Exponential Lower Bound for tree-like Lovász-Schrijver proof systems

Arist Kojevnikov and Dmitry Itsykson

St. Petersburg Department of Steklov Institute of Mathematics

Complexity of Constraints

Dagstuhl, Germany
October 5, 2006
Definition ([Cook and Reckhow, 1979])

A proof system for a language $L$ is a polynomial-time computable function mapping strings in some finite alphabet (proof candidates) onto $L$ (whose elements are considered as theorems).

Definition

Let $\text{TAUT}$ denote the co-NP-complete language of tautologies in DNF (equivalently, $\text{UNSAT}$ is language of unsatisfiable formulas in CNF). A propositional proof system is proof system for $\text{TAUT}$ ($\text{UNSAT}$).

Resolution

\[
\begin{align*}
A \lor x & \quad B \lor \neg x \\
\hline
A \lor B
\end{align*}
\]
Proof Systems

Definition ([Cook and Reckhow, 1979])

A proof system for a language $L$ is a polynomial-time computable function mapping strings in some finite alphabet (proof candidates) onto $L$ (whose elements are considered as theorems).

Definition

Let $\text{TAUT}$ denote the co-NP-complete language of tautologies in DNF (equivalently, $\text{UNSAT}$ is language of unsatisfiable formulas in CNF). A propositional proof system is proof system for $\text{TAUT}$ ($\text{UNSAT}$).

Resolution

$$
\begin{align*}
A \lor x & \quad B \lor \neg x \\
\hline 
A \lor B
\end{align*}
$$
Proof Systems

Definition ([Cook and Reckhow, 1979])

A *proof system* for a language $L$ is a polynomial-time computable function mapping strings in some finite alphabet (proof candidates) onto $L$ (whose elements are considered as theorems).

Definition

Let $\text{TAUT}$ denote the co-NP-complete language of tautologies in DNF (equivalently, $\text{UNSAT}$ is language of unsatisfiable formulas in CNF). A *propositional proof system* is proof system for $\text{TAUT}$ ($\text{UNSAT}$).

Resolution

$$
\frac{A \lor x \quad B \lor \neg x}{A \lor B}
$$
Proof System Complexity

Motivation:

• NP $\neq$ co-NP (and therefore $P \neq NP$) if and only if no short, easily-verifiable proofs of some tautology exist [Cook and Reckhow, 1979].

• Proof system is the extension of SAT algorithm. If $A$ is SAT algorithm then proof of $\phi$ is the protocol of $A(\phi)$.

• Resolution is equivalent to Davis-Putnam procedure.
Proof System Complexity

Motivation:

• NP ≠ co-NP (and therefore P ≠ NP) if and only if no short, easily-verifiable proofs of some tautology exist [Cook and Reckhow, 1979].

• Proof system is the extension of SAT algorithm. If A is SAT algorithm then proof of φ is the protocol of A(φ).

• Resolution is equivalent to Davis-Putnam procedure.
Semi-algebraic Proof Systems

\[ \bigvee x_i \lor \bigvee \neg y_i \rightarrow \sum x_i + \sum (1 - y_i) - 1 \geq 0 \]

\[ x^2 - x \geq 0 \quad x \geq 0 \quad 1 - x \geq 0 \]

Gomory-Chvátal (CP)

Lovász-Schrijver (LS)

\[ \sum ca_i x_i \geq A \quad h \geq 0 \]

\[ \sum a_i x_i \geq \lceil A/c \rceil \quad hx \geq 0 \]

\[ c, a_i \text{ and } A \text{ are integers} \]

\[ h \geq 0 \quad h(1 - x) \geq 0 \]

\[ \text{where } h \text{ is linear} \]

The proof is derivation of \(-1 \geq 0\).
Semi-algebraic Proof Systems

\[ \bigvee x_i \lor \bigvee \neg y_i \quad \rightarrow \quad \sum x_i + \sum (1 - y_i) - 1 \geq 0 \]

\[
\begin{align*}
 x^2 - x & \geq 0 \\
x & \geq 0 \\
1 - x & \geq 0 \\
f & \geq 0 \\
g & \geq 0 \\
\alpha f + \beta g & \geq 0
\end{align*}
\]

