Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 103 (2001)

Complexity of semi-algebraic proofs*

Dima Grigoriev† Edward A. Hirsch‡ Dmitrii V. Pasechnik§

Abstract

It is a known approach to translate propositional formulas into systems of polynomial inequalities and to consider proof systems for the latter ones. The well-studied proof systems of this kind are the *Cutting Planes* proof system (CP) utilizing linear inequalities and the *Lovasz-Schrijver calculi* (LS) utilizing quadratic inequalities. We introduce generalizations LS^d of LS that operate with polynomial inequalities of degree at most d.

It turns out that the obtained proof systems are 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 proofs), and *Tseitin's tautologies* (which are 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 and on the "Boolean degree" of Positivstellensatz Calculus refutations. We use the latter bound to obtain an exponential lower bound on the size of *static* LS^d and *tree-like* LS^d refutations.

Keywords: computational complexity, propositional proof system.

---

*Extended abstracts containing parts of the results of this paper appear in the proceedings of STACS 2002 and ICALP 2002.

†IRMAR, Université de Rennes, Campus de Beaulieu, 35042 Rennes, cedex France. Email: `dima@maths.univ-rennes1.fr`. Web: `http://www.maths.univ-rennes1.fr/~dima/`.

‡Steklov Institute of Mathematics at St.Petersburg, 27 Fontanka, 191011 St.Petersburg, Russia. Email: `hirsch@pdmi.ras.ru`. Web: `http://logic.pdmi.ras.ru/~hirsch/`. Work partially done while visiting Delft University of Technology. Partially supported by grant of RAS contest-expertise of young scientists projects and grants from CRDF (RM1-2409-ST-02) and RFBR (02-01-00089).

§Department of Technical Mathematics and Informatics, Faculty ITS, Delft University of Technology, Mekelweg 4, 2628 CD Delft, The Netherlands. Email: `d.pasechnik@its.tudelft.nl`. Web: `http://ssor.twi.tudelft.nl/~dima/`.

ISSN 1433-8092

Contents

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 **Subsection 2.2** below (we do not dwell much here on the history of this rich area, several nice historical overviews one could find in e.g., [BIK$^+$96, BIK$^+$97, Raz98, IPS99, CEI96, BGIP01]).

For these proof systems several interesting complexity lower bounds on the degrees of the derived polynomials were obtained [Raz98, IPS99, BGIP01]. 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) [IPS99]. 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 [GH01].

Systems of polynomial *inequalities* yield much more powerful proof systems than these operating with equations only, such as NS or PC. Historically first such a proof system is Cutting Planes (CP) [Gom63, Chv73, CCT87, CCH89], see also **Subsection 2.3**. This system uses linear inequalities (with integer coefficients). Exponential lower bounds on proof size were established for CP with polynomially bounded coefficients [BPR95] as well as for the general case [Pud97].

Another family of well-studied proof systems are so-called Lovász-Schrijver calculi (LS) [LS91, Lov94], see also [Pud99] and **Subsection 2.3** 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 **Section 4**). On the other hand, for these tautologies an exponential lower bound on the complexity of CP proofs was obtained in [Pud97], relying on the lower bound for the monotone complexity [Raz85]. Furthermore, we construct a short proof for the clique-coloring tautologies in the proof system $\mathrm{LS} + \mathrm{CP}^2$ (see **Section 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 $\mathrm{LS} + \mathrm{CP}^2$ have monotone effective interpolation, while for a system $\mathrm{LS} + \mathrm{CP}^1$ where the use of rounding rule is limited to linear inequalities, a (non-monotone) effective interpolation is known [Pud99].

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 **Section 3**, namely, every system of inequalities of degree at most d having no real solutions posseses an LS^{2d} refutation.

A proof system manipulating polynomial inequalities called the Positivstellensatz Calculus was introduced in [GV01]. Lower bounds on the degree in this system were established for the parity principle, for Tseitin's tautologies [Gri01b] and for the knapsack problem [Gri01a]. 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 [GV01].

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.) We consider a static version of Lovász-Schrijver calculi and prove an exponential lower bound on the size of refutation of the symmetric knapsack problem (**Section 9**); this bound also translates into the bound for the tree-like version of (dynamic) LS. The key ingredient of the proof is a linear lower bound on the "Boolean degree" of Positivstellensatz Calculus refutations (**Section 8**). Note that exponential lower bounds on the size of (static!) Positivstellensatz refutations are still unknown.

Also the lower bound on the Positivstellensatz Calculus degree of the knapsack problem [Gri01a] entails (see **Subsection 7.2**) a lower bound on the so-called LS-rank [LS91, Lov94]. 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 [ST99, CD01, Das01, GT01]. For a counterpart notion in CP, the so-called Chvátal rank [Chv73], lower bounds were established in [CCT87, CCH89]. 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 [BEHS99, ES99]. As a rule, however, diverse versions of the rank grow at most linear, 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. In particular, there are short proofs for the pigeon-hole principle (PHP) in CP [CCT87] and in LS [Pud97], while we exhibit in **Subsection 7.3** 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 **Section 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 **Section 6** we extend this technique to Tseitin's tautologies (which have no polynomial-size proofs in resolution [Urq87], Polynomial Calculus [BGIP01] and bounded-depth Frege systems [BS01]). In **Section 5** we also consider a certain extended version $LS_{*,\mathrm{split}}$ 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] [Pud99] and Krajíček [Kra98]) and allows also to multiply inequalities. We show that $LS_{*,\mathrm{split}}$ 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 **Section 10**.

2 Definitions

2.1 Proof systems

A *proof system* [CR79] 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 $t_1, t_2, \ldots \in L$ 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.

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 systems[1] for L.

2.2 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 $v_{j_1}, \ldots, v_{j_t}$ $(t \le k)$ is translated into an equation

$$(1 - l_1) \cdot \ldots \cdot (1 - l_t) = 0, \tag{2.1}$$

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.

Remark 2.1. Observe that it does not make sense to consider this translation for formulas in general DNF (rather than k-DNF for constant k), because an exponential lower bound for any system using such encoding would be trivial (note that $(1 - v_1)(1 - v_2) \ldots (1 - v_n)$ denotes a polynomial with exponentially many monomials).

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

Nullstellensatz (NS) [BIK⁺96]. A proof in this system is a collection of polynomials $g_1, \ldots, g_m$ such that

$$\sum_i f_i g_i = 1.$$

---

[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.

Polynomial Calculus (PC) [CEI96]. This system has two derivation rules:

$$\frac{p_1 = 0;\ p_2 = 0}{p_1 + p_2 = 0} \quad \text{and} \quad \frac{p = 0}{p \cdot q = 0}. \tag{2.2}$$

I.e., one can take a sum[2] 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.

Positivstellensatz [GV01]. A proof in this system consists of polynomials $g_1, \ldots, g_m$ and $h_1, \ldots, h_l$ such that

$$\sum_i f_i g_i = 1 + \sum_j h_j^2 \tag{2.3}$$

Positivstellensatz Calculus [GV01]. A proof in this system consists of polynomials $h_1, \ldots, h_l$ and a derivation of $1 + \sum_j h_j^2 = 0$ from S using the rules (2.2).

2.3 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 $v_{j_1}, \ldots, v_{j_t}$ into the inequality

$$l_1 + \cdots + l_t \geq 1, \tag{2.4}$$

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

$$x \geq 0, \tag{2.5}$$

$$x \leq 1 \tag{2.6}$$

for every variable x.

Cutting Planes (CP) [Gom63, Chv73, CCT87, CCH89], cf. also [Pud99]. 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:

$$\frac{f_1 \geq 0;\ \ldots;\ f_t \geq 0}{\sum_{i=1}^{t} \lambda_i f_i \geq 0} \quad \text{(where } \lambda_i \geq 0\text{)}, \tag{2.7}$$

$$\frac{\sum_i a_i x_i \geq c}{\sum_i a_i x_i \geq \lceil c \rceil} \quad \text{(where } a_i \in \mathbb{Z}\text{, and } x_i \text{ is a variable).} \tag{2.8}$$

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

---

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

Lovász-Schrijver calculus (LS) [LS91, Lov94], cf. also [Pud99]. In the weakest of Lovász-Schrijver proof systems, the contradiction must be obtained using the rule (2.7) applied to linear or quadratic f_i's and the rules

$$\frac{f \geq 0}{fx \geq 0}; \qquad \frac{f \geq 0}{f(1-x) \geq 0} \qquad \text{(where } f \text{ is linear, } x \text{ is a variable).} \tag{2.9}$$

Also, the system S is extended by the axioms

$$x^2 - x \geq 0, \quad x - x^2 \geq 0 \tag{2.10}$$

for every variable x.

LS$_+$ [LS91, Lov94, Pud99]. This system has the same axioms and derivation rules as LS, and also has the axiom

$$l^2 \geq 0 \tag{2.11}$$

for every linear l.

LS$_*$ [LS91, Lov94, Pud99]. This system has the same axioms and derivation rules as LS, and also the derivation rule

$$\frac{f \geq 0;\ g \geq 0}{fg \geq 0} \quad (f, g \text{ are linear).} \tag{2.12}$$

LS$_{+,*}$. This system unites LS$_+$ and LS$_*$.

LS + CP^1 [Pud99]. It has the same axioms and derivation rules as LS and also the rounding rule (2.8) 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.

2.4 New dynamic systems

In this paper we consider several extensions of Lovász and Schrijver proof systems. First, we define system LS + CP^2 which is slightly stronger than Pudlák's LS + CP^1.

LS + CP^2. It has the same axioms and rules as LS and also the extension of rounding rule (2.8) of CP to quadratic inequalities:

$$\frac{\sum_{i,j} a_{ij}x_ix_j + \sum_i a_ix_i \geq c}{\sum_{i,j} a_{ij}x_ix_j + \sum_i a_ix_i \geq \lceil c \rceil} \qquad \text{(where } a_i, a_{ij} \in \mathbb{Z}, \text{ and } x_i \text{ is a variable).} \tag{2.13}$$

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

$\mathbf{LS}^d$. This system is an extension of LS. The difference is that rule (2.9) is now restricted to f of degree at most $d-1$ rather than to linear inequalities. Rule (2.7) can be applied to any collection of inequalities of degree at most d.

Remark 2.2. Note that LS=LS^2.

Similarly, we consider $\mathbf{LS}^d_*$, transforming in (2.12), the condition "f, g are linear" into "$\deg(fg) \le d$".

$\mathbf{LS}^d_{\mathbf{split}}$. This system allows not only inequalities of the form $f \ge 0$, but also of the form $f > 0$. The derivation rules (2.7) and (2.9) are extended in a clear way to handle both types of inequalities, and $f > 0$ can be always relaxed to $f \ge 0$. 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 $f \ge 0$ and $f \le 0$) there is an $\mathrm{LS}^d_{\mathrm{split}}$ derivation of inequality $h \ge 0$, then we say that $h \ge 0$ is derived in $\mathrm{LS}^d_{\mathrm{split}}$.

Remark 2.3. Observe the difference of splitting in $\mathrm{LS}^d_{\mathrm{split}}$ and in Chvátal's "CP with subsumptions", an extension of CP formulated e.g. in [Pud99]. The tautology "$f > 0$ or $f < 0$ or $f = 0$" which we consider is valid for all real f's, while the tautology "$f \ge 1$ or $f \le 0$" is valid only for integer ones.

