Several notes on the power of Gomory-Chvátal cuts ⋆

Edward A. Hirsch Arist Kojevnikov

Steklov Institute of Mathematics at St.Petersburg, 27 Fontanka, 191023, St.Petersburg, Russia.

Abstract

We prove that the Cutting Plane proof system based on Gomory-Chvátal cuts polynomially simulates the lift-and-project system with integer coefficients written in unary. The restriction on the coefficients can be omitted when using Krajíček's cut-free Gentzen-style extension of both systems. We also prove that Tseitin tautologies have short proofs in this extension (of any of these systems and with any coefficients).

Key words: propositional proof complexity, integer programming
1991 MSC: 03F20

1 Introduction

A *proof system* [1] for a language L is a polynomial-time computable function mapping strings in some finite alphabet (proof candidates) onto L (whose elements are considered as theorems). In this paper we are interested in a specific (yet very important) kind of proof systems: proof systems for co-NP-complete languages, i.e., *propositional* proof systems. It is well-known (and easy to see) that if there existed a propositional proof system having a polynomial-size proof (i.e., inverse image) for every element of L, then NP would be equal to co-NP.

⋆ Supported in part by Russian Science Support Foundation, INTAS (grants 04-77-7173 and 04-83-3836), RFBR (grant 05-01-00932), and CRDF.

Email addresses: `hirsch@pdmi.ras.ru` (Edward A. Hirsch), `arist@logic.pdmi.ras.ru` (Arist Kojevnikov).
URLs: `http://logic.pdmi.ras.ru/~hirsch/` (Edward A. Hirsch), `http://logic.pdmi.ras.ru/~arist/` (Arist Kojevnikov).

The most natural (and historically first) propositional proof systems are proof systems for languages of Boolean tautologies: for example, resolution (for tautologies in disjunctive normal form), Frege systems (for Boolean formulas either of constant or arbitrary depth). However, proof systems for other co-NP-complete languagues are by no means worse (note that there is a polynomial-time reduction between any two co-NP-complete languages). For example, recently there was an increased interest in proof systems for unsolvable systems of polynomial equations [2,3], linear inequalities [4–7], and polynomial inequalities [8–13]. It is more natural to regard these systems as "*refutation* systems", because the "theorems" here are exactly the systems of (in)equalities that have *no* appropriate (e.g., 0/1 or integer) solutions. The most part of known proof systems uses *DAG-like* deduction: a proof consists of *lines*; the initial lines are axioms; in the course of deduction one derives more and more lines using certain derivation rules applied to already obtained lines, until the goal (particularly, a contradiction) is derived. A system is called *tree-like* if we put the following restriction: if we want to use again a line that was already used, we must derive it once more.

A proof system A *polynomially simulates* a proof system B if for every "theorem" $x \in L$ the length of the shortest proof of x in A is bounded by a polynomial in the length of the shortest proof of x in B. If, instead, there is an $x \in L$ that has exponentially shorter proof in B than in A, we say that this x certifies an *exponential separation* of B from A. If, in addition, B polynomially simulates A, then we say that B is *exponentially stronger* than A. To compare proof systems for different (even co-NP-complete) languages, one has to fix a particular reduction between the languages, which can influence the result of comparison more than the systems themselves do. Therefore, it is more convenient to compare proof systems as proof systems for the intersection of their languages (provided the intersection is co-NP-complete). In particular, the Cutting Plane and lift-and-project systems that we study are exponentially stronger than the resolution proof system, if all systems are viewed as proof systems for Boolean tautologies in disjunctive normal form.

There were several attempts to combine reasoning about equations or inequalities with "traditional logic" inference such as Frege systems or Gentzen-style systems [14–16,13]. In this paper we consider the approach of Krajíček [15] that allows one to reason about inequalities in a Gentzen-style proof system, or in a resolution proof system where literals are replaced by inequalities (this approach generalizes earlier ideas of Chvátal [unpublished, mentioned in [10]]). Krajíček considers a Gentzen-style extension of the Cutting Plane proof system. Grigoriev et al. [13] considered similar extension of the Lovász-Schrijver proof system. In this paper we consider Gentzen-style extensions of weaker systems: the lift-and-project proof system and linear programming. These extensions can be also considered as DAG-like extensions of tree-like branch-and-cut proofs (concerning lift-and-project proof system and branch-and-cut proofs see, e.g., [11,12] and references therein).

