Journal on Satisfiability, Boolean Modeling and Computation 6 (2008) 53-69

Complexity of Semialgebraic Proofs with Restricted Degree of Falsity[∗†]

Edward A. Hirsch
Arist Kojevnikov arist@logic.pdmi.ras.ru
Alexander S. Kulikov kulikov@logic.pdmi.ras.ru
Sergey I. Nikolenko sergey@logic.pdmi.ras.ru
Steklov Institute of Mathematics at St. Petersburg
27 Fontanka, 191023 St.Petersburg
Russia

Abstract

The *degree of falsity* of an inequality in Boolean variables shows how many variables are enough to substitute in order to satisfy the inequality. Goerdt introduced a weakened version of the Cutting Plane (CP) proof system with a restriction on the degree of falsity of intermediate inequalities [6]. He proved an exponential lower bound for CP proofs with degree of falsity bounded by $\frac{n}{\log^2 n+1}$, where n is the number of variables.

In this paper we strengthen this result by establishing a direct connection between CP and Resolution proofs. This result implies an exponential lower bound on the proof length of Tseitin-Urquhart tautologies when the degree of falsity is bounded by cn for some constant c. We also generalize the notion of degree of falsity for extensions of Lovász-Schrijver calculi (LS), namely for LS^k+CP^k proof systems introduced by Grigoriev et al. [8]. We show that any LS^k+CP^k proof with bounded degree of falsity can be transformed into a Res(k) proof. We also prove lower and upper bounds on the proof length of tautologies in LS^k+CP^k with bounded degree of falsity.

Keywords: *propositional proof system, lower bound, algebraic proof system, Cutting Planes, Lovasz-Schrijver proof system*

Submitted January 2008; revised July 2008; published November 2008

1. Introduction

The systematic study of propositional proof complexity was initiated by Cook and Reckhow in [4]. It was motivated by the fact that the NP≠co-NP assumption is equivalent to the existence of hard examples for any proof system. In this paper we deal with *semialgebraic* proof systems. They restate a Boolean tautology as a set of inequalities and prove that this set has no solutions in $\{0, 1\}$-variables. For many semialgebraic proof systems, no hard examples are known, while classical hard examples, e.g. the pigeonhole principle or Tseitin-Urquhart tautologies, enjoy short proofs.

[∗] Supported in part by the Russian Foundation for Basic Research (grants 05-01-00932, 06-01-00502, 06-01-00584), RAS Program for Fundamental Research ("Modern Problems of Theoretical Mathematics"), Russian presidential leading science school support grant N.Sh. 4392.2008.1, and Russian Science Support Foundation. The first author is also supported by the Dynasty Foundation Fellowship.

[†] This is a joint journal version of two papers earlier presented at SAT 2005 and SAT 2006 [9, 11].

The *degree of falsity* of an inequality in Boolean variables measures how many variables are enough to substitute in order to satisfy the inequality (we discuss its formal definitions in Section 2.3). A weakened version of the Cutting Plane (CP) proof system with a restriction on the degree of falsity of intermediate inequalities was introduced by Goerdt [6]. He proved an exponential lower bound for CP proofs with degree of falsity bounded by $\frac{n}{\log^2 n+1}$, where n is the number of variables.

In this work we strengthen this result by establishing a direct connection between CP and Resolution proofs. Basically, we show that if an inequality has low degree of falsity, it is equivalent to a small amount of Boolean clauses. This allows us to reason that if all inequalities in a CP proof have low degree of falsity, then the CP proof can be simulated step-by-step by Resolution with reasonably low overhead. This implies an exponential lower bound on the proof length of the Tseitin-Urquhart tautologies for the proofs with degree of falsity bounded by cn for some constant c.

Then we proceed to extending the notion of the degree of falsity to higher degree semialgebraic proof systems and prove lower and upper bounds for the considered systems. We prove that an LS^k+CP^k proof with restricted degree of falsity can be transformed into a Res(k) proof. Hence, strongly exponential lower bounds for Res(k) imply strongly exponential lower bounds for LS^k+CP^k with restricted degree of falsity. We also provide exponential separations of the new (restricted) proof system from CP and Res(k) by giving short proofs of the Pigeonhole Principle and the Weak Clique Coloring tautologies.

There is a longstanding open question about an exponential lower bound on Tseitin-Urquhart formulas for semialgebraic proof systems that use the rounding rule. Only partial results in this direction are known, namely exponential lower bound for tree-like systems [10] and systems with bounded degree of falsity [6]. In this paper we give a simplified proof of Goerdt's result and extend it to higher degree proof systems.

Let us discuss the main ideas of transforming LS^k+CP^k proofs into Res(k) proofs. Given an LS^k+CP^k proof Π we first linearize this proof, that is, replace each monomial by a new variable. This allows us to work with linear inequalities only. By a Boolean representation of a linear inequality we mean a CNF formula equivalent to this inequality. By bounding the degree of falsity of an inequality one bounds the size of this formula. We show that for any step of the proof Π it is possible to derive the Boolean representation of the conclusion from the Boolean representations of the premise(s). Thus, we transform an LS^k+CP^k proof into a Resolution proof of an auxiliary formula (with additional variables). This implies the existence of a Res(k) proof of an initial formula.

The paper is organized as follows. Section 2 contains the necessary definitions. The main results begin to unveil in Section 3 where we show how any Cutting Plane proof can be transformed into a Resolution proof and how the exponent of this transformation depends on the upper bound on the degree of falsity. In Section 4.1 we show that any LS^k+CP^k proof with bounded degree of falsity can be transformed into a Res(k) proof. Finally, in Section 5 we prove exponential lower bounds for LS^k+CP^k with restricted degree of falsity; we also present short proofs of the Pigeonhole Principle and Weak Clique Coloring with restricted degrees of falsity.

