Electronic Colloquium on Computational Complexity, Report No. 6 (2005)

Simulating Cutting Plane proofs with restricted degree of falsity by Resolution

Edward A. Hirsch[*] Sergey I. Nikolenko[†]

December 28, 2004

Abstract

Goerdt [Goe91] considered a weakened version of the Cutting Plane proof system with a restriction on the degree of falsity of intermediate inequalities. (The degree of falsity of an inequality written in the form $\sum a_i x_i + \sum b_i(1-x_i) \geq c,\ a_i, b_i \geq 0$ is its constant term c.) He proved a superpolynomial lower bound on the proof length of Tseitin tautologies when the degree of falsity is bounded by $\frac{n}{\log^2 n+1}$ (n is the number of variables).

In this short note we show that if the degree of falsity of a length l proof is bounded by $b(n) = o(n)$, this proof can be easily transformed into a resolution proof of length $O(l \cdot \binom{n}{b(n)-1} 64^{b(n)})$. Therefore, a superpolynomial bound on the proof length of Tseitin tautologies in this system for $b(n) = o(\frac{n}{\log n})$ follows immediately from Urquhart's lower bound for resolution proofs [Urq87].

1 Introduction

During the past forty years the research concerning propositional proof systems was advancing mostly by proving exponential lower bounds on the length of proofs of specific tautologies in specific systems. For example, the resolution proof system had been a subject of a very thorough study that yielded exponential lower bounds for the propositional pigeonhole principle [Hak85], Tseitin tautologies [Tse68, Urq87], random formulas [BSW01] and many other families of tautologies. Also algebraic proof systems (the ones that deal with polynomial equalities) attracted a lot of attention in the 90s and similar lower bounds were proved for them (see [BGIP01] and references therein).

Much less is known about semialgebraic proof systems, which restate a Boolean tautology as a system of inequalities and prove that this system has no 0/1-solutions. No exponential lower bounds are known for higher degree proof systems (though there are exponential bounds for systems of inequalities that are *not* produced from Boolean tautologies;

[*] St.Petersburg Department of Steklov Institute of Mathematics, 27 Fontanka, 191023 St.Petersburg, Russia. Web: `http://logic.pdmi.ras.ru/~hirsch/`. Supported in part by Russian Science Support Foundation and grant #NSh-2203-2003-1 of the President of RF for leading scientific schools support.

[†] St.Petersburg State University. Web: `http://logic.pdmi.ras.ru/~sergey/`.

ISSN 1433-8092

see [GHP02] and definitions and references therein). Concerning proof systems that work with linear inequalities, exponential lower bounds are known only for variations of the clique-coloring principle (see [Pud97] for a bound for the Cutting Plane proof system and [Das02] for a bound for a restricted version of the Lovasz-Schrijver system [LS91]).

The technique that allows to prove the bounds for linear semialgebraic proofs uses monotone interpolation and Razborov's lower bound on the monotone complexity of the clique problem [Raz85]. Therefore it is not suitable for proving lower bounds, for example, for Tseitin tautologies. Goerdt [Goe91] introduced a weaker version of Cutting Plane proofs by restricting the *degree of falsity* of inequalities (see Definition 1 below). He proved a superpolynomial lower bound on the proof length of Tseitin tautologies in the restricted system when the degree of falsity is bounded by $\frac{n}{\log^2 n+1}$, n being the number of variables. Goerdt's proof is a purely combinatorial argument obtained by modifying Urquhart's proof for resolution [Urq87].

In this paper we show the relation between the Cutting Plane proofs with restricted degree of falsity and the resolution proofs. Namely, we show that if the degree of falsity of a length l proof is bounded by $b(n) = o(n)$, this proof can be easily transformed into a resolution proof of length $O(l \cdot \binom{n}{b(n)-1} 64^{b(n)})$. Therefore, a superpolynomial bound on the proof length of Tseitin tautologies for $b(n) = o(\frac{n}{\log n})$ follows immediately from Urquhart's lower bound [Urq87] on the length of resolution proofs.

2 Definitions

2.1 Propositional proof systems and formulas

A *proof system* [CR79] 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). In this paper we are interested in a specific (yet very important) kind of proof systems: proof systems for the co-NP-complete language of unsatisfiable formulas in CNF (equivalently, tautologies in DNF).