In the remaining part of this section we explain in more detail the proof systems we study, and give an outline of our results. The proofs of these results are not hard. The main purpose of the paper is to summarize facts concerning polynomial simulations between systems based on inequalities and between their extensions, and state the remaining open questions. The open questions, conclusions implied by our results, and general discussion are given in Section 5.

1.1 Proof systems based on linear programming.

We now describe several propositional proof systems for the language of systems of linear inequalities that have no 0/1-solutions. To see that this language is co-NP-complete, translate a clause $l_1 \vee \ldots \vee l_k$ of a Boolean formula in conjunctive normal form into the inequality $l_1 + \ldots + l_k - 1 \geqslant 0$ (in what follows we will omit "$\geqslant 0$"), where negative literals $l_i = \neg x_i$ are written as $1 - x_i$; the obtained system of linear inequalities has the same 0/1-solutions as the original set of clauses (where 1 corresponds to True, and 0 corresponds to False). In what follows we describe proof systems that allow to derive a contradiction (i.e., the inequality -1) if and only if the original set of inequalities has no 0/1-solutions.

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

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

for every variable x. The main derivation rule is

$$\frac{f_1, \ldots, f_k}{\sum_{i=1}^{k} \lambda_i f_i} \qquad \text{(where } \lambda_i \text{ are positive rational constants).} \tag{2}$$

(Here and in what follows f, f_i and g denote affine functions with rational coefficients.)

We call the above pre-proof system [1] LP (= Linear Programming). To design a (complete) proof system, one needs to express the fact that the variables take values in $\{0, 1\}$. There are several ways to do it, and several corresponding systems.

[1] It is not yet a proof system for our language, because it is *not complete*: it has no refutations for some systems of inequalities that have no 0/1-solutions.

The lift-and-project proof system (L&P) combines LP with the additional rule

$$\frac{f, \qquad\qquad g}{(fx + g(1-x)) \bmod (x^2 - x)} \qquad \text{(provided the result is linear).} \tag{3}$$

The Cutting Plane proof system (CP) combines LP with the Gomory-Chvátal cut rule:

$$\frac{f - \lambda}{f - \lceil \lambda \rceil} \qquad \text{(provided the coefficients of } f \text{ are integers).} \tag{4}$$

The completeness of L&P is proved in [17]. The completeness[2] of CP is proved in [4].

Usually, the size of the proof is measured as the number of bits needed to write it. In particular, all coefficients are written in binary. We also consider restrictions of our systems LP_1, CP_1, $\mathrm{L\&P}_1$, etc. where the coefficients are *integers*[3] written in *unary.*

Remark 1 *Note that polynomial-size CP_1 proofs correspond to polynomial-size CP proofs with coefficients bounded by a polynomial in the length of input (and vice versa). The latter system was considered, e.g., in [18,13]. The same applies to other systems with coefficients written in unary.*

Pudlák [19] proved an exponential lower bound on the size of CP proofs. Dash [11,12] proved an exponential lower bound on the size of L&P proofs. Grigoriev et al. [13] proved that CP_1 proofs (see Remark 1) can be polynomially simulated in a generalization of $\mathrm{L\&P}_1$.

In Section 3 we prove that $\mathrm{L\&P}_1$ can be polynomially simulated in CP_1. We do not know whether our result can be strengthened by removing the restriction on the coefficients. However, we do not need this restriction when proving a similar statement for a Gentzen-style extension of these systems described below.

1.2 Krajíček's Gentzen-style extensions.

Following Krajíček's [15] definition of R(CP), we define an extension $\mathrm{R}(\mathfrak{S})$ of any proof system $\mathfrak{S}$ as follows. The lines of the new system are sets of lines f_i

[2] If one omits the axioms (1), then the result extends to systems having no *integer* (and not just 0/1) solutions.