2. General Setting

2.1 Proof Systems

A *proof system* [4] for a language L is a polynomial-time computable function mapping words in some alphabet (treated as proof candidates) to L (whose elements are treated as theorems). A *propositional proof system* is a proof system for the co-NP-complete language TAUT of all Boolean tautologies in disjunctive normal form (DNF). Since this language is in co-NP, any proof system for a co-NP-hard language L can be considered as a propositional proof system. However, we need to fix a concrete reduction of TAUT to L before we can compare proof systems.

The proof systems we consider are dag-like derivation systems, where a proof is a sequence of *lines* such that every line is either an axiom or is obtained by applying a derivation rule to several previous lines. The proof finishes with a line called *goal*. Such a proof system can be defined by its notions of a line, a goal, a set of axioms and a set of derivation rules.

The *Resolution* proof system [17] has clauses (disjunctions of literals) as its proof lines and the empty clause as its goal. Given a formula F in DNF, one takes clauses of the CNF of $\neg F$ as axioms and uses the following rules:

$$\text{Resolution:} \quad \frac{A \vee x \quad \neg x \vee B}{A \vee B}, \qquad \text{Weakening:} \quad \frac{A}{A \vee l}.$$

The *Res(k)* proof system [12] is a generalization of Resolution where one uses k-DNFs (disjunctions of at most k terms, i.e. conjunctions of literals) as lines. The goal is to derive an empty clause. We take clauses of the formula $\neg F$ as axioms and use the following inference rules:

$$\text{Weakening:} \quad \frac{A}{A \vee l}, \qquad \text{AND-introduction:} \quad \frac{A \vee l_1 \cdots A \vee l_j}{A \vee \bigwedge_{i=1}^{j} l_i},$$

$$\text{Cut:} \quad \frac{A \vee \bigwedge_{i=1}^{j} l_i \quad B \vee \bigvee_{i=1}^{j} \neg l_i}{A \vee B}, \qquad \text{AND-elimination:} \quad \frac{A \vee \bigwedge_{i=1}^{j} l_i}{A \vee l_i}.$$

Let us now turn to semialgebraic proof systems. To define a propositional proof system dealing with inequalities, we should translate each formula F in DNF with n variables into a system $\mathcal{D}$ of linear inequalities such that F is a tautology if and only if the system $\mathcal{D}$ has no solutions in $\{0,1\}$-variables. We usually do it as follows: for a given tautology F, we translate each clause C_i of $\neg F$ with variables $x_{i_1}, \ldots, x_{i_t}$ into the inequality

$$l_1 + \ldots + l_t \geq 1, \tag{2.1}$$

where $l_k = x_{i_k}$ if the variable x_{i_k} occurs positively in the clause, and $l_k = 1 - x_{i_k}$ if x_{i_k} occurs negatively. For every variable x_k, $1 \leq k \leq n$, we also add inequalities $0 \leq x_k$ and $x_k \leq 1$ to the system $\mathcal{D}$.

The proof lines in the *Cutting Plane* proof system (CP) [5, 7] are linear inequalities with integer coefficients. The goal is a trivial contradiction $0 \geq 1$. We use the system of linear inequalities $\mathcal{D}$ provided by the translation described above as axioms. The inference rules are

$$\text{Addition:} \quad \frac{f \geq 0 \quad g \geq 0}{f + g \geq 0}, \qquad \text{Rounding:} \quad \frac{af \geq c}{f \geq \lceil \frac{c}{a} \rceil}, \qquad \text{Multiplication:} \quad \frac{f \geq c}{af \geq ac},$$

where a, c are constants, $a > 0$, f, g are polynomials.

Another well-known semialgebraic system is the *Lovász-Schrijver* system LS [13, 14]. This system operates with quadratic inequalities. It includes the Addition rule as above and introduces the Multiplication by Literal rule:

$$\frac{f \geq 0}{fx \geq 0}\ , \qquad \frac{f \geq 0}{f(1-x) \geq 0}\ , \tag{2.2}$$

where f is linear. In order to fix variables to be 0-1, one also needs to introduce the following axioms for each variable:

$$x^2 - x \geq 0, \qquad x - x^2 \geq 0. \tag{2.3}$$

It is straightforward to define an extension of LS by allowing LS to deal with polynomials of higher degree; if we bound the polynomials to degree k, we call the resulting system LS$^{\mathrm{k}}$.

The system LS^k was introduced and studied by Grigoriev, Hirsch, and Pasechnik [8]. They also considered a combination of this system with CP: the proof system LS^k+CP^k operates with inequalities of degree at most k with integer coefficients as lines, using the same set of axioms as LS^k. The rules are the CP rules restricted to premises of degree k and the Multiplication by Literal rule restricted to premises of degree $(k-1)$.

2.2 Proof Linearization

In order to transform an LS^k+CP^k proof into a Res(k) proof we transform the initial proof into a Resolution proof of an auxiliary formula. We show the connection between Res(k) proofs of the initial formula and Resolution proofs of the auxiliary formula below. The construction closely follows [3], where it is used to prove non-automatizability results for Res(k).

For every set of distinct and non-opposite literals $l_1, \ldots, l_m$ of a formula F $(2 \leq m \leq k)$ we define a new variable $z(l_1, \ldots, l_m)$ denoting the conjunction of all these literals. This can be expressed by the following $m + 1$ clauses:

$$(z(l_1, \ldots, l_m) \vee \neg l_1 \vee \cdots \vee \neg l_m),\ (\neg z(l_1, \ldots, l_m) \vee l_1),\ \ldots,\ (\neg z(l_1, \ldots, l_m) \vee l_m)\ .$$

By $F(k)$ we denote the conjunction of F with all such clauses. We need the following property of $F(k)$:

Proposition 2.1 ([3]) *If $F(k)$ has a Resolution proof of size S, then F has a Res(k) proof of size $O(kS)$.*

Definition 2.2 *For a variable $z_i = z(l_1, \ldots, l_s)$ of $F(k)$ and a variable x of F, by $z(z_i, x)$ we mean the variable $z(l_1, \ldots, l_s, x)$. For an inequality ι of degree at most k, by lin(ι) we denote the linear inequality obtained from ι by replacing each of its monomials $x_1 \cdot \cdots \cdot x_m$ by the linear monomial $z(x_1, \ldots, x_m)$.*

To prove the main theorem we also need the following simple lemma:

Lemma 2.3 *Let C be a clause containing variables of $F(k)$ and x be a variable of F. Let C' be a clause obtained from C by replacing each of the variables z_i by $z(z_i, x)$. Then the clause*

$$(C' \vee \neg x)$$

can be inferred from C and clauses of $F(k)$ in at most $O(n^k)$ Resolution steps. If, in addition, C contains at least one negated variable z_i, then one can also derive C'.