Remark 2.4. One can also consider a more powerful system by transforming $\mathrm{LS}^d_{\mathrm{split}}$ into a sequent calculus similarly to $R(\mathrm{CP})$ in [Kra98].

$\mathbf{LS}^d_{*,\mathbf{split}}$ is defined similarly. Note that the version of (2.12) for strict inequalities is

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

Remark 2.5. Observe that the analogue of (2.10) (with the condition "$\deg(l^2) \le d$" instead of "l is linear") can be easily derived in $\mathrm{LS}^d_{\mathrm{split}}$, i.e., $\mathrm{LS}^d_{+,\mathrm{split}}$=$\mathrm{LS}^d_{\mathrm{split}}$ and $\mathrm{LS}^d_{+,*,\mathrm{split}}$=$\mathrm{LS}^d_{*,\mathrm{split}}$.

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

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

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

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

2.5 New static systems

Nullstellensatz is a "static" version of Polynomial Calculus; Positivstellensatz is a "static" version of Positivstellensatz Calculus. Similarly, we define "static" versions of the new proof systems defined in the previous subsection.

Static LS^n. A proof in this system is a a refutation of a system of inequalities $S = \{s_i \geq 0\}_{i=1}^t$, where each $s_i \geq 0$ is either an inequality given by the translation (2.4), an inequality of the form $x_j \geq 0$ or $1 - x_j \geq 0$, or an inequality of the form $x_j^2 - x_j \geq 0$. The refutation consists of positive real coefficients $\omega_{i,l}$ and multisets $U_{i,l}^+$ and $U_{i,l}^-$ defining the polynomials

$$u_{i,l} = \omega_{i,l} \cdot \prod_{k \in U_{i,l}^+} x_k \cdot \prod_{k \in U_{i,l}^-} (1 - x_k)$$

such that

$$\sum_{i=1}^t s_i \sum_l u_{i,l} = -1. \tag{2.14}$$

Static LS$_+^n$. The difference from the previous system is that S is extended by inequalities $s_{t+1} \geq 0, \ldots, s_{t'} \geq 0$, where each polynomial s_j ($j \in [t+1..t']$) is a square of another polynomial s'_j. The requirement (2.14) transforms into

$$\sum_{i=1}^{t'} s_i \sum_l u_{i,l} = -1. \tag{2.15}$$

Static LS$_+$. The same as static LS$_+^n$, but the polynomials s'_i can be only linear.

Remark 2.6. Note that static LS$_+$ includes static LS^n.

Remark 2.7. Note that these static systems are not propositional proof systems in the sense of Cook and Reckhow [CR79], but are something more general, since there is no clear way to verify (2.14) in deterministic polynomial time (cf. [Pit97]). However, they can be easily augmented to match the definition of Cook and Reckhow, e.g., by including a proof of the equality (2.14) or (2.15) using axioms of a ring (cf. F-NS of [GH01]). Clearly, if we prove a lower bound for the original system, the lower bound will be valid for any augmented system as well.

Remark 2.8. The size of a refutation in these systems is the length of a reasonable bit representation of all polynomials $u_{i,l}$, s_i (for $i \in [1..t]$) and s'_j (for $j \in [t+1..t']$) and is thus at least the number of $u_{i,l}$'s.

Example 2.1. We now present a very simple static LS$_+$ proof of the propositional pigeonhole principle. (It is easy to see that the same proof can be also conducted in (dynamic) LS$_+$=LS$_+^2$; there is even a polynomial-size (dynamic) LS proof [Pud99], but it is slightly longer.) The negation of this tautology is given by the following system of inequalities (later denoted by *PHP*):

$$\sum_{\ell=1}^{m-1} x_{k\ell} \geq 1; \qquad 1 \leq k \leq m; \tag{2.16}$$

$$x_{k\ell} + x_{k'\ell} \leq 1; \qquad 1 \leq k < k' \leq m;\ 1 \leq \ell \leq m-1. \tag{2.17}$$

(That says that the k-th pigeon must get into a hole, while two pigeons k and k' cannot share the same hole ℓ.)

Here is the static LS_+ proof:

$$\begin{aligned}
&\sum_{k=1}^{m}\left(\sum_{\ell=1}^{m-1} x_{k\ell} - 1\right) + \\
&\sum_{\ell=1}^{m-1}\left(\sum_{k=1}^{m} x_{k\ell} - 1\right)^2 + \\
&\sum_{\ell=1}^{m-1}\sum_{k=1}^{m}\sum_{k\neq k'=1}^{m} (1 - x_{k\ell} - x_{k'\ell})x_{k\ell} + \\
&\sum_{\ell=1}^{m-1}\sum_{k=1}^{m}(x_{k\ell}^2 - x_{k\ell})(m-1) \\
&= -1.
\end{aligned}$$

□

3 Encodings of formulas in LS^d and upper bounds on the refutation degree

In LS^d, Boolean formulas are encoded as linear inequalities. However, this is not the only possible way to encode them, since in 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 (2.1).

Consider system $\overline{\mathrm{LS}^d}$ that has the same derivation rules as LS^d, but uses the encoding (2.1) instead of (2.4). It is clear that when $d = n$ is the number of variables, $\overline{\mathrm{LS}^n}$ polynomially simulates Polynomial Calculus. Does LS^n polynomially simulate $\overline{\mathrm{LS}^n}$ (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 3.1. There is a polynomial-size LS^t derivation of (2.1) from (2.4), (2.5)–(2.10).

Proof. We multiply (2.4) by $(1 - l_1)$, then by $(1 - l_2)$, ... , $(1 - l_{t-1})$, eliminating terms $l_i(1 - l_i)$ using (2.10) and (2.7) as soon as they appear. In this way, we obtain

$$(1 - l_1)\ldots(1 - l_n) \leq 0.$$

The opposite inequality of (2.1) is trivial. □

Corollary 3.1. LS^d polynomially simulates $\overline{\mathrm{LS}^d}$ (and, hence, LS^n polynomially simulates Polynomial Calculus).

Corollary 3.2. LS^n_+ polynomially simulates Positivstellensatz Calculus.

Remark 3.1. Note that there is a linear lower bound [Gri01a] on the degree of Positivstellensatz Calculus refutation of the symmetric knapsack problem $m - x_1 - x_2 - \ldots - x_n = 0$ (where $m \notin \mathbb{Z}$, $m > \lceil n/4 \rceil - 2$). However, by the completeness of LS [LS91, Theorem 1.4] there is an LS (i.e., degree two) refutation of this problem.

It turns out that the converse of Lemma 3.1 is also true. In particular, that means that for there is an LS^k refutation of every formula in k-CNF. Below, we also show (Theorem 3.1) that there is an LS^{2k} refutation of any system of polynomial inequalities of degree at most k.

Lemma 3.2. There is a polynomial-size LS^t derivation of (2.4) from (2.1) and (2.5)–(2.10).

Proof. We derive

$$(l_1 + \ldots + l_i - 1)(1 - l_{i+1}) \ldots (1 - l_t) \geq 0 \tag{3.1}$$

inductively. The base ($i = 1$) is trivial. Suppose that the inequality holds for $i = m$. Note that it can be rewritten as

$$(l_1 + \ldots + l_m + l_{m+1} - 1 - l_1 l_{m+1} - \ldots - l_m l_{m+1})(1 - l_{m+2}) \ldots (1 - l_t) \geq 0.$$

We then add $l_j l_{m+1}(1-l_{m+2}) \ldots (1-l_t) \geq 0$ (which easily follows from axioms) for $j = 1, \ldots, m$ obtaining (3.1) for $i = m + 1$. □

Corollary 3.3. $\overline{\mathrm{LS}^d}$ polynomially simulates LS^d.

Corollary 3.4. There is an $\overline{\mathrm{LS}^k}$ refutation of every formula in k-CNF.

Theorem 3.1. There is a polynomial-size LS^{2k} refutation of any unsolvable system of polynomial inequalities of degree at most k.

Proof. Consider an unsolvable system S of polynomial inequalities of degree at most k. We linearize it in the following way. Consider a monomial $m = uvm'$ of degree at least two, where v and v are variables (it is possible that this is the same variable). Replace uv by a new variable x_{uv} and add the following three inequalities to the system:

$$\begin{aligned} x_{uv} &\leq u \\ x_{uv} &\leq v \\ x_{uv} &\geq u + v - 1. \end{aligned}$$

Note that every 0-1 solution to the new system corresponds to a 0-1 solution to the old system, and vice versa. Therefore, the new system is unsolvable. Continue modifying the system in this way until it becomes a system S' of linear inequalities. Note that each new variable corresponds to a monomial in the old variables of degree at most k. We denote a variable corresponding to a monomial m by x_m (note that x_m may be not uniquely defined, but it is not important for our argument).

By [LS91, Theorem 1.4], there is an LS (i.e., degree two) refutation of S'. For every added variable x_m, replace x_m by m in this refutation. We thus obtain a "proof" of S using only old variables.

We now must transform this "proof" into a valid LS^{2k} proof. The added inequalities become easily derivable from the axioms. The steps (2.7) remain valid steps. In (2.9), instead of multiplying by a new variable $x_{u_1u_2\ldots u_s}$, we now multiply by the (old) variables $u_1, u_2, \ldots, u_s$.

We also have to replace steps (2.9) that use multiplying $f \geq 0$ by $(1 - x_{u_1u_2\ldots u_s})$. Instead, we multiply $f \geq 0$ by $(1 - u_1)$, besides multiply $f \geq 0$ by u_1 and by $(1 - u_2)$, besides multiply $f \geq 0$ by u_1, u_2 and $(1 - u_3)$, etc. Summing all the obtained inequalities, we get $f(1 - x_{u_1u_2\ldots u_s}) \geq 0$.

Since each added variable corresponds to a monomial of degree at most k, and the LS refutation of S' contains only monomials of degree at most two, we thus obtain a valid LS^{2k} refutation of the system S. □

4 Short $\mathrm{LS}+\mathrm{CP}^2$ and LS^4 proofs of the clique-coloring tautologies

Theorem 4.1. There is a set of inequalities that has polynomial-size refutations in LS^4 and $\mathrm{LS} + \mathrm{CP}^2$, 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 [Pud97]. 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 LS^4 and $\mathrm{LS} + \mathrm{CP}^2$.

Clique-coloring tautologies. Given a graph G with n vertices, we try to color it with $m-1$ colors, while assuming the existense 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 $\{1 \ldots m\}$ denoting the vertices of a m-clique to the set $\{1 \ldots n\}$ 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 color ℓ to the node i is represented by a variable $r_{i\ell}$.

The following inequalities [Pud97] state that G has an m-clique and is $(m-1)$-colorable. The correctness of coloring is expressed by

$$p_{ij} + r_{i\ell} + r_{j\ell} \leq 2, \tag{4.1}$$

where i, j and ℓ satisfy $1 \leq i < j \leq n$, $\ell = 1 \ldots m-1$.

To make sure that each node gets colored, write

$$\sum_{\ell=1}^{m-1} r_{i\ell} \geq 1 \tag{4.2}$$

for each $i = 1 \ldots n$.

Then, every label of a clique is mapped to at least one vertex of G:

$$\sum_{i=1}^{n} q_{ki} \geq 1 \tag{4.3}$$

for each $k = 1 \ldots m$.

Also, the mapping encoded by q_{ki} is injective:

$$\sum_{k=1}^{m} q_{ki} \leq 1 \tag{4.4}$$

for each $i = 1 \ldots n$.