[3] Except for λ in (4).

of $\mathfrak{S}$. We denote these sets by disjunctions[4]: e.g., $f_1 \bigvee \ldots \bigvee f_t$. The derivation rules are (we denote by Γ an arbitrary disjunction of lines of $\mathfrak{S}$)

$$\frac{f_1 \bigvee \Gamma, \ldots, f_k \bigvee \Gamma}{h \bigvee \Gamma} \quad \text{(provided } \tfrac{f_1,\ldots,f_k}{h} \text{ is a valid derivation step of } \mathfrak{S}\text{)}, \tag{5}$$

$$\frac{\Gamma}{\Gamma \bigvee f}, \tag{6}$$

$$\frac{f \bigvee f \bigvee \Gamma}{f \bigvee \Gamma}. \tag{7}$$

Note that one can omit -1 from $-1 \bigvee \ldots$ because the contradiction -1 is easily transformable into any other inequality. If the lines of $\mathfrak{S}$ are inequalities in 0/1-variables, we add also the axiom

$$x - 1 \bigvee -x \qquad \text{(for a variable } x\text{)} \tag{8}$$

(otherwise one needs another notion of the negation). Note that while LP is not a complete refutation system for systems of inequalities in 0/1-variables, R(LP) *is* complete.

Krajíček [15] proved an exponential lower bound on the size of R(CP_1) proofs when every disjunction contains a sublinear number of inequalities (more exactly, it is sufficient that disjunctions contain $O(n^{\varepsilon})$ inequalities for a formula containing n variables and ε small enough). Dash [11,12] proved an exponential lower bound for branch-and-bound (a restricted case of tree-like R($\cdot$)) L&P proofs.

In Section 2 we discuss the relations between R(LP), R(L&P) and R(CP). In Section 4 we prove that Tseitin tautologies have short proofs in R(LP), the weakest of these systems.

2 R(LP), R(L&P), and R(CP)

2.1 R(L&P) vs R(LP).

Trivially, R(LP) proofs form a subset of R(L&P) proofs. It is not hard to see that also R(LP) polynomially simulates R(L&P), i.e., these systems are *polynomially equivalent*.

[4] To understand why this extension is called Gentzen-style, transform a disjunction into a sequent $\rightarrow f_1, \ldots, f_t$.

Proposition 1 *R(LP) polynomially simulates R(L&P),*

PROOF. The only difference between these two systems is the rule (3) of the basic system, and the simulation of this rule (inside (5)) in R(LP) is quite simple[5] :

$$\dfrac{\dfrac{\dfrac{f \vee \Gamma \qquad x-1 \vee -x}{fx+g(1-x) \bmod (x^2-x) \vee -x \vee \Gamma} \qquad g \vee \Gamma}{fx+g(1-x) \bmod (x^2-x) \vee fx+g(1-x) \bmod (x^2-x) \vee \Gamma}}{fx+g(1-x) \bmod (x^2-x) \vee \Gamma}$$

The justification of the first step is as follows. We sum f with $x-1$ multiplied by a certain coefficient (if the coefficient is negative, we use the axiom $1-x$ instead of $x-1 \vee -x$; then we reach the goal already after the first step). Namely, let $f = ax+b+F$, $g = cx+d+F$ (we can write so because $(fx+g(1-x)) \bmod (x^2-x)$ is linear). To get $fx+g(1-x) \bmod (x^2-x) = (a+b-d)x+d+F$ from f and $x-1$ (resp., $1-x$), we just add $(b-d)(x-1)$ to f. The justification of the second step is similar. □

2.2 R(CP) vs R(LP).

Again, R(LP) proofs form a subset of R(CP) proofs. We do not know whether R(CP) can be polynomially simulated in R(LP). However, proofs with integer coefficients written in unary can be polynomially simulated as follows.

