Size-Degree Trade-offs for Sums-of-Squares Proofs

Tuomas Hakoniemi

Universitat Politècnica de Catalunya

Joint work with Albert Atserias

The setup

Let

$$Q = \{p_1 = 0, \ldots, p_m = 0, q_1 \geq 0, \ldots, q_\ell \geq 0\}$$

be a set of polynomial constraints of degree at most k in variables

$$x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n,$$

and denote by I_n the ideal generated by

$$\{x_i^2 - x_i, \bar{x}_i^2 - \bar{x}_i, x_i + \bar{x}_i - 1 : i \in [n]\}.$$

SOS proofs over the Boolean hypercube

A Sums-of-Squares (SOS) proof of non-negativity of a polynomial r from Q is an identity of the form

$$r \equiv s_0 + \sum_{i \in [\ell]} s_i q_i + \sum_{j \in [m]} t_j p_j \mod I_n,$$

where s_0 and s_i are sums of squares and t_j are arbitrary polynomials.

SOS proofs over the Boolean hypercube

A Sums-of-Squares (SOS) proof of non-negativity of a polynomial r from Q is an identity of the form

$$r \equiv s_0 + \sum_{i \in [\ell]} s_i q_i + \sum_{j \in [m]} t_j p_j \mod I_n,$$

where s_0 and s_i are sums of squares and t_j are arbitrary polynomials.

An SOS refutation of Q is a proof of non-negativity of -1 from Q.

SOS proofs over the Boolean hypercube

Complexity measures:

- Degree: maximum degree of the summands on the right hand side.
- Monomial size: number of monomials in explicit representations of s_0, s_i's as sums of squares and t_j's.

SOS proofs over the Boolean hypercube

Complexity measures:

- Degree: maximum degree of the summands on the right hand side.
- Monomial size: number of monomials in explicit representations of s_0, s_i's as sums of squares and t_j's.

Notation:

- $Q \vdash_d p \geq q$: there is a degree d SOS proof of non-negativity of $p - q$ from Q.

Dual view: Pseudoexpectations

A degree d *pseudoexpectation* for Q is a linear functional $E\colon \mathbb{R}[x]_{\leq d} \to \mathbb{R}$ such that

- $E(1) = 1$;
- $E(p) \geq 0$ if $Q \vdash_d p \geq 0$.

Dual view: Pseudoexpectations

A degree d *pseudoexpectation* for Q is a linear functional $E\colon \mathbb{R}[x]_{\leq d} \to \mathbb{R}$ such that

- $E(1) = 1$;
- $E(p) \geq 0$ if $Q \vdash_d p \geq 0$.

Theorem (Duality theorem for SOS)

For any polynomial p of degree at most 2d,

$$\sup\{r \in \mathbb{R} : Q \vdash_{2d} p \geq r\} = \inf\{E(p) : E \in \mathcal{E}_{2d}(Q)\}.$$

Moreover, if $\mathcal{E}_{2d}(Q) \neq \emptyset$, then the infimum is attained.

Duality theorem

The key lemma in proving the duality theorem is the following.

Lemma

For any $p \in \mathbb{R}[x]_{2d}$, there is $r \in \mathbb{R}_+$ such that

$$Q \vdash_{2d} r \geq p.$$

Then the duality theorem follows from a general duality for pre-ordered vector spaces with order units.

The trade-off theorem

Theorem

If there is a refutation of Q of monomial size s, then there is a refutation of Q of degree at most

$$4\sqrt{2(n+1)\log s} + k + 4.$$

The trade-off theorem

Theorem

If there is a refutation of Q of monomial size s, then there is a refutation of Q of degree at most

$$4\sqrt{2(n+1)\log s} + k + 4.$$

Corollary

If $d(Q) \geq k+4$, then

$$s(Q) \geq \exp((d(Q)-k-4)^2/(32(n+1))),$$

where $s(Q)$ and $d(Q)$ are the minimum monomial size and degree of an SOS refutation for Q.

Related work

Theorem (Clegg, Edmonds, Impagliazzo '96)

Let F be a k-CNF. If there is a Resolution refutation of F of length s, then there is a Polynomial Calculus refutation of F of degree $O(\sqrt{n \log s} + k)$.

