Complexity of semi-algebraic proofs

Grigoriev, Dima; Hirsch, Edward A.; Pasechnik, Dmitrii V.

2002

Grigoriev, Dima., Hirsch, Edward A., & Pasechnik, Dmitrii V. (2002). Complexity of Semi-algebraic Proofs. Lecture Notes in Computer Science, 2285, 419-430.

<https://hdl.handle.net/10356/95181>

https://doi.org/10.1007/3-540-45841-7_34

© 2002 Springer-Verlag Berlin Heidelberg. This is the author created version of a work that has been peer reviewed and accepted for publication by Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg. It incorporates referee's comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [http://dx.doi.org/10.1007/3-540-45841-7_34].

Downloaded on 26 Apr 2023 17:58:59 SGT

Complexity of Semi-algebraic Proofs^{*}

Dima Grigoriev¹, Edward A. Hirsch^{2**}, and Dmitrii V. Pasechnik³

¹ IRMAR, Université de Rennes, Campus de Beaulieu, 35042 Rennes, cedex France.

dima@maths.univ-rennes1.fr.

<http://www.maths.univ-rennes1.fr/~dima/>

² Steklov Institute of Mathematics at St.Petersburg, 27 Fontanka, 191011
St.Petersburg, Russia.

hirsch@pdmi.ras.ru. <http://logic.pdmi.ras.ru/~hirsch/>

³ Department of Technical Mathematics and Informatics, Faculty ITS, Delft
University of Technology, Mekelweg 4, 2628 CD Delft, The Netherlands.

d.pasechnik@its.tudelft.nl.

<http://ssor.twi.tudelft.nl/~dima/>

Abstract. Proof systems for polynomial inequalities in 0-1 variables include the well-studied *Cutting Planes* proof system (CP) and the *Lovász-Schrijver calculi* (LS) utilizing linear, respectively, quadratic, inequalities. We introduce generalizations LS^d of LS involving polynomial inequalities of degree at most d .

Surprisingly, the systems LS^d turn out to be very strong. We construct polynomial-size bounded degree LS^d proofs of the *clique-coloring tautologies* (which have no polynomial-size CP proofs), the *symmetric knapsack problem* (which has no bounded degree Positivstellensatz Calculus (PC) proofs), and *Tseitin's tautologies* (hard for many known proof systems). Extending our systems with a division rule yields a polynomial simulation of *CP with polynomially bounded coefficients*, while other extra rules further reduce the proof degrees for the aforementioned examples.

Finally, we prove lower bounds on Lovász-Schrijver *ranks*, demonstrating, in particular, their rather limited applicability for proof complexity.

1 Introduction

An observation that a propositional formula can be written as a system of polynomial equations has lead to considering, in particular, the Nullstellensatz (NS) and the Polynomial Calculus (PC) proof systems, see Sect. 2.1 below (we do not dwell much here on the history of this rich area, several nice historical overviews one could find in e.g., [2,3,4,5,6,7]).

^{*} Due to the space considerations we had to shorten this text rather drastically. For the full version, that also contains new results not mentioned here, the reader is referred to [1].

^{**} A part of this work was completed while visiting Delft University of Technology. Partially supported by grant #1 of the 6th RAS contest-expertise of young scientists projects (1999) and a grant from NATO.

For these proof systems several interesting complexity lower bounds on the degrees of the derived polynomials were obtained [4,5,7]. When the degree is close enough to linear (in fact, greater than the square root), these bounds imply exponential lower bounds on the proof complexity (more precisely, on the number of monomials in the derived polynomials) [5]. If polynomials are given by formulas rather than by sums of monomials as in NS or in PC, then the complexity could decrease significantly. Several gaps between these two kinds of proof systems were demonstrated in [8].

Systems of polynomial *inequalities* yield much more powerful proof systems than these operating with equations only, such as NS or PC. Historically first such system is Cutting Planes (CP) [9,10,11,12], see also Sect. 2.2. This system uses linear inequalities (with integer coefficients). Exponential lower bounds on proof size were established for CP with polynomially bounded coefficients [13] as well as for the general case [14].