Proof. For each variable $z_i = z(l_1, \dots, l_s)$ we can derive clauses $(z_i \vee \neg z(z_i, x))$ and $(\neg z_i \vee z(z_i, x) \vee \neg x)$ by resolving $(z_i \vee \neg l_1 \vee \cdots \vee \neg l_s)$, $(\neg z(z_i, x) \vee l_1)$, …, $(\neg z(z_i, x) \vee l_s)$ and $(z(z_i, x) \vee \neg l_1 \vee \cdots \vee \neg l_s \vee \neg x)$, $(\neg z_i \vee l_1)$, …, $(\neg z_i \vee l_s)$, respectively.

For a literal z_i of the clause C, we resolve C with $(\neg z_i \vee z(z_i, x) \vee \neg x)$ and for a literal $\neg z_i$ we resolve C with $(z_i \vee \neg z(z_i, x))$. The result of these operations is either the clause C' or the clause $(C' \vee \neg x)$. If it is C', we derive $(C' \vee \neg x)$ by applying the Weakening rule. If C contains at least one negated variable, we resolve $(C' \vee \neg x)$ with $(\neg z(z_i, x) \vee x)$ for $\neg z_i \in C$.

The number of steps is as required, since the number of variables in C does not exceed $O(n^k)$. □

2.3 Degree of Falsity

The definition of the degree of falsity of a linear inequality was given by Goerdt [6].

Definition 2.4 *For a linear inequality ι of the form $\sum_{i=1}^{s} \alpha_i x_i \geq c$, $\mathtt{DGF_1}(\iota)$ is the difference of c and the minimal value of its left-hand side over $x_i \in \{0, 1\}$:*

$$\mathtt{DGF_1}(\iota) = c - \min_{x_1, \dots, x_s} \sum_{i=1}^{s} \alpha_i x_i .$$

We present a more combinatorial definition of the same object that also turns out to be more useful.

Definition 2.5 *A* literal form *of a linear inequality is its representation in the form*

$$\sum_{i=1}^{s} \alpha_i x_i + \sum_{i=s+1}^{s'} \alpha_i (1 - x_i) \geq c \ ,$$

where $\alpha_i > 0$ for $1 \leq i \leq s'$. For an inequality ι, $\mathtt{DGF_2}(\iota)$ is the free coefficient of the literal form of ι.

It is easy to see that these definitions are equivalent, i.e., for any linear inequality ι, $\mathtt{DGF_1}(\iota) = \mathtt{DGF_2}(\iota)$. Both these definitions can be extended naturally to inequalities of arbitrary degrees (one can just replace variables by monomials in both definitions). However, the new definitions would not be equivalent. E.g., $\mathtt{DGF_1}(xy + xz - xyz \geq 2) = 2$, while $\mathtt{DGF_2}(xy + xz - xyz \geq 2) = 3$. Moreover, it is not difficult to show that $\mathtt{DGF_1}$ never exceeds $\mathtt{DGF_2}$.

Lemma 2.6 *For any inequality ι,*

$$\mathtt{DGF_1}(lin(\iota)) = \mathtt{DGF_2}(lin(\iota)) = \mathtt{DGF_2}(\iota) \geq \mathtt{DGF_1}(\iota)\,.$$

Proof. The first equality is discussed above. The second one is obvious, because the literal form does not change when we replace monomials by new variables. For the inequality consider an inequality ι of the form

$$\sum_{i=1}^{s} \alpha_i m_i(x_1, \ldots, x_n) + \sum_{i=s+1}^{s'} \alpha_i(1 - m_i(x_1, \ldots, x_n)) \geq c\,,$$

where m_i's are products of Boolean variables and α_i's are positive. Then $\mathtt{DGF_2}(\iota) = c$, but the minimum of the left-hand side of ι over all its variables is obviously non-negative and may be even positive; in example above,

$$\mathtt{DGF_1}(xy+xz-xyz \geq 2) = \mathtt{DGF_1}(xy+xz+(1-xyz) \geq 3) = 3-\min_{x,y,z}\{xy+xz+(1-xyz)\} = 2\,.$$

Thus, $\mathtt{DGF_1}(\iota) = c - \min_{x_1,\ldots,x_n}\{\text{left-hand side}\} \leq c$. □

Therefore, for nonlinear inequalities $\mathtt{DGF_1}$ is stronger. However, we use $\mathtt{DGF_2}$ in this paper since only $\mathtt{DGF_2}$ remains invariant under linearization (we need this fact in Theorem 4.1). In what follows, we use $\mathtt{DGF}$ as $\mathtt{DGF_2}$. The explicit definition is as follows.

Definition 2.7 *A* literal form *of a polynomial inequality is its representation in the form*

$$\sum_{i=1}^{s} \alpha_i m_i + \sum_{i=s+1}^{s'} \alpha_i(1 - m_i) \geq c \;\;,$$

where α_i's are positive constants, m_i's are monomials (i.e. products of variables). For an inequality ι, $\mathtt{DGF}(\iota)$ is the free coefficient of the literal form of ι. The degree of falsity of an LS^k+CP^k *proof is the maximal degree of falsity of all inequalities in this proof.*

2.4 Boolean Representations of Linear Inequalities

By a Boolean representation of a linear inequality we mean a CNF formula that is equivalent to this inequality. Of course, such a formula is not unique. However, for the simulation we select one specific Boolean representation, and below we describe formally our construction of this representation.