Finally, to encode that indeed one has a clique, write

$$q_{ki} + q_{k',j} \leq p_{ij} + 1 \tag{4.5}$$

for all i, j, k, k' satisfying $k \neq k'$ and $1 \leq i < j \leq n$.

Weak clique-coloring tautologies. The inequalities (4.1)–(4.5) are the original inequalities of [Pud97]. We now add one more family of inequalities to this system without affecting applicability of [Pud97, 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

$$\sum_{i=1}^{n} q_{ki} \leq 1 \tag{4.6}$$

for all $k = 1 \ldots m$. This inequality means that the k-th vertex of the clique does not get mapped to more than one vertex of G.

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 colored with the color ℓ is encoded as $q_{ki}r_{i\ell} \geq 1$. Then the fact that the k-th vertex of the clique has color 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 $\{1, \ldots, m\}$ to $\{1, \ldots, m-1\}$. Below, we show that the PHP inequalities (2.16), (2.17) hold for $x_{k\ell}$'s, furthermore, there are short LS^4 as well as $\mathrm{LS}+\mathrm{CP}^2$ derivations of these inequalities.

There is a polynomial-size CP refutation for PHP [CCT87]. In our notation (note that x_{kl} denotes a quadratic polynomial) such refutation translates into an $\mathrm{LS} + \mathrm{CP}^2$ refutation. Alternatively, Pudlák [Pud99] shows that PHP also has polynomial-size refutation in LS. In our notation, this translates into an LS^4 refutation. Note that both of these refutations make use of the following technical statement.

Lemma 4.1. Given a sum of variables $S = \sum_{k=1}^{N} a_k$ and inequalities $a_i + a_j \leq 1$ for all $1 \leq i < j \leq N$, there are short proofs of $S \leq 1$ in LS and in CP.

Proof. For CP, this is established in the proof of Proposition 7 in [CCT87]. (It proceeds by induction: from $a_1 + \sum_{i \in F} \leq 1$ and $a_2 + \sum_{i \in F} \leq 1$ for $F \subset \{1 \dots N\} - \{1, 2\}$ one derives by summming these two inequalities and $a_1 + a_2 \leq 1$ that $a_1 + a_2 + \sum_{i \in F} \leq 3/2$. The rounding down of the righthand side of the latter completes the proof of the induction step.)

For LS, this is Lemma 1 of [Pud99], where the case $N = 3$ is dealt with, and an argument in the proof of Proposition 1 of [Pud99]. □

In what follows we show that there is a polynomial-size derivation of (2.16)–(2.17) from (4.1)–(4.6) in LS^4 as well as in $\mathrm{LS} + \mathrm{CP}^2$.

Deriving PHP from weak clique-coloring tautologies. Let us derive (2.16). For each i, multiply both sides of (4.2) by q_{ki} and sum the resulting inequalities over i. One obtains

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

Adding (4.3) to this inequality, one gets (2.16).

Deriving (2.17) is less straighforward. First, we prove an easy lemma.

Lemma 4.2. In LS, there is a short proof of $(a - b)^2 \geq 0$ for any variables a and b.

Proof. Multiplying both sides of $a \leq 1$ by b, one obtains $b^2 - ab \geq 0$. Similarly, one derives $a^2 - ab \geq 0$. Summing the obtained two inequalities, one gets $a^2 + b^2 - 2ab \geq 0$, as required. □

Next, note that one can eliminate p_{ij} from (4.1) and (4.5) and obtain

$$q_{ki} + q_{k',j} + r_{i\ell} + r_{j\ell} \leq 3, \qquad 1 \leq i < j \leq n,\ 1 \leq \ell \leq m-1,\ 1 \leq k \neq k' \leq m. \tag{4.7}$$

Using $q_{ki}^2 \leq q_{ki}$ and similar inequalities for $q_{k',j}$, $r_{i\ell}$ and $r_{j\ell}$, the inequality (4.7) can be rewritten as

$$(q_{ki} - r_{i\ell})^2 + 2q_{ki} r_{i\ell} + (q_{k',j} - r_{j\ell})^2 + 2q_{k',j} r_{j\ell} \leq 3.$$

Using Lemma 4.2, the latter is simplified to

$$2q_{ki} r_{i\ell} + 2q_{k',j} r_{j\ell} \leq 3.$$

Applying the rounding rule, one obtains

$$q_{ki} r_{i\ell} + q_{k',j} r_{j\ell} \leq 1 \qquad 1 \leq i < j \leq n,\ 1 \leq \ell \leq m-1,\ 1 \leq k \neq k' \leq m. \tag{4.8}$$

Alternatively, we can derive (4.8) in LS^4 using the following lemma:

Lemma 4.3. In LS, there is a short proof that $a + b \leq 3/2$ implies $a + b \leq 1$.

Proof. Note that multiplying $a \leq 1$ by $1 - b$ gives $a + b \leq 1 + ab$. It remains to show that $ab \leq 0$.

Indeed, multiplying $a + b \leq 3/2$ by a (respectively, by $1 - b$) and using $a = a^2$ and $b = b^2$ one obtains $ab - a/2 \leq 0$ (respectively, $a - ab \leq 3/2 - 3/2b$). Adding these two inequalities, one obtains $a/2 + 3b/2 \leq 3/2$. Multiplying the latter by b and using $b^2 = b$, one obtains $ab \leq 0$. ☐

Using $q_{ki}r_{i\ell} \leq q_{ki}$ and (4.6), one obtains

$$(x_{k\ell} =) \sum_{i=1}^{n} q_{ki}r_{i\ell} \leq 1 \qquad 1 \leq \ell \leq m-1,\ 1 \leq k \leq m. \tag{4.9}$$

Now take (4.4) and add it to $0 \leq q_{k''i}$ for each k'' different from k and k'. We get $q_{ki} + q_{k'i} \leq 1$. After multiplying the latter inequality by r_{il} and adding $r_{il} \leq 1$ to it, one obtains

$$q_{ki}r_{il} + q_{k'i}r_{il} \leq 1. \tag{4.10}$$

Now (4.8)–(4.10) imply that any length 2 subsum of monomials in the sum

$$S = \sum_{i=1}^{n} (q_{ki}r_{i\ell} + q_{k'i}r_{i\ell}) \quad (\text{for } 1 \leq k \neq k' \leq m)$$

is bounded by 1 from above.

From these inequalities, one can easily derive $S \leq 1$ either in LS^4 or in $\mathrm{LS} + \mathrm{CP}^2$ by using Lemma 4.1. As $S = x_{k\ell} + x_{k'\ell}$, (2.17) holds, and we are done for $\mathrm{LS} + \mathrm{CP}^2$.

For LS^4 it remains to show that all the $x_{k\ell}$'s are boolean, as follows. Multiplying both sides of (4.9) by $x_{k\ell}$, one obtains $x_{k\ell}^2 \leq x_{k\ell}$. On the other hand, $x_{k\ell}^2 = x_{k\ell} + \sum_{i \neq j} q_{ki}r_{i\ell}q_{kj}r_{j\ell} \geq x_{k\ell}$ holds, as one can derive in LS^4 for each i and j that $q_{ki}r_{i\ell}q_{kj}r_{j\ell} \geq 0$.

5 Reasoning about integers

In this section we explain how 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 $\mathrm{LS}_{0/1\text{-split}}$) proofs of the symmetric knapsack problem, and that CP with polynomially bounded coefficients can be simulated in $\mathrm{LS}^3_{/}$ (as well as in $\mathrm{LS}_{*,\text{split}}$).

Lemma 5.1. Let

- $Y = \sum_{i=1}^{n} a_i x_i$,

- $f_d(Y) = (Y - (d-1))(Y - d)$,
- a_i are integers,
- x_i are variables.

Then the inequality $f_d(Y) \geq 0$ has a derivation of size polynomial in d, n and $\max_i |a_i|$ in the following systems:

1. LS^3.
2. $\mathrm{LS}_{0/1\text{-split}}$.

Proof. W.l.o.g. rewrite Y as $\sum_{i=1}^{t} s_i x_{l_i}$, where $s_i \in \{-1, 1\}$ and it is possible that $l_i = l_j$. We derive the inequalities $f_c(Y_j) \geq 0$ inductively for $Y_j = \sum_{i=1}^{j} s_i x_{l_i}$ and for each $c \in [d-t+j \mathrel{..} d+t-j]$. The base ($j = 1$) is trivial. Suppose that such inequalities are already derived for $j \leq k$. We now derive $(Y_{k+1} - (c-1))(Y_{k+1} - c) \geq 0$ for every $c \in [d-t+k+1 \mathrel{..} d+t-k-1]$.

1. If $s_{k+1} = 1$, multiply $f_{c-1}(Y_k) \geq 0$ by x_{k+1}, multiply $f_c(Y_k) \geq 0$ by $(1 - x_{k+1})$, and sum the obtained inequalities. We thus get in the left-hand side

$$\begin{aligned}
&f_{c-1}(Y_k)x_{k+1} + f_c(Y_k)(1 - x_{k+1}) = \\
&(f_c(Y_k) + 2(Y_k - (c-1)))x_{k+1} + f_c(Y_k)(1 - x_{k+1}) = \\
&f_c(Y_k) + 2(Y_k - (c-1))x_{k+1} = \\
&Y_k^2 - (2c-1)Y_k + c(c-1) + 2Y_k x_{k+1} - 2(c-1)x_{k+1}.
\end{aligned}$$

Using $x_{k+1}^2 - x_{k+1} = 0$, we transform this into $f_c(Y_{k+1})$ which is $(Y_k + x_{k+1})^2 - (2c-1)(Y_k + x_{k+1}) + c(c-1)$.

Else if $s_{k+1} = -1$, multiply $f_{c+1}(Y_k) \geq 0$ by x_{k+1}, multiply $f_c(Y_k) \geq 0$ by $(1 - x_{k+1})$, and sum the obtained inequalities. We thus get in the left-hand side

$$\begin{aligned}
&f_{c+1}(Y_k)x_{k+1} + f_c(Y_k)(1 - x_{k+1}) = \\
&(f_c(Y_k) - 2(Y_k - c))x_{k+1} + f_c(Y_k)(1 - x_{k+1}) = \\
&f_c(Y_k) - 2(Y_k - c)x_{k+1} = \\
&Y_k^2 - (2c-1)Y_k + c(c-1) - 2Y_k x_{k+1} + 2c x_{k+1}.
\end{aligned}$$

Using $x_{k+1}^2 - x_{k+1} = 0$, we transform this into $f_c(Y_{k+1})$ which is in this case $(Y_k - x_{k+1})^2 - (2c-1)(Y_k - x_{k+1}) + c(c-1)$.

2. The proof in $\mathrm{LS}_{0/1\text{-split}}$ follows the proof in LS^3 given above. However, before multiplying by x_{k+1} and $1 - x_{k+1}$, we make an assumption $x_{k+1} = r$ for $r = 0, 1$ (and thus multiply by constants, without increasing the degree). It is clear from the arguments above (just substitute the value for x_{k+1}), that both assumptions lead to $f_c(Y_{k+1}) \geq 0$ (which looks as $f_c(Y_k) \geq 0$ under assumption $x_{k+1} = 0$, as $f_{c+1}(Y_k) \geq 0$ under assumption $x_{k+1} = s_{k+1}$ and as $f_{c-1}(Y_k) \geq 0$ under assumption $x_{k+1} = -s_{k+1}$). ☐

Let us also note a general fact unrelated to integers: it is possible to substitute equalities into inequalities.