Another family of well-studied proof systems are so-called Lovász-Schrijver calculi (LS) [15,16], see also [17] and Sect. 2.2 below. In these systems one is allowed to deal with quadratic inequalities. No non-trivial complexity lower bounds are known for them so far. Moreover, generalizing LS to systems LS^d that use inequalities of degree at most d (rather than 2 as in $LS=LS^2$) yields a very powerful proof system. In particular, there exists a short LS^4 proof of the clique-coloring tautologies (see Sect. 4). On the other hand, for these tautologies an exponential lower bound on the complexity of CP proofs was obtained in [14], relying on the lower bound for the monotone complexity [18]. Furthermore, we construct a short proof for the clique-coloring tautologies in the proof system $LS + CP^2$ (see Sect. 4) that manipulates just quadratic inequalities, endowed with the rounding rule (it generalizes directly the rounding rule for linear inequalities in CP). These results mean, in particular, that neither LS^4 nor $LS + CP^2$ have monotone effective interpolation, while for a system $LS + CP^1$ where the use of rounding rule is limited to linear inequalities, a (non-monotone) effective interpolation is known [17].

An analogue of (already mentioned) non-trivial lower bounds on the degree of derived polynomials in PC would fail in LS^d as we show in Sect. 3, namely, every system of inequalities of degree at most d having no real solutions possesses an LS^{2d} refutation.

A proof system manipulating polynomial inequalities called the Positivstellensatz Calculus was introduced in [19]. Lower bounds on the degree in this system were established for the parity principle, for Tseitin's tautologies [20] and for the knapsack problem [21]. Lower bounds on the Positivstellensatz Calculus degree are possible because its “dynamic” part is restricted to an ideal and an element of a cone is obtained from an element of ideal by adding the sum of squares to it. On the contrary, LS is a completely “dynamic” proof system. (The discussion on static and dynamic proof systems can be found in [19]. Briefly, the difference is that in LS a derivation constructs gradually an element of the cone generated by the input system of inequalities, while in the Positivstellensatz Calculus the sum of squares is given explicitly.)

Also the lower bound on the Positivstellensatz Calculus degree of the knapsack problem [21] entails (see Theorem 6) a lower bound on the so-called LS-rank [15,16]. Roughly speaking, the LS-rank counts the *depth* of multiplications invoked in a derivation. A series of lower bounds for various versions of the LS-rank were obtained in the context of optimization theory [22,23,24,25]. For a counterpart notion in CP, the so-called Chvátal rank [10], lower bounds were established in [11,12]. To the best of our knowledge, the connection between the Chvátal rank and CP proof complexity is not very well understood, despite a number of interesting recent results [26,27]. As a rule, however, diverse versions of the rank grow at most linearly, while we are looking for non-linear (exponential as a dream) lower bounds on the proof complexity. It turns out that for the latter purpose the rank is a too weak invariant. Indeed, there are short proofs for the pigeon-hole principle (PHP) in CP [11] and in LS [14], while we exhibit in Theorem 7 a linear lower bound on the LS-rank of the PHP. Another example of this sort is supplied by the symmetric knapsack problem for which in Sect. 5 we give a short LS^3 -proof.

The above-mentioned LS^3 -proof of the symmetric knapsack follows from a general fact that LS^d systems allow to reason about integers. In Sect. 6 we extend this technique to Tseitin's tautologies (which have no polynomial-size proofs in resolution [28], Polynomial Calculus [7] and bounded-depth Frege systems [29]). In Sect. 5 we also consider a certain extended version $LS_{*,\text{split}}$ of LS that, apart from the issue with integers, allows one to perform a trial of cases with respect to whether $f > 0$, $f < 0$, $f = 0$ for a linear function f (similar sorts of an extension of CP were introduced by Chvátal [unpublished] [17] and Krajíček [30]) and allows also to multiply inequalities. We show that $LS_{*,\text{split}}$ polynomially simulates CP with small coefficients. The same effect can be achieved by replacing the multiplication and the trial of cases by the *division rule* that derives $g \geq 0$ from $fg \geq 0$ and $f > 0$.

Finally, we formulate numerous open questions in Sect. 8.

2 Definitions

A *proof system* [31] for a language L is a polynomial-time computable function mapping words (proof candidates) onto L (whose elements are considered as theorems). A *propositional proof system* is a proof system for any fixed co-NP-complete language of Boolean tautologies (e.g., tautologies in DNF). When we have two proof systems Π_1 and Π_2 for the same language L , we can compare them. We say that Π_1 *polynomially simulates* Π_2 , if there is a function g mapping proof candidates of Π_2 to proof candidates of Π_1 so that for every proof candidate π for Π_2 , one has $\Pi_1(g(\pi)) = \Pi_2(\pi)$ and $g(\pi)$ is at most polynomially longer than π . Proof system Π_1 is *exponentially separated* from Π_2 , if there is an infinite sequence of words $t_1, t_2, \dots \in L$ such that the length of the shortest Π_1 -proof of t_i is polynomial in the length of t_i , and the length of the shortest Π_2 -proof of t_i is exponential. Proof system Π_1 is *exponentially stronger* than Π_2 , if Π_1 polynomially simulates Π_2 and is exponentially separated from it.

