COMPLEXITY OF SEMIALGEBRAIC PROOFS

DIMA GRIGORIEV, EDWARD A. HIRSCH, AND DMITRII V. PASECHNIK

Dedicated to Yuri I. Manin on the occasion of his 65th birthday

Abstract. It is a known approach to translate propositional formulas into systems of polynomial inequalities and consider proof systems for the latter. The well-studied proof systems of this type are the Cutting Plane proof system (CP) utilizing linear inequalities and the Lovász–Schrijver calculi (LS) utilizing quadratic inequalities. We introduce generalizations LS\(d\) of LS that operate on 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 those examples.

Finally, we prove lower bounds on the Lovász–Schrijver ranks and on the size and the “Boolean degree” of Positivstellensatz calculus refutations. We use the latter bound to obtain an exponential lower bound on the size of Positivstellensatz calculus, static LS\(d\), and tree-like LS\(d\) refutations.


Key words and phrases. Computational complexity, propositional proof system.

“Mathematical proof is a social phenomenon.”
Yu. I. Manin, from the lecture at Leningrad Branch of Steklov Mathematical Institute, 1977.

“(...) proof system (...) is a function.”
S. A. Cook, A. R. Reckhow [CR79].

1. Introduction

The observation that a propositional formula can be written as a system of polynomial equations has led to considering, in particular, the Nullstellensatz (NS)
and polynomial calculus (PC) proof systems (see Section 2.2 below). We do not
dwell much on the history of this rich area; nice historical overviews can be found
in, e.g., [BIK+96], [BIK+97], [Raz98], [IPS99], [CEI96], [BGIP01].

For these proof systems, several interesting complexity lower bounds on the de-
gees of derived polynomials were obtained [Raz98], [IPS99], [BGIP01]. When the
degree is close enough to linear (in fact, greater than the square root) in the num-
ber of input variables, these bounds imply exponential lower bounds on the proof
complexity (more precisely, on the number of monomials in the derived polyno-
mials) [IPS99]. When polynomials are given by formulas rather than by sums of
monomials, as in NS or in PC, the complexity may 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
those operating on equations only, such as NS or PC. The first proof system based
on inequalities was the Cutting Plane system (CP) [Gom63], [Chv73], [CCT87],
[CCH89] (see also Section 2.3). This system uses linear inequalities (with integer co-
efficients). Exponential lower bounds on proof size were established for the CPs with
polynomially bounded coefficients in [BPR95] and for the general case in [Pud97].

Another family of well-studied proof systems are the so-called Lovász–Schrijver
calculi (LS) [LS91], [Lov94] (see also [Pud99] and Section 2.3 below). These systems
allow dealing with quadratic inequalities. No nontrivial complexity lower bounds
for them are known so far. Moreover, generalizing LS to systems LS\(d\) that use in-
equalities 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 taut-
ologies (see Section 4). On the other hand, for these tautologies, Pudlák obtained
an exponential lower bound on the complexity of CP proofs [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 LS + CP\(2\) (see
Section 4), which manipulates only quadratic inequalities, endowed with the rounding
rule (it generalizes directly a rounding rule for linear inequalities in CP). These
results mean, in particular, that neither LS\(4\), nor LS + CP\(2\) have monotone effective
interpolation; for the system LS + CP\(1\), where the use of rounding rule is limited
to linear inequalities, a (nonmonotone) effective interpolation is known [Pud99].

The (already mentioned) nontrivial lower bounds on the degree of derived poly-
nomials in PC have no analogue in LS\(d\), as we show in Section 3; namely, every
system of inequalities of degree at most \(d\) without real solutions possesses an LS\(2d\)
refutation.

Another proof system manipulating polynomial inequalities known as the Positivstellensatz calculus was introduced in [GV02]. 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 exist because its “dynamic” part is restricted to an ideal and an
element of a cone of real polynomials is obtained by adding a sum of squares to an
element of an ideal. On the contrary, LS is a completely “dynamic” proof system.
(Static and dynamic proof systems are discussed in [GV02]. 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 the (dynamic) LS. The key ingredient of the proof is a linear lower bound on the “Boolean degree” of Positivstellensatz calculus refutations (Section 8), which also implies a (previously unknown) exponential lower bound on the size of Positivstellensatz calculus refutations.

