# 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

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

## Resolution

$$\frac{A \vee x \qquad B \vee \neg x}{A \vee B}$$

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

## Resolution

$$\frac{A \vee x \qquad B \vee \neg x}{A \vee B}$$

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

### Resolution

$$\frac{A \vee x \qquad B \vee \neg x}{A \vee B}$$

# 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$\neq$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.

# Semi-algebraic Proof Systems

$$\bigvee x_i \vee \bigvee \neg y_i \quad \rightarrow \quad \sum x_i + \sum (1 - y_i) - 1 \geq 0$$

$$\frac{}{x^2 - x \geq 0} \qquad \frac{}{x \geq 0} \qquad \frac{}{1 - x \geq 0} \qquad \frac{f \geq 0 \qquad g \geq 0}{\alpha f + \beta g \geq 0}$$

Gomory-Chvátal (CP)

$$\frac{\sum c a_i x_i \geq A}{\sum a_i x_i \geq \lceil A/c \rceil}$$

$c$, $a_i$ and $A$ are integers

Lovász-Schrijver (LS)

$$\frac{h \geq 0}{hx \geq 0} \qquad \frac{h \geq 0}{h(1 - x) \geq 0}$$

where $h$ is linear

The proof is derivation of $-1 \geq 0$.

# Semi-algebraic Proof Systems

$$\bigvee x_i \vee \bigvee \neg y_i \quad \rightarrow \quad \sum x_i + \sum (1 - y_i) - 1 \geq 0$$

$$\frac{}{x^2 - x \geq 0} \qquad \frac{}{x \geq 0} \qquad \frac{}{1 - x \geq 0} \qquad \frac{f \geq 0 \qquad g \geq 0}{\alpha f + \beta g \geq 0}$$

Gomory-Chvátal (CP)

$$\frac{\sum c a_i x_i \geq A}{\sum a_i x_i \geq \lceil A/c \rceil}$$

$c$, $a_i$ and $A$ are integers

Lovász-Schrijver (LS)

$$\frac{h \geq 0}{hx \geq 0} \qquad \frac{h \geq 0}{h(1-x) \geq 0}$$

where $h$ is linear

The proof is derivation of $-1 \geq 0$.

# Semi-algebraic Proof Systems

$$\bigvee x_i \vee \bigvee \neg y_i \quad \rightarrow \quad \sum x_i + \sum (1 - y_i) - 1 \geq 0$$

$$\frac{}{x^2 - x \geq 0} \qquad \frac{}{x \geq 0} \qquad \frac{}{1 - x \geq 0} \qquad \frac{f \geq 0 \qquad g \geq 0}{\alpha f + \beta g \geq 0}$$

Gomory-Chvátal (CP)

$$\frac{\sum c a_i x_i \geq A}{\sum a_i x_i \geq \lceil A/c \rceil}$$

$c$, $a_i$ and $A$ are integers

Lovász-Schrijver (LS)

$$\frac{h \geq 0}{hx \geq 0} \qquad \frac{h \geq 0}{h(1 - x) \geq 0}$$

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

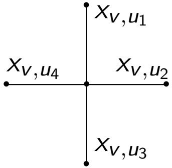
- Starting from lower bound for Resolution [Tseitin, 1968]
- Exponential size lower bound for CP on Clique-Coloring Tautologies [Pudlák, 1997]
- Exponential size lower bound for tree-like LS on Symmetric Knapsack Problem (that has not short notation as a Boolean formula) [Grigoriev et al., 2002]
- Conditional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

$G = (V, E)$, to each $e \in E$ attach $\{0,1\}$-variable $x_e$, fix $V' \subseteq V$, $|V'|$ is odd,




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

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

$T_G$ is contradiction.

