geq 0$$

where each $P_i \geq 0$ is

a) an axiom, or
b) a given inequality, or
c) is derived by an inference.

Refutations:

proofs of unsatisfiability $\equiv$ derivations of $-1 \geq 0$

Shape of a proof

$$P_1 \geq 0, \ldots, P_t \geq 0$$

DAG TREE STAR

Dag-like: unrestricted shape, as long as acyclic.
Tree-like: tree; derived inequalities are used at most once.
Star-like (aka static): star; a single inference.

Complexity measures of a proof

$$P_1 \geq 0, \ldots, P_t \geq 0$$

Measures:

Size: bit-size of all coefficients (explicit sums of monomials),
Monomial size: number of monomials,
Length: number of inequalities,
Degree: largest degree of all polynomials and inferences.
Height: longest path from an assumption to the conclusion.

Complexity measures of a proof

$$P_1 \geq 0, \ldots, P_t \geq 0$$

Measures:

Size: bit-size of all coefficients (explicit sums of monomials),
Monomial size: number of monomials,
Length: number of inequalities,
Degree: largest degree of all polynomials and inferences.
Height: longest path from an assumption to the conclusion.

Notation:

$$P_1 \geq 0, \ldots, P_m \geq 0 \;\; \vdash_D^H \;\; P \geq 0$$

Notes

Original Lovasz-Schrijver $\equiv$ dag-like degree-2 LS and LS^+

Notes

Original Lovasz-Schrijver	$\equiv$	dag-like degree-2 LS and LS$^+$
Sherali-Adams	$\equiv$	star-like LS
Lasserre/SOS	$\equiv$	star-like LS$^+$

Notes

Original Lovasz-Schrijver	$\equiv$	dag-like degree-2 LS and LS$^+$
Sherali-Adams	$\equiv$	star-like LS
Lasserre/SOS	$\equiv$	star-like LS$^+$

$$A \ \vdash_D^H \ B \implies A \ \vdash_{HD}^1 \ B$$

Dual view of inferences

Degree-d pseudoexpectations for LS:

$\mathcal{E}_d(S)$: set of linear functionals $E : \mathbb{R}[X_1, \ldots, X_n]_d \to \mathbb{R}$ s.t.

1. $E(1) = 1$,
2. $E(Q) \geq 0$ for nn-junta Q with $\deg(Q) \leq d$,
3. $E(PQ) \geq 0$ for $P \in S$, and nn-junta Q with $\deg(PQ) \leq d$.

Dual view of inferences

Degree-d pseudoexpectations for LS:

$\mathcal{E}_d(S)$: set of linear functionals $E : \mathbb{R}[X_1, \ldots, X_n]_d \to \mathbb{R}$ s.t.

1. $E(1) = 1$,
2. $E(Q) \geq 0$ for nn-junta Q with $\deg(Q) \leq d$,
3. $E(PQ) \geq 0$ for $P \in S$, and nn-junta Q with $\deg(PQ) \leq d$.

Theorem:

$$\max\{ \; c \; : \; S \;\; \vdash^1_d \;\; P \geq c \;\; \text{in LS} \; \} = \min\{ \; E(P) \; : \; E \in \mathcal{E}_d(S) \; \}$$

Dual view of inferences

Degree-d pseudoexpectations for LS:

$\mathcal{E}_d(S)$: set of linear functionals $E : \mathbb{R}[X_1, \ldots, X_n]_d \to \mathbb{R}$ s.t.

1. $E(1) = 1$,
2. $E(Q) \geq 0$ for nn-junta Q with $\deg(Q) \leq d$,
3. $E(PQ) \geq 0$ for $P \in S$, and nn-junta Q with $\deg(PQ) \leq d$.

Theorem:

$$\max\{\ c\ :\ S\ \ \vdash^1_d\ \ P \geq c\ \ \text{in LS}\ \} = \min\{\ E(P)\ :\ E \in \mathcal{E}_d(S)\ \}$$

Corollary:

If $\mathcal{E}^+_d(S) \neq \emptyset$ **then** $S\ \ \nvdash^1_d\ \ -1 \geq 0$ in LS.

Dual view of inferences

Degree-d pseudoexpectations for LS$^+$:

$\mathcal{E}_d^+(S)$: set of linear functionals $E : \mathbb{R}[X_1, \ldots, X_n]_d \to \mathbb{R}$ s.t.

1. $E(1) = 1$,
2. $E(Q) \geq 0$ for square/nnj Q with $\deg(Q) \leq d$,
3. $E(PQ) \geq 0$ for $P \in S$ and square/nnj Q with $\deg(PQ) \leq d$.

Dual view of inferences

Degree-d pseudoexpectations for LS$^+$:

$\mathcal{E}_d^+(S)$: set of linear functionals $E : \mathbb{R}[X_1, \ldots, X_n]_d \to \mathbb{R}$ s.t.

1. $E(1) = 1$,
2. $E(Q) \geq 0$ for square/nnj Q with $\deg(Q) \leq d$,
3. $E(PQ) \geq 0$ for $P \in S$ and square/nnj Q with $\deg(PQ) \leq d$.

Theorem:

$$\max\{ \ c \ : \ S \ \ \vdash_d^1 \ \ P \geq c \ \text{ in LS}^+ \ \} \leq \min\{ \ E(P) \ : \ E \in \mathcal{E}_d^+(S) \ \}$$

Dual view of inferences

Degree-d pseudoexpectations for LS$^+$:

$\mathcal{E}_d^+(S)$: set of linear functionals $E : \mathbb{R}[X_1, \ldots, X_n]_d \to \mathbb{R}$ s.t.

1. $E(1) = 1$,
2. $E(Q) \geq 0$ for square/nnj Q with $\deg(Q) \leq d$,
3. $E(PQ) \geq 0$ for $P \in S$ and square/nnj Q with $\deg(PQ) \leq d$.

Theorem:

$$\max\{\, c \;:\; S \;\vdash_d^1\; P \geq c \text{ in LS}^+ \,\} \leq \min\{\, E(P) \;:\; E \in \mathcal{E}_d^+(S) \,\}$$

Corollary:

If $\mathcal{E}_d^+(S) \neq \emptyset$ **then** $S \;\not\vdash_d^1\; -1 \geq 0$ in LS$^+$.

Some upper bounds

1. basic counting: pigeonhole principle
2. advanced counting: expansion of the noisy hypercube

Basic counting in LS

From

$$X_i + X_j \leq 1 \qquad \text{for all } i, j \in [n], i \neq j$$

it is possible to derive

$$X_1 + \cdots + X_n \leq 1$$

in size-$O(n^3)$ degree-2 height-$2n$ LS

Basic counting (from 2 to 3)

From

$$X + Y \leq 1$$
$$Y + Z \leq 1$$
$$X + Z \leq 1$$

it is possible to derive

$$X + Y + Z \leq 1$$

in size-$O(1)$ degree-2 height-2 LS.

