On semantic cutting planes with very small coefficients

Massimo Lauria[a], Neil Thapen[b]

[a] *Dipartimento di Scienze Statistiche — Sapienza Università di Roma, Italy*
massimo.lauria@uniroma1.it
[b] *Institute of Mathematics — Czech Academy of Sciences, Czech Republic*
thapen@math.cas.cz

Abstract

Cutting planes proofs for integer programs can naturally be defined both in a syntactic and in a semantic fashion. Filmus et al. (STACS 2016) proved that semantic cutting planes proofs may be exponentially stronger than syntactic ones, even if they use the semantic rule only once. We show that when semantic cutting planes proofs are restricted to have coefficients bounded by a function growing slowly enough, syntactic cutting planes can simulate them efficiently. Furthermore if we strengthen the restriction to a constant bound, then the simulating syntactic proof even has polynomially small coefficients.

Keywords: theory of computation, proof complexity, cutting planes

1. Introduction

The field of *proof complexity* studies the length of proofs for propositional unsatisfiability, also called refutations. The historical motivation was the P vs NP problem. If there are unsatisfiable formulas without short refutations, then it must be that NP is different from co-NP, and therefore that P is different from NP [11]. In this context a proof must be efficiently verifiable and therefore written in some clear format, in some specific *proof system*. If this format is simple enough, we can sometimes show strong lower bounds on the length of such proofs. As in circuit complexity, proving lower bounds is hard even for some apparently simple proof systems.

There are other good reasons to study proof systems. Algorithms which solve unsatisfiability implicitly produce refutations in a relatively simple proof system. See for example the well known connection between DPLL algorithms, decision trees and tree-like resolution proofs [14, 13, 4, 5]. Another classic example, more relevant for this paper, is the use of Gomory cuts to solve integer programs [22]. Algorithms that mix branch and bound techniques, linear programming and Gomory cuts can often be formalized as proofs in the *cutting planes* proof system [9, 10].

Despite the importance of the system, the only method we know to lower-bound the length of cutting planes proofs is *interpolation* [24], which was used to prove the first lower bounds [26]. Recently a variant of this method has been applied to random k-CNFs, with $k = \omega(1)$, as well [20, 23].

Most systems studied in proof complexity, including cutting planes, are actually inference systems. A proof is developed line by line, and each line is either an axiom of the system or is derived from some previous lines according to a specific inference rule. Nevertheless it turns out that the specifics of the inference rules are not important for many results in the area, and the main factor in the power of the proof system is the expressivity of the proof lines. Thus it makes sense to study both *syntactic* and *semantic* proofs. In the former a specific set of inference rules are available to derive a new proof line from lines derived before. In the latter a new line can be an arbitrary logical consequence of a constant number of previously derived lines.[1]

A similar (but more powerful) form of semantic proofs naturally occur in the study of proof space [15, 1]. In this framework a proof is seen as a sequence of memory configurations, each consisting of a set of proof lines, and each configuration is semantically implied by the previous one. This approach can be used to study the memory usage of proof verification algorithms. Most successful lower-bound techniques related to proof space, either based on connection to other complexity measures [2, 18], to pebbling games [25, 21, 8], or to matching games [19, 3, 6, 17], work against this type of semantic proofs. Only limited results are known for the space complexity of CP proofs, though (see [27]).

If we study proof length, the appropriate semantic version of cutting planes is the one that infers any new inequality ℓ which logically follows (over $\{0,1\}^n$) from two previously derived inequalities. Observe that this is not a proof system in the technical sense, because there is no known efficient algorithm to verify whether an inference step is sound. Indeed, even to check whether the two linear inequalities $\sum_i a_i x_i \leq b$ and $\sum_i a_i x_i \geq b$ are simultaneously satisfiable over $x_i \in \{0,1\}$ is NP-complete if the coefficients have exponential magnitude with respect to the number of variables (it is the Subset Sum problem). The situation is different with small coefficients – see the discussion at the end of this note.