Let ι be a linear inequality of the form $\sum_{i=1}^{s} \alpha_i x_i + \sum_{i=s+1}^{s'} \alpha_i(1-x_i) \geq c$, where $\alpha_i > 0$, for $1 \leq i \leq s'$. By satisfying a literal of ι we mean assigning either the value 1 to x_i, where $1 \leq i \leq s$, or the value 0 to x_i, where $s+1 \leq i \leq s'$. Let ι_0 be an inequality obtained from ι by satisfying some literals, such that no literal of ι_0 can be satisfied without trivializing ι_0. In what follows, we call an inequality *trivial* if it is satisfied for all values of input variables. Note that an inequality ι is trivial if and only if $\mathtt{DGF}(\iota) \leq 0$.

It is easy to see that ι_0 is equivalent to a clause (since it is falsified by exactly one assignment to its variables). By $\mathcal{B}(\iota)$ we denote the set of all such clauses, and in the rest of the paper by the Boolean representation of an inequality ι we mean exactly the set $\mathcal{B}(\iota)$. The following lemma shows that this construction is correct and provides an upper bound on the size of the constructed set.

Lemma 2.8 *For any linear inequality ι, $\mathcal{B}(\iota)$ is equivalent to ι. Moreover, the number of clauses in $\mathcal{B}(\iota)$ is at most $\binom{n}{d-1}$, where $d < n/2$ is the degree of falsity of ι.*

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 whatever coefficient we would choose next (every coefficient is greater or equal to the degree of falsity); we consider all inequalities that can be obtained from ι in this way (dropping duplicates, of course). It is easy to see that these inequalities are equivalent to Boolean clauses. Indeed, consider an inequality

$$\sum_{i=1}^{n} a_i l_i \geq c, \text{ where } \forall i \; a_i \geq c.$$

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 do not.

We have so far established a set of clauses that follows from the initial inequality. To prove the converse (that the inequality follows from the clauses), 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. □

Lemma 2.9 *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 2.8, 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). □

We also use the following simple property of $\mathcal{B}(\iota)$ that follows immediately from the construction.

Lemma 2.10 *Let ι be a linear inequality of the form*

$$\sum_{i=1}^{s} \alpha_i x_i + \sum_{i=s+1}^{s'} \alpha_i (1 - x_i) \geq c \enspace ,$$

where $\alpha_i > 0$. Then the set of clauses of $\mathcal{B}(\iota)$ that do not contain a literal x_i for $1 \leq i \leq s$ (or a literal $\neg x_i$ for $s+1 \leq i \leq s'$) is exactly the set $\mathcal{B}(\iota|_{x_i=1})$ (respectively, $\mathcal{B}(\iota|_{x_i=0})$).

3. Lower Bounds for CP Proofs with Restricted Degree of Falsity

3.1 Translating CP Proofs into Resolution Proofs

In this section we present the first main result of this paper. We use the Boolean representation as described in the previous section to prove lower bounds on CP proof size for CP with restricted degree of falsity. Our reasoning is as follows: we translate the CP proof into a Resolution proof via these Boolean representations and show that the size does not grow too much. This means that if a formula has only long Resolution proofs then it cannot have short CP proofs.

To make this reasoning precise, we begin with lemmas showing that applications of CP rules do not hurt the Boolean representation much.

Lemma 3.1 *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) $\forall j \in J$

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

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

The same holds for the multiplication rule; the argument is easier yet very similar. □

Lemma 3.2 *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 2.8) 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 canceled by the application of the addition rule, X contains literals that are partially canceled, and Y contains literals that are canceled completely. We denote $X = \{x_1, \ldots, x_K\}$, $Y = \{y_1, \ldots, y_L\}$, $Z = \{z_1, \ldots, z_N\}$. Let us also denote $\overline{S} = \{\overline{s} \mid s \in S\}$ for any set S.

By Lemma 2.9, 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 2.9 provides Π that does not contain any negative occurrences of z_i's. Let π be the assignment that turns ι into C; we denote $Z_\pi = \{z \in Z \mid \pi(z) = 1\}$ 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 $\texttt{DGF}(\iota|_\pi)$ would be non-positive, and the clause C would be a constant $\texttt{True}$. 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. □

3.2 Exponential Lower Bounds for CP Proofs with Restricted Degree of Falsity

We now have all we need to prove the following theorem.

Theorem 3.3 *A Cutting Plane proof* Π *with* $\max_{\iota \in \Pi} \texttt{DGF}(\iota) \leq d \leq n/2$ *of a formula in CNF with* n *variables can be transformed into a Resolution proof of size at most* $\binom{n}{d-1}|\Pi|2^{6d}$.

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 2.8) 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 3.2, for other steps it is not needed by Lemma 3.1.) □

Remark. The restriction $d \leq n/2$ is purely technical: if d exceeds $n/2$, the binomial coefficient $\binom{n}{d-1}$ begins to drop, while the condition on $\texttt{DGF}$ weakens further.

Corollary 3.4 *If formulas* F_n *(where* F_n *contains* n *variables) have no Resolution proofs containing less than* $2^{c_{\text{res}} n}$ *clauses* ($c_{\text{res}} > 0$ *being a constant), then these formulas do not* *have Cutting Plane proofs of size less than $2^{c_{\mathrm{CP}}n}$ and degree of falsity bounded by $c_{\mathtt{DGF}}n$ for every choice of positive constants $c_{\mathrm{CP}} < c_{\mathrm{res}}$ and $c_{\mathtt{DGF}} \leq \frac{1}{2}$ such that*

$$c_{\mathrm{CP}} + 6c_{\mathtt{DGF}} - c_{\mathtt{DGF}} \log_2 c_{\mathtt{DGF}} - (1 - c_{\mathtt{DGF}}) \log_2(1 - c_{\mathtt{DGF}}) \leq c_{\mathrm{res}} \quad . \tag{3.1}$$

In particular, formulas F_n have only exponential-size Cutting Plane proofs of degree of falsity bounded by an appropriate linear function of n.

