Electronic Colloquium on Computational Complexity, Report No. 128 (2013)

A note on semantic cutting planes

Pavel Hrubeš*

September 16, 2013

Abstract

We show that the *semantic cutting planes* proof system has feasible interpolation via monotone real circuits. This gives an exponential lower bound on proof length in the system, answering a question from [5].

We also pose the following problem: can every multivariate non-decreasing function be expressed as a composition of non-decreasing functions in two variables?

1 Introduction

Cutting planes is a proof system designed to show that a given set of linear inequalities $\mathcal{L}$ has no $0,1$-solution. A cutting planes proof starts from the inequalities in $\mathcal{L}$, produces new inequalities by means of simple syntactic rules (namely, adding two inequalities and the "rounding-up" rule), until it reaches the contradictory inequality $0 \geq 1$. The system is based on the procedure of Gomory and Chvátal [6, 3]; as a proof system, it was introduced in [4]. The complexity of cutting plane proofs has been intensively studied. The most interesting result is due to Pudlák [11], who proved that there exists a set of unsatisfiable linear inequalities which require exponential size cutting planes refutation (moreover, the inequalities represent a Boolean formula in a conjunctive normal form). His proof is a beautiful example of the so-called "feasible interpolation technique", and it required extending monotone Boolean circuit lower bounds to the new class of real monotone circuits.

In this note, we consider a stronger system called *semantic cutting planes*. In a semantic cutting planes proof, we are allowed to derive from inequalities L_1 and L_2 any inequality L which semantically follows from L_1 and L_2 – i.e., such that every $0,1$-assignment which satisfies L_1 and L_2, satisfies also L. A cutting planes proof is automatically a semantic cutting planes proof, but the latter system is stronger. This is suggested by the fact that it is NP-hard to check whether a semantic inference is correct (the knapsack problem can be stated in terms of just two inequalities). That semantic cutting planes are indeed exponentially more powerful was proved by Y. Filmus and M. Lauria in [5], who also gave the system its name. However, semantic inferences were investigated earlier in [7] or [2]. In [2], Beame, Pitassi and Segerlind consider semantic inferences using polynomial inequalities of degree k. Their results, together with the new lower bounds on communication complexity of disjointness [8, 12], imply exponential lower bounds on the *tree-like* version of such systems – including the tree-like semantic cutting planes. Here, we will prove an exponential lower bound on length of semantic cutting planes refutations. As in Pudlák's lower bound, we show that the semantic cutting planes system has feasible interpolation via monotone real circuits – in fact, our proof is a straightforward adaptation of Pudlák's original proof; the changes are all but cosmetic.

In Section 3 we discuss semantic inferences which can use more than two assumptions. In this context, we come across the following problem: can every multivariate non-decreasing function be expressed as a composition of non-decreasing functions in two variables?

*Department of Computer Science, University of Washington, pahrubes@gmail.com. Supported by the National Science Foundation under agreement CCF-1016565.

ISSN 1433-8092

2 Feasible interpolation for semantic cutting planes

The proof system

A (linear) inequality in variables $x_1, \dots, x_n$ is an expression of the form

$$a_1x_1 + \cdots + a_nx_n \geq b\,, \quad \text{with } a_1, \dots, a_n, b \in \mathbb{R}\,.$$

We view the left hand side simply as a linear function $U : \mathbb{R}^n \to \mathbb{R}$, with $U(0) = 0$. We say that a 0, 1-assignment $\sigma \in \{0,1\}^n$ *satisfies* the inequality $U \geq b$, if $U(\sigma) \geq b$. A linear inequality L *semantically follows* from a set inequalities $\mathcal{L}$, if every 0, 1-assignment, which satisfies every inequality in $\mathcal{L}$, also satisfies L. A set of inequalities $\mathcal{L}$ is *satisfiable*, if there exists an assignment which satisfies every inequality in $\mathcal{L}$.

Let $\mathcal{L}$ be a set of inequalities. *A semantic cutting planes proof* of an inequality L from $\mathcal{L}$ is a sequence of inequalities $L_1, \dots, L_m$ such that $L_m = L$, and for every $i \in \{1, \dots, m\}$,

(*i*). $L_i \in \mathcal{L}$, or

(*ii*). there exist $j_1, j_2 < i$ such that L_i follows from L_{j_1}, L_{j_2}.

