Semantic versus syntactic cutting planes

Yuval Filmus[1], Pavel Hrubeš[2], and Massimo Lauria[3]

1 **Institute for Advanced Study**
Princeton, NJ
`yfilmus@ias.edu`

2 **Institute of Mathematics of ASCR**
Prague, Czech Republic
`pahrubes@gmail.com`

3 **KTH Royal Institute of Technology**
Stockholm, Sweden
`lauria@kth.se`

Abstract

In this paper, we compare the strength of the semantic and syntactic version of the *cutting planes* proof system.

First, we show that the lower bound technique of [22] applies also to semantic cutting planes: the proof system has feasible interpolation via monotone real circuits, which gives an exponential lower bound on lengths of semantic cutting planes refutations.

Second, we show that semantic refutations are stronger than syntactic ones. In particular, we give a formula for which any refutation in syntactic cutting planes requires exponential length, while there is a polynomial length refutation in semantic cutting planes. In other words, syntactic cutting planes does not p-simulate semantic cutting planes. We also give two incompatible integer inequalities which require exponential length refutation in syntactic cutting planes.

Finally, we pose the following problem, which arises in connection with semantic inference of arity larger than two: can every multivariate non-decreasing real function be expressed as a composition of non-decreasing real functions in two variables?

1998 ACM Subject Classification F.2.2 Complexity of proof procedures

Keywords and phrases proof complexity, cutting planes, lower bounds

Digital Object Identifier 10.4230/LIPIcs.xxx.yyy.p

1 Introduction

Cutting planes is a proof system designed to show that a given set of linear inequalities has no $0,1$-solution. After the resolution system, it is one of the best known proof systems. As a procedure for solving integer linear programs, it was considered by Gomory and Chvátal [12, 6]. The idea is to compute the optimum of the program as if it were a linear program. If the optimum is achieved at a fractional point, it is possible to deduce an inequality which can be rounded in order to remove the point from the set of feasible solutions. Another way to describe the rounding rule is as follows: if the inequality $\sum_i a_i x_i \geq b$ holds and all

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 1–14
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

a_i are integers divisible by $c > 0$, then any integer solution will also satisfy $\sum_i \frac{a_i}{c} x_i \geq \lceil \frac{b}{c} \rceil$. Cutting planes was later proposed as a proof system in [9]. Indeed, it is possible to view the previous optimization process as a sequence of inferences: a new inequality is obtained either as a non-negative linear combination or by a rounding of previously derived inequalities. In a finite number of steps, cutting planes can prove the false inequality "$0 \geq 1$" from an unsatisfiable integer program. For further information about cutting planes refutations and the notion of rank (also called Chvátal rank) we refer the reader to [15, Chapter 19].

Analysing the length of such proofs is a way of studying the running time of integer programming solvers based on the rounding rule. The complexity of cutting planes proofs has been intensively studied. A lower bound for cutting planes with small coefficients was obtained by [4] and [18], and [14] gave a lower bound for the tree-like version of the system. The strongest result is due to Pudlák [22], who proved that there exists a set of unsatisfiable linear inequalities which require exponential size cutting planes refutations (moreover, the inequalities represent a Boolean formula in conjunctive normal form). His proof is a beautiful example of the so-called "feasible interpolation technique" (used also by [4, 18]), and it required extending monotone Boolean circuit lower bounds of Razborov [23] to the new class of real monotone circuits.

It is interesting that the aforementioned lower bound for tree-like cutting planes works for any kind of deduction rule, no matter how strong. In this paper, we consider the proof system *semantic cutting planes* for which the deduction rule is the following: from any two linear inequalities L_1 and L_2 we can deduce any inequality L which is a sound consequence assuming $\{0,1\}$-assignments. Semantic inferences of similar kind were investigated earlier, in [18, 4, 17, 3]. In [18, 4], Krajíček and (independently) Beame, Pitassi and Raz consider a restricted version of semantic cutting planes in which coefficients are restricted to polynomial size, and prove exponential lower bounds for this restricted version. In [3], 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 [19, 25], imply exponential lower bounds on the *tree-like* version of such systems—including the tree-like semantic cutting planes.