Proof. By Theorem 3.3, Cutting Plane proofs of size less than $2^{c_{\mathtt{DGF}}n}$ can be converted into Resolution proofs of size less than

$$\binom{n}{c_{\mathtt{DGF}}n-1} 2^{c_{\mathrm{CP}}n+6c_{\mathtt{DGF}}n} = o(2^{(c_{\mathrm{CP}}+6c_{\mathtt{DGF}}-c_{\mathtt{DGF}}\log_2 c_{\mathtt{DGF}}-(1-c_{\mathtt{DGF}})\log_2(1-c_{\mathtt{DGF}}))n}) = o(2^{c_{\mathrm{res}}n})$$

(the first equality uses Stirling's formula).

Finally, note that $f(c) = 6c - c \log_2 c - (1 - c) \log_2(1 - c)$ decreases to 0 as c decreases from $\frac{1}{2}$ to 0. Therefore, for every $c_{\mathrm{CP}} < c_{\mathrm{res}}$ there is $c_{\mathtt{DGF}}$ that satisfies (3.1). □

We now recollect Urquhart's theorem. In the following proposition, S_m is a certain set of formulas based on Tseitin tautologies.

Proposition 3.5 ([19], Theorem 5.7**)** *There is a constant $c > 1$ such that for sufficiently large m, any Resolution refutation of S_m contains c^n distinct clauses, where S_m is of length $O(n)$, $n = m^2$.*

Corollary 3.4 and Proposition 3.5 immediately yield the following corollary.

Corollary 3.6 *There exists a positive constant δ such that Tseitin-Urquhart formulas of n variables (described in [19]) have only $2^{\Omega(n)}$-size Cutting Plane proofs with degree of falsity bounded by δn.*

4. Lower Bounds for LS^k+CP^k with Restricted Degree of Falsity

4.1 Transforming LS^k+CP^k Proofs with Restricted Degree of Falsity into Res(k) Proofs

In Section 3 we proved new lower bounds on restricted CP proofs via their translations into Resolution proofs. The rest of the paper is devoted to applying the same basic technique to a more complicated case of the LS^k+CP^k proof system. Here we translate LS^k+CP^k proofs with restricted degree of falsity into Res(k) proofs.

Theorem 4.1 *For any LS^k+CP^k proof Π of a CNF formula F, there exists a Res(k) proof of F of size $O\left(\binom{n}{d-1}|\Pi|(n^k + 2^{6d})\right)$, where n is the number of variables of F and $d \leq n/2$ is the degree of falsity of Π.*

Proof. We show that for any step $\frac{\iota_1 \quad \iota_2}{\iota}$ or $\frac{\iota_1}{\iota}$ of the proof Π, it is possible to derive all clauses of $\mathcal{B}(lin(\iota))$ from clauses of $\mathcal{B}(lin(\iota_1))$ (and $\mathcal{B}(lin(\iota_2))$) and clauses of $F(k)$ in at most $O\left(\binom{n}{d-1}(n^k + 2^{6d})\right)$ Resolution steps, where $lin(\iota)$ is the linearization introduced in Definition 2.2 (recall that $\mathtt{DGF}(lin(\iota)) = \mathtt{DGF}(\iota)$, so the degree of falsity of all linearized inequalities of the proof is also bounded by d). Note that, by Definition 2.2, if an inequality ι_0 is an axiom of the proof Π, then $\mathcal{B}(lin(\iota_0))$ is a clause of F. Observe also that $\mathcal{B}(lin(0 \geq 1))$ consists of the empty clause. Thus, the constructed proof is a Resolution proof of F.

The Addition and Rounding rules are covered by Lemmas 3.1 and 3.2. Therefore, it remains to consider the Multiplication by literal rule.

Let ι_p be a premise of the Multiplication by literal rule, ι_c be its conclusion, and x be a literal of this rule (so that ι_c is obtained from ι_p by multiplying by x). Note that since we are rewriting the original LS^k+CP^k proof, this literal cannot be one of the z variables introduced in Definition 2.2. Let also the literal form of $lin(\iota_p)$ be $\sum_{i=1}^{s} \alpha_i z_i + \sum_{i=s+1}^{s'} \alpha_i(1-z_i) \geq c$, where $\alpha_i > 0$, for $1 \leq i \leq s'$. The literal form of ι_c depends on the sign of $(\sum_{i=s+1}^{s'} \alpha_i - c)$. Consider two cases.

1. $\left(\sum_{i=s+1}^{s'} \alpha_i - c\right) \geq 0$. In this case, the literal form of $lin(\iota_c)$ is

$$\sum_{i=1}^{s} \alpha_i z(z_i, x) + \sum_{i=s+1}^{s'} \alpha_i \left(1 - z(z_i, x)\right) + \left(\sum_{i=s+1}^{s'} \alpha_i - c\right) x \geq \sum_{i=s+1}^{s'} \alpha_i \ .$$

   Note that each clause of $\mathcal{B}(lin(\iota_c))$ contains a literal $\neg z(z_i, x)$ for some $s+1 \leq i \leq s'$ (since $lin(\iota_c)$ becomes trivial when all these literals are assigned the value 0). Each clause of $\mathcal{B}(lin(\iota_c))$ containing x can be obtained by the Weakening rule from the clause $(\neg z(z_i, x) \vee x)$.

   Now consider all clauses of $\mathcal{B}(lin(\iota_c))$ that do not contain x, that is, the Boolean representation of $lin(\iota_c)|_{x=1}$. Observe that $lin(\iota_c)|_{x=1}$ can be obtained from $lin(\iota_p)$ just by replacing each variable z_i by $z(z_i, x)$, thus, we can apply Lemma 2.3.