Lemma 1 *Define $I_m(Y) \equiv Y-m \vee m-1-Y$. If Y contains only integer coefficients, then there is a derivation of $I_m(Y)$ in R(LP$_1$) of size polynomial in the absolute value of m, the absolute values of the coefficients of Y, and the number n of variables appearing in Y.*

PROOF. The proof goes by induction on the number of monomials. The base follows directly either from the axiom (8) or the axioms (1). We now suppose that there is a polynomial-size derivation of $I_l(Z)$ for every l, and prove $I_k(Z+ax)$, where x is a variable and a is a constant. Let $a>0$ (the

[5] Here and in what follows, we do not mention rules (6) and (7) explicitly when using them.

proof for the case $a < 0$ is similar). Then

$$\dfrac{\dfrac{\dfrac{Z-k\bigvee k-1-Z \qquad x \qquad -x\bigvee x-1}{Z+ax-k\bigvee k-1-(Z+ax)\bigvee x-1} \quad Z-(k-a)\bigvee (k-a)-1-Z}{Z+ax-k\bigvee k-1-(Z+ax)\bigvee (k-a)-1-Z} \qquad 1-x}{Z+ax-k\bigvee k-1-(Z+ax)}.$$

Note that the subscripts k that we use in the whole induction fall into the interval $[m+\min_{\{0,1\}^n} Y \ .\,.\ m+\max_{\{0,1\}^n} Y]$ (except for the trivial cases). □

Remark 2 *Note that in Lemma 1 we make essential use of DAG-likeness. For a tree-like proof, we would not be able to bound the number of lines in our proof using the bounds* $[m+\min_{\{0,1\}^n} Y \ .\,.\ m+\max_{\{0,1\}^n} Y]$ *on* k*, because some lines would appear exponentially many times.*

Now the simulation of (4) (inside rule (5)) follows from Lemma 1:

$$\dfrac{\dfrac{f-\lambda \vee \Gamma \qquad -f+\lfloor\lambda\rfloor \vee f-\lceil\lambda\rceil}{\lfloor\lambda\rfloor-\lambda \vee \Gamma \vee f-\lceil\lambda\rceil}}{\Gamma \vee f-\lceil\lambda\rceil}$$

since $\lfloor\lambda\rfloor-\lambda < 0$. This implies the following proposition.

Proposition 2 *If line* P *has a polynomial-size R(*CP_1*) derivation from set of lines* $\{Q_i\}_{i\in I}$*, then* $P \vee \Gamma$ *has a polynomial-size R(*LP_1*) derivation from* $\{Q_i \vee \Gamma\}_{i\in I}$.

3 Polynomial simulation of L&P$_1$ in CP$_1$

Theorem 1 *Every L&P proof whose lines contain only integer numbers can be transformed into a correct CP proof of size bounded by a polynomial in the size of the original proof and the absolute values of the coefficients.*

Corollary 1 *CP*$_1$ *polynomially simulates L&P*$_1$.

PROOF of Theorem 1. We show how to replace an application of (3) by a CP derivation. Since $(fx+g(1-x)) \bmod (x^2-x)$ in (3) is linear, we can represent f and g as

$$A+c, \tag{9}$$
$$A+kx, \tag{10}$$

respectively, where k and c are integers. Hence, $(fx+g(1-x)) \bmod (x^2-x) =$

$$A + cx \tag{11}$$

is what we have to derive.

We prove by induction on c that we can derive it in CP in $\max\{2c, 1\}$ steps.

First of all, if $c \geqslant k$ or $c \leqslant 0$, then (11) is a nonnegative linear combination of either (9) or (10) with axioms. Therefore, we can assume that $0 < c < k$; in particular, $c \geqslant 1$, $k \geqslant 2$. The induction base is thus $c \leqslant 0$.

We now prove the induction step. First we make a linear combination

$$(1 - \tfrac{1}{k})(A + c) + \tfrac{1}{k}(A + kx) \tag{12}$$

and round it to

$$A + x + (c - 1). \tag{13}$$

If $c = 1$, we are done (we just modify the linear combination (12) by adding $(k - 1)x$).

Otherwise, we can apply the induction hypothesis to (13) represented as $(A + x) + (c-1)$ and (10) represented as $(A+x)+(k-1)x$. Then in $\max\{2(c-1), 1\} \leqslant 2(c-1)$ steps we can derive $(A + x) + (c - 1)x$, which is the desired inequality.