[exercise]

Basic counting (from k to $k+1$)

From

$$\begin{array}{ccccccccccc} X_i & + & X_{i+1} & + & \cdots & + & X_{i+k-1} & & & \leq 1 \\ & & X_{i+1} & + & \cdots & + & X_{i+k-1} & + & X_{i+k} & \leq 1 \\ X_i & & & & + & & & & X_{i+k} & \leq 1 \end{array}$$

it is possible to derive

$$X_i + X_{i+1} + \cdots + X_{i+k-1} + X_{i+k} \leq 1$$

in size-$O(k)$ degree-2 height-2 LS.

[mimic the 2-to-3 derivation]

Pigeonhole principle

From

$$X_{i,k} + X_{j,k} \leq 1 \qquad \text{for all } i, j \in [n], i \neq j, k \in [n-1]$$
$$X_{i,1} + \cdots + X_{i,n-1} \geq 1 \qquad \text{for all } i \in [n]$$

it is possible to derive

$$-1 \geq 0$$

Pigeonhole principle

From

$$
\begin{aligned}
&X_{i,k} + X_{j,k} \le 1 && \text{for all } i, j \in [n], i \neq j, k \in [n-1] \\
&X_{i,1} + \cdots + X_{i,n-1} \ge 1 && \text{for all } i \in [n]
\end{aligned}
$$

it is possible to derive

$$-1 \ge 0$$

in size-$O(n^4)$ degree-2 height-$2n$ LS

Pigeonhole principle

From

$$X_{i,k} + X_{j,k} \leq 1 \qquad \text{for all } i, j \in [n], i \neq j, k \in [n-1]$$
$$X_{i,1} + \cdots + X_{i,n-1} \geq 1 \qquad \text{for all } i \in [n]$$

it is possible to derive

$$-1 \geq 0$$

in size-$O(n^4)$ degree-2 height-$2n$ LS
and also
in size-$O(n^4)$ degree-$2n$ height-1 LS

Pigeonhole principle

From

$$X_{i,k} + X_{j,k} \leq 1 \qquad \text{for all } i, j \in [n], i \neq j, k \in [n-1]$$
$$X_{i,1} + \cdots + X_{i,n-1} \geq 1 \qquad \text{for all } i \in [n]$$

it is possible to derive

$$-1 \geq 0$$

in size-$O(n^4)$ degree-2 height-$2n$ LS
and also
in size-$O(n^4)$ degree-$2n$ height-1 LS (relies on twin variables!)

Tightness (up to constants)

Theorem:

Every height-1 LS-refutation of PHP$^n_{n-1}$ has degree $\geq n$.
Every degree-2 LS-refutation PHP$^n_{n-1}$ has height $\geq n/2$.

Lower bound for PHP^n_{n-1}

Define a degree-$(n-1)$ pseudoexpectation for LS:

$$E\Big(\prod_{\ell=1}^{d} X_{i_\ell,j_\ell}^{c_\ell}\Big) := ?$$

Lower bound for PHP^n_{n-1}

Define a degree-$(n-1)$ pseudoexpectation for LS:

$$E\Big(\prod_{\ell=1}^{d} X_{i_\ell,j_\ell}^{c_\ell}\Big) := ?$$

1. choose $i^* \in [n] - \{i_1, \ldots, i_d\}$ arbitrarily (use $d \leq n-1$)

Lower bound for PHP^n_{n-1}

Define a degree-$(n-1)$ pseudoexpectation for LS:

$$E\Big(\prod_{\ell=1}^{d} X_{i_\ell,j_\ell}^{c_\ell}\Big) := ?$$

1. choose $i^* \in [n] - \{i_1, \ldots, i_d\}$ arbitrarily (use $d \leq n-1$)
2. consider 1-1 maps $\alpha : [n] - \{i^*\} \xrightarrow{1-1} [n-1]$

Lower bound for PHP^n_{n-1}

Define a degree-$(n-1)$ pseudoexpectation for LS:

$$E\Big(\prod_{\ell=1}^{d} X_{i_\ell,j_\ell}^{c_\ell}\Big) := ?$$

1. choose $i^* \in [n] - \{i_1, \ldots, i_d\}$ arbitrarily (use $d \leq n-1$)
2. consider 1-1 maps $\alpha : [n] - \{i^*\} \xrightarrow{1-1} [n-1]$
3. define

$$E\Big(\prod_{\ell=1}^{d} X_{i_\ell,j_\ell}^{c_\ell}\Big) := \Pr_{\alpha}\Big[\alpha(i_1) = j_1, \ldots, \alpha(i_d) = j_d\Big]$$

with α chosen **u.a.r.** as in 2.

Basic counting in LS$^+$

Lemma:

There is a size-$O(n^2)$ degree-2 height-1 LS$^+$-derivation of $X_1 + \cdots + X_n \leq 1$ from $X_i + X_j \leq 1$

Basic counting in LS$^+$

Lemma:

There is a size-$O(n^2)$ degree-2 height-1 LS$^+$-derivation of $X_1 + \cdots + X_n \leq 1$ from $X_i + X_j \leq 1$

$$\sum_{i \neq j} (1 - X_i - X_j) X_j + (n-2) \sum_i (X_i^2 - X_i) + \Big(1 - \sum_i X_i\Big)^2$$

$$=$$

$$1 - \sum_i X_i$$

Basic counting in LS$^+$

Lemma:

There is a size-$O(n^2)$ degree-2 height-1 LS$^+$-derivation of $X_1 + \cdots + X_n \leq 1$ from $X_i + X_j \leq 1$

$$\sum_{i \neq j}(1 - X_i - X_j)X_j + (n-2)\sum_i (X_i^2 - X_i) + \Big(1 - \sum_i X_i\Big)^2$$

$$=$$

$$1 - \sum_i X_i$$

Corollary:

There is a size-$O(n^3)$ degree-2 height-1 LS$^+$-refutation of PHP$^n_{n-1}$.

Advanced counting: SSE of δ-noisy hypercube

Vertices:

$$V := \{+1, -1\}^m$$

Edge-weights:

$$W(a,b) := \Pr_{\substack{\mathbf{u}\sim V \\ \mathbf{v}\sim N_\delta(\mathbf{u})}} \left[\mathbf{u} = a \text{ and } \mathbf{v} = b \right]$$

Advanced counting: SSE of δ-noisy hypercube

Vertices:

$$V := \{+1, -1\}^m$$

Edge-weights:

$$W(a,b) := \Pr_{\substack{\mathbf{u}\sim V \\ \mathbf{v}\sim N_\delta(\mathbf{u})}} \left[\, \mathbf{u} = a \text{ and } \mathbf{v} = b \,\right]$$

Note:

$$W(A,B) = \mathop{\mathbb{E}}_{\substack{\mathbf{u}\sim V \\ \mathbf{v}\sim N_\delta(\mathbf{u})}} \left[\, A(\mathbf{u})B(\mathbf{v}) \,\right] \quad \textbf{and} \quad W(A,V) = \frac{|A|}{2^m}$$

Advanced counting: SSE of δ-noisy hypercube

Vertices:

$$V := \{+1, -1\}^m$$

Edge-weights:

$$W(a,b) := \Pr_{\substack{\mathbf{u}\sim V \\ \mathbf{v}\sim N_\delta(\mathbf{u})}} \left[\ \mathbf{u} = a \text{ and } \mathbf{v} = b\ \right]$$

Note:

$$W(A,B) = \mathop{\mathbb{E}}_{\substack{\mathbf{u}\sim V \\ \mathbf{v}\sim N_\delta(\mathbf{u})}} \left[\ A(\mathbf{u})B(\mathbf{v})\ \right] \quad \textbf{and} \quad W(A,V) = \frac{|A|}{2^m}$$

Theorem:

$$W(A,\overline{A}) \geq \frac{|A|}{2^m}\left(1 - \sqrt[1+\delta]{\frac{|A|}{2^m}}\right)$$

Motivation

Small-Set Expansion (SSE(ϵ,δ) Problem):

Given a weighted n-vertex regular graph $G = (V, E, W)$, distinguish between:

YES: all $A \subseteq V$ with $|A| = \delta n$ have $W(A, \overline{A}) \geq (1 - \epsilon)\delta$,
NO: exists $A \subseteq V$ with $|A| = \delta n$ such that $W(A, \overline{A}) \leq \epsilon\delta$.