2. $\left(\sum_{i=s+1}^{s'} \alpha_i - c\right) < 0$. In this case, the literal form of $lin(\iota_c)$ is

$$\sum_{i=1}^{s} \alpha_i z(z_i, x) + \sum_{i=s+1}^{s'} \alpha_i \left(1 - z(z_i, x)\right) + \left(c - \sum_{i=s+1}^{s'} \alpha_i\right) (1 - x) \geq c \ .$$

   Consider all clauses of $\mathcal{B}(lin(\iota_c))$ that do not contain $\neg x$. By Lemma 2.10, these clauses form a Boolean representation of $lin(\iota_c)|_{x=0}$. As in the previous case, all these clauses contain a literal $\neg z(z_i, x)$ for some $s+1 \leq i \leq s'$. Note that $lin(\iota_c)|_{x=0}$ can be obtained from $lin(\iota_p)$ by replacing each variable z_i by $z(z_i, x)$ and reducing the free coefficient from c to $\sum_{i=s+1}^{s'} \alpha_i$. Thus, $\mathcal{B}(lin(\iota_c)|_{x=0})$ can be derived from $\mathcal{B}(lin(\iota_p))$ by applying the steps described in Lemma 2.3 and the Weakening rule.

   Each clause C of $\mathcal{B}(lin(\iota_c))$ containing $\neg x$ corresponds to a clause C_0 of $\mathcal{B}(lin(\iota_p))$ resulting from C by removing $\neg x$ and replacing each variable $z(z_i, x)$ of C by z_i. All these clauses can be derived by Lemma 2.3.

The Boolean representation of $lin(\iota_c)$ contains at most $\binom{n}{d-1}$ clauses, so the number of steps is as required. □

4.2 An Exponential Lower Bound for LS^k+CP^k with Bounded Degree of Falsity

Lemma 4.2 *If a formula F with n variables has no Res(k) proof containing less then 2^{cn}, $c > 0$, clauses, then for sufficiently large n this formula does not have an LS^k+CP^k proof of size less than $\exp(\epsilon n)$ and degree of falsity bounded by dn for every choice of positive constants $\epsilon < c/2$ and $d < 1/2$ such that*

$$2\epsilon + 6d - d\log_2 d - (1-d)\log_2(1-d) \le c \ . \tag{4.1}$$

Moreover, for every $\epsilon < 1/2$ there exists a positive d satisfying this inequality.

Proof. By Theorem 4.1, any LS^k+CP^k proof of size $2^{\epsilon n}$ can be transformed into a Res(k) proof of size

$$\binom{n}{dn-1} 2^{\epsilon n + 6dn + k\log_2 n} = o(2^{(\epsilon + 6d + k\log_2 n/n - d\log_2 d - (1-d)\log_2(1-d))n})$$

(as in Theorem 3.4, we use Stirling's formula). This is $o(2^{cn})$ since for sufficiently large n, $k\log_2(n)/n < \epsilon$. Note that $f(x) = 6x - x\log_2 x - (1-x)\log_2(1-x)$ decreases to 0 as x decreases from 1/2 to 0. Thus, for every $\epsilon < c/2$ there exists a d satisfying (4.1). □

Below we show that this lemma implies an exponential lower bound on the size of LS^k+CP^k proofs with bounded degree of falsity for a class of formulas that encode a linear system $Ax = b$ that has no solution over $\mathbb{GF}_2$, where A is a matrix of a "good" expander.

Recall the definition of hard formulas based on expander matrices [2] which basically generalize Tseitin-Urquhart tautologies. For a set of rows I of a matrix $A \in \{0,1\}^{m\times n}$, we define its *boundary* ∂I as the set of all columns J of A such that there is exactly one row $i \in I$ such that:

- $a_{ij} = 1$ for some $j \in J$;
- for all other $i' \in I$, $i' \ne i$, $a_{i',j} = 0$.

Definition 4.3 *A is an (r, s, c)-*boundary expander *if the following conditions hold.*

1. *Each row contains at most s ones.*
2. *For a set of rows I, if $|I| \le r$, then $|\partial I| \ge c \cdot |I|$.*

Let b be a vector from $\{0,1\}^n$. Then $\Phi(A, b)$ is a formula expressing the equality $Ax = b$ modulo 2, namely, every equation $\oplus_{l=1}^{s} a_{ij_l} x_{j_l} = b_i$ is transformed into the 2^s clauses on $x_{j_1}, \dots, x_{j_s}$ satisfying all its solutions.

We need the following result that was proven in [1].

Theorem 4.4 *Any Res(k) proof of a formula $\Phi(A, b)$ with respect to an $(r, 3, c)$-boundary expander $A \in \{0,1\}^{m\times n}$ in which every column contains at most Δ ones, $r = \Omega(n/\Delta)$, has size* $\exp(\Omega(n/2^{O(k^2)}))$.

Theorem 4.5 *There exists a positive constant δ such that formulas $\Phi(A, b)$ with respect to an $(\Omega(n/\Delta), 3, c)$-expander A in which every column contains at most Δ ones, have only* $\exp(\Omega(n))$*-size* CP *and* LS^k+CP^k *proofs with degree of falsity bounded by δn.*

Proof. The proof follows from Lemma 4.2 and Proposition 4.4. □

5. Upper Bounds for LS^k+CP^k with Restricted Degree of Falsity

In this section we give lower and upper bounds for LS^k+CP^k with restricted degree of falsity. Namely, we give short proofs of the Pigeon-Hole Principle (which was proven in [18] to be hard for Res(k) when $k \leq \sqrt{\log n / \log\log n}$, later improved to $k \leq \epsilon \log n / \log\log n$ in [16]) and the Weak Clique-Coloring tautologies (which are known to be hard for CP [15]). This gives exponential separation of the new system from Res(k) and CP. We also show how exponential lower bounds for the LS^k+CP^k with DGF bounded by cn for some constant c follow from strongly exponential lower bounds for Res(k).

5.1 Short Proof of the Pigeon-Hole Principle

In this subsection we briefly describe the Pigeon-Hole Principle formulas and reprove Goerdt's result in the form we need in the next subsection for the polynomial upper bound for clique-coloring formulas.