The semantic system is clearly as strong as *syntactic* cutting planes, and – as we show in this paper – it is in fact stronger. The latter is suggested by the fact that it is coNP-hard to check whether a semantic inference is correct (the subset-sum problem can be stated in terms of just two inequalities). Nevertheless, we show that there exist unsatisfiable inequalities which require exponential semantic cutting planes refutations:

▶ **Theorem 1** (Lower bound). *For every n, there exists an unsatisfiable CNF of polynomial size which requires semantic cutting planes refutations with $2^{n^{\Omega(1)}}$ proof lines.*

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. Second, we prove a separation between the semantic and syntactic version of cutting planes:

▶ **Theorem 2** (Separation). *For every n, there exists an unsatisfiable CNF of polynomial size which has a semantic cutting planes refutation of polynomial size but every syntactic cutting planes refutation has $2^{n^{\Omega(1)}}$ proof lines.*

Theorem 1 is proved in Section 3, Theorem 2 in Section 4. In Section 5, we discuss semantic inferences which can use more than two assumptions. In this context, we come across the following problem: can every real multivariate non-decreasing function be expressed as a composition of non-decreasing real functions in two variables? This is analogous to Hilbert's 13th problem where the same question is posed for continuous functions.

2 Preliminaries

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

$$a_1 x_1 + \cdots + a_n x_n \geq b\,, \quad \text{with } a_1, \dots, a_n, b \in \mathbb{Z}\,.$$

We say that a $0,1$-assignment $\sigma \in \{0,1\}^n$ *satisfies* the inequality, if $\sum_{i=1}^n a_i \sigma_i \geq b$. A set of inequalities $\mathcal{L}$ is called *satisfiable*, if there exists a $0,1$-assignment which satisfies every inequality in $\mathcal{L}$.

As is customary, we will often use inequalities with "$\leq$" instead of "$\geq$", or with constants and variables appearing on both sides of the inequality. In this case, we identify $\sum_i a_i x_i \leq b$ with $\sum_i -a_i x_i \geq -b$, and $\sum_i a_i x_i + b \geq \sum_i a'_i x_i + b'$ with $\sum_i (a_i - a'_i) x_i \geq b' - b$, etc.

We now describe the two systems for refuting unsatisfiable linear inequalities.

Syntactic cutting planes Let $\mathcal{L}$ be a set of inequalities. *A syntactic 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 $i \in \{1, \dots, m\}$,

1. $L_i \in \mathcal{L}$, or it is a *Boolean axiom*

   $$x \geq 0\,, -x \geq -1\,,$$

   where x is a variable , or
2. there exist $j_1, j_2 < i$ such that L_i is obtained from L_{j_1}, L_{j_2} by means of the following rules:

(Sum) $$\frac{\sum_i a_i x_i \geq b\,, \qquad \sum_i a'_i x_i \geq b'}{\sum_i (\alpha a_i + \beta a'_i) x_i \geq \alpha b + \beta b'}\,, \qquad \text{for } \alpha, \beta \in \mathbb{N},$$

(Division) $$\frac{\sum_i a_i x_i \geq b}{\sum_i \frac{a_i}{c} x_i \geq \lceil \frac{b}{c} \rceil}\,, \qquad \text{when } 0 < c \in \mathbb{N} \text{ divides all } a_i.$$

The division rule is only valid for integer values of x_i, so it may cut away unwanted fractional solutions.

The *length* of the proof is m, i.e., the number of proof lines. A syntactic cutting planes *refutation of* $\mathcal{L}$ is a proof of $0 \geq b$ from $\mathcal{L}$, where b is any positive integer.

Semantic cutting planes *Semantic cutting planes* proofs and refutations are defined as above, except we can use the rule

$$\frac{L',\ L''}{L'''}\,,$$

where L', L'' and L''' are such that L''' semantically follows from L' and L'': every $0,1$-assignment which satisfies both L' and L'' satisfies also L'''. Note that the Boolean axioms semantically follow from any inequality and do not have to be introduced separately.

Clearly, a syntactic cutting planes proof is automatically also a semantic cutting planes proof. Semantic inference is very powerful, and there is no efficient way to verify of even witness its soundness, unless $\mathsf{NP} = \mathsf{coNP}$. Observe that the equation $\sum a_i x_i = b$ has no $0,1$-solution iff the following is a correct semantic inference:

$$\frac{\sum_i a_i x_i \geq b \qquad \sum_i a_i x_i \leq b}{0 \geq 1}.$$

However, deciding if $\sum_i a_i x_i = b$ has a $0,1$-solution is the NP-hard subset-sum problem. This shows that semantic cutting planes is not a proof system in the sense of Cook and Reckhow [8] (unless $\mathsf{P} = \mathsf{NP}$), who require proofs to be efficiently verifiable.