$G = (V, E)$ 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:



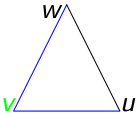

$\partial(v) = \{(v, w), (v, u)\}$
$(1, 2, 2)$-expander

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.*

$G = (V, E)$ 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

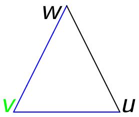
**Lemma ([Alekhnovich et al., 2004])**

*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:




$\partial(v) = \{(v, w), (v, u)\}$
$(1, 2, 2)$-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.*

# Tree-like and Static $\mathrm{LS}_+$

Tree-like $\mathrm{LS}_+$

$$\frac{}{\sum x_i + \sum (1 - y_i) - 1 \geq 0} \qquad \text{for all initial } C_i = \bigvee x_i \vee \bigvee \neg y_i$$

$$\frac{}{x \geq 0} \qquad \frac{}{1 - x \geq 0} \qquad \frac{}{x^2 - x \geq 0} \qquad \frac{}{h^2 \geq 0}$$

$$\frac{f \geq 0 \qquad g \geq 0}{\alpha f + \beta g \geq 0} \qquad \frac{h \geq 0}{xh \geq 0} \qquad \frac{h \geq 0}{(1 - x)h \geq 0} \qquad h \text{ is linear}$$

Goal is to derive $-1 \geq 0$

Static $\mathrm{LS}_+$ [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$_+$

$$\frac{}{\sum x_i + \sum (1 - y_i) - 1 \geq 0} \qquad \text{for all initial } C_i = \bigvee x_i \vee \bigvee \neg y_i$$

$$\frac{}{x \geq 0} \qquad \frac{}{1 - x \geq 0} \qquad \frac{}{x^2 - x \geq 0} \qquad \frac{}{h^2 \geq 0}$$

$$\frac{f \geq 0 \qquad g \geq 0}{\alpha f + \beta g \geq 0} \qquad \frac{h \geq 0}{xh \geq 0} \qquad \frac{h \geq 0}{(1 - x)h \geq 0} \qquad h \text{ is linear}$$

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 exept 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 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 exept 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 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 exept 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]

$$\bigvee x_i \vee \bigvee \neg y_i \quad \rightarrow \quad \prod (1 - x_i) \cdot \prod y_i = 0$$

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]

$$\bigvee x_i \vee \bigvee \neg y_i \quad \rightarrow \quad \prod (1 - x_i) \cdot \prod y_i = 0$$

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]

$$\bigvee x_i \vee \bigvee \neg y_i \quad \to \quad \prod (1 - x_i) \cdot \prod y_i = 0$$

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 special property as possible

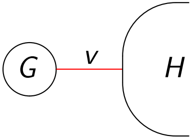



removing bridges and variables from small components

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

# Substitutions

- removing as many polynomials with special property as possible




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!

Alekhnovich, M., Hirsch, E. A., and Itsykson, D. (2004).
Exponential lower bounds for the running time of DPLL algorithms on satisfiable formulas.
In *Proceedings of the 31st International Colloquium on Automata, Languages and Programming, ICALP 2004*, volume 3142 of *Lecture Notes in Computer Science*, pages 84–96. Springer-Verlag.

Beame, P., Pitassi, T., and Segerlind, N. (2005).
Lower bounds for lovasz-schrijver systems and beyond follow from multiparty communication complexity.
In *Proceedings of the Thirty-second Annual Colloquium on Automata, Languages, and Programming*, Lecture Notes in Computer Science, pages 1176–1188. Springer-Verlag.

Clegg, M., Edmonds, J., and Impagliazzo, R. (1996).
Using the Groebner basis algorithm to find proofs of unsatisfiability.
In *STOC'96*, pages 174–183.

Cook, S. A. and Reckhow, R. A. (1979).
The Relative Efficiency of Propositional Proof Systems.
*The Journal of Symbolic Logic*, 44(1):36–50.

Grigoriev, D. (2001).
Linear lower bound on degrees of Positivstellensatz Calculus proofs for the Parity.
*TCS*, 259:613–622.

Grigoriev, D., Hirsch, E. A., and Pasechnik, D. V. (2002).
Complexity of semialgebraic proofs.
*Moscow Mathematical Journal*, 2(4):647–679.

Pudlák, P. (1997).
Lower bounds for resolution and cutting plane proofs and monotone computations.
*Journal of Symbolic Logic*, 62(3):981–998.

Tseitin, G. S. (1968).
On the complexity of derivation in the propositional calculus.
*Zapiski nauchnykh seminarov LOMI*, 8:234–259.