L_i will be called a *proof line* in the proof. A semantic cutting planes *refutation of* $\mathcal{L}$ is a proof $0 \geq b$ from $\mathcal{L}$, where b is a positive real number.

We deviate from the definition in [5] in two details. First, we do not add the inequalities $x_i \geq 0$ and $-x_i \geq -1$ as extra axioms. However, both of those inequalities are satisfied by every assignment, and hence can be derived from an arbitrary inequality. Second, we work with inequalities with real rather than integer coefficients. But, as we are dealing with the Boolean cube, every inequality with real coefficients is equivalent to an equality with integers (see [10]).

The semantic cutting planes system is sound and complete, i.e.:

- $\mathcal{L}$ has a semantic cutting planes refutation iff $\mathcal{L}$ is unsatisfiable.

Soundness is obvious, and completeness follows from completeness of the cutting planes system.

We are chiefly interested in sets of inequalities which arise from a Boolean formula in conjunctive normal form. A disjunction such as $x_1 \vee \neg x_2 \vee \neg x_3$ is represented as the inequality $x_1 + (1 - x_2) + (1 - x_3) \geq 1$ (or rather, $x_1 - x_2 - x_3 \geq -1$). A conjunction of disjunctions is then represented by the set of inequalities representing the disjunctions. Clearly, an assignment satisfies the Boolean formula iff it satisfies the corresponding set of inequalities.

Feasible interpolation via monotone real circuits

Let X, Y_1, Y_2 be disjoint sets of variables with $X = \{x_1, \dots, x_n\}$. An inequality L of the form $U \geq b$ in the variables $X \cup Y_1 \cup Y_2$ can be uniquely written as $U^x + U^{y_1} + U^{y_2} \geq b$, where U^x, U^{y_1} and U^{y_2} depend only on the variables X, Y_1, Y_2, respectively. If $\sigma \in \{0,1\}^n$ is an assignment to the variables X, $L(\sigma)$ will denote the inequality

$$U^{y_1} + U^{y_2} \geq b - U^x(\sigma)\,. \tag{1}$$

Let $\mathcal{L}_1 = \{L_1, \dots, L_p\}$ and $\mathcal{L}_2 = \{L'_1, \dots, L'_q\}$ be two sets of inequalities, such that every inequality in $\mathcal{L}_1$ depends only the variables $X \cup Y_1$, and every inequality in $\mathcal{L}_2$ depends only the variables $X \cup Y_2$. We say that a Boolean function $f : \{0,1\}^n \to \{0,1\}$ *interpolates* $\mathcal{L}_1$ and $\mathcal{L}_2$, if for every $\sigma \in \{0,1\}^n$

(*i*). if $f(\sigma) = 0$ then the set $\mathcal{L}_1(\sigma) = \{L_1(\sigma), \dots, L_p(\sigma)\}$ is unsatisfiable, and

(*ii*). if $f(\sigma) = 1$ then the set $\mathcal{L}_2(\sigma) = \{L'_1(\sigma), \dots, L'_q(\sigma)\}$ is unsatisfiable.

Recall the definition of monotone real circuit from [11]. A monotone real circuit C computes a non-decreasing function $f : \mathbb{R}^n \to \mathbb{R}$. A gate can be *any* nondecreasing function $: \mathbb{R} \to \mathbb{R}$ or $: \mathbb{R}^2 \to \mathbb{R}$. If $f(\{0,1\}^n) \subseteq \{0,1\}$, C is said to compute the Boolean function $f|_{\{0,1\}^n}$. Clearly, the Boolean function must be monotone.