Krajíček [18] and Beame, Pitassi and Raz [4] consider a restricted version of semantic cutting planes in which all lines have polynomially bounded coefficients. Such a semantic inference can be checked in polynomial time using dynamic programming, and so is a proof system in the sense of Cook and Reckhow.

Size of coefficients We measure the complexity of a proof in terms of the number of inferences. However, the coefficients in the linear inequalities can be quite large and the bit representation of a proof can be much larger than the number of proof lines. Fortunately, Buss and Clote [5] proved that any syntactic cutting planes refutation can be transformed into another one in which the coefficients are at most exponential in the number of variables. Hence, each coefficient can be represented with a linear number of bits. For semantic cutting planes, we can use a more general argument: every threshold function over $\{0,1\}^n$ can be represented as a linear inequality with coefficients of bit length $O(n \log n)$ [21]. This also means that in semantic cutting planes, we can use arbitrary real coefficients instead of integer coefficients, without changing the strength of the system.

Syntactic simulation of semantic inferences Syntactic cutting planes is a complete proof system, as shown by Chvátal [6]. Results of Chvátal, Cook and Hartmann [7] and Eisenbrand and Schulz [10] show that any semantic cutting planes inference, even with an unbounded number of premises, can be simulated by a syntactic cutting planes proof of length $\exp \tilde{O}(n^2)$. This simulation is general but very inefficient. One of the main results of this paper is that an efficient simulation does not exist.

Propositional logic and CNF encoding In proof complexity, we are chiefly interested in refutations of propositional formulas, more specifically formulas in conjunctive normal form. Given a CNF A, we can represent it as a set of linear inequalities $\mathcal{L}_A$ as follows. 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, $x_1 - x_2 - x_3 \geq -1$), and $\mathcal{L}_A$ consists of all the inequalities corresponding to the clauses in A. Clearly, an assignment satisfies A iff it satisfies $\mathcal{L}_A$. We will refer to $\mathcal{L}_A$ as the *standard encoding of* A. This allows us to talk about cutting planes refutations of CNFs: a refutation of A is a refutation of the standard encoding of A.

3 Feasible interpolation for semantic cutting planes

In this section, we prove Theorem 1. This is achieved by showing that semantic cutting planes have feasible interpolation via monotone real circuits, as was shown in [22] for syntactic cutting planes.

Let X, Y_1, Y_2 be disjoint sets of variables with $X = \{x_1, \ldots, x_n\}$. 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

$$U^{y_1} + U^{y_2} \geq b - U^x(\sigma)\,. \tag{3.1}$$

Let $\mathcal{L}_1 = \{L_1, \ldots, L_p\}$ and $\mathcal{L}_2 = \{L'_1, \ldots, L'_q\}$ 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 assume that the sets $\mathcal{L}_1$ and $\mathcal{L}_2$ are contradictory: no assignment satisfies $\mathcal{L}_1 \cup \mathcal{L}_2$. We say that a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ *interpolates* $\mathcal{L}_1$ and $\mathcal{L}_2$, if for every $\sigma \in \{0,1\}^n$

1. if $f(\sigma) = 0$ then the set $\mathcal{L}_1(\sigma) = \{L_1(\sigma), \ldots, L_p(\sigma)\}$ is unsatisfiable, and
2. if $f(\sigma) = 1$ then the set $\mathcal{L}_2(\sigma) = \{L'_1(\sigma), \ldots, L'_q(\sigma)\}$ is unsatisfiable.

Recall the definition of monotone real circuit from [22]. A monotone real circuit C computes a nondecreasing function $f\colon \mathbb{R}^n \to \mathbb{R}$. 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 3.** *Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be as above. Assume that the variables X have non-positive coefficients in every inequality in $\mathcal{L}_2$ (or non-negative coefficients in $\mathcal{L}_1$), 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.

▶ **Theorem 4.** *([22]) Let $f\colon \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ be a monotone Boolean function which rejects all $k-1$-colorable graphs and accepts all graphs with a k-clique, with $k = \lceil (n/\log n)^{2/3}/8 \rceil$. Then every monotone real circuit computing f has size $2^{\Omega(n/\log n)^{1/3}}$.*

In order to deduce a lower bound on semantic cutting planes from Theorem 3 and Theorem 4, it is enough to find suitable formulas $Color_n$ and $Clique_n$ expressing that an n-vertex graph is $(k-1)$-colorable, and that it has a k-clique, respectively. We write them down for completeness.