Lemma 5.2. Let f be a polynomial in variables $v_1, \ldots, v_n$, and X and Y be polynomials in variables $v_2, \ldots, v_n$. Let $g(v_2, \ldots, v_n) = f(X, v_2, \ldots, v_n)$ and $h(v_2, \ldots, v_n) = f(Y, v_2, \ldots, v_n)$. Suppose that the degree of g and h is at most d. Then there is a polynomial-size LS^d derivation of $h \geq 0$ from $g \geq 0$ and $X - Y = 0$.

Proof. We rewrite $g \geq 0$ as

$$\sum_{i \geq 1} (p_i - n_i) X^i + c \geq 0, \tag{5.1}$$

where p_i and n_i are polynomials of $v_2, \ldots, v_n$ consisting only of positive monomials, and c does not depend on X. Then we multiply $Y - X = 0$ by p_i (i.e., multiply it by its monomials and sum with the same coefficients as in p_i) and multiply $X - Y = 0$ by n_i. The sum of the obtained two equalities is $(Y - X)(p_i - n_i) = 0$. We then multiply it by X^{i-1}, again representing it as a difference of two polynomials containing only positive monomials. Summing (5.1) with the obtained equalities for every i, we get

$$\sum_{i \geq 2} ((p_i - n_i)Y) X^{i-1} + (p_1 - n_1)Y + c \geq 0.$$

We now represent $(p_i - n_i)Y$ as a difference $p_i' - n_i'$ of two polynomials containing only positive monomials and repeat this procedure. Repeating it d times proves the claim. $\square$

It follows that there are short LS^3 (as well as $\mathrm{LS}_{0/1\text{-split}}$) refutations of the *symmetric knapsack problem.*

Theorem 5.1. There is a polynomial-size LS^3 (as well as $\mathrm{LS}_{0/1\text{-split}}$) refutation of

$$m - x_1 - x_2 - \ldots - x_n = 0, \tag{5.2}$$

where $m \notin \mathbb{Z}$.

Proof. Using Lemma 5.2 substitute (5.2) into $f_{\lfloor m \rfloor}(\sum_{i=1}^n x_i) \geq 0$ given by Lemma 5.1. $\square$

To show that $\mathrm{LS}_{*,\mathrm{split}}$ and $\mathrm{LS}^3_{/}$ polynomially simulate CP, we first (equivalently) redefine CP so that it will manipulate linear inequalities of the form $A \geq a$, where $A = a_1 x_1 + \ldots + a_n x_n$, $x_1, \ldots, x_n$ are (integer) variables, and $a_1, \ldots, a_n, a$ are integers. The rounding rule (2.8) transforms into

$$\frac{\sum_i a_i x_i \geq a}{\sum_i \frac{a_i}{d} x_i \geq \lceil \frac{a}{d} \rceil} \qquad (\text{where } d \in \mathbb{N};\ d | a_1, \ldots, a_n). \tag{5.3}$$

We define *CP with polynomially bounded coefficients* (cf. [BPR95]) if the absolute values of a_i are bounded by a polynomial in the length of a CP refutation.

Theorem 5.2. The following systems polynomially simulate CP with polynomially bounded coefficients:

1. $\mathrm{LS}_{*,\mathrm{split}}$.

2. $\mathrm{LS}^3_{/}$.

Proof. We fix a CP refutation and simulate it rule by rule. Simulating the rule (2.7) goes literally in LS, so we need to simulate just the rule (5.3). By Lemma 5.1 we can derive in $\mathrm{LS}_{0/1\text{-split}}$ (as well as in LS^3) the inequality $f_c(A/d) \geq 0$ for $c = \lceil a/d \rceil$.

1. In $\mathrm{LS}_{*,\text{split}}$, we then have that $A/d \geq c$ since the assumption $A/d - c < 0$ multiplied by $A/d - (c-1) > 0$ contradicts $f_c(A/d) \geq 0$.

2. In $\mathrm{LS}^3_{/}$, we get $A/d \geq c$ by dividing $f_c(A/d) \geq 0$ by $A/d - (c-1) > 0$. □

Remark 5.1. In the proof of Theorem 5.2 the hypotheses $f > 0$, $f < 0$, $f = 0$ used for $\mathrm{LS}_{*,\text{split}}$ derivations are just linear.

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., [BGIP01, GH01]) 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 [BGIP01, Urq87] 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. The respective negation $T = T_G$ of Tseitin's tautologies is given by the following equalities (due to Lemmas 3.1 and 3.2 we give them directly in PC translation):

$$\prod_{e \in S'_v} x_e \cdot \prod_{e \notin S'_v} (1 - x_e) = 0 \tag{6.1}$$

(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 6.1. For every constant $d \geq 1$ and every d-regular graph G, there is a polynomial-size refutation of (6.1) in LS^{d+2}.

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 $c \in [0 \mathinner{..} i(d-1)/2]$, we will prove inductively $f_c(Y_i/2) \geq 0$ for odd $i = n, n-2, n-4, \ldots$ and $f_c((Y_i - 1)/2) \geq 0$ for even $i = n-1, n-3, \ldots$. Then $f_0((Y_0 - 1)/2) \geq 0$ gives a contradiction.

The induction base ($i = n$) follows from Lemma 5.1, 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 $f_c((Y - y)/2) \geq 0$ for all $c \in [0 \mathinner{..} i(d-1)/2]$.

Fix some subset $S \subseteq S_{v_{i+1}}$ of odd size. Let $t = |S|$, $c' = c + (t-1)/2 \in [c \mathinner{..} c + (d-1)/2] \subseteq [0 \mathinner{..} (i+1)(d-1)/2]$. Denote $P(S) = \prod_{e \in S} x_e \prod_{e \notin S} (1 - x_e)$. Since we have $f_{c'}((Y-1)/2) \geq 0$ by the induction hypothesis,

$$f_{c'}((Y-1)/2) \cdot P(S) \geq 0$$

follows by (2.9), and can be rewritten as

$$((Y-1)/2-c')\cdot(((Y-y)/2-(c-1))P(S)+(y/2-t/2)P(S))\geq 0. \tag{6.2}$$

Also

$$yP(S)=tP(S) \tag{6.3}$$

follows directly from (2.10) and (2.9). Substituting (6.3) into (6.2) by Lemma 5.2 we get

$$((Y-1)/2-c')\cdot((Y-y)/2-(c-1))\cdot P(S)\geq 0$$

which can be rewritten as

$$(((Y-y)/2-c)P(S)+(y/2-t/2)P(S))\cdot((Y-y)/2-(c-1))\geq 0$$

Substituting (6.3) again we get

$$f_c((Y-y)/2)\cdot P(S)\geq 0. \tag{6.4}$$

We complete induction step by summing (6.4) for all $S\subseteq S_{v_{i+1}}$ of odd size. By Lemma 5.2, it remains then to prove that

$$1=\sum_{\substack{S\subseteq S_v\\ |S|\text{ is odd}}} P(S)$$

This last equality is the sum of the equalities (6.1) for fixed vertex v, because one can rewrite $1=x+(1-x)=xy+(1-x)y+x(1-y)+(1-x)(1-y)=\ldots$ for any collection of variables $x,y,\ldots$. □

Remark 6.1. Sometimes Tseitin's tautologies are formulated in a different way. One takes G with arbitrary (not necessarily odd) number of vertices, attaches weight $w_v\in\{0,1\}$ to each vertex v and writes Boolean formulas expressing $\bigoplus_{e\ni v}x_e=w_v$. Then if $\bigoplus_{v\in V}w_v=1$, this set of formulas is contradictory. Note that our technique works for this kind of Tseitin's tautologies as well.

Remark 6.2 (A. Kojevnikov). The degree of proof of Tseitin's tautologies can be reduced by the use of the rounding rule (2.8) applied to higher degree inequalities. For example, there is a short proof of degree 6 tautologies in "LS^6+CP^3" proof system. First, one notes that $(y_v-1)(y_v-3)(y_v-5)=0$ because it is an integer linear combination of the equalities (6.1). Then, one sums all the obtained equalities, getting $2c\sum_{e\in E}x_e=2k+1$ for certain integers c and k. Applying the rounding rule to each of the inequalities constituting this equality and summing the results gives a contradiction.

7 Lower bounds on Lovász-Schrijver rank

In this section we prove two lower bounds on Lovász-Schrijver rank. There is a series of lower bounds on Lovász-Schrijver rank in the literature (see e.g. [CD01, GT01] 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.

We first prove (Subsection 7.2) a linear lower bound on the LS_+-rank (and a logarithmic lower bound on the $\mathrm{LS}_{+,*}$-rank) of symmetric knapsack problem by reducing it to a lower bound on the degree of Positivstellensatz Calculus refutation [Gri01a]. 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.

Then in Subsection 7.3 we prove an $\Omega(2^{\sqrt{n}})$ lower bound on the LS-rank of PHP. Note (cf. Subsection 2.5) that the LS_+-rank of PHP is a constant.

7.1 More definitions

We now consider the standard geometric setting for the Lovász-Schrijver procedures LS and LS_+ [LS91]. A comprehensive explanation of its equivalence with propositional proof complexity setting can be found in [Das01].

Given a system $Ax \leq b$ of m linear inequalities in variables $x_1, \ldots, x_n$, we homogenize it by adding an extra variable x_0 and writing the system as

$$x_0 \geq 0, \quad Ax \leq x_0 b. \tag{7.1}$$

Then let K denote the set of feasible points of (7.1) and K_I denote the cone generated by all 0-1 vectors in K. Also, let Q denote the cone generated by the 0-1 vectors of length $n+1$ with the first coordinate equal to 1. In what follows, e_j denotes j-th unit vector, and $Diag(Y)$ is the vector of the main diagonal entries of a square matrix Y. We write $Y \succeq 0$ if Y is positive semidefinite.

The set $M(K)$ (denoted usually $M(K,Q)$, but this generality is not needed here) consists of $(n+1) \times (n+1)$ real matrices Y satisfying

(i) $Y = Y^T$;

(ii) $Ye_0 = Diag(Y)$;

(iii) $Ye_i \in K$ and $Y(e_0 - e_i) \in K$ for all $0 \leq i \leq n$.

Also, define $M_+(K) := \{Y \in M(K) \mid Y \succeq 0\}$.

Next, define the projections of $M(K)$ and $M_+(K)$ onto $\mathbb{R}^{n+1}$ as follows.

$$\begin{aligned} N(K) &:= \{Diag(Y) \mid Y \in M(K)\} \\ N_+(K) &:= \{Diag(Y) \mid Y \in M_+(K)\}. \end{aligned}$$

Iterated operators $N^r(K)$ and $N^r_+(K)$ are defined naturally as $N^0_{(+)}(K) := K$ and $N^r_{(+)}(K) := N_{(+)}(N^{r-1}_{(+)}(K))$.

It is shown in [LS91] that

$$K_I \subseteq N^n_{(+)}(K) \subseteq N^{n-1}_{(+)}(K) \subseteq \cdots \subseteq N^k_{(+)}(K) \subseteq \cdots \subseteq N_{(+)}(K) \subseteq K. \tag{7.2}$$

The LS-*rank* (respectively, LS$_+$-*rank*) of a system of linear inequalities $Ax \le b$ is the minimal k in (7.2) 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 $f \ge 0$ and $g \ge 0$ iff g is derived from f (and maybe something else) in one step. We now drop the edges corresponding to the rule (2.7). 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$^d_{+,*}$.