Motivation

Small-Set Expansion (SSE(ϵ,δ) Problem):

Given a weighted n-vertex regular graph $G = (V, E, W)$, distinguish between:

YES: all $A \subseteq V$ with $|A| = \delta n$ have $W(A, \overline{A}) \geq (1 - \epsilon)\delta$,
NO: exists $A \subseteq V$ with $|A| = \delta n$ such that $W(A, \overline{A}) \leq \epsilon\delta$.

SSE Hypothesis:

$\forall \epsilon > 0$ $\exists \delta > 0$ s.t. SSE(ϵ,δ) is NP-hard.

Motivation

Small-Set Expansion (SSE(ϵ,δ) Problem):

Given a weighted n-vertex regular graph $G = (V, E, W)$, distinguish between:

YES: all $A \subseteq V$ with $|A| = \delta n$ have $W(A, \overline{A}) \geq (1 - \epsilon)\delta$,
NO: exists $A \subseteq V$ with $|A| = \delta n$ such that $W(A, \overline{A}) \leq \epsilon\delta$.

SSE Hypothesis:

$\forall\epsilon > 0$ $\exists\delta > 0$ s.t. SSE(ϵ,δ) is NP-hard.

Question:

Noisy hypercube is a YES instance.
Can low-degree SOS certify so?

Version to be proved in SOS

Case $\delta = 1/3$ **of SSE**:

$$W(A, \overline{A}) \geq \frac{|A|}{2^m} \left(1 - \sqrt[\frac{4}{3}]{\frac{|A|}{2^m}}\right)$$

Version to be proved in SOS

Case $\delta = 1/3$ **of SSE**:

$$W(A, \overline{A}) \geq \frac{|A|}{2^m}\left(1 - \sqrt[\frac{4}{3}]{\frac{|A|}{2^m}}\right)$$

We'll prove:

$$W(A, A) \leq \frac{|A|}{2^m}\left(\frac{3\epsilon}{4} + \frac{1}{4\epsilon^3}\frac{|A|}{2^m}\right) \qquad \text{for all } \epsilon > 0$$

Version to be proved in SOS

Case $\delta = 1/3$ **of SSE**:

$$W(A, \overline{A}) \geq \frac{|A|}{2^m} \left(1 - \sqrt[\frac{4}{3}]{\frac{|A|}{2^m}}\right)$$

We'll prove:

$$W(A, A) \leq \frac{|A|}{2^m} \left(\frac{3\epsilon}{4} + \frac{1}{4\epsilon^3} \frac{|A|}{2^m}\right) \qquad \text{for all } \epsilon > 0$$

which, by choosing $\epsilon = \sqrt[4]{|A|/2^m}$, **implies**:

$$W(A, \overline{A}) \geq \frac{|A|}{2^m} \left(1 - \sqrt[4]{\frac{|A|}{2^m}}\right)$$

Statement of small-set expansion

If $X_a \equiv$ "a is in the set A", **then**

$$W(A, A) = \sum_{a \in V} \sum_{b \in V} W(a, b) X_a X_b \quad \textbf{and} \quad \frac{|A|}{2^m} = \sum_{a \in V} \frac{1}{2^m} X_a$$

Statement of small-set expansion

If $X_a \equiv$ "a is in the set A", **then**

$$W(A, A) = \sum_{a \in V} \sum_{b \in V} W(a, b) X_a X_b \quad \textbf{and} \quad \frac{|A|}{2^m} = \sum_{a \in V} \frac{1}{2^m} X_a$$

Theorem: For every $\epsilon > 0$,

$$\sum_{a \in V} \sum_{b \in V} W(a, b) X_a X_b \leq \left(\sum_{a \in V} \frac{1}{2^m} X_a \right) \left(\frac{3\epsilon}{4} + \frac{1}{4\epsilon^3} \left(\sum_{a \in V} \frac{1}{2^m} X_a \right) \right)$$

has a size-$2^{O(m)}$ degree-8 height-1 LS$^+$-derivation.

How is it proved?

by induction on m
and Cauchy-Schwartz

(and, believe it or not, that's it)

$$XY \le \frac{1}{2}X^2 + \frac{1}{2}Y^2$$

or

$$\frac{1}{2}X^2 + \frac{1}{2}Y^2 - XY = \frac{1}{2}(X - Y)^2$$

How is it proved?

by induction on m
and Cauchy-Schwartz

(and, believe it or not, that's it)

$$XY \leq \tfrac{1}{2}X^2 + \tfrac{1}{2}Y^2$$

or

$$\tfrac{1}{2}X^2 + \tfrac{1}{2}Y^2 - XY = \tfrac{1}{2}(X-Y)^2$$

$$X^3Y \leq \tfrac{3}{4}X^4 + \tfrac{1}{4}Y^4$$

or

$$\tfrac{3}{4}X^4 + \tfrac{1}{4}Y^4 - X^3Y = \tfrac{1}{2}X^2(X-Y)^2 + \tfrac{1}{4}(X^2-Y^2)^2$$

Human-readable proof

$$W(A, A) = \mathop{\mathbb{E}}_{\substack{\mathbf{u} \sim V \\ \mathbf{v} \sim N_\delta(\mathbf{u})}} \left[\, A(\mathbf{u}) A(\mathbf{v}) \, \right]$$

Human-readable proof

$$W(A, A) = \underset{\substack{\mathbf{u} \sim V \\ \mathbf{v} \sim N_\delta(\mathbf{u})}}{\mathbb{E}} \left[\, A(\mathbf{u}) A(\mathbf{v}) \, \right] = \underset{\mathbf{u} \sim V}{\mathbb{E}} \left[\, A(\mathbf{u}) \mathrm{T}_\delta A(\mathbf{u}) \, \right]$$