We will prove the following:

Theorem 1. *Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be as above. Assume that the variables X have non-positive coefficients in every inequality in $\mathcal{L}_2$, and that $\mathcal{L}_1 \cup \mathcal{L}_2$ has a semantic cutting planes refutation with m proof lines. Then there exists a Boolean function which interpolates $\mathcal{L}_1$ and $\mathcal{L}_2$ and which can be computed by a monotone real circuit of size $O(m + (p+q)n)$.*

Fortunately, Pudlák has also provided an exponential lower bound on the size of real monotone circuits interpolating the "clique versus coloring" tautologies. He used this to obtain an exponential lower bound for syntactic cutting planes. In the same manner, Theorem 1 implies

Corollary 2. *Let $\mathcal{L}$ be the set of inequalities representing the "clique versus coloring" tautology as in Corollary 7 in [11]. Then any semantic cutting planes refutation of $\mathcal{L}$ has an exponential number of lines.*

Note that in Theorem 1, the assumption that "X have non-positive coefficients in every inequality in $\mathcal{L}_2$" can be replaced by the assumption "X have non-negative coefficients in every inequality in $\mathcal{L}_1$".

Proof of Theorem 1

Let us first imagine that $X = \emptyset$. That is, the sets of inequalities $\mathcal{L}_1$ and $\mathcal{L}_2$ depend on disjoint sets of variables Y_1 and Y_2, respectively. Assume we have a refutation R of $\mathcal{L}_1 \cup \mathcal{L}_2$ with m proof lines. This means that at least one of $\mathcal{L}_1$ or $\mathcal{L}_2$ is unsatisfiable. We will prove a stronger statement, that at least one of $\mathcal{L}_1, \mathcal{L}_2$ has a refutation with m proof lines:

Claim. *There exists $e \in \{1,2\}$ and a refutation R_e of $\mathcal{L}_e$ with m proof-lines.*

Proof. Let R be the sequence $U_1 \geq b_1, \ldots, U_m \geq b_m$ with $U_m = 0$ and b_m positive. For $e \in \{1,2\}$ Let R_e be the sequence of inequalities

$$U_1^{y_e} \geq c_1^e, \ldots, U_m^{y_e} \geq c_m^e\,,$$

where the constants $c_1^e, \ldots, c_m^e$ are defined as follows:

(i). if $(U_i \geq b_i) \in \mathcal{L}_e$, let $c_i^e := b_i$, else

(ii). if $(U_i \geq b_i) \in \mathcal{L}_{e'}$, $e' \neq e$, let $c_i^e := 0$, else

(iii). if $U_i \geq b_i$ semantically follows from $U_{j_1} \geq b_{j_1}$ and $U_{j_2} \geq b_{j_2}$ with $j_1, j_2 < i$, let

$$c_i^e := \min\{U_i^{y_e}(\rho) \in \mathbb{R} \,:\, \rho \in A_i^e\}\,,$$
$$\text{where } A_i^e = \{\rho \in \{0,1\}^{|Y_e|} \,:\, U_{j_1}^{y_e}(\rho) \geq c_{j_1}^e,\, U_{j_2}^{y_e}(\rho) \geq c_{j_2}^e\}\,.$$

If $A_i^e = \emptyset$, let $c_i^e := \infty$ (or rather, a fixed but large enough real number).

The construction guarantees that

(a) For $e \in \{1,2\}$, R_e is a correct proof of $0 \geq c_m^e$ from $\mathcal{L}_e$, and

(b) for every $i \in \{1,\ldots,m\}$, $c_i^1 + c_i^2 \geq b_i$, unless $U_i \geq b_i$ is *vacuous*: i.e., $U_i = 0$ and b_i is negative.

The statement (a) is straightforward. Part (b) is proved by induction on $i \in \{1,\ldots,m\}$. In cases (i) and (ii) equality holds, except when $(U_i \geq b_i) \in \mathcal{L}_1 \cap \mathcal{L}_2$. Then $U_i = 0$ and $c_i^1 = c_i^2 = b_i$, and so $c_i^1 + c_i^2 = 2b_i$. Hence $c_i^1 + c_i^2 \geq b_i$ unless b_i is negative, and $U_i \geq b_i$ is indeed vacuous. For (iii), the non-trivial case is when none of $U_i \geq b_i, U_{j_1} \geq b_{j_1}, U_{j_2} \geq b_{j_2}$ is vacuous and $A_i^1, A_i^2 \neq \emptyset$. Then there exist $\rho_1 \in \{0,1\}^{|Y_1|}$ and $\rho_2 \in \{0,1\}^{|Y_2|}$ such that $c_i^1 = U_i^{y_1}(\rho_1)$ and $c_i^2 = U_i^{y_2}(\rho_2)$, and

$$U_{j_1}^{y_1}(\rho_1) \geq c_{j_1}^1,\, U_{j_2}^{y_1}(\rho_1) \geq c_{j_2}^1\,,$$
$$U_{j_1}^{y_2}(\rho_2) \geq c_{j_1}^2,\, U_{j_2}^{y_2}(\rho_2) \geq c_{j_2}^2\,.$$