Gomory-Chvátal (CP)

\[
\frac{\sum ca_ix_i}{\sum a_ix_i} \geq \lceil A/c \rceil
\]

c, a_i and A are integers

Lovász-Schrijver (LS)

\[
\begin{align*}
h & \geq 0 \\
hx & \geq 0 \\
h(1 - x) & \geq 0
\end{align*}
\]

where h is linear

The proof is derivation of \(-1 \geq 0\).
Semi-algebraic Proof Systems

\[ \bigvee x_i \lor \bigvee \neg y_i \rightarrow \sum x_i + \sum (1 - y_i) - 1 \geq 0 \]

\[ \frac{x^2 - x \geq 0}{x \geq 0} \quad \frac{1 - x \geq 0}{\alpha f + \beta g \geq 0} \]

Gomory-Chvátal (CP)  
Lovász-Schrijver (LS)

\[ \sum ca_i x_i \geq A \]
\[ \sum a_i x_i \geq \lceil A/c \rceil \]

\[ h \geq 0 \]
\[ hx \geq 0 \]
\[ h(1 - x) \geq 0 \]

\[ c, a_i \text{ and } A \text{ are integers} \]

where \( h \) is linear

The proof is derivation of \(-1 \geq 0\).
Related Work

Lower Bounds

• Starting from lower bound for Resolution [Tseitin, 1968]
• Exponential size lower bound for CP on Clique-Coloring Tautologies [Pudlák, 1997]
• Exponential size lower bound for tree-like LS on Symmetric Knapsack Problem (that has not short notation as a Boolean formula) [Grigoriev et al., 2002]
• Conditional exponential size lower bound for tree-like LS [Beame et al., 2005]
Related Work

Lower Bounds

• Starting from lower bound for Resolution [Tseitin, 1968]

• Exponential size lower bound for CP on Clique-Coloring Tautologies [Pudlák, 1997]

• Exponential size lower bound for tree-like LS on Symmetric Knapsack Problem (that has not short notation as a Boolean formula) [Grigoriev et al., 2002]

• Conditional exponential size lower bound for tree-like LS [Beame et al., 2005]
Related Work

Lower Bounds

• Starting from lower bound for Resolution [Tseitin, 1968]

• Exponential size lower bound for CP on Clique-Coloring Tautologies [Pudlák, 1997]

• Exponential size lower bound for tree-like LS on Symmetric Knapsack Problem (that has not short notation as a Boolean formula) [Grigoriev et al., 2002]

• Conditional exponential size lower bound for tree-like LS [Beame et al., 2005]
Our Result (Informally)

We prove exponential lower bound for tree-like LS as propositional proof system.
Tseitin formulas

\[ G = (V, E), \text{ to each } e \in E \text{ attach } \{0, 1\}-\text{variable } x_e, \text{ fix } V' \subseteq V, \]

\[ |V'| \text{ is odd,} \]

\[ T_G = \begin{cases} 
\oplus_{v \in V} y_e = 1, & \text{for all } x \in V' \\
\oplus_{v \in V} y_e = 0, & \text{for all } x \in V \setminus V'
\end{cases} \]

\[ \sum x_{v,u_i} = 1 \mod 2 \]

\( T_G \) is contradiction.
Expander graphs

\[ G = (V, E) \] is \((r, d, c)\)-expander iff degrees of \( v \in V \) are less than \( d \) and for any \( A \subset V, |A| \leq r, |\partial(A)| \geq c|A| \), where boundary \( \partial(A) = \{(v, w) | v \in A, w \in V \setminus A \} \).

Example:

\[
\begin{align*}
\partial(v) &= \{(v, w), (v, u)\} \\
(1, 2, 2)-\text{expander}
\end{align*}
\]

Lemma ([Alekhnovich et al., 2004])

If \( G \) is \((r, d, c)\)-expander and we remove not more than \( cr/4 \) edges from it, then we can obtain a \((r/2, d, c/2)\)-expander by removing some other edges and vertices.
Expander graphs

\(G = (V, E)\) is \((r, d, c)\)-expander iff degrees of \(v \in V\) are less than \(d\) and for any \(A \subset V, |A| \leq r, |\partial(A)| \geq c|A|\), where boundary \(\partial(A) = \{(v, w) | v \in A, w \in V \setminus A\}\).