7.2 LS$_+$- and LS$_{+,*}$-ranks of symmetric knapsack

The system of inequalities for the symmetric knapsack problem is given by (5.2) and usual axioms (2.5), (2.6), (2.10). We restrict our attention to system K obtained by setting $m = \lfloor \frac{n}{2} \rfloor + \frac{1}{2}$.

Theorem 7.1.

1. LS$_+$-rank of K is at least $n/4$.
2. LS$_{+,*}$-rank of K is at least $\log_2 n - 1$.

Proof. 1. Fix an LS$_+$-refutation of K. We now modify it into a Positivstellensatz refutation (See Subsection 2.2).

For each polynomial f derived in LS$_+$ with LS$_+$-rank at most k we construct its representation in the form

$$f = \sum_i (x_i - x_i^2)u_i + (m - \sum_i x_i)u_0 + \sum_j v_j^2 \tag{7.3}$$

in such a way that all the degrees $\deg(x_i - x_i^2)u_i, \deg(m - \sum_i x_i)u_0, \deg v_j^2 \le 2k$ (by recursion on k). Indeed, the recursive step is obvious for the rules (2.10), (2.11). Furthermore, we replace the first rule of (2.9) by the multiplication by $x = (x - x^2) + x^2$ providing the representation

$$fx = \left(\sum (x_i - x_i^2)u_i x + (x - x^2)\sum v_j^2 + (m - \sum x_i)u_0 x\right) + \sum (v_j x)^2,$$

that gives the form of fx similar to (7.3). Similarly, we replace the second rule of (2.9) by the multiplication by $(1 - x) = (x - x^2) + (1 - x)^2$.

At the end of the derivation in LS_+ of LS_+-rank k_+ we get a representation of the form

$$-1 = \sum (x_i - x_i^2)\overline{u_i} + (m - \sum x_i)\overline{u_0} + \sum \overline{v_j}^2$$

where $\deg(x_i - x_i^2)\overline{u_i}, \deg(m - \sum x_i)\overline{u_0}, \deg \overline{v_j}^2 \leq 2k_+$ by recursion. This provides a Positivstellensatz Calculus refutation of the knapsack problem with the degree less or equal to $2k_+$. Applying [Gri01a] we conclude that $2k_+ \geq n/2$, thus LS_+-rank of K is at least $n/4$.

2. We fix an $\mathrm{LS}_{+,*}$-refutation of K and observe in a similar way that if two derived polynomials f and

$$g = \sum (x_i - x_i^2)u_i' + (m - \sum x_i)u_0' + \sum (v_j')^2$$

of $\mathrm{LS}_{+,*}$-rank at most k are already in the form (7.3) where

$$\deg(x_i - x_i^2)u_i, \deg(m - \sum x_i)u_0, \deg v_j^2, \deg(x_i - x_i^2)u_i', \deg(m - \sum x_i)u_0', \deg(v_j')^2 \leq 2^k,$$

their product

$$fg = \Big(\sum (x_i - x_i^2)u_i g + \sum (x_i - x_i^2)u_i' \sum v_j^2 + (m - \sum x_i)u_0 g + (m - \sum x_i)u_0' \sum v_j^2\Big) + \sum (v_{j_1} v_{j_2}')^2$$

can be written again in the desired form (7.3) with the degrees of the occurring polynomials bounded by 2^{k+1}. This allows one to replace the rule (2.12). By recursion at the end of the derivation in $\mathrm{LS}_{+,*}$ of the $\mathrm{LS}_{+,*}$-rank k_* we get a representation

$$-1 = \sum (x_i - x_i^2)\widetilde{u_i} + (m - \sum x_i)\widetilde{u_0} + \sum \widetilde{v_j}^2$$

with the degrees $\deg(x_i - x_i^2)\widetilde{u_i}, \deg(m - \sum x_i)\widetilde{u_0}, \deg \widetilde{v_j}^2 \leq 2^{k_*}$. Again as above applying [Gri01a] we conclude that $2^{k_*} \geq n/2$ and thereby, $\mathrm{LS}_{+,*}$-rank of K is at least $\log_2 n - 1$. ☐

Remark 7.1. Similarly to Theorem 7.1(2), a logarithmic lower bound on the $\mathrm{LS}_{+,*}$-rank can be obtained for the parity principle and for Tseitin's tautologies relying on [Gri01b].

7.3 LS-rank of PHP

Let $\mathbf{e}_k$ denote all-1 vector of length k.

Let $Q_n \subset \mathbb{R}^n$ denote the n-dimensional 0-1 hypercube and let P_{m-1} be the feasible set of the system (2.16)-(2.17). This is the well-known "PHP polytope".

Theorem 7.2. *At least $m-2$ iterations of the N-operator are needed to prove that P_{m-1} does not contain integer points, that is, LS-rank of P_{m-1} is at least $m-2$.*

It will follow from Lemma 7.2 below.

Write $x \in \tilde{N}^r(m-1)$ iff $(1, x) \in N^r(P_{m-1})$. We also identify $\tilde{N}^0(m-1)$ with P_{m-1} itself.

Let $x \in \tilde{N}^0(m-1)$. Define $w^{ab} = w^{ab}(x) \in Q_{m(m+1)}$, where $1 \leq a \leq m+1$, $1 \leq b \leq m$, as follows.

$$w^{ab}_{ij} = \begin{cases} x_{i,j} & \text{if } 1 \leq i < a,\ 1 \leq j < b; \\ x_{i,j-1} & \text{if } 1 \leq i < a,\ b < j \leq m; \\ x_{i-1,j} & \text{if } a < i \leq m+1,\ 1 \leq j < b; \\ x_{i-1,j-1} & \text{if } a < i \leq m+1,\ b < j \leq m; \\ 1 & \text{if } i = a,\ j = b; \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 7.1. Let $x \in \tilde{N}^r(m-1)$. Then $w^{ab}(x) \in \tilde{N}^r(m)$.

Proof. It is trivial to check the statement for $r = 0$.

We make an induction assumption that for any x and any $t < r$, $x \in \tilde{N}^t(m-1)$ implies $w^{ab}(x) \in \tilde{N}^t(m)$. Without loss in generality, assume $a = b = 1$.

We fix a particular basis $(e_1, \ldots, e_{m(m-1)})$ in $\mathbb{R}^{m(m-1)}$:

$$(x_{1,1} \ldots x_{1,m-1}, x_{2,1} \ldots x_{m,1}, x_{2,2} \ldots x_{2,m-1}, x_{3,2} \ldots, x_{m,m-1}).$$

(it just gives a particularly nice ordering of variables for the purpose.) In such a basis, $w^{11}(x) = (1, 0 \ldots 0, x)$.

Assume $x \in \tilde{N}^r(m-1)$. Thus there exists $Y = \left(\begin{smallmatrix} 1 & x^T \\ x & Y' \end{smallmatrix}\right) \in M(N^{r-1}(P_{m-1}))$. Define

$$\overline{Y} = \begin{pmatrix} 1 & 1 & (0 \ldots 0)^T & x^T \\ 1 & 1 & (0 \ldots 0)^T & x^T \\ (0 \ldots 0) & (0 \ldots 0) & \mathbf{0}_{2m-1,2m-1} & \mathbf{0}_{2m-1,m(m-1)} \\ x & x & \mathbf{0}_{m(m-1),2m-1} & Y' \end{pmatrix},$$

where $\mathbf{0}_{s,q}$ denotes the all-0 matrix of size $s \times q$. We show that $\overline{Y} \in M(N^{r-1}(P_m))$, implying the statement of the lemma.

By construction, $\overline{Y}^T = \overline{Y}$, $Y_{0,j} = Y_{jj}$ and $\overline{Y}_{0,j} = \overline{Y}_{jj}$.

Note that if $Y_{0,j} = 0$ then $Ye_j = 0$, as $P_{m-1} \subseteq Q_{m(m-1)}$. Hence $\overline{Y}_{0,j} = 0$ implies $\overline{Y}e_j = 0$. Thus if $\overline{Y}e_j \neq 0$ then we can normalize $\frac{1}{\overline{Y}_{0,j}}\overline{Y}e_j$. Hence, by induction assumption applied to $x = Ye_j$, one has $\frac{1}{\overline{Y}_{0,j}}\overline{Y}e_j \in N^{r-1}(P_m)$ for all j such that $\overline{Y}_{0,j} \neq 0$. Hence $\overline{Y}e_j \in N^{r-1}(P_m)$ for all j.

Similarly, as any nonzero vector of the form $Y(e_0 - e_k)$ satisfies $Y(e_0 - e_k)_0 = 1 - Y_{0,k} > 0$, normalizing a nonzero $\overline{Y}(e_0 - e_j)$ with its 0-th coordinate, one obtains, for $j > 0$, that either $\overline{Y}(e_0 - e_j) = 0$ or $\frac{1}{1-\overline{Y}_{0,j}}\overline{Y}(e_0 - e_j) \in N^{r-1}(P_m)$. Hence $\overline{Y}(e_0 - e_j) \in N^{r-1}(P_m)$ for all $j > 0$. □

Lemma 7.2. $\frac{1}{m-1}\mathbf{e}_{m(m-1)} \in \tilde{N}^{m-3}(m-1)$ for $m \geq 3$.

Proof. Trivial for $m = 3$. Denote $x_k = \frac{1}{k}\mathbf{e}_{k(k+1)}$.

By induction, assume $x_k \in \tilde{N}^{k-2}(k)$ for all $1 < k < m-1$. Set the matrix Y to have columns $(1, x_{m-1})$, $\frac{1}{m-1}(1, w^{11}(x_{m-2}))$, $\frac{1}{m-1}(1, w^{12}(x_{m-2}))$, … , $\frac{1}{m-1}(1, w^{m,m-1}(x_{m-2}))$. Then $Y^T = Y$, $Y_{0,j} = Y_{jj}$.

By induction assumption and Lemma 7.1, $Ye_j \in N^{m-4}(P_{m-1})$ for each $j > 0$.

Next, observe that

$$Ye_0 = \sum_{p=1}^{m-1} Ye_{(q,p)} \qquad \text{for any } 1 \le q \le m \tag{7.4}$$

(here we use notation identifying $(q,p) = j$). Hence $Ye_0 \in N^{m-4}(P_{m-1})$.

Finally, from (7.4) we have $Y(e_0 - e_{(q,p)}) = \sum_{s=1,\ s\neq q}^{m-1} Ye_{(q,s)}$.

Thus $Y \in M(N^{m-4}(P_{m-1}))$, and the statement follows. □

8 Linear lower bound on the "Boolean degree" of Positivstellensatz Calculus refutations of the knapsack

We use the following notation from [IPS99, Gri01a]. For a polynomial f, its *multilinearization* $\overline{f}$ is a polynomial obtained by the reduction of f modulo $(x - x^2)$ for every variable x, i.e., $\overline{f}$ is the unique multilinear polynomial equivalent to f modulo these ("Boolean") polynomials. When $f = \overline{f}$ we say that f is reduced.