Related work

Theorem (Clegg, Edmonds, Impagliazzo '96)

Let F be a k-CNF. If there is a Resolution refutation of F of length s, then there is a Polynomial Calculus refutation of F of degree $O(\sqrt{n \log s} + k)$.

Theorem (Impagliazzo, Pudlák, Sgall '99)

Let Q be a set of equality constraints of degree at most k. If there is a Polynomial Calculus refutation of Q with at most s monomials, then there is one of degree $O(\sqrt{n \log s} + k)$.

Related work

Theorem (Clegg, Edmonds, Impagliazzo '96)

Let F be a k-CNF. If there is a Resolution refutation of F of length s, then there is a Polynomial Calculus refutation of F of degree $O(\sqrt{n \log s} + k)$.

Theorem (Impagliazzo, Pudlák, Sgall '99)

Let Q be a set of equality constraints of degree at most k. If there is a Polynomial Calculus refutation of Q with at most s monomials, then there is one of degree $O(\sqrt{n \log s} + k)$.

Theorem (Ben-Sasson, Wigderson '01)

Let F be a k-CNF. If there is a Resolution refutation of F of length s, then there is one of width $O(\sqrt{n \log s} + k)$.

The trade-off theorem

Proof strategy:

- First show that:
  - there is a refutation of Q with at most s many (explicit) monomials of degree at least d

$$\Longrightarrow$$

there is a refutation of degree $c(d + (n/d) \log s) + k$.

The trade-off theorem

Proof strategy:

- First show that:
  - there is a refutation of Q with at most s many (explicit) monomials of degree at least d

$$\Longrightarrow$$

  there is a refutation of degree $c(d + (n/d)\log s) + k$.
- Theorem follows by choosing $d \approx \sqrt{n \log s}$.

The trade-off theorem

Proof sketch: Given a refutation Π of Q with at most s wide monomials:

The trade-off theorem

Proof sketch: Given a refutation Π of Q with at most s wide monomials:

- Find a popular literal ℓ among the wide monomials of the proof.

The trade-off theorem

Proof sketch: Given a refutation Π of Q with at most s wide monomials:

- Find a popular literal ℓ among the wide monomials of the proof.
- Set the literal to 0 and 1 to obtain refutations $\Pi[\ell/0]$ and $\Pi[\ell/1]$ of $Q[\ell/0]$ and $Q[\ell/1]$.

The trade-off theorem

Proof sketch: Given a refutation Π of Q with at most s wide monomials:

- Find a popular literal ℓ among the wide monomials of the proof.
- Set the literal to 0 and 1 to obtain refutations $\Pi[\ell/0]$ and $\Pi[\ell/1]$ of $Q[\ell/0]$ and $Q[\ell/1]$.
- Inductively obtain refutations of $Q[\ell/0]$ and $Q[\ell/1]$ of degree $2d' - 2$ and $2d'$, respectively.

The trade-off theorem

Proof sketch: Given a refutation Π of Q with at most s wide monomials:

- Find a popular literal ℓ among the wide monomials of the proof.
- Set the literal to 0 and 1 to obtain refutations $\Pi[\ell/0]$ and $\Pi[\ell/1]$ of $Q[\ell/0]$ and $Q[\ell/1]$.
- Inductively obtain refutations of $Q[\ell/0]$ and $Q[\ell/1]$ of degree $2d' - 2$ and $2d'$, respectively.
- Combine these refutations into a refutation of Q of degree at most $2d'$.

Unrestricting lemmas

$Q[\ell/0] \vdash_{2d-2} -1 \geq 0$

Unrestricting lemmas

$$Q[\ell/0] \vdash_{2d-2} -1 \geq 0$$
$$\Downarrow$$
$$Q \cup \{\ell = 0\} \vdash_{2d-2} -1 \geq 0$$