Since $c^1_{j_1} + c^2_{j_1} \geq b_{j_1}$ and $c^1_{j_2} + c^2_{j_2} \geq b_{j_2}$, we have

$$U^{y_1}_{j_1}(\rho_1) + U^{y_2}_{j_1}(\rho_2) \geq b_{j_1}\,, \text{ and } U^{y_1}_{j_2}(\rho_1) + U^{y_2}_{j_2}(\rho_2) \geq b_{j_2}\,.$$

Since $U_i \geq b_i$ semantically follows from $U_{j_1} \geq b_{j_1}$ and $U_{j_2} \geq b_{j_2}$, we have

$$b_i \leq U^{y_1}_i(\rho_1) + U^{y_2}_i(\rho_2) = c^1_i + c^2_i\,.$$

Finally, $b_m > 0$ and (b) shows that either c^1_m or c^2_m is positive, and hence R_1 is a refutation of $\mathcal{L}_1$, or R_2 is a refutation of $\mathcal{L}_2$. □

To prove the theorem, the main observation is that in the case (*iii*), c_i is a non-decreasing function of c_{j_1} and c_{j_2}: increasing c_{j_1} or c_{j_2} means that in (*iii*), the minimum is taken over a smaller set.

Let $\mathcal{L}_1$, $\mathcal{L}_2$ be as in the statement of the theorem, and R a refutation of $\mathcal{L}_1 \cup \mathcal{L}_2$ with m lines. For an assignment σ to the variables X, let $R(\sigma)$ be the refutation obtained by replacing every line L in R by $L(\sigma)$. It is indeed a correct refutation of $\mathcal{L}_1(\sigma) \cup \mathcal{L}_2(\sigma)$, where the two sets now have disjoint variables. Let R^σ_1, R^σ_2 be the two proofs constructed as in the Claim, and consider the c^1_m and c^2_m as functions of σ. By (a), if $c^2_m(\sigma) > 0$ then R^σ_2 is a refutation of $\mathcal{L}_2(\sigma)$ and so $\mathcal{L}_2(\sigma)$ is unsatisfiable. If $c^2_m(\sigma) \leq 0$ then, by (b), $c^1_m(\sigma) > 0$ and so $\mathcal{L}_1(\sigma)$ is unsatisfiable. In other words, if we define the Boolean function f by

$$f(\sigma) = 1 \quad \text{iff} \quad c^2_m(\sigma) > 0\,,$$

then f interpolates $\mathcal{L}_1$ and $\mathcal{L}_2$. Moreover, if X have non-positive coefficients in $\mathcal{L}_2$, the function f can be computed by a monotone real circuit with $O(m+pn)$ gates. This is because in (*i*), $c^2_i(\sigma)$ is a linear function with non-negative coefficients (in (1), $U^x(\sigma)$ is moved to the right hand side), in (*ii*), it is a constant, and in (*iii*), c^2_i is a non-decreasing function of $c^2_{j_1}$ of $c^2_{j_2}$.