The lower bound on the Positivstellensatz calculus degree of the knapsack problem [Gri01a] entails (see Section 7.2) a lower bound on the so-called LS-rank [LS91], [Lov94]. Roughly speaking, the LS-rank counts the depth of multiplications involved in 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 linearly, while we are looking for nonlinear (ideally, exponential) lower bounds on the proof complexity. It turns out that the rank is too weak to be an invariant for this purpose. In particular, there are short proofs for the pigeon-hole principle (PHP) in CP [CCT87] and in LS [Pud97], while the LS-rank of the PHP has a linear (in the number of pigeons) lower bound, as we show in Section 7.3. We also prove several lower bounds on the rank of the symmetric knapsack refutations.

The above-mentioned LS³ proof for the symmetric knapsack problem follows from the general fact that LS⁴ systems allow reasoning 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 [BS02]). In Section 5 we also consider a certain extended version LS∗,split of LS that, apart from dealing with integers, allows us to perform case analysis, namely, determine whether \( f > 0, f < 0, \) or \( f = 0 \) for a linear function \( f \) (similar extensions of CP were introduced by Chvátal (unpublished), Pudlák [Pud99], and Krajačić [Kra98]), and finally allows us to multiply inequalities. We show that LS∗,split polynomially simulates CP with small coefficients. The same effect can be achieved by replacing the multiplication and the case analysis by a division rule deriving \( g \geq 0 \) 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 (treated as proof candidates) to \( L \) (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 disjunctive normal form (DNF)). When we have two proof systems \( \Pi_1 \) and \( \Pi_2 \) for the same language \( L \), we can compare them. We say that \( \Pi_1 \) polynomially simulates \( \Pi_2 \) if there is a function \( g \)
mapping proof candidates of $\Pi_2$ to proof candidates of $\Pi_1$ so that, for every proof candidate $\pi$ for $\Pi_2$, we have $\Pi_1(g(\pi)) = \Pi_2(\pi)$ and $g(\pi)$ is at most polynomially longer than $\pi$.

A proof system $\Pi_1$ is \textit{exponentially separated} from $\Pi_2$ if there is an infinite sequence of words $t_1, t_2, \ldots \in L$ such that the length of the shortest $\Pi_1$-proof of $t_i$ is polynomial in the length of $t_i$, and the length of the shortest $\Pi_2$-proof of $t_i$ is exponential.

A proof system $\Pi_1$ is \textit{exponentially stronger} than $\Pi_2$ if $\Pi_1$ polynomially simulates $\Pi_2$ 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 by fixing a reduction between these languages. However, the result of the comparison may be determined by the reduction more than by the systems themselves. For this reason, 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 polynomial equations. There is a series of proof systems for languages consisting of unsolvable systems of polynomial equations. To show that such a proof system is a propositional proof system, we must 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 $v_{j_1}, \ldots, v_{j_t}$ ($t \leq k$) is translated into the equation

$$(1 - l_1) \cdots (1 - l_t) = 0,$$

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 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. Throughout the paper, polynomials are represented by ordered lists (lexicographically or otherwise) of all their nonzero monomials. Note that it does not make sense to consider our translation for general DNF formulas (rather than in $k$-DNF for constant $k$), because an exponential lower bound for any system using such encoding would be trivial ($(1 - v_1)(1 - v_2) \cdots (1 - v_n)$ provides an example of encoding with exponentially many monomials).

Note that $F$ is a tautology if and only if the obtained system $S$ of polynomial equations $f_1 = 0, f_2 = 0, \ldots, f_m = 0$ 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

$$\sum_i f_i g_i = 1.$$
Polynomial calculus (PC) [CEI96]. This system has two derivation rules,
\[
\frac{p_1 = 0; \quad p_2 = 0}{p_1 + p_2 = 0} \quad \text{and} \quad \frac{p = 0}{p \cdot q = 0}.
\]
That is, we 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 \(q\). A proof in this system is a derivation of \(1 = 0\) from \(S\) using these rules.

Positivstellensatz [GV02]. A proof in this system consists of polynomials \(g_1, \ldots, g_m\) and \(h_1, \ldots, h_l\) such that
\[
\sum_i f_i g_i = 1 + \sum_j h_j^2.
\]

Positivstellensatz calculus [GV02]. A proof in this system consists of polynomials \(h_1, \ldots, h_l\) and a derivation of \(1 + \sum h_j^2 = 0\) from \(S\) using rules (2.2).