For a monomial t one can define its *Boolean degree* $\mathrm{Bdeg}(t)$ as $\deg(\overline{t})$, in other words, the number of occurring variables; then one extends the concept of Bdeg to polynomials: $\mathrm{Bdeg}(f) = \max \mathrm{Bdeg}(t_i)$, where the maximum is taken over all non-zero monomials t_i occurring in f. Thereby, one can define Bdeg of a derivation in PC and subsequently in Positivstellensatz and Positivstellensatz Calculus as maximum Bdeg of *all* polynomials in the derivation (in Positivstellensatz and Positivstellensatz Calculus, this includes polynomials h_j^2, cf. definition in Subsection 2.2).

The following lemma extends the argument in the proof of [IPS99, Theorem 5.1] from deg to Bdeg.

Lemma 8.1. Let $f(x_1, \dots, x_n) = c_1x_1 + \dots + c_nx_n - m$, where $c_1, \dots, c_n \in \mathbb{R} \setminus \{0\}$. Let q be deducible in PC from the knapsack problem $f = 0$ with $\mathrm{Bdeg} \le \lceil (n-1)/2 \rceil$. Then one can represent

$$q = \sum_{i=1}^{n} (x_i - x_i^2) g_i + fg, \tag{8.1}$$

where $\deg(fg) \le \mathrm{Bdeg}(q)$.

Proof. Similarly to the proof of [IPS99, Theorem 5.1], we conduct the induction along a (fixed) deduction in PC. Assume (8.1) and consider a polynomial qx_1 obtained from q by multiplying it by a variable x_1. W.l.o.g. one can suppose that g is reduced. Then $\overline{qx_1} = \overline{fgx_1}$; denote $h = \overline{gx_1}$. Let $d = \deg(h) - 1$. We need to verify that $d + 2 = \deg(fh) \le \mathrm{Bdeg}(qx_1)$. Taking into account that

$$d + 1 = \deg(h) \le \deg(g) + 1 = \deg(fg) \le \mathrm{Bdeg}(q) \le \mathrm{Bdeg}(qx_1),$$

the mere case to be brought to a contradiction is when $\mathrm{Bdeg}(qx_1) = \mathrm{Bdeg}(q) = \deg(g) + 1 = d + 1$.

We write $g = p + x_1 p_1$ where all the terms of g not containing x_1 are gathered in p. Clearly, $\deg(p) \leq \deg(g) = d$. Moreover, $\deg(p) = d$ because if $\deg(p) < d$, we would have $d + 1 = \deg(h) \leq \mathrm{Bdeg}(gx_1) \leq \max(\mathrm{Bdeg}(x_1 p), \mathrm{Bdeg}(x_1^2 p_1)) \leq d$.

On the other hand, $d = \mathrm{Bdeg}(q) - 1 \leq \lceil (n-1)/2 \rceil - 1$. Therefore, [IPS99, Lemma 5.2] applied to the instance $c_2x_2 + \ldots + c_nx_n - 0$ of symmetric knapsack states that

$$\deg(\overline{(c_2x_2 + \ldots + c_nx_n)p}) = \deg(p) + 1 = d + 1$$

(one should add to the formulation of [IPS99, Lemma 5.2] the condition that p is reduced).

Hence there exists a monomial $x^J = \prod_{j \in J} x_j$ occurring in p for a certain $J \subseteq \{2, \ldots, n\}$, $|J| = d$, and besides, there exists $i \in [2..n]$ such that the monomial $x_i x^J$, being of the degree $d + 1$, occurs in the polynomial $\overline{(c_2x_2 + \cdots + c_nx_n)p}$, in particular $i \notin J$.

Because of that the monomial $T = x_i x^J x_1$ with $\deg(T) = d + 2$ occurs in

$$p' = \overline{(c_2x_2 + \cdots + c_nx_n)px_1}.$$

Furthermore, T occurs in

$$\overline{fgx_1} = \overline{((c_2x_2 + \cdots + c_nx_n) + (c_1x_1 - m))(p + x_1p_1)x_1}$$

since after opening the parenthesis in the right-hand side of the latter expression we obtain only p' and two subexpressions

$$\overline{(c_1x_1 - m)(p + x_1p_1)x_1} = \overline{(c_1 - m)gx_1} \quad \text{and} \quad \overline{(c_2x_2 + \cdots + c_nx_n)x_1p_1x_1}$$

of Boolean degree at most $d+1$ (thereby, any monomial from these subexpressions cannot be equal to the *reduced* monomial T). Finally, due to the equality $\overline{qx_1} = \overline{fgx_1}$, we conclude that $\mathrm{Bdeg}(qx_1) \geq \deg(\overline{qx_1}) = \deg(\overline{fgx_1}) \geq d + 2$; the achieved contradiction proves the induction hypothesis for the case of the rule of the multiplication by a variable (note that the second rule in (2.2) can be replaced by the multiplication by a variable with a multiplicative constant).

Now we proceed to the consideration of the rule of taking the sum of two polynomials q and r. By the induction hypothesis we have

$$r = \sum_{i=1}^{n} (x_i - x_i^2)u_i + fu,$$

where u is reduced and $\deg(fu) \leq \mathrm{Bdeg}(r)$. Then making use of (8.1) we get $\overline{r + q} = \overline{fv}$ where $v = \overline{g + u}$. The inequality

$$\deg(v) \leq \max\{\deg(g), \deg(u)\} \leq \max\{\mathrm{Bdeg}(q), \mathrm{Bdeg}(r)\} - 1 \leq \lceil (n-1)/2 \rceil - 1 \leq \lceil n/2 \rceil - 1$$

enables us to apply [IPS99, Lemma 5.2] to v, this implies that $\deg(\overline{fv}) = \deg(v) + 1 = \deg(fv)$. Therefore, $\mathrm{Bdeg}(r + q) \geq \deg(\overline{r + q}) = \deg(\overline{fv}) = \deg(fv)$. □

The next corollary extends [IPS99, Theorem 5.1].

Corollary 8.1. Any PC deduction of the knapsack f has Bdeg greater than $\lceil (n-1)/2 \rceil$.

Now we can formulate the following theorem extending the theorem of [Gri01a] from deg to Bdeg. Denote by δ a stairs-form function which equals to 2 out of the interval $(0, n)$ and which equals to $2k+4$ on the intervals $(k, k+1)$ and $(n-k-1, n-k)$ for all integers $0 \le k < n/2$.

Theorem 8.1. Any Positivstellensatz Calculus refutation of the symmetric knapsack problem $f = x_1 + \cdots + x_n - m$ has Bdeg greater or equal to $\min\{\delta(m), \lceil (n-1)/2 \rceil + 1\}$.

Proof. The proof of the theorem follows the proof of the theorem [Gri01a]. First, we apply Lemma 8.1 to the deduction in PC being an ingredient of the deduction in Positivstellensatz Calculus (see definitions in 2.2). This provides a refutation in Positivstellensatz Calculus of the form

$$1 + \sum_j h_j^2 = \sum_{i=1}^{n} (x_i - x_i^2) g_i + fg. \tag{8.2}$$

The rest of the proof follows the idea from [Gri01a] of applying to (8.2) the linear mapping B to both sides of (8.2), defined on the monomials x^I as

$$B : \mathbb{R}[x_1, \dots, x_n] \to \mathbb{R}, \quad \text{where } B(x^I) = B_k = \frac{\binom{m}{k}}{\binom{n}{k}}, \quad \text{for } k = |I|, \tag{8.3}$$

and by linearity on the rest of $\mathbb{R}[x_1, \dots, x_n]$.

It is worthwhile to mention that B is defined on the quotient algebra $\mathbb{R}[x_1, \dots, x_n]/(x_1 - x_1^2, \dots, x_n - x_n^2)$, thereby, the proof in [Gri01a] actually, estimates Bdeg rather than just deg.

We would like to sketch here a streamlined version of the latter proof, invoking at some point technique from the theory of association schemes, cf. e.g. [BI84].

Lemma 8.2. (cf. [Gri01a, Lemma 1.3].) Let $g_0 \in \mathbb{R}[x_1, \dots, x_n]$, and $\text{Bdeg} g_0 < n$. Then $B(g_0) = 0$.

Proof. Verify that B is vanishing on all the monomials of g_0, as B satisfies the recurrence $(n-k)B_{k+1} = (m-k)B_k$. □

Introduce on (the coefficient space of) $\mathbb{R}[x_1, \dots, x_n]/(x_1 - x_1^2, \dots, x_n - x_n^2)$ a quadratic form Q by setting $Q(x^I, x^J) = B(x^{I \cup J})$ and denote by Q_ℓ the restriction of Q onto the subspace of polynomials of degree at most ℓ. In the sequel we allow ourselves to denote by Q_ℓ also the matrix of Q_ℓ. It is interesting to mention that Q is known as the *moment matrix* of B, see e.g. [Las01, Lau01].

Lemma 8.3. (cf. [Gri01a, Lemma 1.4].) The form Q_ℓ is positive semidefinite if and only if $\ell - 1 < m < n - \ell + 1$ and $\ell \le \lfloor n/2 \rfloor$.

A proof for this lemma is given below, and this is where the promised streamlining happens. We now demonstrate how to deduce the proof of the theorem from this lemma.

Apply B to the both sides of (8.2). The right-hand side vanishes, as $B(fg) = 0$ due to Lemma 8.2, and as $B((x_i - x_i^2)g_i) = B(x_i g_i) - B(x_i^2 g_i) = 0$. The left-hand side then evaluates to $C = 1 + \sum_j h_j^T Q h_j$, where h_j stands for the vector of coefficients of the polynomials h_j. As the maximal degree of h_j^2 cannot be larger than the maximal degree of the right-hand side of (8.2), $h_j^T Q h_j = h_j^T Q_\ell h_j$, where ℓ falls into the range covered by Lemma 8.3. Hence $h_j^T Q h_j \geq 0$ and thus $C > 0$, the desired contradiction. □

Proof of Lemma 8.3. Let us order the subsets of $\{1, \ldots, n\}$ with respect to the size (i.e. degree), and in arbitrary (but fixed) way within each size, and fix the ordering on the rows and columns of Q_ℓ accordingly. Denote by $Q_{\ell\ell}$ the principal submatrix of Q_ℓ corresponding to the ℓ-element subsets of $\{1, \ldots, n\}$ (so that $Q_{\ell\ell}$ occupies the south-east corner of Q_ℓ).

We show now that Q_ℓ has at least $T - \binom{n}{\ell}$ zero eigenvalues, where $T = \sum_{j=0}^{\ell} \binom{n}{j}$. To this end, let us exhibit a basis for a subspace of such a dimension of the nullspace $\ker Q_\ell$ of Q_ℓ. The coefficient vectors of fx^I, lie in $\ker Q_\ell$ as long as $|I| < \ell$, as can be seen by invoking Lemma 8.2 on $B(fx^I x^J)$, where $|J| \leq \ell$. These fx^I will form the desired basis, as these vectors are linearly independent. This can be seen by building a basis for the subspace they generate, adding first the vector of coefficients of fx^I, where I is the greatest (w.r.t. the ordering specified above) subset of size $|I| < \ell$, then the second greatest I, and so on. At each step a new, smaller, monomial of the form Dx^I for $D \in \mathbb{R} - \{0\}$ appears in fx^I, implying that the dimension increases, and we are done.