The formula $Clique_n$ is a conjunction of the following clauses (k is the parameter from the theorem):

1. $\bigvee_{i \in [n]} y_{j,i}$, for every $j \in [k]$, $\neg y_{j_1,i} \vee \neg y_{j_2,i}$, for every $j_1 \neq j_2 \in [k]$, $i \in [n]$,
2. $\neg y_{j_1,i_1} \vee \neg y_{j_2,i_2} \vee x_{i_1,i_2}$, for every $j_1 \neq j_2 \in [k], i_1 < i_2 \in [n]$.

$Color_n$ is a conjunction of the following clauses:

1. $\bigvee_{j\in[k-1]} z_{i,j}$, for every $i \in [n]$, $\neg z_{i,j_1} \vee \neg z_{i,j_2}$, for every $i \in [n]$, $j_1 \neq j_2 \in [k-1]$,
2. $\neg z_{i_1,j} \vee \neg z_{i_2,j} \vee \neg x_{i_1,i_2}$, for every $j \in [k-1], i_1 < i_2 \in [n]$.

The formulas are in variables $X = \{x_{i_1,i_2} : i_1 < i_2 \in [n]\}$, $Y = \{y_{j,i} : j \in [k], i \in [n]\}$, $Z = \{z_{i,j} : i \in [n], j \in [k-1]\}$. We think of X as representing edges of an n-vertex graph, Y as picking a clique in the graph, and Z as defining a coloring of the graph.

▶ **Corollary 5.** *Every semantic cutting planes refutation of $Clique_n \wedge Color_n$ has at least $2^{\Omega((n/\log n)^{1/3})}$ lines.*

Proof. The particular formulation of the clique and color formulas is quite irrelevant. It matters that, first, the variables X occur only positively in $Clique_n$ (and only negatively in $Color_n$), and, second, that every interpolant of $Clique_n$ and $Color_n$ must reject on $(k-1)$-colorable graphs and accept on graphs with k-clique. ◀

Proof of Theorem 3

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

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

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

1. if $(U_i \geq b_i) \in \mathcal{L}_e$, let $c_i^e := b_i$, else
2. if $(U_i \geq b_i) \in \mathcal{L}_{e'}$ for $e' \neq e$, let $c_i^e := 0$, else
3. 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 $j_1, j_2 < i$, then c_m^e is the largest possible integer such that $U_{j_1}^{y_e} \geq c_{j_1}^e$ and $U_{j_2}^{y_e} \geq c_{j_2}^e$ imply $U_i^{y_e} \geq c_i^e$. In symbols,

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

   If the minimum is over the empty set, 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 $i \in \{1, \dots, m\}$, $c_i^1 + c_i^2 \geq b_i$, unless $U_i \geq b_i$ is *vacuous*: i.e., $U_i = 0$ and b_i is negative.

The statement (a) is true by definition. Part (b) is proved by induction on $i \in \{1, \ldots, m\}$. In case 1 and case 2 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, in which case $U_i \geq b_i$ is indeed vacuous. For case 3, 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 $c_i^1, c_i^2 < \infty$. 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 $c_{j_1}^1 + c_{j_1}^2 \geq b_{j_1}$ and $c_{j_2}^1 + c_{j_2}^2 \geq b_{j_2}$, we have

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

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

$$b_i \leq U_i^{y_1}(\rho_1) + U_i^{y_2}(\rho_2) = c_i^1 + c_i^2\,.$$

Finally, $b_m > 0$ and (b) show that either c_m^1 or c_m^2 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 case 3, 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 case 3, 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_1^σ, R_2^σ be the two proofs constructed in the Claim, and consider c_m^1 and c_m^2 as functions of σ. By (a), if $c_m^2(\sigma) > 0$ then R_2^σ is a refutation of $\mathcal{L}_2(\sigma)$ and so $\mathcal{L}_2(\sigma)$ is unsatisfiable. If $c_m^2(\sigma) \leq 0$ then, by (b), $c_m^1(\sigma) > 0$ and so $\mathcal{L}_1(\sigma)$ is unsatisfiable. In other words, if we define the Boolean function f by

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

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 case 1, $c_i^2(\sigma)$ is a linear function with non-negative coefficients (in (3.1), $U^x(\sigma)$ is moved to the right hand side), in case 2, it is a constant, and in case 3, c_i^2 is a non-decreasing function of $c_{j_1}^2$ of $c_{j_2}^2$.

4 Separation between semantic and syntactic cutting planes

In this section, we separate semantic and syntactic cutting planes, proving Theorem 2. In order to do that, we modify the "clique versus coloring" contradiction in such a way that any refutation in syntactic cutting planes must remain long, while there is a short refutation in semantic cutting planes. The main observation is that systems of unsatisfiable linear *equations* have short semantic refutations. Hence, it will be enough to restate the "clique versus coloring" as a set of linear equations, in a way that its hardness for syntactic proofs is preserved.