Semantic cutting planes seems to be a much stronger proof system than syntactic cutting planes, and indeed even allowing just one application of the semantic rule (together with the usual syntactic rules) gives an exponential advantage over purely syntactic cutting planes [16]. Still, the same paper shows that the formula that [26] proved to be hard for syntactic CP is hard for semantic CP as well. If semantic CP is stronger in general, is there any condition under which syntactic CP efficiently simulates semantic CP? In this paper we show that

Theorem 1 (Informal)**.** *A semantic cutting planes proof in which all coefficients have very small size can be transformed into a syntactic cutting planes proof with at most a polynomial blowup in size. If the coefficients in the semantic proof are constant, the coefficients in the syntactic proof can be made polynomial.*

The idea of the proof is to realize that if the coefficients have small size, then the linear inequalities involved in the inference must have a lot of symmetries, hence the argument can be viewed as proving the soundness of an inference rule with a small number of variables. The main contribution of this paper is to show that this can be

[1] The limitation to a constant number of premises keeps the proof systems from being trivial.

done in syntactic CP. Compare this result with the separation in [16]. They exhibit a short semantic CP refutation for a CNF which is hard for syntactic CP. Such a refutation uses exponential magnitude coefficients.

The paper is organized as follows. In Section 2 we give the necessary definitions and notation. In Section 3 we discuss implicational completeness of CP and prove some upper bounds. Finally in Section 4 we show our main result, namely that semantic proofs with very small coefficients can be simulated by syntactic proofs. We conclude the paper with some open problems.

2. Preliminaries

We consider *cutting planes (CP)* [9, 12], a proof system based on manipulation of inequalities over variables $x_1, \ldots, x_n$. Each line in the proof is an inequality of the form $\sum_i a_i x_i \geq b$ where $a_i, b \in \mathbb{Z}$. Variables $x_1, \ldots, x_n$ are understood to take integer values.

A *syntactic CP derivation* of an inequality ℓ_τ from a set of inequalities $\mathcal{S}$ is denoted as $\mathcal{S} \vdash \ell_\tau$ and is a sequence of inequalities $(\ell_1, \ldots, \ell_\tau)$ such that for $1 \leq i \leq \tau$ the inequality ℓ_i is either in $\mathcal{S}$ or is obtained by one of the following rules.

- **Sum:** We can add two earlier inequalities.
- **Multiplication:** We can multiply an inequality by a positive integer.
- **Division:** From an inequality $\sum_i a_i x_i \geq b$ we can derive

$$\sum_i (a_i/c) x_i \geq \lceil b/c \rceil$$

  if c is a positive integer which divides all coefficients a_i.

When used as a propositional proof system a syntactic CP derivation may also include

- **Boolean axioms:** We can introduce inequalities $x_i \geq 0$ and $-x_i \geq -1$.

A *semantic CP derivation* of an inequality ℓ_τ from a set of inequalities $\mathcal{S}$ is a sequence of inequalities $(\ell_1, \ldots, \ell_\tau)$ such that for $1 \leq i \leq \tau$ the inequality ℓ_i is either in $\mathcal{S}$ or follows semantically from two earlier inequalities ℓ_j and ℓ_k, in the sense that ℓ_i holds for every point in $\{0,1\}^n$ where ℓ_j and ℓ_k both hold. We will also consider semantic entailment over $\mathbb{Z}^n$ rather than $\{0,1\}^n$, but we do not need a formal definition of derivations of this kind.

A syntactic (resp. semantic) CP refutation of $\mathcal{S}$ is a syntactic (resp. semantic) CP derivation of $0 \geq 1$ from $\mathcal{S}$.

If we do not care to specify the coefficients, we abbreviate $\sum_i a_i x_i \geq b$ as $A\bar{x} \geq b$. For our convenience we sometimes write $A\bar{x} \leq b$ as an alias for $-A\bar{x} \geq -b$ and $A\bar{x} = b$ as a shorthand for the conjunction of the inequalities $A\bar{x} \geq b$ and $A\bar{x} \leq b$. The *length* of a CP derivation is the number of steps. The *magnitude* of a CP derivation is the maximum absolute value among the coefficients and constants in all its inequalities. The *size* of a CP derivation is the sum, over all inequalities, of the binary length of all coefficients and the constant of each inequality. Clearly the size is at most polynomial in the length times $\log_2$ of the magnitude.