Human-readable proof

$$
\begin{aligned}
W(A, A) &= \mathop{\mathbb{E}}_{\substack{\mathbf{u} \sim V \\ \mathbf{v} \sim N_\delta(\mathbf{u})}} \left[\, A(\mathbf{u}) A(\mathbf{v}) \,\right] = \mathop{\mathbb{E}}_{\mathbf{u} \sim V} \left[\, A(\mathbf{u}) \mathrm{T}_\delta A(\mathbf{u}) \,\right] \\
&\leq \frac{3\epsilon}{4} \mathop{\mathbb{E}}_{\mathbf{u} \sim V} \left[\, A(\mathbf{u})^2 \,\right] + \frac{1}{4\epsilon^3} \mathop{\mathbb{E}}_{\mathbf{u} \sim V} \left[\, (\mathrm{T}_\delta A(\mathbf{u}))^4 \,\right]
\end{aligned}
$$

Human-readable proof

$$
\begin{aligned}
W(A, A) = \underset{\substack{\mathbf{u} \sim V \\ \mathbf{v} \sim N_\delta(\mathbf{u})}}{\mathbb{E}} \left[\, A(\mathbf{u}) A(\mathbf{v}) \,\right] &= \underset{\mathbf{u} \sim V}{\mathbb{E}} \left[\, A(\mathbf{u}) \mathrm{T}_\delta A(\mathbf{u}) \,\right] \\
&\le \frac{3\epsilon}{4} \underset{\mathbf{u} \sim V}{\mathbb{E}} \left[\, A(\mathbf{u})^2 \,\right] + \frac{1}{4\epsilon^3} \underset{\mathbf{u} \sim V}{\mathbb{E}} \left[\, (\mathrm{T}_\delta A(\mathbf{u}))^4 \,\right] \\
&\le \frac{3\epsilon}{4} \underset{\mathbf{u} \sim V}{\mathbb{E}} \left[\, A(\mathbf{u})^2 \,\right] + \frac{1}{4\epsilon^3} \underset{\mathbf{u} \sim V}{\mathbb{E}} \left[\, A(\mathbf{u})^2 \,\right]^2
\end{aligned}
$$

Human-readable proof

$$
\begin{aligned}
W(A, A) &= \mathop{\mathbb{E}}_{\substack{\mathbf{u}\sim V \\ \mathbf{v}\sim N_\delta(\mathbf{u})}} \left[\, A(\mathbf{u}) A(\mathbf{v}) \,\right] = \mathop{\mathbb{E}}_{\mathbf{u}\sim V} \left[\, A(\mathbf{u}) \mathrm{T}_\delta A(\mathbf{u}) \,\right] \\
&\leq \frac{3\epsilon}{4} \mathop{\mathbb{E}}_{\mathbf{u}\sim V} \left[\, A(\mathbf{u})^2 \,\right] + \frac{1}{4\epsilon^3} \mathop{\mathbb{E}}_{\mathbf{u}\sim V} \left[\, (\mathrm{T}_\delta A(\mathbf{u}))^4 \,\right] \\
&\leq \frac{3\epsilon}{4} \mathop{\mathbb{E}}_{\mathbf{u}\sim V} \left[\, A(\mathbf{u})^2 \,\right] + \frac{1}{4\epsilon^3} \mathop{\mathbb{E}}_{\mathbf{u}\sim V} \left[\, A(\mathbf{u})^2 \,\right]^2 \\
&= \mathop{\mathbb{E}}_{\mathbf{u}\sim V} \left[\, A(\mathbf{u})^2 \,\right] \left(\frac{3\epsilon}{4} + \frac{1}{4\epsilon^3} \mathop{\mathbb{E}}_{\mathbf{u}\sim V} \left[\, A(\mathbf{u})^2 \,\right] \right)
\end{aligned}
$$

Human-readable proof

$$
\begin{aligned}
W(A,A) &= \mathop{\mathbb{E}}_{\substack{\mathbf{u}\sim V \\ \mathbf{v}\sim N_\delta(\mathbf{u})}} \left[\, A(\mathbf{u})A(\mathbf{v}) \,\right] = \mathop{\mathbb{E}}_{\mathbf{u}\sim V} \left[\, A(\mathbf{u})\mathrm{T}_\delta A(\mathbf{u}) \,\right] \\
&\leq \frac{3\epsilon}{4} \mathop{\mathbb{E}}_{\mathbf{u}\sim V} \left[\, A(\mathbf{u})^2 \,\right] + \frac{1}{4\epsilon^3} \mathop{\mathbb{E}}_{\mathbf{u}\sim V} \left[\, (\mathrm{T}_\delta A(\mathbf{u}))^4 \,\right] \\
&\leq \frac{3\epsilon}{4} \mathop{\mathbb{E}}_{\mathbf{u}\sim V} \left[\, A(\mathbf{u})^2 \,\right] + \frac{1}{4\epsilon^3} \mathop{\mathbb{E}}_{\mathbf{u}\sim V} \left[\, A(\mathbf{u})^2 \,\right]^2 \\
&= \mathop{\mathbb{E}}_{\mathbf{u}\sim V} \left[\, A(\mathbf{u})^2 \,\right] \left(\frac{3\epsilon}{4} + \frac{1}{4\epsilon^3} \mathop{\mathbb{E}}_{\mathbf{u}\sim V} \left[\, A(\mathbf{u})^2 \,\right] \right)
\end{aligned}
$$

2-to-4 hypercontractivity; two-function version:

$$
\mathop{\mathbb{E}}_{\mathbf{u}\sim V} \left[\, (\mathrm{T}_\delta F(\mathbf{u}))^2 \, (\mathrm{T}_\delta G(\mathbf{u}))^2 \,\right] \leq \mathop{\mathbb{E}}_{\mathbf{u}\sim V} \left[\, F(\mathbf{u})^2 \,\right] \mathop{\mathbb{E}}_{\mathbf{u}\sim V} \left[\, G(\mathbf{u})^2 \,\right]
$$

Roadmap for rest of the talk

1. size-degree trade-offs
2. expanding systems of parity equations
3. interpolation
4. some open problems
5. credit

Trade-offs

Let F be an unsatisfiable 3-CNF on N variables.
Then:

$$D = O(\sqrt{N \log(S)}) \quad \textbf{or} \quad S = 2^{\Omega(D^2/N)}$$

Trade-offs

Let F be an unsatisfiable 3-CNF on N variables.
Then:

$$D = O(\sqrt{N \log(S)}) \quad \textbf{or} \quad S = 2^{\Omega(D^2/N)}$$

for Resolution:

S: minimum length of resolution refutations of F
D: minimum width of resolution refutation of F

Trade-offs

Let F be an unsatisfiable 3-CNF on N variables.
Then:

$$D = O(\sqrt{N \log(S)}) \quad \textbf{or} \quad S = 2^{\Omega(D^2/N)}$$

for Resolution:

S: minimum length of resolution refutations of F
D: minimum width of resolution refutation of F

for PC:

S: minimum monomial-size of PC refutations of F
D: minimum degree of PC refutations of F

Size-degree trade-off for height-1 LS

Theorem: For height-1 LS-refutations of a 3-CNF F we have

$$D = O(\sqrt{N \log S}) \quad \textbf{or} \quad S = 2^{\Omega(D^2/N)}$$

where

S: minimum monomial-size of height-1 LS-refutations of F
D: minimum degree of height-1 LS-refutations of F

Sanity checks

Check 1:

S of EPHP^n_{n-1} is $O(n^4)$
D of EPHP^n_{n-1} is n
BUT
N of EPHP^n_{n-1} is $\geq n^2$.