2.3. Proof systems manipulating inequalities. To define a propositional proof system manipulating 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 of its clauses containing variables \(v_{j_1}, \ldots, v_{j_t}\) into the inequality
\[
\sum_{i} l_i x_i \geq 1
\]
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
\[
x \geq 0,
\]
\[
x \leq 1
\]
for every variable \(x\) in \(S\).

Cutting Plane (CP) [Gom63], [Chv73], [CCT87], [CCH89], see also [Pud99]. In this proof system, we must refute the system \(S\) defined above (i.e., obtain the contradiction \(0 \geq 1\)) using the following two derivation rules:
\[
\frac{f_1 \geq 0; \, \ldots; \, f_t \geq 0}{\sum_{i=1}^{t} \lambda_i f_i \geq 0} \quad \text{(where } \lambda_i \geq 0),
\]
\[
\frac{\sum_{i} a_i x_i \geq c}{\sum_{i} a_i x_i \geq \lceil c \rceil} \quad \text{(where } a_i \in \mathbb{Z}, \text{ and } x_i \text{ is a variable).}
\]
We restrict the intermediate inequalities in a CP derivation to the ones having integer coefficients (except the constant term).

Lovász–Schrijver calculus (LS) [LS91], [Lov94], see also [Pud99]. In the weakest of the Lovász–Schrijver proof systems, we must obtain the contradiction using the rule (2.7) applied to linear or quadratic \(f_i\)'s and the rules
\[
\frac{f \geq 0}{fx \geq 0}, \quad \frac{f \geq 0}{f(1-x) \geq 0} \quad \text{(where } f \text{ is linear and } x \text{ is a variable).}
\]

\(^2\)An arbitrary linear combination is usually allowed, but clearly, it can be replaced by two multiplications and one addition.
Also, the system $S$ is extended by the axioms
\[ x^2 - x \geq 0, \quad x - x^2 \geq 0 \] (2.10)
for every variable $x$.

$LS_+$ [LS91], [Lov94], [Pud99]. This system has the same axioms and derivation rules as LS and the additional axiom
\[ l^2 \geq 0 \] (2.11)
for every linear $l$.

$LS_*$ [LS91], [Lov94], [Pud99]. This system has the same axioms and derivation rules as LS and the additional rule
\[ f \geq 0; \quad g \geq 0; \quad fg \geq 0 \] (2.12)
\[ \text{if } f \text{ and } g \text{ are linear} \]

This system unites $LS_+$ and $LS_*$.

$LS_+CP$ [Pud99]. This system includes the same axioms and derivation rules as LS and the rounding rule (2.8) of CP; the latter can be applied only to linear inequalities.

Note that all Lovász–Schrijver systems described in Section 2.3 deal with either 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 a system $LS + CP^2$ which is slightly stronger than Pudlák’s $LS + CP^1$.

$LS + CP^2$. This system includes the same axioms and rules as LS and the following extension of the rounding rule (2.8) of CP to quadratic inequalities:
\[ \sum_{i,j} a_{ij} x_i x_j + \sum_i a_i x_i \geq c \]
\[ \sum_{i,j} a_{ij} x_i x_j + \sum_i a_i x_i \geq \lceil c \rceil \] (where $a_{ij}, a_i \in \mathbb{Z}$, and $x_i$ is a variable). (2.13)

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 (2.9) is now restricted to $f$’s 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. The degree $d$ can be either $\infty$ or a natural number greater than 1 (in the former case, the degree is unrestricted).

Remark 2.3. Note that $LS = LS^2$.

Similarly, we consider $LS_+^d$, $LS_*^d$, and $LS_{+,*,*}^d$, where the condition “$l$ is linear” (“$f$ and $g$ are linear”) in (2.11) (respectively, in (2.12)), is transformed into “deg($l^2$) ≤ $d$” (respectively, into “deg($fg$) ≤ $d$”).

$LS_{split}^d$. This system allows inequalities not only of the form $f \geq 0$, but also of the form $f > 0$. The derivation rules (2.7) and (2.9) are extended in an obvious way to handle both types of inequalities, and $f > 0$ can always be relaxed to $f \geq 0$. The axiom $1 > 0$ is added. We also allow making assumptions of form $f > 0$ and, if we can derive in $LS_{split}^d$ a contradiction from such an assumption, we conclude that $f \leq 0$. 