Cutting planes never needs coefficients or constants of magnitude more than exponential in the proof length, hence proofs of polynomial length can be made of polynomial size [12]. Restricting to polynomial magnitude, which is the goal of one of our simulations, gives a robust, natural, complete system CP* [7]. It can be thought of as cutting planes in which all constants and coefficients are written in unary. The system restricted to coefficients in the set $\{-2, -1, 0, 1, 2\}$ is already exponentially stronger than resolution, as it has short refutations of the pigeonhole principle [12].

3. Completeness

To prove our main result in the next section we need to show, with good bounds, that syntactic CP is implicationally complete, in the sense that every inequality ℓ that follows from $\mathcal{S}$ over the integers is provable in a finite number of steps.

Cutting planes was originally introduced as a complete implicational system in [9], but no quantitative bound was given there on the number of steps, nor on the magnitude of the coefficients involved. The refutational version of cutting planes was introduced in [12], partly because, if you only consider refutations, there is a general upper bound on proof length in terms of dimension – see Theorem 6 below.

In our setting, we consider implications from systems of axioms which explicity include upper and lower bounds on the values of all variables. Here it is straightforward to get useful upper bounds on implicational completeness by using results from [12]. We also prove a version of implicational completeness from scratch to get the bounds we want on the magnitude of coefficients (which almost, but not quite, follow from [12]).

Theorem 2. *Let $\mathcal{S}$ be a set of linear inequalities over n variables, which contains $0 \leq x_i \leq \gamma$ for each variable x_i. Suppose that $\mathcal{S}$ entails $C\bar{x} \geq d$ over the integers and that μ is a bound on the magnitude of $\mathcal{S} \cup \{C\bar{x} \geq d\}$.*

Then there is a derivation $\mathcal{S} \vdash C\bar{x} \geq d$ of length $O(n^{3n+2}\mu\gamma)$, and also a derivation simultaneously of length and magnitude $\mathrm{poly}(\mu, \gamma)$ (if we treat n as constant).

The proof of this theorem is deferred to the end of the section. We first need Lemma 4 which is a kind of deduction theorem, allowing us, under some conditions, to get rid of a hypothesis by paying for it with a weaker conclusion. We also need the following simple fact.

Fact 3. *Let $\mathcal{S}$ be a system of linear inequalities on n variables that contains axioms $0 \leq x_i \leq \gamma$ for every variable x_i. For every $a_1, \ldots, a_n$, there is a syntactic CP proof from $\mathcal{S}$ of $\sum_i a_i x_i \geq \left(-\sum_{i:a_i<0} a_i \gamma\right)$ of length $O(n)$ and magnitude at most $n\gamma \cdot \max_i\{|a_i|\}$.*

Proof. This is the sum of axioms $-x_i \geq -\gamma$ multiplied by $-a_i$, for every i with $a_i < 0$, and axioms $x_i \geq 0$ multiplied by a_i, for every i with $a_i > 0$. □

Lemma 4. *Let $\mathcal{S}$ be a system of linear inequalities on n variables. Suppose that $\mathcal{S}$ contains axioms $0 \leq x_i \leq \gamma$ for every variable x_i, and that*

$$\mathcal{S} \cup \{A\bar{x} \geq b, A\bar{x} \leq b\} \vdash C\bar{x} \geq d$$

in length τ and magnitude μ. Then we can find an integer $K \geq 0$ so that

$$\mathcal{S} \cup \{A\bar{x} \geq b\} \vdash K(A\bar{x} - b) + C\bar{x} \geq d \tag{1}$$

either in length $O(\tau)$, or simultaneously in length $\tau \cdot \mathrm{poly}(\mu, n, \gamma)$ and magnitude $\mathrm{poly}(\mu, n, \gamma)$.