It is clear that the coefficients in the obtained proof are bounded by a polynomial in the original coefficients. □

4 Short proofs of Tseitin tautologies

This section resembles [13, Section 6] (several sentences follow [13] almost literally), where short proofs of Tseitin tautologies for a different proof system are presented. The difference is that [13] does not use Gentzen-style extension, but generalizes L&P to higher (yet constant) degree instead. To transform this proof into an R(LP) proof, we need two lemmas. Then the proof goes along the same lines as in [13] with evident changes needed to get rid of high degree in favor of the case distinction arguments provided by R(LP) (in fact, the proof in R(LP) is more natural, and the proof in [13] is easier to understand after reading the R(LP) proof below).

We recall the construction of Tseitin tautologies. Let $G = (V, E)$ be a graph with an odd number n of vertices. Attach to each edge $e \in E$ a 0/1-variable x_e. The negation T_G of Tseitin tautologies with respect to G (see, e.g., [20–22]) is a family of formulas meaning that for each vertex v of G the sum $\sum_{e \ni v} x_e$ ranging over the edges incident to v is odd. Clearly, T_G is contradictory.

In recent applications to the proof theory [21,22] the construction of G is usually based on an expander. In particularly, G is d-regular, i.e., each vertex has degree d, where d is a constant. Then T_G is given by the inequalities

$$\sum_{e \in S_v \setminus S'_v} x_e + \sum_{e \in S'_v} (1 - x_e) - 1 \tag{14}$$

for each vertex v and each subset S'_v of even cardinality of the set S_v of edges incident to v. There are 2^{d-1} inequalities for each vertex of G.

We first prove two lemmas.

Lemma 2 *Denote $Y_{T,\ell} \equiv \sum_{i \in T} x_i - \ell$. Let $c \geqslant 1$ be an integer. Then there is a CP derivation of $Y_{U,c+1}$ from $\{Y_{U',c} \mid U' \subseteq U,\ |U'| = |U| - 1\}$ of size and coefficients bounded by a polynomial in c and $|U|$. Hence, there is a CP derivation of $Y_{U,c+k}$ from $\{Y_{U',c} \mid U' \subseteq U,\ |U'| = |U| - k\}$ of size and coefficients bounded by a polynomial in c, k, and $|U|$.*

PROOF. Sum all the inequalities $Y_{U',c}$ obtaining $(|U| - 1) \sum_{i \in U} x_i - c|U|$. Then divide the obtained inequality by $|U| - 1$ and round it. □

Lemma 3 *For every constant $d \geqslant 1$, odd constant t, d-regular graph G with an odd number of vertices, and every vertex v there is a polynomial-size derivation of*

$$\sum_{e \ni v} x_e - (t+2) \bigvee t - \sum_{e \ni v} x_e \tag{15}$$

from (14) in R(LP) of size and (integer) coefficients bounded by a polynomial in d and t.

PROOF. Let $0 \leqslant t \leqslant \frac{d-1}{2} = \lfloor \frac{d}{2} \rfloor$ (the opposite case $d \geqslant t \geqslant \frac{d+1}{2} = \lceil \frac{d}{2} \rceil$ is symmetrical, and the cases $t \geqslant d - 1$ and $t \leqslant -1$ are trivial). We denote $y_v \equiv \sum_{e \ni v} x_e$. By Lemma 1 we have $y_v - (t+1) \bigvee t - y_v$. For every $S'_v \subseteq S_v$ of cardinality $t+1$, let $y'_v \equiv \sum_{e \in S_v \setminus S'_v} x_e$, sum the first inequality $y_v - (t+1)$ with (14), divide it by two, and round using Lemma 1 obtaining $y'_v - 1 \bigvee t - y_v$. Applying Lemma 2 (using Proposition 2) to the first inequality (for all sets $S'_v \subseteq S$ of cardinality $t+1$), we obtain the desired line. □

Theorem 2 *For every constant $d \geqslant 1$ and every d-regular graph G with an odd number of vertices, there is a polynomial-size refutation of (14) in $R(LP_1)$.*