4.1 Equations in cutting planes

In the following, we will allow cutting planes to use linear equations as well as inequalities. Formally, we will treat an equation $U = b$ as a pair of inequalities $U \geq b$ and $U \leq b$. Hence, a refutation of a set of equations or inequalities is understood as a refutation of the underlying set of inequalities.

▶ Proposition 7. If a set of m linear equations is unsatisfiable then it has a semantic cutting planes refutation with $O(m)$ lines.

Proof. Assume that the equations are $\sum_i a_{j,i}x_i = b_j$, $j \in [m]$. Let $M \geq 2$ be the smallest natural number satisfying $M > |b_j| + \sum_i |a_{j,i}|$ for all j. From the given equations we can deduce the following equation:

$$\sum_{j=1}^{m} \left(\sum_i a_{j,i}x_i - b_j \right) M^{j-1} = 0\,, \tag{4.1}$$

using only integer scalar multiplications and sums, by separately deriving the two corresponding inequalities $0 \leq \sum_{j=1}^{m} \left(\sum_i a_{j,i}x_i - b_j\right) M^{j-1} \leq 0$. The equation is unsatisfiable, as we show below. Hence, we can deduce $0 \geq 1$ from (4.1) in a single step of semantic refutation.

It remains to show that (4.1) is unsatisfiable. Suppose that some $0,1$-assignment satisfies (4.1), and let $s_j = \sum_i a_{j,i}x_i - b_j$. By construction, $|s_j| < M$ and $\sum_{j=1}^{m} s_j M^{j-1} = 0$. Since $|s_j| < M$,

$$\left| \sum_{j=1}^{m-1} s_j M^{j-1} \right| \leq (M-1) \sum_{j=1}^{m-1} M^{j-1} < M^{m-1}.$$

This shows that $s_m = 0$, and similarly we can deduce that all other equations are satisfied. ◀

The next proposition shows that a pair of inequalities $b \leq U \leq b+1$ can be replaced by a single equality $U = b + \sigma$, where σ is a fresh variable, without changing length of syntactic proofs.

▶ Proposition 8. Let $\mathcal{L} = \mathcal{L}_0 \cup \{\sum a_i x_i \geq b\}$ be a set of linear inequalities such that $\sum_i a_i x_i \leq b + 1$ has a syntactic proof of length s from $\mathcal{L}$. Let

$$\mathcal{L}' = \mathcal{L}_0 \cup \{\textstyle\sum_i a_i x_i = b + \sigma\},$$

where σ is a variable not appearing in $\mathcal{L}$. In syntactic cutting planes, the lengths of the shortest refutations of $\mathcal{L}'$ and $\mathcal{L}$ differ at most by an additive term of $O(s)$.

Proof. Consider a refutation of $\mathcal{L}$. We want to get a refutation of $\mathcal{L}'$ of similar length. The only missing axiom in $\mathcal{L} \setminus \mathcal{L}'$ is $\sum_i a_i x_i \geq b$, which can be derived from $\sum_i a_i x_i \geq b + \sigma$ and $\sigma \geq 0$, the former being an axiom in $\mathcal{L}'$ and the latter a Boolean axiom.

In the opposite direction, start with a refutation R of $\mathcal{L}'$ with r lines and consider the substitution $\sigma \mapsto \sum_i a_i x_i - b$ applied to its lines. After this substitution, we construct a refutation of $\mathcal{L}$ with $r + s$ lines.

Axioms not mentioning σ stay the same. The substitution in the remaining axioms is

$$\begin{array}{lll}\sum_i a_i x_i = b + \sigma & \mapsto & 0 = 0; \\ \sigma \geq 0 & \mapsto & \sum_i a_i x_i \geq b; \\ \sigma \leq 1 & \mapsto & \sum_i a_i x_i \leq b + 1;\end{array}$$

where the second is an axiom in $\mathcal{L}$ and the third has a derivation with s lines. After the substitution, the sum of two lines and the product by a scalar remain correct inference steps. For the division step, consider $0 < c \in \mathbb{N}$ and the inference

$$\frac{\sum_i c a_i' x_i + cp\sigma \geq q}{\sum_i a_i' x_i + p\sigma \geq \lceil \frac{q}{c} \rceil}.$$