Proof. Let $\ell_1, \ldots, \ell_\tau$ be the the proof of $C\bar{x} \geq d$. We will inductively define lines $\ell_1^*, \ldots, \ell_\tau^*$ of the form required by the lemma, and show that each ℓ_i^* can be derived from $\ell_1^*, \ldots, \ell_{i-1}^*$. Let us first ignore the bound on the magnitude, and just focus on building a proof of length $O(\tau)$. We distinguish various cases.

1. **Axiom:** If ℓ_i is the axiom $-A\bar{x} \geq -b$ (that is, $A\bar{x} \leq b$), we put $K = 1$, so that ℓ_i^* is the line

$$\ell_i^* : (A\bar{x} - b) - A\bar{x} \geq -b$$

   which is just another way of writing $0 \geq 0$. Other axioms are unchanged.
2. **Sum, multiplication:** These are immediate from the definition.
3. **Division:** ℓ_i is derived from ℓ_j for some $j < i$ by division. So we have

$$\begin{aligned} \ell_j &: gE\bar{x} \geq f \\ \ell_i &: E\bar{x} \geq \lceil f/g \rceil \, . \end{aligned}$$

   By the inductive hypothesis, for some integer $K \geq 0$ we have derived

$$\ell_j^* : K(A\bar{x} - b) + gE\bar{x} \geq f \, .$$

   We multiply the axiom $A\bar{x} \geq b$ by $gK - K$ to derive $(gK - K)(A\bar{x} - b) \geq 0$ and add this to ℓ_j^* to get

$$gK(A\bar{x} - b) + gE\bar{x} \geq f \, .$$

   Dividing by g now gives an inequality ℓ_i^* of the right form.

The construction so far gives a derivation of length $O(\tau)$ with no guarantee on the magnitude. Suppose now we are considering the i-th line $E\bar{x} \geq f$ in the original proof, and that for every previous line ℓ_j we have derived some ℓ_j^* in which $K \leq (n\gamma + 1)\mu$. We want to derive a ℓ_i^* with the same bound, by a short proof of small magnitude. We first derive

$$K(A\bar{x} - b) + E\bar{x} \geq f \tag{2}$$

using one of the schemes 1, 2 and 3 explained above. Notice that none of these schemes increases K very much from the earlier lines ℓ_j^*, and in particular its value is, inductively, polynomial in $n\gamma\mu$. Let $-\delta$ be the minimum value which can be taken by $E\bar{x}$ for $0 \leq \bar{x} \leq \gamma$. We derive $E\bar{x} \geq -\delta$ from $\mathcal{S}$ in $O(n)$ steps using Fact 3. We can assume $f > -\delta$ as otherwise we could now set $K = 0$. Note that $|\delta| \leq n\mu\gamma$.

We will reduce K in (2) step by step until it reaches size $f + \delta \leq \mu + n\mu\gamma$, and will set ℓ_i^* to be the resulting line. So suppose $K > f + \delta$. We first multiply (2) by $K - 1$ and add $E\bar{x} \geq -\delta$ to it, giving

$$(K - 1)K(A\bar{x} - b) + KE\bar{x} \geq Kf - f - \delta. \tag{3}$$

Then, since $f + \delta < K$, by dividing by K and rounding up we get

$$(K-1)(A\bar{x} - b) + E\bar{x} \geq f.$$

We repeat this step until we get K down to $f + \delta$.

Such a derivation has magnitude and length at most $\mathrm{poly}(n, \mu, \gamma)$. □

Corollary 5. *Let $\mathcal{S}$ be a system of linear inequalities on n variables. Suppose $\mathcal{S}$ contains axioms $0 \leq x_i \leq \gamma$ for every variable x_i, and that*

$$\mathcal{S} \cup \{A\bar{x} \leq b, A\bar{x} \geq b\} \vdash 0 \geq 1$$

in length τ and magnitude μ. Then

$$\mathcal{S} \cup \{A\bar{x} \geq b\} \vdash A\bar{x} \geq b + 1 \tag{4}$$

either in length $O(\tau)$, or simultaneously in length $\tau \cdot \mathrm{poly}(\mu, n, \gamma)$ and magnitude $\mathrm{poly}(\mu, n, \gamma)$.