In what follows, we use x to denote a variable (if not otherwise stated), l to denote a literal (i.e., a variable x or the negation $\overline{x}$ of it), and a, b, c, d, e, A, B to denote non-negative integers (all these letters may bear subscripts). A formula in CNF is a set of clauses, which are disjunctions (i.e., again sets) of literals and are usually denoted by letters C, D. We assume that a clause cannot contain a variable together with its negation.

A truth assignment π for a set of variables assigns a value (either 0 or 1) to each variable; the result of substituting π into a formula F is denoted $F|_\pi$ (where the clauses containing satisfied literals are removed, and falsified literals are dropped from the remaining clauses). We define the result of substituting π into other objects (clauses, inequalities, etc.) by analogy.

The proof systems we consider are dag-like derivation systems, i.e., a proof is a sequence of *lines* such that every line is either an axiom or is obtained by an application of a derivation rule to several previous lines. The proof finishes with a line called *goal* (in our case, this will be a simple form of contradiction). Such a proof system is thus determined by its set of axioms, set of derivation rules and the notion of a goal. Note that different proof system may have different notions of a line (it may be a clause, or an inequality, or anything else).

2.2 Resolution

The resolution proof system [Rob68] has clauses as its proof lines. Given a formula in CNF, one takes its clauses as the axioms and uses two rules:

- Resolution:
$$\frac{C \cup l \qquad D \cup \bar{l}}{C \cup D}$$
provided there is no literal $l' \in C$ such that $\overline{l'} \in D$.

- Weakening:
$$\frac{C}{C \cup l}$$
provided $\bar{l} \notin C$.

The goal is to derive the empty clause.

2.3 The Cutting Plane proof system

The proof lines in the Cutting Plane proof system (**CP**) are linear inequalities with integer coefficients. To refute a formula in CNF in this system, one translates each its clause $l_1 \vee \ldots \vee l_k$ into the inequality $l_1 + \ldots + l_k \geq 1$, where a negative literal $l_i = \neg x_i$ is written as $1 - x_i$; the obtained system of linear inequalities has the same 0/1-solutions as the original set of clauses (where 1 corresponds to True, and 0 corresponds to False). The proof lines are *algebraic*, i.e., when we write $x + (1 - y) \geq 1$, we mean $x - y \geq 0$. **CP** allows to derive a contradiction (i.e., the inequality $0 \geq 1$) if and only if the original set of inequalities has no 0/1-solutions.

We state the initial inequalities as axioms, and add also the axioms

$$\frac{}{x \geq 0}, \qquad \frac{}{1 - x \geq 0} \tag{1}$$

for every variable x. The derivation rules are (x_i's denote variables, i ranges over all variables subscripts, other letters denote integer constants):

- Addition:
$$\frac{\sum a_i x_i \geq A \qquad \sum b_i x_i \geq B}{\sum (a_i + b_i) x_i \geq A + B}. \tag{2}$$

- Rounding rule:
$$\frac{\sum a_i x_i \geq A}{\sum \frac{a_i}{c} x_i \geq \lceil \frac{A}{c} \rceil}, \tag{3}$$
provided $c \geq 1$ and $\forall i \ \ c | a_i$.

- Multiplication rule:
$$\frac{\sum a_i x_i \geq A}{\sum c a_i x_i \geq cA}, \tag{4}$$
where $c \geq 1$.

The notion of the degree of falsity of an inequality was introduced by Goerdt in [Goe91] as follows:

Definition 1. *Consider an inequality ι of the form $\sum_{i=1}^{n} a_i x_i \geq A$, and let π be a truth assignment for the variables of ι. The* degree of falsity *of ι under π is given by*

$$\mathtt{DGF}(\iota,\pi) = A - \mathtt{LHS}(\iota,\pi),$$

where $\mathtt{LHS}(\iota,\pi)$ is the value of the left-hand side of ι under π.