The assumption and the conclusion of the rule are transformed as

$$\begin{array}{lllll}\sum_i c a_i' x_i + cp\sigma \geq q & \mapsto & \sum_i c a_i' x_i + cp(\sum_i a_i x_i - b) \geq q & \equiv & \sum_i (c a_i' + cp a_i) x_i \geq q + cpb. \\ \sum_i a_i' x_i + p\sigma \geq \lceil \frac{q}{c} \rceil & \mapsto & \sum_i a_i' x_i + p(\sum_i a_i x_i - b) \geq \lceil \frac{q}{c} \rceil & \equiv & \sum_i (a_i' + p a_i) x_i \geq \lceil \frac{q}{c} \rceil + pb.\end{array}$$

Since b is an integer, $\left\lceil \frac{q+cpb}{c} \right\rceil = \lceil \frac{q}{c} \rceil + pb$, and so substitution after rounding is the same as rounding after substitution. ◀

4.2 The separating formula

Let A be a CNF

$$A = \bigwedge_{i \in [k]} (u_{i,1} \vee \cdots \vee u_{i,m_i}), \tag{4.2}$$

where each $u_{i,j}$ is a literal, i.e., a variable or its negation. We will define three reformulations of A: $T(A)$, $S(A)$ and $F(A)$, where $T(A)$ is a set of equations and inequalities, $S(A)$ is a set of equations only, and $F(A)$ is a CNF. It is the last CNF which is used in the separation between semantic and syntactic proofs.

T(A) **and S**(A). For every $i \in [k], j \in [m_i]$, introduce a new variable $\eta_{i,j}$. Then $T(A)$ is the union, over all $i \in [k]$ and $j \in [m_i]$, of the following:

$$\eta_{i,1} + \cdots + \eta_{i,m_i} = 1, \tag{4.3}$$

$$u_{i,j} - \eta_{i,j} \geq 0. \tag{4.4}$$

In (4.4) we identify $\neg x$ with $1 - x$, if $u_{i,j}$ is the literal $\neg x$ in A. Furthermore, let $S(A)$ be the set of equations obtained by replacing every inequality in (4.4) by the equation

$$u_{i,j} - \eta_{i,j} = \sigma_{i,j}, \tag{4.5}$$

where $\sigma_{i,j}$ are fresh variables.

It is easy to see that A is unsatisfiable iff $T(A)$ is unsatisfiable iff $S(A)$ is unsatisfiable. Moreover, we note that:

▶ **Lemma 9.** *Let A be an unsatisfiable CNF as in (4.2), with $m := \max m_i$. Then:*

1. *$S(A)$ has a semantic refutation with $O(mk)$ lines.*

2. *If $S(A)$ has a syntactic refutation with s lines, then $T(A)$ has a syntactic refutation with $s + O(mk)$ lines.*
3. *If A is the "clique versus coloring" CNF as in Section 3, then every semantic (hence, also syntactic) refutation of $T(A)$ requires $2^{\Omega((n/\log n)^{1/3})}$ lines.*

Proof. Item 1 follows from Proposition 7, since $S(A)$ is an unsatisfiable set of equations.

Item 2. For every inequality $u_{i,j} - \eta_{i,j} \geq 0$ in (4.4), the inequality $u_{i,j} - \eta_{i,j} \leq 1$ has a constant size syntactic proof. Hence, we can apply Proposition 8 to eliminate the variables $\sigma_{i,j}$.

Item 3 follows from Theorem 3 and Theorem 4 in the same manner as Corollary 5. In Clique_n, the variables $X = \{x_{i,j} : i < j \in [n]\}$ occur only positively. Hence, in the translation $T(\mathit{Clique}_n)$, they have only non-negative coefficients (similarly, X have non-positive coefficients in $T(\mathit{Color}_n)$). ◀

Lemma 9 already implies that for the "clique versus color" contradiction, $S(A)$ has a polynomial size semantic refutation, whereas it requires an exponential size syntactic refutation. However, $S(A)$ is a system of linear inequalities rather than a CNF. In order to fix this, we define the CNF $F(A)$, equivalent to $S(A)$.