Proof. We apply Lemma 4. This gives

$$\mathcal{S} \cup \{A\bar{x} \geq b\} \vdash K(A\bar{x} - b) + 0 \geq 1$$

for some integer $K \geq 0$. If $K = 0$ then we can get (4) by summing $A\bar{x} \geq b$ and $0 \geq 1$. Otherwise with one more division step we get

$$\mathcal{S} \cup \{A\bar{x} \geq b\} \vdash A\bar{x} \geq b + \lceil 1/K \rceil = b + 1.$$

Length and magnitude depend on which derivation we use from Lemma 4. □

We will now state two versions of quantitative refutational completeness for CP, which we will then use to give bounds on implicational completeness.

Theorem 6. *Let $\mathcal{S}$ be a set of linear inequalities over n variables with no integral solution. There exists a syntactic CP refutation of $\mathcal{S}$ of length $O(n^{3n+1})$.*

Proof. We observe that [12, Theorem 1'] and [12, Remark 2] give the bound n^{3n} on the number of lines in a refutation, in which each line is obtained by taking a positive linear combination of earlier lines and rounding up. By Carathéodory's theorem, we may assume that each linear combination uses no more than $n + 2$ previous lines. □

Cook et al. [12] also shows bounds on the magnitude of such a refutation, namely that the binary size of all coefficients and constant terms is polynomial in the binary size of $\mathcal{S}$. This guarantees that the magnitude increases at most quasi-polynomially. Here we guarantee a polynomially bounded increase, but our bound only works for a constant number of bounded variables, as we will have in our applications, and we pay for this improvement with a worse bound on the final length of the refutation.

Theorem 7. *Let $\mathcal{S}$ be a set of linear inequalities over n variables of magnitude μ, with no integral solution, which contains $0 \leq x_i \leq \gamma$ for every variable x_i. When n is a constant, $\mathcal{S}$ has a syntactic CP refutation of length and magnitude polynomial in μ and γ.*

Proof. We will use the notation $\vdash_\mu^\tau$ to indicate a syntactic derivation of length τ and magnitude μ. Consider any tuple $\bar{a} \in \mathbb{Z}^n$ with $0 \leq a_i \leq \gamma$ for $i \in [n]$. Since $\mathcal{S}$ is unsatisfiable, it contains some axiom $\sum_i b_i x_i \geq c$ such that $\sum_i b_i a_i = d < c$. We first construct a derivation

$$\{x_i = a_i\}_{i=1}^n \vdash_{n\mu\gamma}^{3n-1} \sum_i -b_i x_i \geq -d$$

which is a positive combination of summands $x_i \geq a_i$ for $b_i < 0$ and $-x_i \geq -a_i$ for $b_i > 0$. Then we add $\sum_i b_i x_i \geq c$ and divide by $c - d$, to get

$$\mathcal{S} \cup \{x_i = a_i\}_{i=1}^n \vdash_{n\mu\gamma}^{3n+1} 0 \geq 1 \ .$$

Now fix any $\bar{a} \in \mathbb{Z}^{n-1}$ with $0 \leq a_i \leq \gamma$ for $i \in [n-1]$. For each $0 \leq b \leq \gamma$ we have

$$\mathcal{S} \cup \{x_i = a_i\}_{i=1}^{n-1} \cup \{x_n = b\} \vdash_{n\mu\gamma}^{3n+1} 0 \geq 1$$

so by Corollary 5 we have

$$\mathcal{S} \cup \{x_i = a_i\}_{i=1}^{n-1} \cup \{x_n \geq b\} \vdash_{\mathrm{poly}(\mu,n,\gamma)}^{\mathrm{poly}(\mu,n,\gamma)} x_n \geq b + 1.$$

Stringing these derivations together, and using the axioms $0 \leq x_n \leq \gamma$, we get

$$\mathcal{S} \cup \{x_i = a_i\}_{i=1}^{n-1} \vdash_{\mathrm{poly}(\mu,n,\gamma)}^{\mathrm{poly}(\mu,n,\gamma)} 0 \geq 1,$$

where we have multiplied the length by $\gamma + 1$, and not increased the magnitude. The theorem follows by repeating these steps for $x_{n-1}, \ldots, x_1$ with n being a constant. $\square$

We are now ready to prove Theorem 2, the main result of this section.