D. Grigoriev, E.A. Hirsch, and D.V. Pasechnik

When we have two proof systems for different languages L_1 and L_2 , we can also compare them if we fix a reduction between these languages. However, it can be the case that the result of the comparison is more due to the reduction than to the systems themselves. Therefore, if we have propositional proof systems for languages L_1 and L_2 , and the intersection $L = L_1 \cap L_2$ of these languages is co-NP-complete, we will compare these systems as systems¹ for L .

2.1 Proof Systems Manipulating with Polynomial Equations

There is a series of proof systems for languages consisting of unsolvable systems of polynomial equations. To transform such a proof system into a propositional proof system, one needs to translate Boolean tautologies into systems of polynomial equations.

To translate a formula F in k -DNF, we take its negation $\neg F$ in k -CNF and translate each clause of $\neg F$ into a polynomial equation. A clause containing variables $v_{j_1}, \dots, v_{j_t}$ ($t \leq k$) is translated into an equation

$$(1 - l_1) \cdot \dots \cdot (1 - l_t) = 0, \quad (1)$$

where $l_i = v_{j_i}$ if variable v_{j_i} occurs positively in the clause, and $l_i = (1 - v_{j_i})$ if it occurs negatively. For each variable v_i , we also add the equation $v_i^2 - v_i = 0$ to this system.

Note that F is a tautology if and only if the obtained system S of polynomial equations $f_1 = 0, f_2 = 0, \dots, f_m = 0$ has no solutions. Therefore, to prove F it suffices to derive a contradiction from S .

Nullstellensatz (NS) [2]. A proof in this system is a collection of polynomials $g_1, \dots, g_m$ such that

$$\sum_i f_i g_i = 1.$$

Polynomial Calculus (PC) [6]. This system has two derivation rules:

$$\frac{p_1 = 0; p_2 = 0}{p_1 + p_2 = 0} \quad \text{and} \quad \frac{p = 0}{p \cdot q = 0}. \quad (2)$$

I.e., one can take a sum² of two already derived equations $p_1 = 0$ and $p_2 = 0$, or multiply an already derived equation $p = 0$ by an arbitrary polynomial q . The proof in this system is a derivation of $1 = 0$ from S using these rules.

¹ If one can decide in polynomial time for $x \in L_1$, whether $x \in L$, then any proof system for L_1 can be restricted to $L \subseteq L_1$ by mapping proofs of elements of $L_1 \setminus L$ into any fixed element of L . For example, this is the case for L_1 consisting of all tautologies in DNF and L consisting of all tautologies in k -DNF.

² Usually, an arbitrary linear combination is allowed, but clearly it can be replaced by two multiplications and one addition.

Positivstellensatz [19]. A proof in this system consists of polynomials $g_1, \dots, g_m$ and $h_1, \dots, h_l$ such that

$$\sum_i f_i g_i = 1 + \sum_j h_j^2 \quad (3)$$

Positivstellensatz Calculus [19]. A proof in this system consists of polynomials $h_1, \dots, h_l$ and a derivation of $1 + \sum_j h_j^2 = 0$ from S using the rules (2).

2.2 Proof Systems Manipulating with Inequalities

To define a propositional proof system manipulating with inequalities, we again translate each formula $\neg F$ in CNF into a system S of linear inequalities, such that F is a tautology if and only if S has no 0-1 solutions. Given a Boolean formula in CNF, we translate each its clause containing variables $v_{j_1}, \dots, v_{j_t}$ into the inequality

$$l_1 + \dots + l_t \geq 1, \quad (4)$$

where $l_i = v_{j_i}$ if the variable v_{j_i} occurs positively in the clause, and $l_i = 1 - v_{j_i}$ if v_{j_i} occurs negatively. We also add to S the inequalities $x \geq 0$ and $x \leq 1$ for every variable x .