The degree of falsity of ι is given by

$$\mathtt{DGF}(\iota) = \max_{\pi}\ \mathtt{DGF}(\iota,\pi).$$

The degree of falsity of a Cutting Plane proof Π is given by

$$\mathtt{DGF}(\Pi) = \max_{\iota\in\Pi}\ \mathtt{DGF}(\iota).$$

3 Boolean representations of inequalities

Definition 2. *The* literal form *of an inequality is obtained from its canonical form $\sum_i c_i x_i \leq A$ by replacing each summand $c_i x_i$ where $c_i < 0$ with $-c_i(1-x_i)$ and adding the corresponding constant $-c$ to the free coefficient. (The terms of the form x_i or $(1-x_i)$ are called* literals.*)*

Example 1. *For example, $2(1-x)+2y+(1-z) \geq 3$ is the literal form of $-2x+2y-z \geq 0$.*

Lemma 1. *$\mathtt{DGF}(\iota)$ is the free coefficient of ι written in the literal form.*

Proof. Note that minimizing $\mathtt{LHS}(\iota,\pi)$ in the definition of $\mathtt{DGF}(\iota)$ is a trivial task: we should assign 0 to each variable x_i such that $a_i > 0$, and assign 1 to each x_i such that $a_i < 0$ (in terms of Definition 1). This assignment π_0 yields $\mathtt{DGF}(\iota,\pi_0) = A - \sum_{i:a_i<0} a_i$, which is equal to the free coefficient of ι in the literal form. □

Lemma 2. *An integer inequality ι with $\mathtt{DGF}(\iota) \leq \frac{n}{2}$ can be represented as a conjunction of at most $\binom{n}{\mathtt{DGF}(\iota)-1}$ Boolean clauses, where n is the number of variables in it.*

Proof. Consider all inequalities obtained by satisfying literals occurring in the literal form of ι with sum of coefficients up to $\mathtt{DGF}(\iota)-1$. That is, we satisfy literals one by one and stop just before the inequality trivializes (i.e., the degree of falsity becomes non-positive), whatever coefficient we would choose next; we consider all inequalities that can be obtained from ι in this way (dropping duplicates, of course). It is easy to see that the obtained inequalities are equivalent to Boolean clauses. Indeed, consider an inequality $\sum_1^n a_i l_i \geq c$, where $\forall i\ a_i \geq c$. This inequality holds iff any one of l_i is true, which is equivalent to $l_1 \vee l_2 \vee \ldots \vee l_n$.

The number of clauses is as claimed, because we cannot satisfy more than $\mathtt{DGF}(\iota)-1$ literals without making ι trivial, and if an assignment results in a clause, its sub-assignments don't.

We have so far established a set of clauses that follows from the initial inequality. To prove the converse, consider an assignment π that falsifies ι. Substitute its part that satisfies literals of (the literal representation of) ι. The obtained inequality $\sum_{j\in J} a_j l_j \geq c' > 0$ is still non-trivial, because the original assignment falsifies ι. Then continue satisfying the remaining l_j's similarly to the construction above until the inequality becomes a clause. Clearly, this clause is falsified by (the remaining part of) π.

□

Definition 3. *We call the set of clauses obtained from an inequality ι by the procedure described in the proof of Lemma 2 the* Boolean representation *of an inequality ι and denote it by $\mathcal{B}(\iota)$.*

Lemma 3. *If ι is derived from $\{\iota_j\}_{j\in S}$ in* **CP** *then, for each $C \in \mathcal{B}(\iota)$, there is a resolution proof of C from $\bigcup_{j\in S}\mathcal{B}(\iota_j)$ that only contains literals occurring in $\{C\}\cup\bigcup_{j\in S}\mathcal{B}(\iota_j)$.*

Proof. By Lemma 2, ι and $\mathcal{B}(\iota)$ have the same set of 0/1 solutions. Since the Cutting Plane proof system is sound and the resolution proof system is implicationally complete, the lemma follows (it is easy to see that one can get rid of the literals that do not occur in $\{C\}\cup\bigcup_{j\in S}\mathcal{B}(\iota_j)$: it suffices to eliminate the applications of the weakening rule introducing such literals). □

4 Simulation by resolution

In this section we prove the bounds by establishing a direct connection between proofs in **CP** and proofs in the resolution proof system.