The M to N pigeon-hole principle (PHP^M_N) is coded by the following set of clauses:

$$\bigvee_{1\leq \ell\leq N} x_{k,\ell} \quad , \qquad 1 \leq k \leq M \ , \tag{5.1}$$

$$\neg x_{k,\ell} \vee \neg x_{k',\ell} \quad , \qquad 1 \leq k \neq k' \leq M, 1 \leq \ell \leq N \ . \tag{5.2}$$

This set of clauses is translated into the following set of inequalities:

$$\sum_{1\leq \ell\leq N} x_{k,\ell} \geq 1 \ , \qquad 1 \leq k \leq M \ , \tag{5.3}$$

$$(1-x_{k,\ell}) + (1-x_{k',\ell}) \geq 1 \ , \qquad 1 \leq k \neq k' \leq M \ , \quad 1 \leq \ell \leq N \ . \tag{5.4}$$

By an argument similar to Goerdt's [6], we give a short proof of this contradiction in CP (and hence in LS^k+CP^k) with the degree of falsity bounded by $\sqrt{n}$. The following lemma will be of use for us later since Weak Clique-Coloring tautologies generalize the pigeon-hole principle.

Lemma 5.1 *Given a set of inequalities $x_i + x_j \leq 1$ for all $1 \leq i \neq j \leq M$ and an inequality $\sum_{i=1}^M x_i + A \geq 0$, where A is a polynomial not containing variables x_i, $1 \leq i \leq M$, we can deduce an inequality $A+1 \geq 0$ in $O(M^2)$ steps with* DGF *not exceeding the* DGF *of the initial inequalities.*

Proof. We prove by induction on M that $A + \sum_{i=1}^s x_i - x_{s'} + 1 \geq 0$ for all $1 \leq s' \leq s$ can be deduced.

Base: an inequality $A + \sum_{i=1}^{M-1} x_i - x_j + 1 \geq 0$ is the sum of initial inequalities $A + \sum_{i=1}^M x_i \geq 0$ and $1 - x_M - x_j \geq 0$.

Induction step: for all $1 \leq s' \leq s-1$ sum the following three inequalities:

$$\begin{aligned} A + \textstyle\sum_{i=1}^s x_i - x_s + 1 &\geq 0, \\ A + \textstyle\sum_{i=1}^s x_i - x_{s'} + 1 &\geq 0, \\ 1 - x_s - x_{s'} &\geq 0 \end{aligned}$$

and apply the Rounding rule to the result. This will yield the following:

$$A + \sum_{i=1}^{s-1} x_i - x_{s'} + 1 \geq 0 \ .$$

This completes the proof. □

Now, summing up all inequalities (5.3) we have

$$\sum_{j=1}^{N} \sum_{i=1}^{M} x_{i,j} \geq M \ . \tag{5.5}$$

Then apply Lemma 5.1 step by step (for $i = M, \dots, 1$) to obtain A_{i-1} from A_i, where A_i is

$$\sum_{j=1}^{i} \sum_{i=1}^{M} x_{i,j} + (N - i) \geq M \ .$$

It is easy to see that A_0 is a contradiction.

5.2 Short Proof of the Weak Clique-Coloring Tautologies

First, we recall the definition of the Weak Clique-Coloring tautologies. Given a graph G with N vertices, we try to color it with $M-1$ colors, while assuming the existence of a clique of size M in G. The set of variables of this tautology consists of the following three groups:

- for $1 \leq i, j \leq N$, $p_{ij} = 1$ iff there is an edge between i-th and j-th vertices of G,
- for $1 \leq i \leq N$, $1 \leq k \leq M$, $q_{ki} = 1$ iff the i-th vertex of G is the k-th vertex of the clique,
- for $1 \leq i \leq N$, $1 \leq \ell \leq M-1$, $r_{i\ell} = 1$ iff the i-th vertex of G is colored by the color ℓ.

Thus, the number of variables n is equal to $N^2 + NM + N(M-1)$. The contradiction is given by the following set of inequalities:

$$(1 - p_{ij}) + (1 - r_{i\ell}) + (1 - r_{j\ell}) \geq 1 \ , \quad 1 \leq i < j \leq N \ , \quad 1 \leq \ell \leq M-1 \ , \tag{5.6}$$

$$\sum_{\ell=1}^{M-1} r_{i\ell} \geq 1 \ , \quad 1 \leq i \leq N \ , \tag{5.7}$$

$$\sum_{i=1}^{N} q_{ki} \geq 1 \ , \quad 1 \leq k \leq M \ , \tag{5.8}$$

$$(1 - q_{ki}) + (1 - q_{k',i}) \geq 1 \ , \quad 1 \leq k \neq k' \leq M \ , \tag{5.9}$$

$$p_{ij} + (1 - q_{ki}) + (1 - q_{k',j}) \geq 1 \ , \quad 1 \leq i < j \leq N \ , \quad 1 \leq k \neq k' \leq M \ . \tag{5.10}$$

Grigoriev et al. [8] added one more family of inequalities to the list above:

$$(1 - q_{kj}) + (1 - q_{ki}) \geq 1 \ , \quad 1 \leq k \leq M \ , \quad 1 \leq i \neq j \leq N \ . \tag{5.11}$$

However, any CP refutation of the new system still requires at least $2^{\Omega((n/\log n)^{1/3})}$ steps.

Now let us give a short proof of this contradiction with degree of falsity bounded by $\sqrt{n}$.

Theorem 5.2 *The set of inequalities (5.6)–(5.11) has a polynomial-size proof with degree of falsity bounded by $\sqrt{n}$.*

Proof. We rewrite the proof of [8] and put each inequality into its literal form in order to show that the degree of falsity is as required. First, for each i, we multiply (5.7) by q_{ki} and then sum the resulting inequalities to obtain

$$\sum_{i=1}^{N}\sum_{\ell=1}^{M-1} q_{ki}r_{i\ell} + \sum_{i=1}^{N}(1-q_{ki}) \geq N \ ,$$

Adding (5.8) to this inequality yields

$$\sum_{i=1}^{N}\sum_{\ell=1}^{M-1} q_{ki}r_{i\ell} \geq 1 \ . \tag{5.12}$$

Next, we eliminate p_{ij} from (5.6) and (5.10) and obtain

$$(1-q_{ki}) + (1-q_{k',j}) + (1-r_{i\ell}) + (1-r_{j\ell}) \geq 1 \ , \tag{5.13}$$

for $1 \leq i < j \leq N$, $\leq k \neq k' \leq M$.