Proof of Theorem 2. Fact 3 gives an integer δ with $|\delta| \leq n\mu\gamma$ and a derivation $C\bar{x} \geq \delta$ from $\mathcal{S}$ of length $O(n)$ and magnitude $\leq n\mu\gamma$. If $\delta > d$ then we can derive $0 \geq d - \delta$ from any pair of axioms $\{x_i \geq 0, -x_i \geq -\mu\}$, and then add that to $C\bar{x} \geq \delta$.

Otherwise, observe that for $a = \delta, \ldots, d-1$ the set $\mathcal{S} \cup \{C\bar{x} = a\}$ is unsatisfiable over the integers. To bound just the length we use Theorem 6, hence for each a we have

$$\mathcal{S} \cup \{C\bar{x} = a\} \vdash 0 \geq 1$$

in length $O(n^{3n+1})$. Thus by Corollary 5

$$\mathcal{S} \cup \{C\bar{x} \geq a\} \vdash C\bar{x} \geq a + 1$$

also in length $O(n^{3n+1})$. Starting with $C\bar{x} \geq \delta$, and then using these $d - \delta$ derivations in series, gives the theorem (as necessarily $|d| \leq \mu$).

The simultaneous bound on length and magnitude follows by a similar argument, but using Theorem 7 instead of Theorem 6. $\square$

4. Semantic and syntactic CP

In this section we prove the main result of the paper, namely the simulation of semantic CP with small coefficients by syntactic CP. Let $\ell_1, \dots, \ell_\nu$ and ℓ be inequalities such that $\ell_1, \dots, \ell_\nu$ semantically entail ℓ over $0/1$ assignments to the variables $x_1, \dots, x_n$. Suppose that the variables can be partitioned into sets $B_1, \dots, B_m$ such that each inequality in $\ell_1, \dots, \ell_\nu, \ell$ can be written in the form

$$a_1 \sum_{i \in B_1} x_i + \cdots + a_m \sum_{i \in B_m} x_i \geq b. \tag{5}$$

In other words, variables x_i and x_j are in the same set B_k if, in each inequality $\ell_1, \dots, \ell_\nu, \ell$, variable x_i has the same coefficient as x_j. Let $\ell'_1, \dots, \ell'_\nu, \ell'$ be the result of writing all the inequalities in the above form, and then for each B_j replacing $\sum_{i \in B_j} x_i$ with a single variable y_j. For example, Equation (5) becomes

$$a_1 y_1 + \cdots + a_m y_m \geq b. \tag{6}$$

Let T be the set of inequalities $\{0 \leq y_j \leq |B_j| : 1 \leq j \leq m\}$. Then, over the integers,

$$\{\ell'_1, \dots, \ell'_\nu\} \cup T \vDash \ell'.$$

This is because any assignment to the y variables satisfying the left hand side can be made into a $0/1$ assignment to the x variables satisfying $\ell_1, \dots, \ell_\nu$; hence ℓ is true with this assignment to the x variables, and so ℓ' is true with the assignment to the y variables.

If the number m of the y variables is much smaller than n, we can build a relatively efficient syntactic CP derivation

$$\{\ell'_1, \dots, \ell'_\nu\} \cup T \vdash \ell' \tag{7}$$

using the completeness results in Section 3. Now take this derivation, and substitute each variable y_j with the corresponding sum $\sum_{i \in B_j} x_i$. Every inequality in T, after the substitution, has a short derivation from the boolean axioms for the x variables. Hence

$$\{\ell_1, \dots, \ell_\nu\} \vdash \ell$$

with essentially no increase in length of magnitude with respect to the derivation in (7). We get the next two theorems by applying the argument above to each inference step of the semantic CP derivation. The results differ because of the strategy we use to get derivation (7).