Cutting Planes (CP) [9,10,11,12], cf. also [17]. In this proof system, the system S defined above must be refuted (i.e., the contradiction $0 \geq 1$ must be obtained) using the following two derivation rules:

$$\frac{f_1 \geq 0; \dots; f_t \geq 0}{\sum_{i=1}^t \lambda_i f_i \geq 0} \quad (\text{where } \lambda_i \geq 0), \quad (5)$$

$$\frac{\sum_i a_i x_i \geq c}{\sum_i a_i x_i \geq \lceil c \rceil} \quad (\text{where } a_i \in \mathbb{Z}, \text{ and } x_i \text{ is a variable}). \quad (6)$$

We restrict the intermediate inequalities in a CP derivation to the ones having integer coefficients (except the constant term).

Lovász-Schrijver calculus (LS) [15,16], cf. also [17]. In the weakest of Lovász-Schrijver proof systems, the contradiction must be obtained using the rule (5) applied to linear or quadratic f_i 's and the rules

$$\frac{f \geq 0}{fx \geq 0}; \quad \frac{f \geq 0}{f(1-x) \geq 0} \quad (\text{where } f \text{ is linear, } x \text{ is a variable}). \quad (7)$$

Also, the system S is extended by the axioms

$$x^2 - x \geq 0, \quad x - x^2 \geq 0 \quad (8)$$

for every variable x .

LS₊ [15,16,17]. This system has the same axioms and derivation rules as LS, and also has the axiom

$$l^2 \geq 0 \quad (9)$$

for every linear l .

Grigoriev, E.A. Hirsch, and D.V. Pasechnik

LS* [15,16,17]. This system has the same axioms and derivation rules as LS, and also the derivation rule

$$\frac{f \geq 0; g \geq 0}{fg \geq 0} \quad (f, g \text{ are linear}). \quad (10)$$

LS_{+,*}. This system unites LS₊ and LS*.

LS + CP¹ [17]. It has the same axioms and derivation rules as LS and also the rounding rule (6) of CP which can be applied only to linear inequalities.

Note that all Lovász-Schrijver systems described in this subsection deal either with linear or quadratic inequalities.

2.3 New Systems

In this paper we consider several extensions of Lovász and Schrijver proof systems. First, we define system LS + CP² which is slightly stronger than Pudlák's LS + CP¹.

LS + CP². It has the same axioms and rules as LS and also the extension of rounding rule (6) of CP to quadratic inequalities:

$$\frac{\sum_{i,j} a_{ij}x_i x_j + \sum_i a_i x_i \geq c}{\sum_{i,j} a_{ij}x_i x_j + \sum_i a_i x_i \geq \lceil c \rceil} \quad (\text{where } a_i, a_{ij} \in \mathbb{Z}, \text{ and } x_i \text{ is a variable}). \quad (11)$$

We then consider extensions of Lovász-Schrijver proof systems allowing monomials of degree up to d .

LS^d. This system is an extension of LS. The difference is that rule (7) is now restricted to f of degree at most $d-1$ rather than to linear inequalities. Rule (5) can be applied to any inequality of degree at most d .

Similarly, we consider **LS_{*}^d**, transforming in (10) the condition “ f, g are linear” into “ $\deg(fg) \leq d$ ”.

LS_{split}^d. This system allows not only inequalities of the form $f \geq 0$, but also of the form $f > 0$. The derivation rules (5) and (7) are extended in a clear way to handle both types of inequalities, and $f > 0$ can be always relaxed to $f \geq 0$. The axiom $1 > 0$ is added. Also if under each of the three assumptions $f > 0$, $f < 0$ and $f = 0$ (a shorthand for the two inequalities $f \geq 0$ and $f \leq 0$) there is an LS_{split}^d derivation of inequality $h \geq 0$, then we say that $h \geq 0$ is derived in LS_{split}^d.

LS_{*,split}^d is defined similarly. Note that the version of (10) for strict inequalities is

$$\frac{f > 0; g > 0}{fg > 0}.$$

$\mathbf{LS}_{0/1\text{-split}}^d$ is a restricted version of $\mathbf{LS}_{\text{split}}^d$ where the splitting is made for the assumptions $x = 0, x = 1$ only (x is a variable).

$\mathbf{LS}_/^d$ is an extension of $\mathbf{LS}^d$ with strict inequalities by another useful rule:

$$\frac{fg \geq 0; f > 0}{g \geq 0}.$$

$\mathbf{LS}_{\text{split}}, \mathbf{LS}_{*,\text{split}}, \text{etc.}$ are shorthands for the corresponding systems restricted to $d = 2$.