The formula $\mathbf{F}(A)$. For three variables u, η, σ, let $\Gamma(u, \eta, \sigma)$ be the CNF expressing that $u - \eta = \sigma$; i.e., Γ is satisfied by $u, \eta, \sigma \in \{0, 1\}$ iff $u - \eta = \sigma$. Let A be a CNF as in (4.2). Then $F(A)$ is the conjunction, over all $i \in [k]$ and $j \in [m_i]$, of

$$\eta_{i,1} \vee \cdots \vee \eta_{i,m_i}\,, \neg\eta_{i,j_1} \vee \neg\eta_{i,j_2}\,, \text{ for every } j_1 \neq j_2 \in [m_i]\,, \tag{4.6}$$

$$\Gamma(u_{i,j}, \eta_{i,j}, \sigma_{i,j})\,. \tag{4.7}$$

▶ **Lemma 10.** *$S(A)$ and the standard cutting planes encoding of $F(A)$ mutually deduce each other with a polynomial length syntactic cutting planes derivation.*

Proof. Equation (4.5) has a constant size proof from the encoding of (4.7) and vice versa, because cutting planes is a complete system. The encoding of (4.6) is the set of inequalities

$$\eta_{i,1} + \cdots + \eta_{i,m_i} \geq 1\,,\ \ \eta_{i,j_1} + \eta_{i,j_2} \leq 1\,,\ \text{ for every } j_1 \neq j_2 \in [m_i]\,.$$

Comparing this with (4.3), it is enough to show:

▶ Claim 11 ([24]). The inequality $\sum_{i=1}^{n} x_i \leq 1$ has a polynomial size syntactic cutting planes proof from the inequalities $\{x_i + x_j \leq 1 : i < j \in [n]\}$. The opposite direction also holds.

Proof. For the forward direction, we prove by induction on $l - k$ that $\sum_{i=k}^{l} x_i \leq 1$. The cases $l - k \leq 2$ follow directly from the axioms. For $l - k > 2$, consider the sum of $\sum_{i=k}^{l-1} x_i \leq 1$, $\sum_{i=k+1}^{l} x_i \leq 1$ and $x_k + x_l \leq 1$, which is $\sum_{i=k}^{l} 2x_i \leq 3$. A division step concludes the proof.

The opposite direction is easier: given $\sum_{i=1}^{n} x_i \leq 1$ and two indices k and l, we can add $-x_i \leq 0$ for each $i \notin \{k, l\}$ to get $x_k + x_l \leq 1$. ◀

This completes the proof of Lemma 10. ◀

We are now ready to prove Theorem 2. Recall the "clique versus coloring" formulas in Section 3.

▶ **Theorem 12.** *The CNF formula $F(Clique_n \wedge Color_n)$ has a polynomial size semantic cutting planes refutation whereas every syntactic cutting planes refutation requires $2^{\Omega(n/\log n)^{1/3}}$ lines.*

Proof. The upper bound follows from Lemma 10 and part 1 of Lemma 9. The lower bound follows from Lemma 10 and parts 2 and 3 of Lemma 9. ◀

Inspecting Proposition 7, this also implies the following:

▶ **Corollary 13.** *There exists an equation $\sum_{i=1}^n a_i x_i = b$ which has no $0,1$-solution, the bit representation of $a_1, \dots, a_n, b$ is polynomial in n, and every syntactic cutting planes refutation of $\sum_{i=1}^n a_i x_i \geq b, \sum_{i=1}^n a_i x_i \leq b$ requires $2^{n^{\Omega(1)}}$ lines.*

Proof. Consider the set of equations $S(Clique_n \wedge Color_n)$. The proof of Proposition 7 shows how to derive (4.1), which has no $0,1$-solution, using a syntacting cutting planes derivation of polynomial size. On the other hand, parts 2 and 3 of Lemma 9 imply that every syntactic cutting planes refutation of (4.1) requires exponentially many lines. ◀

Observe that in the upper bounds of Theorem 12 and Proposition 7, it is crucial that we use exponentially large coefficients. A natural open problem is the following:

▶ Open Problem 14. Is it possible for syntactic cutting planes to polynomially simulate semantic cutting planes proofs with coefficients which are at most polynomial in the number of variables?

Notice that subset-sum problem with such small coefficients can be solved in polynomial time by dynamic programming.

5 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 follows from at most *two* previously proved inequalities. But why not *three* or a *hundred* inequalities? For a fixed $k \in \mathbb{N}$, define a *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 $L_{j_1}, \dots, L_{j_k}$, with $j_1, \dots, j_k < i$. The obvious question is whether increasing k makes the proof system more powerful:

▶ Open Problem 15. 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 at most $p(m)$ proof lines?

We do not know an answer to this question. On the other hand, we note that Theorem 3 and Corollary 5 can be extended to k-semantic refutations:

- Theorem 3 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 5 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:

▶ Open Problem 16. 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 $\lambda\colon \mathbb{N} \to \mathbb{N}$ 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 at most a factor $\lambda(k)$ loss in size.