To this point we followed [Gri01a] quite closely. Now comes the first shortcut. Namely, we claim that positive definiteness of $Q_{\ell\ell}$ implies positive semidefiniteness of Q_ℓ. Indeed, let $\mu_1 \geq \cdots \geq \mu_{\binom{n}{\ell}}$ (resp. $\lambda_1 \geq \cdots \geq \lambda_T$) be the sequence of the eigenvalues of $Q_{\ell\ell}$ (resp., of Q_ℓ). It is well-known (the result attributed to Cauchy, and as such sometimes referred to as Cauchy interlacing, as well as the *inclusion principle* for eigenvalues) that the first sequence *interlaces* the second, that is, $\lambda_i \geq \mu_i$ for $1 \leq i \leq \binom{n}{\ell}$, cf. e.g. [HJ90, Theorem 4.3.15] or [Lüt96, 5.3.1(11)]. Therefore the first $\binom{n}{\ell}$ eigenvalues of Q_ℓ are not smaller than the smallest eigenvalue of $Q_{\ell\ell}$, and thus positive, and we are done.

Already at this point we can prove that Q_ℓ is positive semidefinite for m sufficiently close to ℓ, as for $m = \ell$ the matrix $Q_{\ell\ell}$ is a positive scalar multiple of the identity matrix, and as the eigenvalues of $Q_{\ell\ell}$ depend continuously on m. (And actually, even for m sufficiently close to $\ell - i$, for $0 \leq i \leq \ell$, as $Q_{\ell-i}$ is a principal submatrix of Q_ℓ.)

To complete the proof for all the values of m under consideration, we show that $Q_{\ell\ell}$ is positive definite. Here we invoke the theory of association schemes, see e.g. [BI84, God93], as follows. For the sake of completeness, we give few definitions first. We denote by $M = M_{\binom{n}{\ell}}(\mathbb{C})$ the algebra of the $\binom{n}{\ell} \times \binom{n}{\ell}$ matrices with entries in the field $\mathbb{C}$ of complex numbers. The *centralizer* $C_M(S)$ of an $S \subseteq M$ in M is defined by $C_M(S) = \{c \in M \mid cs = sc \text{ for any } s \in S\}$. Note that $C_M(S)$ is a *subalgebra* of M.

Let $\rho \subset M$ be the permutation representation of the symmetric group S_n acting on the subsets of size ℓ. That is, one takes each $\pi \in S_n$ as a permutation π' in $S_{\binom{n}{\ell}}$ by setting $\pi'(\{t_1, \ldots, t_\ell\}) = \{\pi(t_1), \ldots, \pi(t_\ell)\}$ and then turning π' into a 0-1 matrix $\rho(\pi)$ by setting $\rho_{I,\pi'(I)}(\pi) = 1$ and $\rho_{IJ}(\pi) = 0$ for the remaining pairs of indices (IJ), $J \neq \pi'(I)$. Then $Q_{\ell\ell} \in C_M(\rho)$. The algebra $C_M(\rho)$ is known under many different names, cf. [BI84], e.g. as the Bose-Mesner algebra of the Johnson scheme $J(n, \ell)$. What is important here is that $C_M(\rho)$ is commutative of dimension $\ell + 1$, and the $0 - 1$ matrices A_i defined as $(A_i)_{IJ} = 1$

iff $|I - J| = i$ form its basis, $0 \le i \le \ell$.

As the $\mathbb{C}$-linear representations of finite groups are completely reducible, see e.g. [BI84, Theorem 1.2.4], there exists an orthogonal linear transformation that decomposes ρ into a direct sum of $\ell + 1$ irreducible representations. By the Schur's Lemma, see e.g. [BI84, Theorem 1.3.2], such a transformation simultaneously diagonalizes all the A_i's, and the restriction of any of the transformed A_i's onto the j-th irreducible constituent is a scalar matrix $p_i(j)I$. Thus each A_i has at most $\ell + 1$ distinct eigenvalues $p_i(j)$. This implies in particular that, as $Q_{\ell\ell} = \sum_{i=0}^{\ell} B_{\ell+i} A_i$ (here B is as in (8.3)), the set of eigenvalues of $Q_{\ell\ell}$ equals the set of eigenvalues of $(\ell + 1) \times (\ell + 1)$ diagonal matrix $\sum_{i=0}^{\ell} B_{\ell+i} \mathrm{diag}(p_i(0), p_i(1), \ldots, p_i(\ell))$.

To summarize, we state the following lemma, writing out the expressions for $p_i(j)$ from [BI84, Corollary to Th. 3.2.9].

Lemma 8.4. The set of eigenvalues of $Q_{\ell\ell}$ is given by

$$\begin{aligned} s_j &= \sum_{i=0}^{\ell} B_{\ell+i} p_i(j), \qquad \text{where} \\ p_i(j) &= \binom{\ell}{i}\binom{n-\ell}{i} {}_3F_2\left(\begin{matrix} -i, & -j, & -n-1+j \\ -\ell, & -n+\ell & \end{matrix} ;1\right). \end{aligned} \tag{8.4}$$

Here ${}_rF_s\left(\begin{matrix} a_1, & \ldots, & a_r \\ b_1, & \ldots, & b_s \end{matrix} ;y\right) = \sum_{t\ge 0} \frac{(a_1)_t \ldots (a_r)_t}{(b_1)_t \ldots (a_s)_t} \frac{y^t}{t!}$ denotes the hypergeometric series and $(a)_t$ the ascending factorial $(a)_t = a(a+1)\ldots(a+t-1)$, $(a)_0 = 1$.

To complete the proof of Lemma 8.3, it suffices to show that $s_j > 0$ for all j. Taking (8.3) and (8.4) into account, we see that it remains to show that

$$\frac{s_j}{B_\ell} = \sum_{i\ge 0} \binom{\ell}{i}\binom{m-\ell}{i} {}_3F_2\left(\begin{matrix} -i, & -j, & -n-1+j \\ -\ell, & -n+\ell & \end{matrix} ;1\right) > 0 \qquad \text{for} \quad 0 \le j \le \ell$$

Changing the order of summation, one obtains

$$\begin{aligned} \frac{s_j}{B_\ell} &= \sum_{t\ge 0} c_t \sum_{i\ge 0} (-i)_t \binom{\ell}{i}\binom{m-\ell}{i} = \\ &= \sum_{t\ge 0} c_t (-t)_t \binom{\ell}{t}\binom{m-\ell}{t} {}_2F_1\left(\begin{matrix} -m+\ell+t, & t-\ell, \\ t+1 & \end{matrix} ;1\right) = \\ &= \sum_{t\ge 0} c_t (-t)_t \binom{\ell}{t}\binom{m-\ell}{t} \frac{\Gamma(-t+1+m)t!}{\Gamma(1+m-\ell)\ell!}, \quad \text{for} \quad c_t = \frac{(-j)_t(-n+j-1)_t}{(-\ell)_t(-n+\ell)_t\, t!}. \end{aligned} \tag{8.5}$$

The equality in the second row is obtained by applying to the inner sum in the first row the procedure described in [PWZ98, Chaper 3] that identifies hypergeometric series. Note that the first non-vanishing term of this sum is the t-th one (i.e. $i = t$) and it equals $(-t)_t \binom{\ell}{t}\binom{m-\ell}{t}$.

The equality in the third row is derived using the Gauss's identity (see [PWZ98, Sect. 3.5]).

Next, we again use the abovementioned procedure from [PWZ98, Chaper 3] to identify the latter sum $\frac{s_j}{B_\ell} = \sum_{t\ge 0} \frac{f_t}{\Gamma(1+m-\ell)\ell!}$ as a hypergeometric series. Pulling the constant term $\frac{1}{\Gamma(1+m-\ell)\ell!}$ outside, one notes that the already the 0-th term does not vanish, and equals

$\Gamma(1+m)$. Thus we just have to compute the ratio of the consecutive summands f_{t+1} and f_t to arrive at

$$\frac{f_{t+1}}{f_t} = \frac{(t-j)(t-n+j-1)(-t+m-\ell)\Gamma(m-t)}{(t-n+\ell)(t+1)\Gamma(m-t+1)} = \frac{(t-j)(t-n+j-1)(t-m+\ell)}{(t-n+\ell)(t+1)(t-m)},$$

where the latter is obtained by using the identity $\Gamma(x+1)/\Gamma(x) = x$. This readily identifies the series and one obtains the following.

$$\frac{s_j}{B_\ell}\frac{\Gamma(1+m-\ell)}{\Gamma(1+m)}\ell! = {}_3F_2\left(\begin{matrix} -m+\ell, & -n+j-1, & -j \\ -n+\ell, & & -m \end{matrix} ;1\right) = \frac{(-n+m)_j(\ell-j+1)_j}{(-n+\ell)_j(m-j+1)_j}.$$

Here the Saalschütz's identity (see [PWZ98, Sect. 3.5]) is applied to the second expression for $j>0$ to obtain the rightmost expression, that is also valid for $j=0$ by definition of the ascending factorial.

We should investigate the sign of $R_j = \frac{(-n+m)_j}{(-n+\ell)_j}$, as the remaining multiplicative term is positive. Note that the multiplicands of the denominator are always negative. On the other hand, the numerator has all the multiplicands negative if and only if $m < n-j+1$ for all j. (and in particular $R_j > 0$.) This completes the proof of the "if" part of the lemma.

Arguing along this line it follows that if $m > n-\ell+1$ then there exists j such that one gets $R_j < 0$. Finally, observe that if $m < \ell - 1$ then $B_\ell < 0$. Thus if a condition on m in the lemma is not satisfied then $Q_{\ell\ell}$ has a negative eigenvalue. This implies that Q_ℓ is not positive semidefinite, completing the proof of Lemma 8.3, and, thereby, of Theorem 8.1. ☐

9 Exponential lower bound on the size of static LS$_+$ refutations of the symmetric knapsack

In this section we apply the results of Section 8 to obtain an exponential lower bound on the size of static LS$_+$ refutations of the symmetric knapsack. We follow the notation introduced in Subsection 2.5 and Section 8. The *Boolean degree of a static LS (LS$_+$) refutation* is the maximum Boolean degree of the polynomials $u_{i,l}$ in Subsection 2.5.

Let us fix for the time being a certain (threshold) d.

Lemma 9.1. Denote by M the number of $u_{i,l}$'s occurring in (2.15) that have Boolean degrees at least d. Then there is a variable x and a value $a \in \{0,1\}$ such that the result of substituting in (2.15) $x=a$ contains at most $M(1-d/(2n))$ non-zero polynomials $u_{i,l}|_{x=a}$ of Boolean degrees at least d. (Note that by substituting in (2.15) a value a for x we obtain a valid static LS$_+$ refutation of the system $S|_{x=a}$).

Proof. Since there are at least Md polynomials $u_{i,l}$ of Boolean degrees at least d containing either x or $1-x$, there is a variable x such that either x or $1-x$ occurs in at least $Md/(2n)$ of these polynomials. Therefore, after substituting the appropriate value for x, at least $Md/(2n)$ polynomials $u_{i,l}$ vanish from (2.15). ☐

For the symmetric knapsack problem (5.2), we can rewrite its static LS$_+$ refutation in the following way. Denote

$$\begin{array}{rcl} f_0 & = & x_1 + \cdots + x_n - m, \\ f_i & = & x_i - x_i^2 \quad (1 \le i \le n), \\ f_i & = & (s_i')^2 \quad (n+1 \le i \le n') \end{array}$$

(m is not an integer). The refutation can be represented in the form

$$\sum_{i=0}^{t} f_i \sum_l g_{i,l} + \sum_{j=n+1}^{n'} f_j t_j + \sum_{j=n'+1}^{n''} t_j = -1, \tag{9.1}$$

where

$$\begin{array}{rcl} g_{i,l} & = & \gamma_{i,l} \cdot \prod_{k \in G_{i,l}^+} x_k \cdot \prod_{k \in G_{i,l}^-} (1 - x_k), \\ t_j & = & \tau_j \cdot \prod_{k \in T_j^+} x_k \cdot \prod_{k \in T_j^-} (1 - x_k) \end{array}$$

for appropriate multisets $G_{i,l}^-$, $G_{i,l}^+$, T_j^- and T_j^+, positive real τ_j and *arbitrary* real $\gamma_{i,l}$.