3 Encodings of Formulas in $\mathbf{LS}^d$ and Upper Bounds on the Refutation Degree

In $\mathbf{LS}^d$, Boolean formulas are encoded as linear inequalities. However, this is not the only possible way to encode them, since in $\mathbf{LS}^d$ we can operate with polynomials of degree up to d . In particular, for formulas in k -CNF, one can use the same encoding as in Polynomial Calculus (1).

Consider system $\overline{\mathbf{LS}}^d$ that has the same derivation rules as $\mathbf{LS}^d$, but uses the encoding (1) instead of (4). It is clear that when $d = n$ is the number of variables, $\overline{\mathbf{LS}}^n$ polynomially simulates Polynomial Calculus. Does $\mathbf{LS}^n$ polynomially simulate $\overline{\mathbf{LS}}^n$ (and Polynomial Calculus)? To give the positive answer, it suffices to show that there is a polynomial-size derivation of the encoding by polynomial equations from the encoding by linear inequalities.

Lemma 1. *There is a polynomial-size $\mathbf{LS}^t$ derivation of (1) from (4), (8) and $0 \leq x \leq 1$.*

Corollary 1. *$\mathbf{LS}^d$ polynomially simulates $\overline{\mathbf{LS}}^d$ (and, hence, $\mathbf{LS}^n$ polynomially simulates Polynomial Calculus).*

Corollary 2. *$\mathbf{LS}_+^n$ polynomially simulates Positivstellensatz Calculus.*

It turns out that the converse of Lemma 1 is also true. In particular, due to [15, Theorem 1.4] that means that there is an $\mathbf{LS}^k$ refutation of every formula in k -CNF. Below, we also show (Theorem 1) that there is an $\mathbf{LS}^{2k}$ refutation of any system of polynomial inequalities of degree at most k .

Lemma 2. *There is a polynomial-size $\mathbf{LS}^t$ derivation of (4) from (1), (8), and $0 \leq x \leq 1$.*

Corollary 3. *$\overline{\mathbf{LS}}^d$ polynomially simulates $\mathbf{LS}^d$.*

Corollary 4. *There is an $\overline{\mathbf{LS}}^k$ refutation of every formula in k -CNF.*

Theorem 1. *There is a polynomial-size $\mathbf{LS}^{2k}$ refutation of any unsolvable system of polynomial inequalities of degree at most k .*

4 Short LS + CP² and LS⁴ Proofs of the Clique-Coloring Tautologies

Theorem 2. *There is a set of inequalities that has polynomial-size refutations in LS⁴ and LS + CP², but has only exponential-size refutations in CP.*

The set of inequalities we use is close to the one used by Pudlák for proving an exponential lower bound for CP [14]. Pudlák's bound remains valid for this system. Therefore, to achieve the result, we show that this set of inequalities has polynomial-size refutations in LS⁴ and LS + CP².

Clique-coloring tautologies. Given a graph G with n vertices, we try to colour it with $m - 1$ colours, while assuming the existence of a clique of size m in G . Each edge (i, j) is represented by a (0-1) variable p_{ij} . Variables q_{ki} encode a (possibly multivalued) function from the integers $\{1 \dots m\}$ denoting the vertices of a m -clique to the set $\{1 \dots n\}$ of the vertices of G . Namely, q_{ki} represents the i -th vertex of G being the k -th vertex of the clique. Variables $r_{i\ell}$ encode a (possibly multivalued) coloring of vertices by $m - 1$ colors. The assignment of the colour ℓ to the node i is represented by a variable $r_{i\ell}$. The inequalities (1)–(5) in [14] (see also [1]) state that G has an m -clique and is $(m - 1)$ -colorable. We now add to them one more family of inequalities, without affecting applicability of [14, Corollary 7], that is, any CP refutation of the new system will still require at least $2^{\Omega((n/\log n)^{1/3})}$ steps. Namely, we add

$$\sum_{i=1}^n q_{ki} \leq 1, \quad k = 1 \dots m. \quad (12)$$

PHP interpretation of weak clique-coloring tautologies. The fact that the i -th vertex of G is the k -th vertex of the clique and is coloured with the colour ℓ is encoded as $q_{ki}r_{i\ell} \geq 1$. Then the fact that the k -th vertex of the clique has colour ℓ is encoded as

$$\sum_{i=1}^n q_{ki}r_{i\ell} \geq 1.$$

Let us denote this sum by $x_{k\ell}$. Note that $x_{k\ell}$'s define an injective (possibly multivalued) mapping from $\{1 \dots m\}$ to $\{1 \dots m - 1\}$.