Problem 16 is reminiscent of the solution to Hilbert's 13th Problem due to Arnold and Kolmogorov [16, 2]. They have shown that every multivariate *continuous* function can be expressed as a composition of unary and binary *continuous* functions (see [20, 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).

Acknowledgments

This paper subsumes and includes the results of the two manuscripts [11, 13].

Part of this research was done while the first author was visiting KTH Royal Institute of Technology. The first author received funding from the European Union's Seventh Framework Programme (FP7/2007–2013) under grant agreement no 238381, and from the National Science Foundation under agreement No. DMS-1128155. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors, and do not necessarily reflect the views of the National Science Foundation. The second author was supported by the National Science Foundation under agreement CCF-1016565. The third author was supported by the European Research Council under the European Union's Seventh Framework Programme (FP7/2007–2013) / ERC grant agreement no 279611.

[1] Hint: for a fixed n, assume that for every k there exists an n-ary non-decreasing function f_k which cannot be computed by a monotone real circuit of size 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.

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. Vladimir N. Arnold. On functions of three variables. *Doklady Akad. Nauk SSSR*, 114:679–681, 1957.
3. Paul Beame, Toniann Pitassi, and Nathan Segerlind. Lower bounds for Lovász-Schrijver systems and beyond follow from multiparty communication complexity. *SIAM J. Comput.*, 37(3):845–869, June 2007.
4. Maria Luisa 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.
5. Samuel R. Buss and Peter Clote. Cutting planes, connectivity, and threshold logic. *Archive for Mathematical Logic*, 35(1):33–62, 1996.
6. Vašek Chvátal. Edmonds polytopes and a hierarchy of combinatorial problems. *Discrete Mathematics*, 4(4):305–337, 1973.
7. Vašek Chvátal, William Cook, and M. Hartmann. On cutting-plane proofs in combinatorial optimization. *Linear Algebra and its Applications*, 114:455–499, 1989.
8. Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44:36–50, 1979.
9. William Cook, Collette R. Coullard, and György Turán. On the complexity of cutting-plane proofs. *Discrete Applied Mathematics*, 18(1):25–38, 1987.
10. Friederich Eisenbrand and Andreas S. Schulz. Bounds on the Chvátal rank of polytopes in the 0/1-cube. *Integer Programming and Combinatorial Optimization*, pages 137–150, 1999.
11. Yuval Filmus and Massimo Lauria. A separation between semantic and syntactic cutting planes. Manuscript, 2013.
12. Ralpha E. Gomory. Outline of an algorithm for integer solutions to linear programs. *Bulletin of the American Mathematical Society*, 64(5):275–278, 1958.
13. Pavel Hrubeš. A note on semantic cutting planes. *Electronic Colloquium on Computational Complexity (ECCC)*, 20:128, 2013.
14. Russell Impagliazzo, Toniann Pitassi, and Alasdair Urquhart. Upper and lower bounds for tree-like cutting planes proofs. In *Logic in Computer Science, 1994. LICS'94. Proceedings., Symposium on*, pages 220–228. IEEE, 1994.
15. Stasys Jukna. *Boolean Function Complexity: Advances and Frontiers*. Springer-Verlag, 2012.
16. Andrey N. Kolmogorov. On the representations of continuous functions of several variables by superpositions of continuous functions of fewer variables. *Doklady Akad. Nauk SSSR*, 108:179–182, 1956.
17. J. Krajíček. Interpolation and approximate semantic derivations. *Mathematical Logic Quarterly*, 48(4):602–606, 2002.
18. Jan Krajíček. Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *Journal of Symbolic Logic*, 62(2):457–486, 1997.

19 Troy Lee and Adi Shraibman. Disjointness is hard in the multi-party number-on-the-forehead model. *2012 IEEE 27th Conference on Computational Complexity*, 0:81–91, 2008.

20 G. G. Lorentz. *Approximations of functions*. Holt, Rinehart and Winston, New York, 1966.

21 Saburo Muroga, Iwao Toda, and Satoru Takasu. Theory of majority decision elements. *Journal of the Franklin Institute*, 271(5):376–418, 1961.

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

23 Alexander A. Razborov. Lower bounds on the monotone complexity of some Boolean functions. *Doklady Akad. Nauk SSSR*, 282:1033–1037, 1985.

24 Martin Rhodes. On the Chvátal rank of the pigeonhole principle. *Theoretical Computer Science*, 410(27-29):2774–2778, 2009.

25 Alexander A. Sherstov. The multiparty communication complexity of set disjointness. In *STOC*, pages 525–548, 2012.