Theorem 8 (Very small coefficients)**.** *Any semantic cutting planes proof of magnitude* $\sigma = O\left(\sqrt[3]{\frac{\log n}{\log \log n}}\right)$ *is polynomially simulated by a syntactic cutting planes proof.*

Proof. Consider an inference step in the refutation. Semantic CP has binary rules, so three inequalities appear and for each variable x_i, the sequence of coefficients in front of x_i is one among $(2\sigma+1)^3$ possibilities. Therefore the n variables can be divided into no more than $(2\sigma+1)^3$ blocks, and the inequalities in the inference can be considered as if they had $m = (2\sigma + 1)^3$ variables bounded between 0 and n. The magnitude is dominated by the bounds on the variables, so it is at most n. Using Theorem 2, we replace each application of the inference rule with a derivation of length $O(m^{3m+2}n^2)$. For $\sigma = O\left(\sqrt[3]{\frac{\log n}{\log\log n}}\right)$, this is polynomial in n. $\square$

Theorem 9 (Constant coefficients)**.** *Any semantic cutting planes proof of constant magnitude is polynomially simulated by a syntactic cutting planes proof of polynomial magnitude.*

Proof. We use the same construction as in Theorem 8, but using the version of Theorem 2 which bounds magnitude. We now have a constant number of variables m, again bounded between 0 and n, and magnitude n. So we can simulate each semantic inference with length and magnitude polynomial in n. $\square$

Conclusions

We managed to efficiently simulate semantic proofs with very small coefficients using syntactic cutting planes, and we know that the simulation cannot be extended to exponentially large coefficients [16]. The natural question left open is to check whether the simulation can be extended to semantic proofs with polynomial coefficients.

This is a proper proof system since there is a known efficient way to verify each application of the semantic inference rule, that we sketch. Suppose we want to verify whether

$$a_1x_1 + \cdots + a_nx_n = b$$

is satisfiable over $\bar{x} \in \{0,1\}^n$, when a_i are integer numbers. Consider a branching program that queries $x_1, \ldots, x_n$ in turn and keeps track of the sum $a_1x_1 + \cdots + a_ix_i$. Such a branching program has depth n and width $2\sum|a_i| + 1$, since the partial sum is between $-\sum|a_i|$ and $\sum|a_i|$ at every step. Hence if the coefficients are small, we can check in polynomial time whether a value b is reachable by some choice of assignments. A simple extension of this procedure is sufficient to verify the soundness of any semantic CP inference with polynomial coefficients. Hence it is even more compelling to understand whether syntactic CP can simulate efficiently this restricted form of inference.

In this paper we focus on a semantic rule with two premises. In [16] they also consider variants where the semantic rule has a constant number $k \geq 2$ of premises. Theorems 8 and 9 can be easily generalized to those variants. In particular Theorem 8 holds with $\sigma = O\left(\sqrt[k+1]{\frac{\log n}{\log\log n}}\right)$.

Acknowledgments. We thank Maria Luisa Bonet and Pavel Hrubeš for discussions on this topic. During part of this work the first author was funded by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement ERC-2014-CoG 648276 AUTAR). The second author is supported in part by grant P202/12/G061 of GAČR and RVO: 67985840.

References

[1] Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Space complexity in propositional calculus. *SIAM J. Comput.*, 31(4):1184–1211, 2002.

[2] Albert Atserias and Víctor Dalmau. A combinatorial characterization of resolution width. *J. Comput. Syst. Sci.*, 74(3):323–334, 2008.

[3] Eli Ben-Sasson and Nicola Galesi. Space complexity of random formulae in resolution. *Random Struct. Algorithms*, 23(1):92–109, 2003.

[4] Eli Ben-Sasson, Russell Impagliazzo, and Avi Wigderson. Near optimal separation of tree-like and general resolution. *Combinatorica*, 24(4):585–603, 2004.

[5] Olaf Beyersdorff, Nicola Galesi, and Massimo Lauria. A characterization of tree-like resolution size. *Information Processing Letters*, 113(18):666–671, 2013.