Lemma 9.2. If $n/4 < m < 3n/4$, then the Boolean degree D of any static LS$_+$ refutation of the symmetric knapsack problem is at least $n/4$.

Proof. Replacing in t_j each occurrence of x_i by $f_i + x_i^2$ and each occurrence of $1 - x_i$ by $f_i + (1 - x_i)^2$ and subsequently opening the parentheses in t_j, one can gather all the terms containing at least one of f_i and separately the products of squares of the form x_i^2, $(1 - x_i)^2$. As a result one gets a representation of the form

$$\sum_{i=0}^{n} f_i g_i + \sum_{j=1}^{n'''} h_j^2 = -1$$

for appropriate polynomials g_i, h_j of Boolean degrees $\mathrm{Bdeg}(g_i), \mathrm{Bdeg}(h_j^2) \le D$, thereby a Positivstellensatz (and Positivstellensatz Calculus) refutation of the symmetric knapsack of Boolean degree at most $D+2$. Then Theorem 8.1 implies that $D \ge \lceil (n-1)/2 \rceil - 1 \ge n/4$. $\square$

Theorem 9.1. For $m = (2n+1)/4$ the number of $g_{i,l}$'s and t_j's in (9.1) is $\exp(\Omega(n))$.

Proof. Now we set $d = \lceil n/8 \rceil$ and apply Lemma 9.1 consecutively $\kappa = \lfloor n/4 \rfloor$ times. The result of all these substitutions in (9.1) we denote by (9.1$'$), it contains $n - \kappa$ variables; denote by $u_{i,l}'$ the polynomial we thus get from $u_{i,l}$. We denote by f_0' the result of substitutions applied to f_0. Note that after all substitutions we obtain again an instance of the knapsack problem. Taking into account that the free term m' of f_0' ranges in the interval $[m - \kappa, m]$ and since $(n - \kappa)/4 < m - \kappa < m < 3(n - \kappa)/4$, we are able to apply Lemma 9.2 to (9.1$'$). Thus, the degree of (9.1$'$) is at least $(n - \kappa)/4 > d$.

Denote by M_0 the number of $u_{i,l}$'s of the degrees at least d in (9.1). By Lemma 9.1 the refutation (9.1′) contains at most $M_0(1-d/(2n))^{\kappa} \leq M_0(1-1/16)^{n/4}$ non-zero polynomials $u'_{i,l}$ of degrees at least d. Since there is at least one polynomial $u'_{i,l}$ of such degree, we have $M_0(1-1/16)^{n/4} \geq 1$, i.e. $M_0 \geq (16/15)^{n/4}$, which proves the theorem. ☐

Corollary 9.1. Any static LS_+ refutation of (5.2) for $m = (2n+1)/4$ must have size $\exp(\Omega(n))$.

Corollary 9.2. Any tree-like LS_+ (or LS^n) refutation of (5.2) for $m = (2n+1)/4$ must have size $\exp(\Omega(n))$.

Proof. The size of such tree-like refutation (even the numer of instances of axioms f_i used in the refutation) is at least the number of polynomials $u_{i,l}$. ☐

Remark 9.1. The value $m = (2n+1)/4$ in Theorem 9.1 and its corollaries above can be changed to any non-integer value between $\lceil n/4 \rceil$ and $\lfloor 3n/4 \rfloor$ by tuning the constants in the proofs (and in the $\Omega(n)$ in the exponent).

10 Open Questions

1. What is the proof complexity of the symmetric knapsack problem in (dag-like dynamic) LS (cf. Sections 5, 7 and 9)? We conjecture it (or the general knapsack problem) as a candidate for a lower bound.
2. Prove an exponential lower bound on the size of Positivstellensatz refutations.
3. Prove an exponential lower bound for a static semi-algebraic *propositional* proof system. Note that we have only proved an exponential lower bound for static LS_+ as a proof system for the co-NP-complete language of *systems of 0-1 linear inequalities*, because the symmetric knapsack problem is not obtained as a translation of a Boolean formula in DNF.
4. Suggest a candidate for a lower bound in LS^d for (arbitrarily large) constant d.
5. How precise is the logarithmic lower bound on the LS_*-rank for the knapsack problem from Subsection 7.2?
6. Can one relax in Theorem 5.2 the condition on the polynomial growth of the coefficients?
7. Is it possible to simulate LS (or static LS^n) by means of a suitable version of CP (e.g. by the R(CP) introduced in [Kra98])? In other words, does there exist an inverse to Theorem 5.2?

Acknowledgment

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

References

[BEHS99] A. Bockmayr, F. Eisenbrand, M. Hartmann, and A. S. Schulz. On the Chvátal rank of polytopes in the 0/1 cube. *Discrete Applied Mathematics*, 98:21–27, 1999.

[BGIP01] S. Buss, D. Grigoriev, R. Impagliazzo, and T. Pitassi. Linear gaps between degrees for the polynomial calculus modulo distinct primes. *Journal of Computer and System Sciences*, 62:267–289, 2001.

[BI84] Eiichi Bannai and Tatsuro Ito. *Algebraic Combinatorics I: Association Schemes.* Benjamin/Cummings, London-Tokyo, 1984.

[BIK$^+$96] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. *Proc. London Math. Soc.*, 73(3):1–26, 1996.

[BIK$^+$97] P. Beame, R. Impagliazzo, J. Krajíček, P. Pudlák, A. A. Razborov, and J. Sgall. Proof complexity in algebraic systems and bounded depth Frege systems with modular counting. *Computational Complexity*, 6(3):256–298, 1996/97.

[BPR95] M. Bonet, T. Pitassi, and 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*, pages 575–584. ACM, 1995.

[BS01] E. Ben-Sasson. Hard examples for bounded depth Frege. Manuscript, 2001.

[CCH89] V. Chvátal, W. Cook, and M. Hartmann. On cutting-plane proofs in combinatorial optimization. *Linear Algebra Appl.*, 114/115:455–499, 1989.

[CCT87] W. Cook, C. R. Coullard, and G. Turán. On the complexity of cutting-plane proofs. *Discrete Appl. Math.*, 18(1):25–38, 1987.

[CD01] William Cook and Sanjeeb Dash. On the matrix-cut rank of polyhedra. *Math. Oper. Res.*, 26(1):19–30, 2001.

[CEI96] M. Clegg, J. Edmonds, and 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*, pages 174–183. ACM, 1996.

[Chv73] V. Chvátal. Edmonds polytopes and a hierarchy of combinatorial problems. *Discrete Math.*, 4:305–337, 1973.

[CR79] S. A. Cook and A. R. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44(1):36–50, 1979.

[Das01] Sanjeeb Dash. *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`.

[ES99] F. Eisenbrand and A. S. Schulz. Bounds on the Chvátal rank of polytopes in the 0/1-cube. In G.J.Woeginger G. Cornuéjos, R.E. Burkard, editor, *IPCO'99*, volume 1610 of *Lecture Notes in Computer Science*, pages 137–150, Berlin Heidelberg, 1999. Springer-Verlag.

[GH01] D. Grigoriev and E. A. Hirsch. Algebraic proof systems over formulas. Technical Report 01-011, Electronic Colloquim on Computational Complexity, 2001. `ftp://ftp.eccc.uni-trier.de/pub/eccc/reports/2001/TR01-011/index.html`.

[God93] C. D. Godsil. *Algebraic Combinatorics.* Chapman and Hall, London, 1993.

[Gom63] R. E. Gomory. An algorithm for integer solutions of linear programs. In *Recent Advances in Mathematical Programming*, pages 269–302. McGraw-Hill, 1963.

[Gri01a] D. Grigoriev. Complexity of Positivstellensatz proofs for the knapsack. *Computational Complexity*, 10:139–154, 2001.

[Gri01b] D. Grigoriev. Linear lower bound on degrees of Positivstellensatz calculus proofs for the parity. *Theoretical Computer Science*, 259:613–622, 2001.

[GT01] M. X. Goemans and L. Tunçel. When does the positive semidefiniteness constraint help in lifting procedures. *Mathematics of Operations Research*, 2001. to appear.

[GV01] D. Grigoriev and N. Vorobjov. Complexity of Null- and Positivstellensatz proofs. *Annals of Pure and Applied Logic*, 113(1-3):153–160, 2001.

[HJ90] R. A. Horn and C. R. Johnson. *Matrix Analysis.* Cambridge University Press, Cambridge, 1990.

[IPS99] R. Impagliazzo, P. Pudlák, and J. Sgall. Lower bounds for the polynomial calculus. *Computational Complexity*, 8(2):127–144, 1999.

[Kra98] J. Krajíček. Discretely ordered modules as a first-order extension of the cutting planes proof system. *Journal of Symbolic Logic*, 63(4):1582–1596, 1998.

[Las01] Jean B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM J. Optim.*, 11(3):796–817 (electronic), 2000/01.

[Lau01] M. Laurent. A comparison of the Sherali-Adams, Lovász-Schrijver and Lasserre relaxations for 0-1 programming. Technical report PNA-R0108, CWI, Amsterdam, 2001.

[Lov94] L. Lovász. Stable sets and polynomials. *Discrete Mathematics*, 124:137–153, 1994.

[LS91] L. Lovász and A. Schrijver. Cones of matrices and set-functions and 0–1 optimization. *SIAM Journal on Optimization*, 1:166–190, 1991.

[Lüt96] H. Lütkepohl. *Handbook of Matrices.* John Wiley & Sons, Chichester, 1996.

[Pit97] T. Pitassi. Algebraic propositional proof systems. In Neil Immerman and Phokion G. Kolaitis, editors, *Descriptive Complexity and Finite Models*, volume 31 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science.* American Mathematical Society, 1997.

[Pud97] P. Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *J. Symbolic Logic*, 62(3):981–998, 1997.

[Pud99] P. Pudlák. On the complexity of propositional calculus. In *Sets and Proofs: Invited papers from Logic Colloquium'97*, pages 197–218. Cambridge University Press, 1999.

[PWZ98] M. Petrovšek, H. Wilf, and D. Zeilberger. *$A = B$*. A. K. Peeters, Wellesley, MA, USA, 1998.

[Raz85] A. Razborov. Lower bounds on the monotone complexity of boolean functions. *Dokl. AN USSR*, 22:1033–1037, 1985.

[Raz98] A. A. Razborov. Lower bounds for the polynomial calculus. *Computational Complexity*, 7:291–324, 1998.

[ST99] Tamon Stephen and Levent Tunçel. On a representation of the matching polytope via semidefinite liftings. *Math. Oper. Res.*, 24(1):1–7, 1999.

[Urq87] A. Urquhart. Hard examples for resolution. *JACM*, 34(1), 1987.

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'