Unrestricting lemmas

$$Q[\ell/0] \vdash_{2d-2} -1 \geq 0$$

$$\Downarrow$$

$$Q \cup \{\ell = 0\} \vdash_{2d-2} -1 \geq 0$$

$$\Downarrow$$

$$\inf\{E(\ell) : E \in \mathcal{E}_{2d-2}(Q)\} > 0$$

Unrestricting lemmas

$$Q[\ell/0] \vdash_{2d-2} -1 \geq 0$$
$$\Downarrow$$
$$Q \cup \{\ell = 0\} \vdash_{2d-2} -1 \geq 0$$
$$\Downarrow$$
$$\inf\{E(\ell) : E \in \mathcal{E}_{2d-2}(Q)\} > 0$$
$$\Downarrow$$
$$\sup\{r \in \mathbb{R} : Q \vdash_{2d-2} \ell \geq r\} > 0$$

Unrestricting lemmas

$$Q[\ell/0] \vdash_{2d-2} -1 \geq 0$$
$$\Downarrow$$
$$Q \cup \{\ell = 0\} \vdash_{2d-2} -1 \geq 0$$
$$\Downarrow$$
$$\inf\{E(\ell) : E \in \mathcal{E}_{2d-2}(Q)\} > 0$$
$$\Downarrow$$
$$\sup\{r \in \mathbb{R} : Q \vdash_{2d-2} \ell \geq r\} > 0$$
$$\Downarrow$$
$$Q \vdash_{2d-2} \ell \geq \epsilon$$

Unrestricting lemmas

$$\begin{array}{c} Q[\ell/0] \vdash_{2d-2} -1 \geq 0 \\ \Downarrow \\ Q \cup \{\ell = 0\} \vdash_{2d-2} -1 \geq 0 \\ \Downarrow \\ \inf\{E(\ell) : E \in \mathcal{E}_{2d-2}(Q)\} > 0 \\ \Downarrow \\ \sup\{r \in \mathbb{R} : Q \vdash_{2d-2} \ell \geq r\} > 0 \\ \Downarrow \\ Q \vdash_{2d-2} \ell \geq \epsilon \end{array}$$

$$\begin{array}{c} Q[\ell/1] \vdash_{2d} -1 \geq 0 \\ \Downarrow \\ Q \cup \{\bar{\ell} = 0\} \vdash_{2d} -1 \geq 0 \\ \Downarrow \\ \inf\{E(\bar{\ell}) : E \in \mathcal{E}_{2d}(Q)\} > 0 \\ \Downarrow \\ \sup\{r \in \mathbb{R} : Q \vdash_{2d} \bar{\ell} \geq r\} > 0 \\ \Downarrow \\ Q \vdash_{2d} \ell \leq 1 - \delta \end{array}$$

Unrestricting lemmas

$$
\begin{tikzcd}[row sep=small, column sep=tiny]
Q[\ell/0] \vdash_{2d-2} -1 \geq 0 \arrow[d, Rightarrow] & & Q[\ell/1] \vdash_{2d} -1 \geq 0 \arrow[d, Rightarrow] \\
Q \cup \{\ell = 0\} \vdash_{2d-2} -1 \geq 0 \arrow[d, Rightarrow] & & Q \cup \{\bar{\ell} = 0\} \vdash_{2d} -1 \geq 0 \arrow[d, Rightarrow] \\
\inf\{E(\ell) : E \in \mathcal{E}_{2d-2}(Q)\} > 0 \arrow[d, Rightarrow] & & \inf\{E(\bar{\ell}) : E \in \mathcal{E}_{2d}(Q)\} > 0 \arrow[d, Rightarrow] \\
\sup\{r \in \mathbb{R} : Q \vdash_{2d-2} \ell \geq r\} > 0 \arrow[d, Rightarrow] & & \sup\{r \in \mathbb{R} : Q \vdash_{2d} \bar{\ell} \geq r\} > 0 \arrow[d, Rightarrow] \\
Q \vdash_{2d-2} \ell \geq \epsilon \arrow[dr, Rightarrow] & & Q \vdash_{2d} \ell \leq 1 - \delta \arrow[dl, Rightarrow] \\
& Q \vdash_{2d} -1 \geq 0 &
\end{tikzcd}
$$