PROOF. Denote $Y_i = y_{v_1} + \ldots + y_{v_i}$, where $v_1, \ldots, v_i$ are pairwise distinct vertices of G and $y_v = \sum_{e \ni v} x_e$. For every $c \in [0 \mathrel{..} i(d-1)/2]$, we will prove inductively $I_c(Y_i/2)$ for odd $i = n, n-2, n-4, \ldots$ and $I_c((Y_i - 1)/2)$ for even $i = n-1, n-3, \ldots$. Then $I_0((Y_0 - 1)/2)$ gives a contradiction. The induction base ($i = n$) follows from Lemma 1, since $Y_n = 2\sum_{e \in E} x_e$ and therefore $Y_n/2$ is an integer linear combination of variables.

To proceed from step $i+1$ to step i of the refutation, denote $Y = Y_{i+1}$ and $y = \sum_{e \ni v_{i+1}} x_e$. We assume for definiteness that i is odd (the case of an even i is treated in a similar way). We need to prove that $I_c((Y - y)/2)$ for all $c \in [0 \mathrel{..} i(d-1)/2]$.

For every odd t, we can do the following. Let $c' = c + (t-1)/2 \in [c \mathrel{..} c + (d-1)/2] \subseteq [0 \mathrel{..} (i+1)(d-1)/2]$. We have $I_{c'}((Y-1)/2)$ by the induction hypothesis, and it can be rewritten as

$$\frac{Y-y}{2} - c + \frac{y-t}{2} \bigvee (c-1) - \frac{Y-y}{2} - \frac{y-t}{2}. \tag{16}$$

Note that using $y = t$ we could easily transform (16) into the desired line. To make this substitution, we use Lemma 1 to obtain

$$y - t \bigvee t - 1 - y, \qquad y - (t+1) \bigvee t - y \tag{17}$$

which yields

$$I_c(\tfrac{Y-y}{2}) \bigvee y - (t+1) \bigvee t - 1 - y. \tag{18}$$

Then for $t = 1$ we also use the original inequality $y - 1$ which yields

$$I_c(\tfrac{Y-y}{2}) \bigvee y - 2 \tag{19}$$

It remains to obtaing a contradiction with (15). Starting with (19), for $s = 1, 3, \ldots$ we will take a sum first with (15):

$$\frac{I_c(\frac{Y-y}{2}) \bigvee y - (s+1) \qquad y - (s+2) \bigvee s - y}{I_c(\frac{Y-y}{2}) \bigvee y - (s+2)}$$

and then with (18):

$$\frac{I_c(\frac{Y-y}{2}) \vee y-(s+2) \qquad I_c(\frac{Y-y}{2}) \vee y-(s+3) \vee (s+1)-y}{I_c(\frac{Y-y}{2}) \vee y-(s+3)}$$

until for $s=d-2$ or $s=d-1$ (whatever is odd) we arrive at

$$I_c(\tfrac{Y-y}{2}) \vee y-(d+1).$$

Adding $d-y$ (which is a sum of axioms) we obtain $I_c(\frac{Y-y}{2})$. □

5 Discussion

We first define one more proof system. The simplest of Lovász-Schrijver systems [9,8,10], denoted LS, is the system LP augmented with the rules

$$\frac{f}{fx \bmod (x^2-x)} \qquad \frac{f}{f(1-x) \bmod (x^2-x)} \quad \text{(where } f \text{ is linear);} \tag{20}$$

now the rule (2) can be applied to quadratic inequalities too.