Sanity checks

Check 1:

S of EPHP$^n_{n-1}$ is $O(n^4)$
D of EPHP$^n_{n-1}$ is n
BUT
N of EPHP$^n_{n-1}$ is $\geq n^2$.

Check 2:

S of G-PHP$^n_{n-1}$ is $O(n^4)$
N of G-PHP$^n_{n-1}$ is $\leq n \cdot \text{maxdeg}(G)$
BUT
D of G-PHP$^n_{n-1}$ is $O(\text{maxdeg}(G))$ [exercise]

Proof of size-degree trade-off

Proof strategy:

$$\text{refutation of } F \text{ with } \leq S \text{ many monomials of degree } \geq D$$
$$\Downarrow$$
$$\text{refutation of } F \text{ with degree } \leq D + (N/D)\ln(S)$$

Proof of size-degree trade-off

Proof strategy:

$$\text{refutation of } F \text{ with } \leq S \text{ many monomials of degree } \geq D$$
$$\Downarrow$$
$$\text{refutation of } F \text{ with degree } \leq D + (N/D)\ln(S)$$

Once this is proved, set:

$$D = \sqrt{N \ln(S)}$$

The inductive argument

Proof by induction on N:

refutation of F with $\leq S$ many monomials of degree $\geq D$

$$\Downarrow$$

refutation of F with degree $\leq D + (N/D)\ln(S)$

The inductive argument

Proof by induction on N:

$$\text{refutation of } F \text{ with} \leq S \text{ many monomials of degree} \geq D$$
$$\Downarrow$$
$$\text{refutation of } F \text{ with degree} \leq D + (N/D)\ln(S)$$

1. Start at a refutation Π with exactly $T \leq S$ monomials of degree $\geq D$.

The inductive argument

Proof by induction on N:

refutation of F with $\leq S$ many monomials of degree $\geq D$

$$\Downarrow$$

refutation of F with degree $\leq D + (N/D)\ln(S)$

1. Start at a refutation Π with exactly $T \leq S$ monomials of degree $\geq D$.
2. Find a variable X that appears $\geq DT/N$ many such monomials.

The inductive argument

Proof by induction on N:

$$\text{refutation of } F \text{ with } \leq S \text{ many monomials of degree } \geq D$$
$$\Downarrow$$
$$\text{refutation of } F \text{ with degree } \leq D + (N/D)\ln(S)$$

1. Start at a refutation Π with exactly $T \leq S$ monomials of degree $\geq D$.
2. Find a variable X that appears $\geq DT/N$ many such monomials.
3. Apply induction hypothesis to $\Pi|_{X=0}$ and $\Pi|_{X=1}$.

The inductive argument

Proof by induction on N:

$$\text{refutation of } F \text{ with } \leq S \text{ many monomials of degree } \geq D$$
$$\Downarrow$$
$$\text{refutation of } F \text{ with degree } \leq D + (N/D)\ln(S)$$

1. Start at a refutation Π with exactly $T \leq S$ monomials of degree $\geq D$.
2. Find a variable X that appears $\geq DT/N$ many such monomials.
3. Apply induction hypothesis to $\Pi|_{X=0}$ and $\Pi|_{X=1}$.
4. (note: $\Pi|_{X=0}$ has $\leq T(1-D/N) \leq S(1-D/N)$ such monomials).

The inductive argument

Proof by induction on N:

$$\text{refutation of } F \text{ with } \leq S \text{ many monomials of degree } \geq D$$
$$\Downarrow$$
$$\text{refutation of } F \text{ with degree } \leq D + (N/D)\ln(S)$$

1. Start at a refutation Π with exactly $T \leq S$ monomials of degree $\geq D$.
2. Find a variable X that appears $\geq DT/N$ many such monomials.
3. Apply induction hypothesis to $\Pi|_{X=0}$ and $\Pi|_{X=1}$.
4. (note: $\Pi|_{X=0}$ has $\leq T(1 - D/N) \leq S(1 - D/N)$ such monomials).
5. (note: $\Pi|_{X=1}$ has still $\leq T \leq S$ such monomials).

The inductive argument

Proof by induction on N:

refutation of F with $\leq S$ many monomials of degree $\geq D$

$$\Downarrow$$

refutation of F with degree $\leq D + (N/D)\ln(S)$

1. Start at a refutation Π with exactly $T \leq S$ monomials of degree $\geq D$.
2. Find a variable X that appears $\geq DT/N$ many such monomials.
3. Apply induction hypothesis to $\Pi|_{X=0}$ and $\Pi|_{X=1}$.
4. (note: $\Pi|_{X=0}$ has $\leq T(1 - D/N) \leq S(1 - D/N)$ such monomials).
5. (note: $\Pi|_{X=1}$ has still $\leq T \leq S$ such monomials).
6. I.H. for $F|_{X=0}$ gives degree $\leq D + (N/D)\ln(S) - 1$.

The inductive argument

Proof by induction on N:

$$\text{refutation of } F \text{ with } \leq S \text{ many monomials of degree } \geq D$$
$$\Downarrow$$
$$\text{refutation of } F \text{ with degree } \leq D + (N/D)\ln(S)$$

1. Start at a refutation Π with exactly $T \leq S$ monomials of degree $\geq D$.
2. Find a variable X that appears $\geq DT/N$ many such monomials.
3. Apply induction hypothesis to $\Pi|_{X=0}$ and $\Pi|_{X=1}$.
4. (note: $\Pi|_{X=0}$ has $\leq T(1 - D/N) \leq S(1 - D/N)$ such monomials).
5. (note: $\Pi|_{X=1}$ has still $\leq T \leq S$ such monomials).
6. I.H. for $F|_{X=0}$ gives degree $\leq D + (N/D)\ln(S) - 1$.
7. I.H. for $F|_{X=1}$ gives degree $\leq D + (N/D)\ln(S)$.

The inductive argument

Proof by induction on N:

$$\text{refutation of } F \text{ with } \leq S \text{ many monomials of degree } \geq D$$
$$\Downarrow$$
$$\text{refutation of } F \text{ with degree } \leq D + (N/D)\ln(S)$$

1. Start at a refutation Π with exactly $T \leq S$ monomials of degree $\geq D$.
2. Find a variable X that appears $\geq DT/N$ many such monomials.
3. Apply induction hypothesis to $\Pi|_{X=0}$ and $\Pi|_{X=1}$.
4. (note: $\Pi|_{X=0}$ has $\leq T(1 - D/N) \leq S(1 - D/N)$ such monomials).
5. (note: $\Pi|_{X=1}$ has still $\leq T \leq S$ such monomials).
6. I.H. for $F|_{X=0}$ gives degree $\leq D + (N/D)\ln(S) - 1$.
7. I.H. for $F|_{X=1}$ gives degree $\leq D + (N/D)\ln(S)$.
8. Combine into degree $\leq D + (N/D)\ln(S)$ for F.