[6] Ilario Bonacina and Nicola Galesi. A framework for space complexity in algebraic proof systems. *J. ACM*, pages 455–472, 2014.

[7] Maria Bonet, Toniann Pitassi, and Ran Raz. Lower bounds for cutting planes proofs with small coefficients. *The Journal of Symbolic Logic*, 62(3):708–728, 1997.

[8] Siu Man Chan, Massimo Lauria, Jakob Nordström, and Marc Vinyals. Hardness of approximation in pspace and separation results for pebble games. In *Proceedings of the 2015 IEEE 56th Annual Symposium on Foundations of Computer Science (FOCS)*, FOCS '15, pages 466–485, Washington, DC, USA, 2015. IEEE Computer Society.

[9] Vašek Chvátal. Edmonds polytopes and a hierarchy of combinatorial problems. *Discrete Mathematics*, 4(4):305–337, 1973.

[10] Vašek Chvátal, William Cook, and M. Hartmann. On cutting-plane proofs in combinatorial optimization. *Linear Algebra and its Applications*, 114:455–499, 1989.

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

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

[13] Martin Davis, George Logemann, and Donald Loveland. A machine program for theorem-proving. *Commun. ACM*, 5:394–397, July 1962.

[14] Martin Davis and Hilary Putnam. A computing procedure for quantification theory. *J. ACM*, 7:201–215, July 1960.

[15] Juan Luis Esteban and Jacobo Torán. Space bounds for resolution. *Inform. Comput.*, 171(1):84–97, 2001.

[16] Yuval Filmus, Pavel Hrubeš, and Massimo Lauria. Semantic Versus Syntactic Cutting Planes. In Nicolas Ollinger and Heribert Vollmer, editors, *33rd Symposium on Theoretical Aspects of Computer Science (STACS 2016)*, volume 47 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 35:1–35:13, Dagstuhl, Germany, 2016. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[17] Yuval Filmus, Massimo Lauria, Mladen Mikša, Jakob Nordström, and Marc Vinyals. Towards an understanding of polynomial calculus: New separations and lower bounds. In FedorV. Fomin and et al., editors, *Automata, Languages, and Programming*, volume 7965 of *Lecture Notes in Computer Science*, pages 437–448. Springer Berlin Heidelberg, 2013.

[18] Yuval Filmus, Massimo Lauria, Mladen Miksa, Jakob Nordström, and Marc Vinyals. From small space to small width in resolution. In *31st International Symposium on Theoretical Aspects of Computer Science, STACS*, pages 300–311, 2014.

[19] Yuval Filmus, Massimo Lauria, Jakob Nordström, Noga Ron-Zewi, and Neil Thapen. Space complexity in polynomial calculus. *SIAM Journal on Computing*, 44(4):1119–1153, August 2015.

[20] Noah Fleming, Denis Pankratov, Toniann Pitassi, and Robert Robere. Random CNFs are hard for cutting planes. Technical Report 045, Electronic Colloquium on Computational Complexity, 2017.

[21] John R. Gilbert, Thomas Lengauer, and Robert Endre Tarjan. The pebbling problem is complete in polynomial space. *SIAM Journal on Computing*, 9(3):513–524, 1980.

[22] Ralph E. Gomory. Outline of an algorithm for integer solutions to linear programs. *Bulletin of the American Mathematical Society*, 64(5):275–278, 1958.

[23] Pavel Hrubeš and Pavel Pudlák. Random formulas, monotone circuits, and interpolation. Technical Report 042, Electronic Colloquium on Computational Complexity, 2017.

[24] Jan Krajíček. Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *The Journal of Symbolic Logic*, 62(2):457–486, 1997.

[25] Jakob Nordström. Pebble games, proof complexity and time-space trade-offs. *Logical Methods in Computer Science*, 9:15:1–15:63, September 2013.

[26] Pavel Pudlák. Lower bounds for Resolution and Cutting Plane proofs and monotone computations. *Journal of Symbolic Logic*, 62(3):981–998, 1997.

[27] Pavel Pudlák, Nicola Galesi, and Neil Thapen. The space complexity of cutting planes refutations. In *CCC*, 2015.