For $x_{k\ell}$'s, the inequalities of another well-known unsolvable system of inequalities hold. Namely, these are inequalities that express the negation of the propositional pigeonhole principle:

$$\sum_{\ell=1}^{m-1} x_{k\ell} \geq 1; \quad 1 \leq k \leq m; \quad (13)$$

$$x_{k\ell} + x_{k'\ell} \leq 1; \quad 1 \leq k < k' \leq m; \quad 1 \leq \ell \leq m - 1. \quad (14)$$

(That says that the k -th pigeon must get into a hole, while two pigeons k and k' cannot share the same hole ℓ .) For short, we denote this system of inequalities by PHP.

There is a polynomial-size CP refutation for PHP [11]. In our notation (note that x_{kl} denotes a quadratic polynomial) such refutation translates into an $LS + CP^2$ refutation. Alternatively, Pudlák shows that PHP also has polynomial-size refutation in LS . In our notation, this translates into an LS^4 refutation. We show that there is a polynomial-size derivation of (13)–(14) from (1)–(5) of [14] and (12) in LS^4 as well as in $LS + CP^2$.

5 Reasoning about Integers

Versions of Lovász-Schrijver calculi can be used for reasoning about integers. In the following lemma the basic primitive for the latter, the family of quadratic inequalities $f_d(Y) \geq 0$, is introduced. The lemma shows that there are short proofs of the fact that an integer linear combination of variables is either at most $d - 1$ or at least d for any integer d . It follows then that there are short LS^3 (as well as $LS_{0/1\text{-split}}$) proofs of the symmetric knapsack problem, and that CP with polynomially bounded coefficients can be simulated in LS^3 (as well as in $LS_{*,\text{split}}$).

Lemma 3. *Let $Y = \sum_{i=1}^n a_i x_i$ and $f_d(Y) = (Y - (d - 1))(Y - d)$, where a_i are integers and x_i are variables. Then the inequality $f_d(Y) \geq 0$ has a derivation in LS^3 and $LS_{0/1\text{-split}}$ of size polynomial in d , n and $\max_i |a_i|$.*

Theorem 3. *For $m \notin \mathbb{Z}$, there is a polynomial-size LS^3 (as well as $LS_{0/1\text{-split}}$) refutation of*

$$m - x_1 - x_2 - \dots - x_n = 0. \quad (15)$$

CP with polynomially bounded coefficients are defined in [13].

Theorem 4. *The systems $LS_{*,\text{split}}$ and LS^3 polynomially simulate CP with polynomially bounded coefficients.*

6 Short Proof of Tseitin's Tautologies in LS^d

We recall the construction of Tseitin's tautologies. Let $G = (V, E)$ be a graph with an odd number n of vertices. Attach to each edge $e \in E$ a Boolean variable x_e , i.e. $x_e^2 = x_e$. The negation $T = T_G$ of Tseitin's tautologies with respect to G (see e.g., [7,8]) 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 is contradictory.

In the applications to the proof theory [7,28] the construction of G is usually based on an expander. In particular, G is d -regular, i.e., each vertex has degree d , where d is a constant. The respective negation $T = T_G$ of Tseitin's tautologies is given by the following equalities (due to Lemmas 1 and 2 we give them directly in PC translation):

$$\prod_{e \in S'_v} x_e \cdot \prod_{e \notin S'_v} (1 - x_e) = 0 \quad (16)$$

D. Grigoriev, E.A. Hirsch, and D.V. Pasechnik

(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} equalities of degree d for each vertex of G .

Theorem 5. *For every constant $d \geq 1$ and every d -regular graph G , there is a polynomial-size refutation of (16) in LS^{d+2} .*

7 Lower Bounds on Lovász-Schrijver Rank

There is a series of lower bounds on Lovász-Schrijver rank in the literature (see e.g. [23,25] and the references there). However, these bounds are not suitable for the use in the propositional proof theory, because these are either bounds for *solvable* systems of inequalities, or bounds for systems with *exponentially many* inequalities.

The standard geometric setting for the Lovász-Schrijver procedures LS and LS_+ [15] involves, given a system $Ax \leq b$ of m linear inequalities in variables $x_1, \dots, x_n$, homogenization by adding an extra variable $x_0 \geq 0$ and considering the cone K (resp., K_I) of (resp. 0-1) solutions to the homogenized system. Lift-and-project operators $N^r(K)$ and $N^r_+(K)$ are introduced, and the inclusions

$$K_I \subseteq N^r_{(+)}(K) \subseteq N^{r-1}_{(+)}(K) \subseteq \dots \subseteq N^k_{(+)}(K) \subseteq \dots \subseteq N_{(+)}(K) \subseteq K \quad (17)$$

are shown in [15]. The LS-*rank* (respectively, LS_+ -*rank*) of a system of linear inequalities $Ax \leq b$ is the minimal k in (17) such that $N^k(K) = K_I$ (respectively, $N^k_+(K) = K_I$), where $K = K(A, b)$, as above.