Lemma 4. *The rounding and multiplication rules do not change the Boolean representation.*

Proof. Suppose that ι' is obtained from ι by the rounding rule

$$\frac{\iota: \quad \sum_{i\in I} c_i l_i \geq A}{\iota': \quad \sum_{i\in I} \frac{c_i}{c} l_i \geq \left\lceil \frac{A}{c} \right\rceil},$$

where $c|c_i$ for all $i \in I$. For each clause $C \in \mathcal{B}(\iota)$, there is a (partial) assignment π that produced C from ι:

$$\iota|_\pi: \quad \sum_{i\in J} c_i l_i \geq A - \sum_{i\in I\setminus J} c_i.$$

Substitute this assignment into ι':

$$\iota'|_\pi: \quad \sum_{i\in J} \frac{c_i}{c} l_i \geq \left\lceil \frac{A}{c} \right\rceil - \sum_{i\in I\setminus J} \frac{c_i}{c}.$$

Then $\iota'|_\pi$ is also equivalent to a clause, because $\lceil \frac{A}{c} \rceil - \sum_{i \in I \setminus J} \frac{c_i}{c} \geq \frac{1}{c} \cdot (A - \sum_{i \in I \setminus J} c_i) > 0$ and (since $c | c_k$ for all k) $\forall j \in J$

$$\frac{c_j}{c} - \left(\left\lceil \frac{A}{c} \right\rceil - \sum_{i \in I \setminus J} \frac{c_i}{c} \right) = \left\lfloor \frac{c_j}{c} - \left(\frac{A}{c} - \sum_{i \in I \setminus J} \frac{c_i}{c} \right) \right\rfloor = \left\lfloor \frac{1}{c} \cdot \left(c_j - \left(A - \sum_{i \in I \setminus J} c_i \right) \right) \right\rfloor \geq 0$$

Similarly, every assignment that produces a clause from ι' also produces a clause from ι.

The same holds (by an easier yet very similar argument) for the multiplication rule. □

Lemma 5. *Let integer inequality ι be an integer linear combination of integer inequalities ι_1 and ι_2, let $\mathtt{DGF}(\iota_1)$, $\mathtt{DGF}(\iota_2) \leq A$. Then every clause C of the Boolean representation $\mathcal{B}(\iota)$ (given by Lemma 2) can be derived from $\mathcal{B}(\iota_1) \cup \mathcal{B}(\iota_2)$ in at most 2^{6A-2} resolution steps.*

Proof. We may rewrite our inequalities as follows (here x_i, y_i, z_i denote literals):

$$\begin{array}{rlllll}
\iota_1: & \sum_1^N e'_i z_i & + \sum_1^K a_i x_i & + \sum_1^L d_i y_i & \geq A_1, \\
\iota_2: & \sum_1^N e''_i z_i & + \sum_1^K b_i (1 - x_i) & + \sum_1^L d_i (1 - y_i) & \geq A_2, \\
\iota: & \sum_1^N e_i z_i & + \sum_1^K (a_i - b_i) x_i & & \geq A_1 + A_2 - \sum_1^K b_i - \sum_1^L d_i.
\end{array}$$

Here all coefficients are strictly positive, possibly except for some of the e'_i's and e''_j's, which are nonnegative. In other words, Z contains literals that are not cancelled by the application of the addition rule, X contains literals that are partially cancelled, and Y contains literals that are cancelled completely. We denote $X = \{x_1, \ldots, x_K\}$, $Y = \{y_1, \ldots, y_L\}$, $Z = \{z_1, \ldots, z_N\}$. Also denote $\overline{S} = \{\overline{s} \,|\, s \in S\}$ for any set S.

By Lemma 3 there exists a resolution proof Π of C from the clauses of $\mathcal{B}(\iota_1) \cup \mathcal{B}(\iota_2)$. Note that $\overline{Z} \cap C = \emptyset$ and $\overline{Z} \cap D = \emptyset$ for every $D \in \mathcal{B}(\iota_1) \cup \mathcal{B}(\iota_2)$. Hence, Lemma 3 provides Π that does not contain any negative occurrences of z_i's. Let π be the assignment that turns ι into C; denote $Z_\pi = \{z \in Z \,|\, \pi(z) = 1\}$ and $Z' = Z \setminus Z_\pi$. Note that $Z' \subseteq C$. Therefore, if one adds Z' to each clause in Π, the proof will remain a valid proof of C from the clauses $D^*_i = D_i \cup Z'$, where $D_i \in \mathcal{B}(\iota_1) \cup \mathcal{B}(\iota_2)$. Note that $|X| + |Y| + |Z_\pi| < 2A$; otherwise $\mathtt{DGF}(\iota|_\pi)$ would be non-positive, and the clause C would be a constant $\mathtt{True}$. There are at most $2^{3|X \cup Y \cup Z_\pi|} \leq 2^{6A-3}$ possible clauses of the form $Z' \cup T$, where $T \subseteq X \cup \overline{X} \cup Y \cup \overline{Y} \cup Z_\pi$, hence the modified (dag-like) version of the proof Π cannot contain more than 2^{6A-3} clauses. It remains to add at most 2^{6A-3} steps needed to obtain D^*_i's from D_i's by the weakening rule.