Combination lemma

Combination lemma:

Combination lemma

Combination lemma:

$F\|_{X=0} \vdash -1 \geq 0$		degree-$(D-1)$, height-1
$F\|_{X=1} \vdash -1 \geq 0$		degree-D, height-1

Combination lemma

Combination lemma:

$F\|_{X=0}$	$\vdash$	$-1 \geq 0$	degree-$(D-1)$, height-1
$F\|_{X=1}$	$\vdash$	$-1 \geq 0$	degree-D, height-1
F	$\vdash$	$X \geq \epsilon$	degree-$(D-1)$, height-1, for some $\epsilon > 0$
F	$\vdash$	$X \leq 1-\delta$	degree-D, height-1, for some $\delta > 0$

Combination lemma

Combination lemma:

$F\|_{X=0}$	$\vdash$	$-1 \geq 0$	degree-$(D-1)$, height-1
$F\|_{X=1}$	$\vdash$	$-1 \geq 0$	degree-D, height-1
F	$\vdash$	$X \geq \epsilon$	degree-$(D-1)$, height-1, for some $\epsilon > 0$
F	$\vdash$	$X \leq 1-\delta$	degree-D, height-1, for some $\delta > 0$
F	$\vdash$	$X\overline{X} \geq \epsilon\overline{X}$	degree-D, height-1
F	$\vdash$	$\epsilon X \leq \epsilon(1-\delta)$	degree-D, height-1

Combination lemma

Combination lemma:

$F\|_{X=0}$	$\vdash$	$-1 \geq 0$	degree-$(D-1)$, height-1
$F\|_{X=1}$	$\vdash$	$-1 \geq 0$	degree-D, height-1
F	$\vdash$	$X \geq \epsilon$	degree-$(D-1)$, height-1, for some $\epsilon > 0$
F	$\vdash$	$X \leq 1-\delta$	degree-D, height-1, for some $\delta > 0$
F	$\vdash$	$X\overline{X} \geq \epsilon\overline{X}$	degree-D, height-1
F	$\vdash$	$\epsilon X \leq \epsilon(1-\delta)$	degree-D, height-1
F	$\vdash$	$X\overline{X} \geq \epsilon\delta$	degree-D, height-1

Combination lemma

Combination lemma:

$F\|_{X=0}$	$\vdash$	$-1 \geq 0$	degree-$(D-1)$, height-1
$F\|_{X=1}$	$\vdash$	$-1 \geq 0$	degree-D, height-1
F	$\vdash$	$X \geq \epsilon$	degree-$(D-1)$, height-1, for some $\epsilon > 0$
F	$\vdash$	$X \leq 1-\delta$	degree-D, height-1, for some $\delta > 0$
F	$\vdash$	$X\overline{X} \geq \epsilon\overline{X}$	degree-D, height-1
F	$\vdash$	$\epsilon X \leq \epsilon(1-\delta)$	degree-D, height-1
F	$\vdash$	$X\overline{X} \geq \epsilon\delta$	degree-D, height-1
F	$\vdash$	$0 \geq \epsilon\delta$	degree-D, height-1

Unrestricting lemma

Unrestricting lemma:

$$
\begin{array}{l}
F|_{X=0} \vdash^1_D -1 \geq 0 \\
\qquad\quad \Downarrow \\
F \cup \{X \leq 0\} \vdash^1_D -1 \geq 0 \\
\qquad\quad \Downarrow \\
\min\{E(X) : E \in \mathcal{E}_D(F)\} > 0 \\
\qquad\quad \Downarrow \\
\max\{c : F \vdash^1_D X \geq c\} > 0
\end{array}
$$

Unrestricting lemma

Unrestricting lemma:

$F\|_{X=0} \vdash^1_D -1 \geq 0$	$F\|_{X=1} \vdash^1_D -1 \geq 0$
$\Downarrow$	$\Downarrow$
$F \cup \{X \leq 0\} \vdash^1_D -1 \geq 0$	$F \cup \{X \geq 1\} \vdash^1_D -1 \geq 0$
$\Downarrow$	$\Downarrow$
$\min\{E(X) : E \in \mathcal{E}_D(F)\} > 0$	$\max\{E(X) : E \in \mathcal{E}_D(F)\} < 1$
$\Downarrow$	$\Downarrow$
$\max\{c : F \vdash^1_D X \geq c\} > 0$	$\min\{c : F \vdash^1_D X \geq c\} < 1$

Consequences: l.b.'s for tree-like LS

Corollary (if done carefully):

Setting

L: minimum length of **tree-like** degree-2 LS-refutations of F
D: minimum degree of height-1 LS-refutation of F

we have

$$D = O(\sqrt{N \log L}) \quad \textbf{or} \quad L = 2^{\Omega(D^2/N)}$$

Feasible interpolation

Problem statement:

Feasible interpolation

Problem statement:
Given a refutation of

$$A_0(\mathbf{a}, \mathbf{y}_0) \wedge A_1(\mathbf{a}, \mathbf{y}_1)$$

find $i \in \{0, 1\}$ so that

$$A_i(\mathbf{a}, \mathbf{y}_i) \text{ is unsatisfiable.}$$

Feasible interpolation for degree-2 LS

The goal is to convert

$$
\begin{aligned}
&K_1(\mathbf{y}) + L_1(\mathbf{z}) + c_1 \geq 0 \\
&K_2(\mathbf{y}) + L_2(\mathbf{z}) + c_2 \geq 0 \\
&\vdots \\
&c_m \geq 0
\end{aligned}
$$

into

$$
\begin{aligned}
&K_1(\mathbf{y}) + a_1 \geq 0 \qquad && L_1(\mathbf{z}) + b_1 \geq 0 \\
&K_2(\mathbf{y}) + a_2 \geq 0 && L_2(\mathbf{z}) + b_2 \geq 0 \\
&\vdots && \vdots \\
&a_m \geq 0 && b_m \geq 0
\end{aligned}
$$

where

$c_i = a_i + b_i$ for all $i = 1, \ldots, m$.

One inference step:

$$
\begin{aligned}
&\textstyle\sum_{i,j} c_i^1 \cdot (K_i(\mathbf{y}) + L_i(\mathbf{z}) + c_i) \cdot y_j && + \\
&\textstyle\sum_{i,j} c_i^2 \cdot (K_i(\mathbf{y}) + L_i(\mathbf{z}) + c_i) \cdot \bar{y}_j && + \\
&\textstyle\sum_{i,j} c_i^3 \cdot (K_i(\mathbf{y}) + L_i(\mathbf{z}) + c_i) \cdot z_j && + \\
&\textstyle\sum_{i,j} c_i^4 \cdot (K_i(\mathbf{y}) + L_i(\mathbf{z}) + c_i) \cdot \bar{z}_j && + \\
&\textstyle\sum_{i} c_i^5 \cdot (K_i(\mathbf{y}) + L_i(\mathbf{z}) + c_i) && + \\
&\textstyle\sum_{j} c_i^6 \cdot (y_j^2 - y_j) && + \\
&\textstyle\sum_{j} c_i^7 \cdot (z_j^2 - z_j) \\
&= \\
&K_t(\mathbf{y}) + L_t(\mathbf{z}) + c_t
\end{aligned}
$$