We then consider extensions of Lovász–Schrijver proof systems allowing monomials of degree up to $d$.
Below, we give a more formal definition similar to Krajíček’s $R(CP)$ [Kra98]. We consider the propositional fragment of (DAG-like) cut-free Gentzen-style calculus with inequalities instead of Boolean formulas. We use one-sided sequents $\rightarrow \Gamma$ (where the right-hand sides are for simplicity treated as multisets; in what follows, $\Gamma$ and $\Delta$ denote arbitrary multisets) and derive a contradiction (the empty sequent $\rightarrow$) from the initial inequalities $\rightarrow f_i \geq 0$ taken from (2.4)–(2.6) and (2.10). In addition to the usual rule

$$\rightarrow \Gamma \quad \rightarrow \Gamma, \Delta$$

for sequents (but not for Boolean connectives!), we use the derivation rules

$$\rightarrow f > 0, -f \geq 0 \quad \rightarrow \Delta, f \geq 0 \quad \rightarrow \Delta, fx \geq 0 \quad \rightarrow \Delta, f(1-x) \geq 0 \quad (\lambda_i > 0).$$

(2.14)

Remark 2.4. Observe the difference between splitting in $L_{split}$ and in Krajíček’s $R(CP)$ [Kra98] or Chvátal’s “CP with subsumptions” (see, e.g., [Pud99]): we use the weaker “real” splitting (2.14) instead of the stronger “integer” splitting \( \rightarrow f \geq 1, -f \geq 0 \).

$LS_{d_{split}}$ is defined similarly. The version of (2.12) for strict inequalities is

$$\rightarrow \Delta, f > 0; \rightarrow \Delta, g > 0 \quad \rightarrow \Delta, fg > 0.$$

In addition, we need one more rule

$$\Delta, 0 > 0 \quad \rightarrow \Delta.$$

Remark 2.5. The analogue of (2.10) (with the condition “deg$(l^2) \leq d$” instead of “$l$ is linear”) can be easily derived in $L_{split}^d$; i.e., $L_{split}^{d,split} = L_{split}^d$ and $L_{split}^{d,+,split} = L_{split}^d$.

$LS_{split}$, $LS_{+,split}$, etc. are shorthands for the corresponding systems restricted to $d = 2$. 

$LS_{d_{split}}$ is the restricted version of $LS_{d_{split}}$ where splitting applies to the assumptions $x = 0$ and $x = 1$ only ($x$ is a variable); i.e., the rule (2.14) is replaced by

$$\rightarrow x \geq 1, -x \geq 0 \quad (x \text{ is a variable})$$

(2.15)

(note that one can easily simulate this rule applying (2.14) to $f = x$ and to $f = 1 - x$).

$LS_d^f$ is the extension of $LS^d$ with strict inequalities (the latter system is defined in a natural way similarly to $LS_{split}^d$) by another useful rule, namely, by

$$\rightarrow fg \geq 0; \ f > 0 \quad \rightarrow g \geq 0.$$
2.5. New static systems. The Nullstellensatz is a “static” version of polynomial calculus; the Positivstellensatz is a “static” version of the Positivstellensatz calculus. Similarly, we define “static” versions of the new proof systems introduced in Section 2.4.

Static LS\(^\infty\). A proof in this system is 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 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 \( U^-_{i,l} \) determining 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
\[ \sum_{i=1}^t s_i \sum_{l} u_{i,l} = -1. \] (2.16)

Static LS\(^\infty+\). The difference from the preceding system is that \( S \) is extended by inequalities \( s_{t+1} \geq 0, \ldots, s_{t'} \geq 0 \), where each polynomial \( s_j \) \( (j \in [t+1, \ldots, t']) \) is a square of another polynomial \( s'_j \). The requirement (2.16) transforms into
\[ \sum_{i=1}^{t'} s_i \sum_{l} u_{i,l} = -1. \] (2.17)

Static LS\(_+\). The same as static LS\(^\infty+\), but the polynomials \( s'_j \) can be only linear.

Remark 2.6. Static LS\(_+\) includes static LS\(^\infty\).