Example:

\[
\partial(v) = \{(v, w), (v, u)\}
\]

\((1, 2, 2)\)-expander

Lemma ([Alekhnovich et al., 2004])

If \(G\) is \((r, d, c)\)-expander and we remove not more than \(cr/4\) edges from it, then we can obtain a \((r/2, d, c/2)\)-expander by removing some other edges and vertices.
Expander graphs

\( G = (V, E) \) is \((r, d, c)\)-expander iff degrees of \( v \in V \) are less than \( d \) and for any \( A \subset V, |A| \leq r, |\partial(A)| \geq c|A| \), where boundary \( \partial(A) = \{(v, w) | v \in A, w \in V \setminus A \} \).

Example:

\[
\begin{align*}
\partial(v) &= \{(v, w), (v, u)\} \\
(1, 2, 2)-expander
\end{align*}
\]

Lemma ([Alekhnovich et al., 2004])

If \( G \) is \((r, d, c)\)-expander and we remove not more than \( cr/4 \) edges from it, then we can obtain a \((r/2, d, c/2)\)-expander by removing some other edges and vertices.
Tree-like and Static $LS_+$

Tree-like $LS_+$

\[
\sum x_i + \sum (1 - y_i) - 1 \geq 0 \quad \text{for all initial } C_i = \lor x_i \lor \lor \neg y_i
\]

\[
x \geq 0 \quad 1 - x \geq 0 \quad x^2 - x \geq 0 \quad h^2 \geq 0
\]

\[
f \geq 0 \quad g \geq 0 \quad h \geq 0 \quad (1 - x)h \geq 0 \quad h \text{ is linear}
\]

\[
xh \geq 0 \quad (1 - x)h \geq 0
\]

Goal is to derive $-1 \geq 0$

Static $LS_+$ [Grigoriev et al., 2002]

\[
\sum_{i=1}^{M} f_i \sum_{l} g_{i,l} = -1
\]

where $g_{i,l} = c_{i,l} \cdot \prod_{k \in U_{i,l}^+} x_k \cdot \prod_{k \in U_{i,l}^-} (1 - x_k)$, coefficients $c_{i,l} \in \mathbb{R}^+$

and $f_i$ are axioms
Tree-like and Static LS$_+$

Tree-like LS$_+$

\[
\sum x_i + \sum (1 - y_i) - 1 \geq 0
\]

for all initial $C_i = \lor x_i \lor \lor \neg y_i$

\[
\begin{align*}
x & \geq 0 \\
1 - x & \geq 0 \\
x^2 - x & \geq 0 \\
h^2 & \geq 0
\end{align*}
\]

\[
\begin{align*}
f & \geq 0 \\
g & \geq 0 \\
h & \geq 0 \\
(1 - x)h & \geq 0
\end{align*}
\]

$h$ is linear

Goal is to derive $-1 \geq 0$

Static LS$_+$ [Grigoriev et al., 2002]

\[
\sum_{i=1}^{M} f_i \sum_l g_{i,l} = -1
\]

where $g_{i,l} = c_{i,l} \cdot \prod_{k \in U_{i,l}^+} x_k \cdot \prod_{k \in U_{i,l}^-} (1 - x_k)$, coefficients $c_{i,l} \in \mathbb{R}^+$ and $f_i$ are axioms
Our result

Theorem
Any tree-like $LS_+$ refutation of Tseitin formula $T_G$ for a connected $d$-regular ($r = n/2$, $d$, $c$)-expander $G$ with $n$ vertices and $c > 2$ has size $\exp(\Omega(n))$. 
Proof Sketch

• Prove that every static $LS_+$ proof of Tsejtin formula based on enough good expander contains at least one polynomial with special property (in fact: polynomials with big enough number of variables).