3 Inferences with higher fan-in and Hilbert's 13th Problem

In the definition of semantic cutting planes, we assumed that in a refutation of $\mathcal{L}$, every line is either an element of $\mathcal{L}$ or it follows from at most *two* previously proved inequalities. But why not *three* or a *hundred* inequalities? For a fixed $k \in \mathbb{N}$, define *k-semantic cutting planes refutation of* $\mathcal{L}$ (k-SCP refutation, for short), as a refutation in which every line $L_i \notin \mathcal{L}$ semantically follows from some $L_{j_1}, \ldots, L_{j_k}$, with $j_1, \ldots, j_k < i$. The obvious question is whether increasing k makes the proof system more powerful:

Problem 1. *For $2 \leq k_1 < k_2$, can we simulate k_2-semantic cutting planes by k_1-semantic cutting planes? More exactly, is there a polynomial p, such that whenever $\mathcal{L}$ has a k_2-SCP refutation with m proof-lines, then it has a k_1-SCP refutation with $\leq p(m)$ proof-lines?*

We do not know an answer to this question. On the other hand, we note that Theorem 1 and Corollary 2 can be extended to k-semantic refutations:

- Theorem 1 holds for k-SCP refutations, if we allow monotone real circuits to use non-decreasing k-ary functions as gates.
- Pudlák's lower bound works for monotone real circuits with k-ary gates, for any fixed k.
- Hence Corollary 2 holds also for k-SCP refutations, giving an exponential lower bound on the number of proof-lines.

In this context, we come across a related question, which is arguably much more interesting as a mathematical problem:

Problem 2. *Can every multivariate* non-decreasing *real function be expressed as a composition of* non-decreasing *unary or binary functions?*

In other words, we want to know whether every non-decreasing function can be computed by a monotone real circuit, with gates of fan-in at most two. If this is the case, there must also exist a function $\lambda : \mathbb{N} \to \mathbb{N}$ such that every non-decreasing n-ary function is computable by a monotone real circuit of size at most $\lambda(n)$.[1] This would mean that we can simulate any monotone real circuit with k-ary gates by a monotone real circuit with binary gates, with loss in size of a factor at most $\lambda(k)$.

Problem 2 is reminiscent of the solution to Hilbert's 13th Problem due to Arnold and Kolmogorov. They have shown that every multivariate *continuous* function can be expressed as a composition of unary and binary *continuous* functions (see [9] Chapter 11). In fact, the only binary function needed is addition: any continuous function can be expressed in terms of addition, and several unary continuous functions. This is rather surprising; Hilbert's 13th problem tacitly assumes that such a representation of continuous functions is impossible. Moreover, such a representation is indeed impossible for many other classes of functions: there exists an analytic function in three variables which cannot be expressed in terms of analytic functions of two variables; similarly for infinitely differentiable or entire functions (see [1] for further references).

Acknowledgement. The author thanks Pavel Pudlák for helpful discussions.

References

[1] S. Akashi and S. Kodama. A version of Hilbret's 13th problem for infinitely differentiable functions. *Fixed point theory and applications*, 2010.

[2] P. Beame, T. Pitassi, and N. Segerlind. Lower bounds for Lovász-Schrijver systems and beyond follow from multiparty communication complexity. *SIAM J. Comput.*, 37(3):845–869, June 2007.

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

[4] W. Cook, C.Coullard, and G. Turán. On the complexity of cutting-plane proofs. *Discrete Applied Mathematics*, 18(1):25–38, 1987.

[5] Y. Filmus and M. Lauria. A separation between semantic and syntactic cutting planes. Manuscript, 2013.

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

[7] J. Krajíček. Interpolatian and approximate semantic derivations. *Mathematical Logic Quarterly*, 48(4):602–606, 2002.

[8] T. Lee and A. Shraibman. Disjointness is hard in the multi-party number-on-the-forehead model. *2012 IEEE 27th Conference on Computational Complexity*, 0:81–91, 2008.

[9] G. Lorentz. *Approximations of functions*. Holt, Rinehart and Winston, New York, 1966.

[10] S. Muroga, I. Toda, and S. Takasu. Theory of majority decision elements. *Journal of the Franklin Institute*, 271(5):376–418, 1961.

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

[12] A. A. Sherstov. The multiparty communication complexity of set disjointness. In *STOC*, pages 525–548, 2012.

[1] Hint: for a fixed n, assume that for every k there exists n-ary non-decreasing function f_k which cannot be computed by a monotone real circuit of size $\leq k$. Then we can "amalgamate" the functions $f_1, f_2, \ldots$ into a single $(n+1)$-ary non-decreasing function, which cannot be computed by a monotone real circuit of any size.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de