Alternative definitions of Lovász-Schrijver ranks in proof systems terms are as follows. A proof in Lovász-Schrijver proof system is a directed acyclic graph whose vertices correspond to the derived inequalities, and there is an edge between $f \geq 0$ and $g \geq 0$ iff g is derived from f (and maybe something else) in one step. We now drop the edges corresponding to the rule (5). The *rank of a refutation* is the length of the longest path from an axiom to the contradiction in this graph. The *LS-rank* of a system is the smallest rank of an LS-refutation for it. The *LS_+ -rank* is the smallest rank of an LS_+ -refutation. Similarly, one can define LS_* - and $LS_{+,*}$ -ranks. Note that this definition generalizes smoothly to LS^d , LS^d_+ , LS^d_* and $LS^d_{+,*}$.

The following Theorem 6 gives a linear lower bound on the LS_+ -rank (and a logarithmic lower bound on the $LS_{+,*}$ -rank) of symmetric knapsack problem by reducing it to a lower bound on the degree of Positivstellensatz Calculus refutation [21]. However, this system of inequalities is not obtained as a translation of a propositional formula, and thus lower bounds for it cannot be directly used in the propositional proof theory.

The system of inequalities for the symmetric knapsack problem is given by (15) and usual axioms $0 \leq x \leq 1$, (8). We restrict our attention to system K obtained by setting $m = \lfloor \frac{n}{2} \rfloor + \frac{1}{2}$.

Theorem 6. *The LS_+ -rank of K is at least $n/4$, while the $LS_{+,*}$ -rank of K is at least $\log_2 n - 1$.*

The following Theorem 7 gives an $O(m)$ lower bound on the LS-rank of PHP. Note that the LS_+ -rank of PHP is a constant.

Theorem 7. *At least $m - 2$ iterations of the N -operator are needed to prove the integer infeasibility of (13)-(14), that is, its LS-rank is at least $m - 2$.*

8 Open Questions

1. What is the proof complexity of the knapsack problem in LS (cf. Sect. 5 and 7)? We conjecture it as a candidate for a lower bound.
2. Prove an exponential lower bound on the size of Positivstellensatz refutations.
3. Suggest a candidate for a lower bound in LS^d for (arbitrarily large) constant d .
4. How precise is the logarithmic lower bound on the LS_* -rank for the knapsack problem from Theorem 6?
5. Can one relax in Theorem 4 the condition on the polynomial growth of the coefficients?
6. Is it possible to simulate LS by means of a suitable version of CP (e.g. by the $\text{R}(\text{CP})$ introduced in [30])? In other words, is there an inverse to Theorem 4?

Acknowledgment. The authors are grateful to Arist Kojevnikov, Alexander Razborov and Hans van Maaren for useful discussions.

References

1. Grigoriev, D., Hirsch, E.A., Pasechnik, D.V.: Complexity of semi-algebraic proofs. Technical report, Electronic Colloquium on Computational Complexity (2001 (submitted)) <http://eccc.uni-trier.de/eccc-local/Lists/TR-2001.html>.
2. Beame, P., Impagliazzo, R., Krajíček, J., Pitassi, T., Pudlák, P.: Lower bounds on Hilbert's Nullstellensatz and propositional proofs. *Proc. London Math. Soc.* **73** (1996) 1–26
3. Beame, P., Impagliazzo, R., Krajíček, J., Pudlák, P., Razborov, A.A., Sgall, J.: Proof complexity in algebraic systems and bounded depth Frege systems with modular counting. *Computational Complexity* **6** (1996/97) 256–298
4. Razborov, A.A.: Lower bounds for the polynomial calculus. *Computational Complexity* **7** (1998) 291–324
5. Impagliazzo, R., Pudlák, P., Sgall, J.: Lower bounds for the polynomial calculus. *Computational Complexity* **8** (1999) 127–144
6. Clegg, M., Edmonds, J., Impagliazzo, R.: Using the Groebner basis algorithm to find proofs of unsatisfiability. In: *Proceedings of the 28th Annual ACM Symposium on Theory of Computing, STOC'96*, ACM (1996) 174–183
7. Buss, S., Grigoriev, D., Impagliazzo, R., Pitassi, T.: Linear gaps between degrees for the polynomial calculus modulo distinct primes. *Journal of Computer and System Sciences* **62** (2001) 267–289