Unrestricting lemmas

$$
\begin{array}{ccc}
Q[\ell/0] \vdash_{2d-2} -1 \geq 0 & & Q[\ell/1] \vdash_{2d} -1 \geq 0 \\
\Downarrow ? & & \Downarrow ? \\
Q \cup \{\ell = 0\} \vdash_{2d-2} -1 \geq 0 & & Q \cup \{\bar{\ell} = 0\} \vdash_{2d} -1 \geq 0 \\
\Downarrow & & \Downarrow \\
\inf\{E(\ell) : E \in \mathcal{E}_{2d-2}(Q)\} > 0 & & \inf\{E(\bar{\ell}) : E \in \mathcal{E}_{2d}(Q)\} > 0 \\
\Downarrow & & \Downarrow \\
\sup\{r \in \mathbb{R} : Q \vdash_{2d-2} \ell \geq r\} > 0 & & \sup\{r \in \mathbb{R} : Q \vdash_{2d} \bar{\ell} \geq r\} > 0 \\
\Downarrow & & \Downarrow \\
Q \vdash_{2d-2} \ell \geq \epsilon & & Q \vdash_{2d} \ell \leq 1 - \delta \\
& \searrow \quad \swarrow & \\
& Q \vdash_{2d} -1 \geq 0 &
\end{array}
$$

Unrestricting lemmas

$$Q[\ell/0] \vdash_{2d-2} -1 \geq 0$$
$$\Downarrow ?$$
$$Q \cup \{\ell = 0\} \vdash_{2d-2} -1 \geq 0$$

$$Q[\ell/1] \vdash_{2d} -1 \geq 0$$
$$\Downarrow ?$$
$$Q \cup \{\bar{\ell} = 0\} \vdash_{2d} -1 \geq 0$$

The problem: The degree of $q[\ell/0]$ might be a lot smaller than the degree of q, and so a naive simulation might exceed the degree bound.

SOS proofs modulo cut-off functions

Call any function $c\colon Q \to \mathbb{N}$ such that

$$c(q) \geq \deg(q)$$

a cut-off function for Q.

SOS proofs modulo cut-off functions

Call any function $c\colon Q \to \mathbb{N}$ such that

$$c(q) \geq \deg(q)$$

a cut-off function for Q. An SOS proof

$$p \equiv s_0 + \sum_i s_i q_i + \sum_j t_j p_j \mod I_n$$

is of degree $2d$ modulo a cut-off function c, if

- $\deg(p), \deg(s_0) \leq 2d$;
- $\deg(s_i) \leq 2d - c(q_i)$ and $\deg(t_j) \leq 2d - c(p_j)$.

Duality for SOS modulo cut-off functions

Theorem (Duality modulo cut-off functions)

Let c be a cut-off function for Q. Then for any polynomial p of degree at most $2d$,

$$\sup\{r \in \mathbb{R} : Q \vdash^{c}_{2d} p \geq r\} = \inf\{E(p) : E \in \mathcal{E}^{c}_{2d}(Q)\}.$$

Moreover, if $\mathcal{E}^{c}_{2d}(Q) \neq \emptyset$, then the infimum is attained.

Updated proof sketch

Given a refutation Π of Q with at most s wide monomials and a cut-off function c for Q:

1. Find a popular literal ℓ among the wide monomials of the proof.
2. Set the literal to 0 and 1 to obtain refutations $\Pi[\ell/0]$ and $\Pi[\ell/1]$.
3. Inductively obtain refutations of $Q[\ell/0]$ and $Q[\ell/1]$ of degree $2d' - 2$ and $2d'$ modulo c, respectively.
4. Combine the refutations into a refutation of Q of degree at most $2d'$ modulo c.