• Make linear number of substitution of variables such a way that:
  1) all except may by exponential small fraction of polynomials with special property will be removed from the proof;
  2) resulting Tseitin formula has enough good expansion property;
  3) resulting formula is not trivially unsatisfiable (does not contain empty clauses).

The initial proof contains exponential number of polynomial with special property
Proof Sketch

• Prove that every static $LS_+$ proof of Tsejitin formula based on enough good expander contains at least one polynomial with special property (in fact: polynomials with big enough number of variables).

• Make linear number of substitution of variables such a way that:
  1) all except may by exponential small fraction of polynomials with special property will be removed from the proof;
  2) resulting Tseitin formula has enough good expansion property;
  3) resulting formula is not trivially unsatisfiable (does not contain empty clauses).

The initial proof contains exponential number of polynomial with special property.
Proof Sketch

• Prove that every static $\text{LS}_+$ proof of Tsejtin formula based on enough good expander contains at least one polynomial with special property (in fact: polynomials with big enough number of variables).

• Make linear number of substitution of variables such a way that:
  1) all except may by exponential small fraction of polynomials with special property will be removed from the proof;
  2) resulting Tseitin formula has enough good expansion property;
  3) resulting formula is not trivially unsatisfiable (does not contain empty clauses).

The initial proof contains exponential number of polynomial with special property
First step: polynomial with special property

- Existence polynomials with special property in all Positivstellensatz proofs of Tseitin formulas on expanders [Grigoriev, 2001]

\[\bigvee x_i \lor \bigvee \neg y_i \rightarrow \prod (1 - x_i) \cdot \prod y_i = 0\]

axioms \(x^2 - x = 0\), proof is the set of polynomials \(g_1, \ldots, g_{m+n}\) and \(h_1, \ldots, h_l\) such that

\[\sum_{i=1}^{m+n} f_i g_i = 1 + \sum_{j=1}^l h_j^2\]

- Simulation of Static LS+ in Positivstellensatz
First step: polynomial with special property

- Existence of polynomials with special property in all Positivstellensatz proofs of Tseitin formulas on expanders [Grigoriev, 2001]

\[
\bigvee x_i \lor \bigvee \neg y_i \rightarrow \prod (1 - x_i) \cdot \prod y_i = 0
\]

axioms \(x^2 - x = 0\), proof is the set of polynomials \(g_1, \ldots, g_{m+n}\) and \(h_1, \ldots, h_l\) such that

\[
\sum_{i=1}^{m+n} f_i g_i = 1 + \sum_{j=1}^l h_j^2.
\]

- Simulation of Static LS+ in Positivstellensatz
First step: polynomial with special property

• Existence polynomials with special property in all Positivstellensatz proofs of Tseitin formulas on expanders [Grigoriev, 2001]

\[
\bigvee x_i \lor \bigvee \neg y_i \rightarrow \prod (1 - x_i) \cdot \prod y_i = 0
\]

axioms \( x^2 - x = 0 \), proof is the set of polynomials \( g_1, \ldots, g_{m+n} \) and \( h_1, \ldots, h_l \) such that

\[
\sum_{i=1}^{m+n} f_i g_i = 1 + \sum_{j=1}^{l} h_j^2.
\]

• Simulation of Static LS\(_+\) in Positivstellensatz
Substitutions

• removing as many polynomials with \textit{special property} as possible

\begin{center}
\begin{tikzpicture}
    \node (G) at (0,0) {G};
    \node (H) at (1,0) {H};
    \draw[->] (G) -- node[above] {$v$} (H);
\end{tikzpicture}
\end{center}

removing \textit{bridges} and variables from small components

• we set such value to $v$, that $T_G$ become satisfiable, after that remove all variables from $T_G$ by satisfying assignment
Substitutions

- removing as many polynomials with **special property** as possible

\[ G \xrightarrow{v} H \]

removing **bridges** and variables from small components

- we set such value to \( v \), that \( T_G \) become satisfiable, after that remove all variables from \( T_G \) by satisfying assignment
Open Questions

• Prove lower bound for DAG-like LS
• Prove lower bound for CP on Tsejtin formulas
Thank you!


In *STOC’96*, pages 174–183.