□

Theorem 1. *A Cutting Plane proof Π with $\max_{\iota \in \Pi} \mathtt{DGF}(\iota) \leq d \leq n/2$ of a formula in CNF with n variables can be transformed into a resolution proof of size $O(\binom{n}{d-1} |\Pi| 2^{6d})$.*

Proof. Each step $\frac{\iota_1,\ \iota_2}{\iota}$ or $\frac{\iota_1}{\iota}$ of Π can be replaced by at most $\binom{n}{d-1}2^{6d-2}$ resolution steps inferring the $\binom{n}{d-1}$ (see Lemma 2) possible clauses of $\mathcal{B}(\iota)$ from $\bigcup_i \mathcal{B}(\iota_i)$, by a 2^{6d-2}-length resolution proof each. (For addition steps such a resolution proof is given by Lemma 5, for other steps it is not needed by Lemma 4.) □

Corollary 1. *For any function $d(n) = o(\frac{n}{\log n})$ there are no polynomial-size proofs of Tseitin-Urquhart tautologies (described in [Urq87]) in* **CP** *with* DGF *bounded by $d(n)$.*

Proof. Tseitin-Urquhart tautologies with n variables (hence, containing $O(n)$ occurrences of all variables in total) have only $2^{\Omega(n)}$-size (dag-like) resolution proofs [Urq87]. By Theorem 1, if such formulas had polynomial-size Cutting Plane proofs with degree of falsity bounded by $d(n)$, they would have resolution proofs of size at most

$$\binom{n}{d(n)-1}\text{poly}(n)2^{6\,d(n)} = \text{poly}(n)\frac{n^{o(\frac{n}{\log n})}}{d(n)!}2^{6\,o(\frac{n}{\log n})} = 2^{o(n)},$$

which contradicts [Urq87].

□

5 Further research

A straightforward open question is to prove an exponential lower bound on the lengths of **CP** refutations of Tseitin tautologies without the restriction on the degree of falsity. One way to do it could be to characterize the inequalities that follow from subformulas of these tautologies and have a large degree of falsity.

References

[BGIP01] Sam Buss, Dima Grigoriev, Russell Impagliazzo, and Toniann Pitassi. Linear gaps between degrees for the polynomial calculus modulo distinct primes. *JCSS*, 62:267–289, 2001.

[BSW01] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow – resolution made simple. *JACM*, 48(2), 2001.

[CR79] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *The Journal of Symbolic Logic*, 44(1):36–50, March 1979.

[Das02] Sanjeeb Dash. Exponential lower bounds on the lengths of some classes of branch-and-cut proofs. IBM Research Report RC22575, September 2002.

[GHP02] Dima Grigoriev, Edward A. Hirsch, and Dmitrii V. Pasechnik. Complexity of semialgebraic proofs. *Moscow Mathematical Journal*, 2(4):647–679, 2002.

[Goe91] Andreas Goerdt. The Cutting Plane proof system with bounded degree of falsity. In *Proceedings of CSL 1991*, volume 626 of *Lecture Notes in Computer Science*, pages 119–133. Springer, 1991.

[Hak85] Armin Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297–308, 1985.

[LS91] L. Lovász and A. Schrijver. Cones of matrices and set-functions and 0-1 optimization. *SIAM J. Optimization*, 1(2):166–190, 1991.

[Pud97] Pavel Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *Journal of Symbolic Logic*, 62(3):981–998, 1997.

[Raz85] A. A. Razborov. Lower bounds on the monotone complexity of some boolean functions. *Doklady Akad. Nauk SSSR*, 282:1033–1037, 1985.

[Rob68] J. A. Robinson. The generalized resolution principle. *Machine Intelligence*, 3:77–94, 1968.

[Tse68] G. S. Tseitin. On the complexity of derivation in the propositional calculus. *Zapiski nauchnykh seminarov LOMI*, 8:234–259, 1968. English translation of this volume: Consultants Bureau, N.Y., 1970, pp. 115–125.

[Urq87] Alasdair Urquhart. Hard examples for resolution. *JACM*, 34(1):209–219, 1987.