(1) To *show an exponential lower bound for LS* (see, e.g., [10]) remains an open question.
(2) *Does R(CP) polynomially simulate LS?* A positive answer would solve the previous open question for the case of unary coefficients.
(3) *Does L&P polynomially simulate LS?* Dash [11,12] has partial results in this direction. Again, a positive answer would give an exponential lower bound for LS.
(4) Show an exponential lower bound for Tseitin tautologies in CP or L&P. Such result would *show that R(LP) is exponentially stronger than CP or, respectively, L&P*. Dash's polynomial simulation of branch-and-cut L&P proofs (which can be regarded as a tree-like version of R(L&P)) in L&P [11,12] is a step in the opposite direction.
(5) The representation of the coefficients (essentially, the upper bound on the coefficients, cf. Remark 1) is an important issue. We do not know *an example showing that a system with coefficients written in binary is exponentially stronger than the same system with coefficients written in unary* (on the other hand, the paper leaves unsolved several questions concerning *generalizations of our results to systems with coefficients written in binary*). Note that if the coefficients are written in binary, it is not impor-

tant[6] whether the coefficients are integer or rational. It can be, however, different if coefficients are written in unary.

References

[1] S. A. Cook, R. A. Reckhow, The relative efficiency of propositional proof systems, The Journal of Symbolic Logic 44 (1) (1979) 36–50.

[2] P. Beame, R. Impagliazzo, J. Krajícek, T. Pitassi, P. Pudlák, Lower bounds on Hilbert's Nullstellensatz and propositional proofs, Proc. London Math. Soc. 3 (73) (1996) 1–26.

[3] M. Clegg, J. Edmonds, R. Impagliazzo, Using the Groebner basis algorithm to find proofs of unsatisfiability, in: Proceedings of the 28th Annual ACM Symposium on Theory of Computing, STOC'96, 1996, pp. 174–183.

[4] R. E. Gomory, An algorithm for integer solutions of linear programs, in: R. L. Graves, P. Wolfe (Eds.), Recent Advances in Mathematical Programming, McGraw-Hill, 1963, pp. 269–302.

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

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

[7] V. Chvátal, W. Cook, M. Hartmann, On cutting-plane proofs in combinatorial optimization, Linear Algebra and its Applications 114/115 (1989) 455–499.

[8] L. Lovász, Stable sets and polynomials, Discrete Mathematics 124 (1994) 137–153.

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

[10] P. Pudlák, On the complexity of the propositional calculus, in: Sets and Proofs: Invited papers from Logic Colloquium'97, Cambridge University Press, 1999, pp. 197–218.

[11] S. Dash, On the matrix cuts of Lovász and Schrijver and their use in integer programming, Ph.D. thesis, Rice University, Houston, Texas, rice University Technical Report 01-08 (March 2001).

[12] S. Dash, An exponential lower bound on the length of some classes of branch-and-cut proofs, in: Proceedings of IPCO 2002, Vol. 2337 of Lecture Notes in Computer Science, 2002, pp. 145–160.

[6] I.e., polynomial-size proofs remain polynomial-size ones.

[13] D. Grigoriev, E. A. Hirsch, D. V. Pasechnik, Complexity of semi-algebraic proofs, Moscow Mathematical Journal 2 (4) (2002) 647–679, `http://www.ams.org/distribution/mmj/`.

[14] T. Pitassi, Algebraic propositional proof systems, in: Descriptive complexity and finite models (Princeton, NJ, 1996), Vol. 31 of DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Amer. Math. Soc., Providence, RI, 1997, pp. 215–244.

[15] J. Krajíček, Discretely ordered modules as a first-order extension of the cutting planes proof system, Journal of Symbolic Logic 63 (4) (1998) 1582–1596.

[16] D. Grigoriev, E. A. Hirsch, Algebraic proof systems over formulas, Theoretical Computer Science 303/1 (2003) 83–102.

[17] E. Balas, S. Ceria, G. Cornuéjols, A lift-and-project cutting plane algorithm for mixed 0-1 programs, Mathematical Programming 58 (1993) 295–324.

[18] M. Bonet, T. Pitassi, R. Raz, Lower bounds for cutting planes proofs with small coefficients, in: Proceedings of the 27th Annual ACM Symposium on Theory of Computing, STOC'95, 1995, pp. 575–584.

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

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

[21] A. Urquhart, Hard examples for resolution, JACM 34 (1) (1987) 209–219.

[22] S. Buss, D. Grigoriev, R. Impagliazzo, T. Pitassi, Linear gaps between degrees for the polynomial calculus modulo distinct primes, JCSS 62 (2001) 267–289.