Inductively $c_i = a_i + b_i$, so also:

$$
\begin{aligned}
&\textstyle\sum_{i,j} c_i^1 \cdot (K_i(\mathbf{y}) + a_i) \cdot y_j &+\quad& \textstyle\sum_{i,j} c_i^1 \cdot (L_i(\mathbf{z}) + b_i) \cdot y_j &+\\
&\textstyle\sum_{i,j} c_i^2 \cdot (K_i(\mathbf{y}) + a_i) \cdot \bar{y}_j &+\quad& \textstyle\sum_{i,j} c_i^2 \cdot (L_i(\mathbf{z}) + b_i) \cdot \bar{y}_j &+\\
&\textstyle\sum_{i,j} c_i^3 \cdot (K_i(\mathbf{y}) + a_i) \cdot z_j &+\quad& \textstyle\sum_{i,j} c_i^3 \cdot (L_i(\mathbf{z}) + b_i) \cdot z_j &+\\
&\textstyle\sum_{i,j} c_i^4 \cdot (K_i(\mathbf{y}) + a_i) \cdot \bar{z}_j &+\quad& \textstyle\sum_{i,j} c_i^4 \cdot (L_i(\mathbf{z}) + b_i) \cdot \bar{z}_j &+\\
&\textstyle\sum_{i} c_i^5 \cdot (K_i(\mathbf{y}) + a_i) &+\quad& \textstyle\sum_{i} c_i^5 \cdot (L_i(\mathbf{z}) + b_i) &+\\
&\textstyle\sum_{j} c_i^6 \cdot (y_j^2 - y_j) &+\quad& &\\
&\textstyle\sum_{j} c_i^7 \cdot (z_j^2 - z_j) & & &\\
&= & & &\\
&K_t(\mathbf{y}) + L_t(\mathbf{z}) + c_t & & &
\end{aligned}
$$

$$\begin{aligned}
&\textstyle\sum_{i,j} c_i^1 \cdot (K_i(\mathbf{y}) + a_i) \cdot y_j + \\
&\textstyle\sum_{i,j} c_i^2 \cdot (K_i(\mathbf{y}) + a_i) \cdot \bar{y}_j + \\
&\textstyle\sum_{i} c_i^5 \cdot (K_i(\mathbf{y}) + a_i) + \\
&\textstyle\sum_{j} c_i^6 \cdot (y_j^2 - y_j) \\
&= \\
&K_t'(\mathbf{y}) + a'
\end{aligned}$$

$$\begin{aligned}
&\textstyle\sum_{i,j} c_i^3 \cdot (L_i(\mathbf{z}) + b_i) \cdot z_j + \\
&\textstyle\sum_{i,j} c_i^4 \cdot (L_i(\mathbf{z}) + b_i) \cdot \bar{z}_j + \\
&\textstyle\sum_{i} c_i^5 \cdot (L_i(\mathbf{z}) + b_i) + \\
&\textstyle\sum_{j} c_i^7 \cdot (z_j^2 - z_j) \\
&= \\
&L_t'(\mathbf{z}) + b'
\end{aligned}$$

$$\begin{aligned}
&\textstyle\sum_{i,j} c_i^1 \cdot (L_i(\mathbf{z}) + b_i) \cdot y_j + \\
&\textstyle\sum_{i,j} c_i^2 \cdot (L_i(\mathbf{z}) + b_i) \cdot \bar{y}_j + \\
&\textstyle\sum_{i,j} c_i^3 \cdot (K_i(\mathbf{y}) + a_i) \cdot z_j + \\
&\textstyle\sum_{i,j} c_i^4 \cdot (K_i(\mathbf{y}) + a_i) \cdot \bar{z}_j \\
&= \\
&K_t''(\mathbf{y}) + L_t''(\mathbf{z}) + c''
\end{aligned}$$

$$\begin{array}{l}\sum_{i,j} c_i^1 \cdot (K_i(\mathbf{y}) + a_i) \cdot y_j + \\ \sum_{i,j} c_i^2 \cdot (K_i(\mathbf{y}) + a_i) \cdot \bar{y}_j + \\ \sum_i c_i^5 \cdot (K_i(\mathbf{y}) + a_i) + \\ \sum_j c_i^6 \cdot (y_j^2 - y_j) \\ = \\ K_t'(\mathbf{y}) + a'\end{array} \qquad \begin{array}{l}\sum_{i,j} c_i^3 \cdot (L_i(\mathbf{z}) + b_i) \cdot z_j + \\ \sum_{i,j} c_i^4 \cdot (L_i(\mathbf{z}) + b_i) \cdot \bar{z}_j + \\ \sum_i c_i^5 \cdot (L_i(\mathbf{z}) + b_i) + \\ \sum_j c_i^7 \cdot (z_j^2 - z_j) \\ = \\ L_t'(\mathbf{z}) + b'\end{array}$$

$$\begin{array}{l}\{K_i(\mathbf{y}) + a_i \geq 0\} \\ \{L_i(\mathbf{z}) + b_i \geq 0\} \\ \{0 \leq y_j \leq 1\} \\ \{0 \leq z_j \leq 1\}\end{array} \quad \models_{\mathbb{R}} \quad K_t''(\mathbf{y}) + L_t''(\mathbf{z}) + c'' \geq 0$$

$$\sum_{i,j} c_i^1 \cdot (K_i(\mathbf{y}) + a_i) \cdot y_j + \sum_{i,j} c_i^2 \cdot (K_i(\mathbf{y}) + a_i) \cdot \bar{y}_j + \sum_i c_i^5 \cdot (K_i(\mathbf{y}) + a_i) + \sum_j c_i^6 \cdot (y_j^2 - y_j) = K'_t(\mathbf{y}) + a'$$

$$\sum_{i,j} c_i^3 \cdot (L_i(\mathbf{z}) + b_i) \cdot z_j + \sum_{i,j} c_i^4 \cdot (L_i(\mathbf{z}) + b_i) \cdot \bar{z}_j + \sum_i c_i^5 \cdot (L_i(\mathbf{z}) + b_i) + \sum_j c_i^7 \cdot (z_j^2 - z_j) = L'_t(\mathbf{z}) + b'$$

$$\begin{array}{l} \{K_i(\mathbf{y}) + a_i \geq 0\} \\ \{L_i(\mathbf{z}) + b_i \geq 0\} \\ \{0 \leq y_j \leq 1\} \\ \{0 \leq z_j \leq 1\} \end{array} \models_{\mathbb{R}} \quad K''_t(\mathbf{y}) + L''_t(\mathbf{z}) + c'' \geq 0$$

Apply Farkas' Lemma!