Then, we sum (5.13) with axioms $(1-q_{ki})r_{i\ell} \geq 0$, $q_{ki}(1-r_{i\ell}) \geq 0$, $q_{k',j}(1-r_{j\ell}) \geq 0$ and $(1-q_{k',j})r_{j\ell} \geq 0$ and apply the Rounding rule:

$$(1-q_{ki}r_{i\ell}) + (1-q_{k',j}r_{j\ell}) \geq 1 \ , \quad 1 \leq i < j \leq N \ , \quad 1 \leq k \neq k' \leq M \ . \tag{5.14}$$

Using $q_{ki}(1-r_{i\ell}) \geq 0$, $q_{kj}(1-r_{j\ell}) \geq 0$ and (5.11), we obtain

$$(1-q_{ki}r_{i\ell}) + (1-q_{kj}r_{j\ell}) \geq 1 \ , \quad 1 \leq \ell \leq M-1 \ , \quad 1 \leq k \leq M \ . \tag{5.15}$$

Multiplying every (5.9) by $r_{i\ell}$ and adding $(1-r_{i\ell}) \geq 0$ to the result, we obtain

$$(1-q_{ki}r_{i\ell}) + (1-q_{k',i}r_{i\ell}) \geq 1 \ . \tag{5.16}$$

Inequalities (5.14)–(5.16) imply that any length 2 sub-sum of monomials in the the sum

$$\sum_{k=1}^{M}\sum_{i=1}^{N} q_{ki}r_{i\ell} \ , \quad 1 \leq \ell \leq M-1 \ ,$$

is bounded by 1.

The proof of the Weak Clique-Coloring tautologies is then as follows. Sum (5.12) for all $1 \leq k \leq M$ to obtain

$$\sum_{k=1}^{M}\sum_{i=1}^{N}\sum_{\ell=1}^{M-1} q_{ki}r_{i\ell} \geq M \ . \tag{5.17}$$

Then, apply Lemma 5.1 to (5.14)–(5.16) and (5.17) for $s = M-1, \ldots, 1$ to obtain

$$\sum_{k=1}^{M}\sum_{i=1}^{N}\sum_{\ell=1}^{s-1} q_{ki}r_{i\ell} + M - 1 - s \geq M \ . \tag{5.18}$$

For $s = 1$ this is a clear contradiction: $-2 \geq 0$. □

6. Further Work

It is clear that the power of proof system diminishes as the degree of falsity decreases. However, we were unable to prove it formally, i.e., to demonstrate an exponential separation between proof systems with different restrictions on the degree of falsity even for CP (except for the separation between very severe restrictions that yield Resolution and very vague restrictions that allow to prove the pigeon-hole principle). It would be interesting to devise a family of formulas that produce a fine hierarchy of systems with different `DGF`'s.

Acknowledgements

We thank the anonymous referees very much for numerous catched bugs and useful suggestions.

References

[1] Michael Alekhnovich. Lower bounds for k-DNF resolution on random 3-CNFs. In *STOC '05: Proceedings of the Thirty–Seventh Annual ACM Symposium on Theory of Computing*, pages 251–256, New York, NY, USA, 2005. ACM Press.

[2] Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Pseudorandom generators in propositional proof complexity. *SIAM Journal on Computing*, **34**(1):67–88, February 2004.

[3] Albert Atserias and Maria Luisa Bonet. On the automatizability of resolution and related propositional proof systems. *Information and Computation*, **189**(2):182–201, 2004.

[4] 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.

[5] William Cook, Collette R. Coullard, and Gyorgy Turán. On the complexity of cutting-plane proofs. *Discrete Applied Mathematics*, **18**(1):25–38, 1987.

[6] Andreas Goerdt. The Cutting Plane Proof System with Bounded Degree of Falsity. In *Proceedings of CSL 1991*, **626** of *Lecture Notes in Computer Science*, pages 119–133. Springer, 1991.

[7] Ralph E. Gomory. An algorithm for integer solutions of linear programs. In R. L. Graves and P. Wolfe, editors, *Recent Advances in Mathematical Programming*, pages 269–302. McGraw-Hill, 1963.

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

[9] Edward A. Hirsch and Sergey I. Nikolenko. Simulating Cutting Plane proofs with restricted degree of falsity by Resolution. In *Proceedings of SAT 2005*, **3569** of *Lecture Notes in Computer Science*, pages 135–142. Springer-Verlag, 2005.

[10] Russell Impagliazzo, Toniann Pitassi, and Alasdair Urquhart. Upper and lower bounds for tree-like cutting planes proofs. In *Symposium on Logic in Computer Science, LICS'94*, pages 220–228, 1994.

[11] Arist Kojevnikov and Alexander S. Kulikov. Complexity of semialgebraic proofs with restricted degree of falsity. In *Proceedings of the Ninth International Conference on Theory and Applications of Satisfiability Testing (SAT 2006)*, **4121** of *Lecture Notes in Computer Science*, pages 11–21. Springer-Verlag, 2006.

[12] Jan Krajíček. On the weak pigeonhole principle. *Fundamenta Mathematicæ*, **170**(1-3):123–140, 2001.

[13] László Lovász. Stable sets and polynomials. *Discrete Mathematics*, **124**(137–153), 1994.

[14] László Lovász and Alexander Schrijver. Cones of matrices and set-functions and 0-1 optimization. *SIAM Journal of Optimization*, **1**(2):166–190, 1991.

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

[16] Alexander A. Razborov. Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution. Available at `http://genesis.mi.ras.ru/∼razborov/`, 2003.

[17] John Alan Robinson. The generalized resolution principle. *Machine Intelligence*, **3**:77–94, 1968.

[18] Nathan Segerlind, Samuel R. Buss, and Russell Impagliazzo. A Switching Lemma for Small Restrictions and Lower Bounds for k-DNF Resolution. *SIAM Journal on Computing*, **33**(5):1171–1200, 2004.

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