Unrestricting lemmas with cut-off functions

$$
\begin{array}{ccc}
Q[\ell/0] \vdash^{c}_{2d-2} -1 \geq 0 & & Q[\ell/1] \vdash^{c}_{2d} -1 \geq 0 \\
\Downarrow & & \Downarrow \\
Q \cup \{\ell = 0\} \vdash^{c[\ell \mapsto 1]}_{2d-2} -1 \geq 0 & & Q \cup \{\bar{\ell} = 0\} \vdash^{c[\bar{\ell} \mapsto 1]}_{2d} -1 \geq 0 \\
\Downarrow & & \Downarrow \\
\inf\{E(\ell) : E \in \mathcal{E}^{c}_{2d-2}(Q)\} > 0 & & \inf\{E(\bar{\ell}) : E \in \mathcal{E}^{c}_{2d}(Q)\} > 0 \\
\Downarrow & & \Downarrow \\
\sup\{r \in \mathbb{R} : Q \vdash^{c}_{2d-2} \ell \geq r\} > 0 & & \sup\{r \in \mathbb{R} : Q \vdash^{c}_{2d} \bar{\ell} \geq r\} > 0 \\
\Downarrow & & \Downarrow \\
Q \vdash^{c}_{2d-2} \ell \geq \epsilon & & Q \vdash^{c}_{2d} \ell \leq 1 - \delta \\
& \searrow \quad \swarrow & \\
& Q \vdash^{c}_{2d} -1 \geq 0 &
\end{array}
$$

Trade-off for Positivstellensatz proofs

The above proof works for Positivstellensatz proofs of bounded product-width, i.e. the maximum number of inequality constraints multiplied together. We have the following.

Theorem

If there is a refutation of Q of monomial size s and product-width w, then there is a refutation of Q of degree at most

$$4\sqrt{2(n+1)\log s} + kw + 4.$$

Applications: Knapsack

Theorem (Grigoriev '01)

For odd k,

$$\mathrm{KNAPSACK}_{n,k} := \{2x_1 + \ldots + 2x_n = k\}$$

requires degree $\Omega(\min\{k, 2n-k\})$ to refute in SOS.

Applications: Knapsack

Theorem (Grigoriev '01)

For odd k,

$$\mathrm{KNAPSACK}_{n,k} := \{2x_1 + \ldots + 2x_n = k\}$$

requires degree $\Omega(\min\{k, 2n - k\})$ to refute in SOS.

Corollary

For odd k, every SOS refutation of $\mathrm{KNAPSACK}_{n,k}$ has monomial size $\exp(\Omega(k^2/n))$.

Applications: Tseitin formulas

Let $(G_n)_{n\in\mathbb{N}}$ be a sequence of degree d expander graphs, and let

$$\mathrm{TS}_n := \{ \prod_{e : u \in e} (1 - 2x_e) = -1 : u \in V(G_n)\}.$$

Theorem (Grigoriev '01)

TS_n *requires degree* $\Omega(n)$ *to refute in SOS.*

Applications: Tseitin formulas

Let $(G_n)_{n \in \mathbb{N}}$ be a sequence of degree d expander graphs, and let

$$\mathrm{TS}_n := \{ \prod_{e : u \in e} (1 - 2x_e) = -1 : u \in V(G_n) \}.$$

Theorem (Grigoriev '01)

TS_n *requires degree* $\Omega(n)$ *to refute in SOS.*

Corollary

Every SOS refutation of TS_n *has monomial size* $\exp(\Omega(n))$.

Applications: sparse random k-CNFs

Theorem (Schoenenbeck '08)

Asymptotically almost surely, a sparse random k-CNF requires degree $\Omega(n)$ to refute in SOS.

Applications: sparse random k-CNFs

Theorem (Schoenenbeck '08)

Asymptotically almost surely, a sparse random k-CNF requires degree $\Omega(n)$ to refute in SOS.

Corollary

Asymptotically almost surely, every SOS refutation of a sparse random k-CNF has monomial size $\exp(\Omega(n))$.

Open problems

- Is the trade-off optimal for small refutations? Is there a set of constraints that has a small SOS refutation, but needs degree $\Omega(\sqrt{n})$ to refute?

Open problems

- Is the trade-off optimal for small refutations? Is there a set of constraints that has a small SOS refutation, but needs degree $\Omega(\sqrt{n})$ to refute?
- Can one minimize both degree and monomial size simultaneously or does one necessarily grow if the other one is minimized?

Open problems

- Is the trade-off optimal for small refutations? Is there a set of constraints that has a small SOS refutation, but needs degree $\Omega(\sqrt{n})$ to refute?
- Can one minimize both degree and monomial size simultaneously or does one necessarily grow if the other one is minimized?
- Does the trade-off hold for general Positivstellensatz proofs?

Thank you!