$$\sum_{i,j} c_i^1 \cdot (K_i(\mathbf{y}) + a_i) \cdot y_j + \sum_{i,j} c_i^2 \cdot (K_i(\mathbf{y}) + a_i) \cdot \bar{y}_j + \sum_i c_i^5 \cdot (K_i(\mathbf{y}) + a_i) + \sum_j c_i^6 \cdot (y_j^2 - y_j) = K_t'(\mathbf{y}) + a'$$

$$\sum_{i,j} c_i^3 \cdot (L_i(\mathbf{z}) + b_i) \cdot z_j + \sum_{i,j} c_i^4 \cdot (L_i(\mathbf{z}) + b_i) \cdot \bar{z}_j + \sum_i c_i^5 \cdot (L_i(\mathbf{z}) + b_i) + \sum_j c_i^7 \cdot (z_j^2 - z_j) = L_t'(\mathbf{z}) + b'$$

$$\sum_i c_i^8 \cdot (K_i(\mathbf{y}) + a_i) + \sum_i c_i^9 \cdot (L_i(\mathbf{z}) + b_i) = K_t''(\mathbf{y}) + L_t''(\mathbf{z}) + c''$$

$$\sum_{i,j} c_i^1 \cdot (K_i(\mathbf{y}) + a_i) \cdot y_j + \sum_{i,j} c_i^2 \cdot (K_i(\mathbf{y}) + a_i) \cdot \bar{y}_j + \sum_i c_i^5 \cdot (K_i(\mathbf{y}) + a_i) + \sum_j c_i^6 \cdot (y_j^2 - y_j) = K_t'(\mathbf{y}) + a'$$

$$\sum_{i,j} c_i^3 \cdot (L_i(\mathbf{z}) + b_i) \cdot z_j + \sum_{i,j} c_i^4 \cdot (L_i(\mathbf{z}) + b_i) \cdot \bar{z}_j + \sum_i c_i^5 \cdot (L_i(\mathbf{z}) + b_i) + \sum_j c_i^7 \cdot (z_j^2 - z_j) = L_t'(\mathbf{z}) + b'$$

$$\sum_i c_i^8 \cdot (K_i(\mathbf{y}) + a_i) + \sum_i c_i^9 \cdot (L_i(\mathbf{z}) + b_i) = K_t''(\mathbf{y}) + L_t''(\mathbf{z}) + c''$$

Split!

$$\begin{aligned}
&\textstyle\sum_{i,j} c_i^1 \cdot (K_i(\mathbf{y}) + a_i) \cdot y_j + \\
&\textstyle\sum_{i,j} c_i^2 \cdot (K_i(\mathbf{y}) + a_i) \cdot \bar{y}_j + \\
&\textstyle\sum_{i} c_i^5 \cdot (K_i(\mathbf{y}) + a_i) + \\
&\textstyle\sum_{j} c_i^6 \cdot (y_j^2 - y_j) \\
&= \\
&K_t'(\mathbf{y}) + a'
\end{aligned}$$

$$\begin{aligned}
&\textstyle\sum_{i,j} c_i^3 \cdot (L_i(\mathbf{z}) + b_i) \cdot z_j + \\
&\textstyle\sum_{i,j} c_i^4 \cdot (L_i(\mathbf{z}) + b_i) \cdot \bar{z}_j + \\
&\textstyle\sum_{i} c_i^5 \cdot (L_i(\mathbf{z}) + b_i) + \\
&\textstyle\sum_{j} c_i^7 \cdot (z_j^2 - z_j) \\
&= \\
&L_t'(\mathbf{z}) + b'
\end{aligned}$$

$$\begin{aligned}
&\textstyle\sum_{i} c_i^8 \cdot (K_i(\mathbf{y}) + a_i) \\
&= \\
&K_t''(\mathbf{y}) + a''
\end{aligned}$$

$$\begin{aligned}
&\textstyle\sum_{i} c_i^9 \cdot (L_i(\mathbf{z}) + b_i) \\
&= \\
&L_t''(\mathbf{z}) + b''
\end{aligned}$$

where $a'' + b'' = c''$.

Consequences: conditional l.b.'s for dag-like

Corollary:

If explicit one-way permutations exist,
then there are explicit 3-CNFs that are
hard for (size of) dag-like degree-2 LS and LS^+.

Consequences: conditional l.b.'s for dag-like

Corollary:

If explicit one-way permutations exist,
then there are explicit 3-CNFs that are hard for (size of) dag-like degree-2 LS and LS^+.

$$(F(Y) = X \wedge Y_i = 0) \wedge (F(Z) = X \wedge Z_i = 1)$$

Open problems

Open problems

1. unconditional size lower bounds for dag-like LS and LS^+?

Open problems

1. unconditional size lower bounds for dag-like LS and LS^+?
2. degree-$\omega(1)$ SOS l.b. for SSE and UG problems?

Open problems

1. unconditional size lower bounds for dag-like LS and LS^+?
2. degree-$\omega(1)$ SOS l.b. for SSE and UG problems?
3. degree-$\omega(1)$ SOS l.b. for 1.99-approx. of vertex cover?

Open problems

1. unconditional size lower bounds for dag-like LS and LS^+?
2. degree-$\omega(1)$ SOS l.b. for SSE and UG problems?
3. degree-$\omega(1)$ SOS l.b. for 1.99-approx. of vertex cover?
4. degree-$\Omega(n)$ SA l.b. for 1.99-approx. of vertex cover?

Open problems

1. unconditional size lower bounds for dag-like LS and LS^+?
2. degree-$\omega(1)$ SOS l.b. for SSE and UG problems?
3. degree-$\omega(1)$ SOS l.b. for 1.99-approx. of vertex cover?
4. degree-$\Omega(n)$ SA l.b. for 1.99-approx. of vertex cover?
5. candidates missing! [SOS killed them]

References (1 of 2)

- **Lovasz-Schrijver 1991**: degree-2 inferences only; iterate.
- **Sherali-Adams 1990**: nn-juntas without twin variables; do not iterate.
- **Parrilo 2000**: beyond 0-1, thus sos only; do not iterate.
- **Lasserre 2000**: beyond 0-1 via primal-dual approach; do not iterate.
- **Pudlak 1997**: explicit inference rules for original LS.
- **Grigoriev-Vorobyov 1999**: Positivstellensatz calculus inspired by PC.
- **Grigoriev-Hirsch-Pasechnik 2002**: many variants, systematic,...
- **Dantchev 2007**: Sherali-Adams with twin variables.

References (2 of 2)

- Upper bounds for $\sum_{i=1}^{n} X_i \leq 1$ and PHP in LS: **Pudlak**.
- Upper bounds for PHP in SA: **Dantchev-Martin-Rhodes 2009**.
- Upper bounds for $\sum_{i=1}^{n} X_i \leq 1$ in SOS: **Lovasz-Schrijver**.
- Upper bounds for PHP in SOS: **Grigoriev-Hirsch-Pasechnik**.
- Lower bound PHP for SA: **Dantchev-Martin-Rhodes 2009**.
- SSE problem: **Raghavendra-Steurer** .
- Hypercontractivity in SOS: **Barak et al. 2012**, **O'Donnell-Zhu 2012**.
- Degree-size tradeoff for LS and LS$^+$: **Pitassi-Segerlind 2009-2012**.
- Interpolation for degree-2 LS: **Pudlak 1997**.
- Interpolation for degree-2 LS$^+$: **Dash 2000**.
- Lower bound Tseitin: **Grigoriev 1999**.
- Lower bound random 3-XOR: **Schoenebeck 2008**.