D. Grigoriev, E.A. Hirsch, and D.V. Pasechnik

8. Grigoriev, D., Hirsch, E.A.: Algebraic proof systems over formulas. Technical Report 01-011, Electronic Colloquium on Computational Complexity (2001) <ftp://ftp.eccc.uni-trier.de/pub/eccc/reports/2001/TR01-011/index.html>.
9. Gomory, R.E.: An algorithm for integer solutions of linear programs. In: Recent Advances in Mathematical Programming. McGraw-Hill (1963) 269–302
10. Chvátal, V.: Edmonds polytopes and a hierarchy of combinatorial problems. Discrete Math. **4** (1973) 305–337
11. Cook, W., Coullard, C.R., Turán, G.: On the complexity of cutting-plane proofs. Discrete Appl. Math. **18** (1987) 25–38
12. Chvátal, V., Cook, W., Hartmann, M.: On cutting-plane proofs in combinatorial optimization. Linear Algebra Appl. **114/115** (1989) 455–499
13. Bonet, M., Pitassi, T., Raz, R.: Lower bounds for Cutting Planes proofs with small coefficients. In: Proceedings of the 27th Annual ACM Symposium on Theory of Computing, STOC’95, ACM (1995) 575–584
14. Pudlák, P.: Lower bounds for resolution and cutting plane proofs and monotone computations. J. Symbolic Logic **62** (1997) 981–998
15. Lovász, L., Schrijver, A.: Cones of matrices and set-functions and 0–1 optimization. SIAM Journal on Optimization **1** (1991) 166–190
16. Lovász, L.: Stable sets and polynomials. Discrete Mathematics **124** (1994) 137–153
17. Pudlák, P.: On the complexity of propositional calculus. In: Sets and Proofs: Invited papers from Logic Colloquium’97. Cambridge University Press (1999) 197–218
18. Razborov, A.: Lower bounds on the monotone complexity of boolean functions. Dokl. AN USSR **22** (1985) 1033–1037
19. Grigoriev, D., Vorobjov, N.: Complexity of Null- and Positivstellensatz proofs. Annals of Pure and Applied Logic **113** (2001) 153–160
20. Grigoriev, D.: Linear lower bound on degrees of Positivstellensatz calculus proofs for the parity. Theoretical Computer Science **259** (2001) 613–622
21. Grigoriev, D.: Complexity of Positivstellensatz proofs for the knapsack. Computational Complexity **10** (2001) 139–154
22. Stephen, T., Tunçel, L.: On a representation of the matching polytope via semidefinite liftings. Math. Oper. Res. **24** (1999) 1–7
23. Cook, W., Dash, S.: On the matrix-cut rank of polyhedra. Math. Oper. Res. **26** (2001) 19–30
24. Dash, S.: On the Matrix Cuts of Lovász and Schrijver and their use in Integer Programming. Technical report tr01-08, Rice University (2001) <http://www.caam.rice.edu/caam/trs/2001/TR01-08.ps>.
25. Goemans, M.X., Tunçel, L.: When does the positive semidefiniteness constraint help in lifting procedures. Mathematics of Operations Research (2001) to appear.
26. Bockmayr, A., Eisenbrand, F., Hartmann, M., Schulz, A.S.: On the Chvátal rank of polytopes in the 0/1 cube. Discrete Applied Mathematics **98** (1999) 21–27
27. Eisenbrand, F., Schulz, A.S.: Bounds on the Chvátal rank of polytopes in the 0/1-cube. In G. Cornuéjols, R.E. Burkard, G., ed.: IPCO’99. Volume 1610 of Lecture Notes in Computer Science., Berlin Heidelberg, Springer-Verlag (1999) 137–150
28. Urquhart, A.: Hard examples for resolution. JACM **34** (1987)
29. Ben-Sasson, E.: Hard examples for bounded depth Frege. Manuscript (2001)
30. Krajíček, J.: Discretely ordered modules as a first-order extension of the cutting planes proof system. Journal of Symbolic Logic **63** (1998) 1582–1596
31. Cook, S.A., Reckhow, A.R.: The relative efficiency of propositional proof systems. Journal of Symbolic Logic **44** (1979) 36–50