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 obvious way to verify (2.16) in deterministic polynomial time (see [Pit97]). However, they can be easily augmented to match the definition of Cook and Reckhow, e.g., by including a proof of equality (2.16) or (2.17) based on the axioms of a ring (see F-NS of [GH01]). Clearly, any lower bound for the original system is 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 \( u_{i,l} \), \( s_i \) \( (i \in [1, \ldots, t]) \) and \( s'_j \) \( (j \in [t+1, \ldots, t']) \); thus it is at least the number of \( u_{i,l} \)’s.

Example 2.1. Below, we give a very simple static LS\(_+\) proof of the propositional pigeonhole principle. (It is easy to see that the same proof can also be carried out 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):
\[ \sum_{\ell=1}^{m-1} x_{k\ell} \geq 1; \quad 1 \leq k \leq m; \] (2.18)
\[ x_{k\ell} + x_{k'\ell} \leq 1; \quad 1 \leq k < k' \leq m; \quad 1 \leq \ell \leq m - 1. \] (2.19)
Figure 1. The known simulations between semialgebraic and other proof systems for formulas in $k$-DNF. $R$ denotes resolution, $CP_p$ denotes CP with polynomially bounded coefficients, $NS_+$ denotes the Positivstellensatz, $PC_+$ denotes the Positivstellensatz calculus, and $sLS...$ denotes static $LS...$. The simulations between the static $LS...$ and other proof systems are not shown because the static $LS...$ are not well-defined proof systems (see Remark 2.7). Some trivial simulations (e.g., the simulation of $LS_d$ by $LS_d$) are not shown for readability. The simulation of $CP_p$ is shown in Theorem 5.2. The simulation of PC (respectively, $PC_+$) in $LS^\infty$ (respectively, $LS^\infty_+$) is shown in Corollary 3.1 (respectively, Corollary 3.2).

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

Here is the static $LS_+$ proof:

$$\sum_{k=1}^{m} \left( \sum_{\ell=1}^{m-1} x_{k\ell} - 1 \right) + \sum_{\ell=1}^{m-1} \left( \sum_{k=1}^{m} x_{k\ell} - 1 \right)^2 + \sum_{\ell=1}^{m-1} \sum_{k=1}^{m-1} \sum_{k' \neq k'=1}^{m} (1 - x_{k\ell} - x_{k'\ell})x_{k\ell}
+ \sum_{\ell=1}^{m-1} \sum_{k=1}^{m} (x_{k\ell}^2 - x_{k\ell})(m - 2) = -1. \quad \square$$

The known simulations and separations between semialgebraic and other systems are given in Figs. 1 and 2.

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 on polynomials of degree up to $d$. In particular, for formulas in $k$-CNF, we can use the same encoding as in the polynomial calculus (2.1).
Figure 2. The known separations between semialgebraic and other proof systems for formulas in DNF (except for PC, which is considered for formulas in $k$-DNF only; thus the PHP system is not a valid counterexample for it); $\pi_A \not\rightarrow \pi_B$ means that there is a formula that has polynomial-size $\pi_A$ proofs and has no polynomial-size $\pi_B$ proofs; $F^c$ denotes constant-depth Frege systems; the other notation is the same as in Fig. 1. Only the strongest separations relevant to semialgebraic systems are shown. The leftmost separation is due to PHP (the positive part is proved in [Pud99], the negative part is proved in [Hak85]). The counterexample for CP (which provides the two separations in the middle) is given by the clique-coloring tautologies (see Theorem 4.1 and [Pud97], respectively). The two rightmost separations are due to Tseitin’s formulas (see Theorem 6.1 and [BS02], respectively). Note that the knapsack problem is not a valid counterexample, because it is not a translation of a formula in DNF.

Consider the system $\text{LS}^d$ that has the same derivation rules as $\text{LS}^d$ but uses encoding (2.1) instead of (2.4) (hence this is a proof system for formulas in $k$-DNF for a constant $k$). Clearly, for $d = \infty$, $\text{LS}^\infty$ polynomially simulates polynomial calculus. Does $\text{LS}^\infty$ polynomially simulate $\text{LS}^\infty$ (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 $\text{LS}^t$ derivation of (2.1) from (2.4) and (2.5)–(2.10).

**Proof.** We multiply (2.4) first by $(1 - l_1)$ and then by $(1 - l_2)$, $\ldots$, $(1 - l_{t-1})$, eliminating the terms $l_i(1 - l_i)$ with the use of (2.10) and (2.7) as soon as they appear. In this way, we obtain

$$(1 - l_1) \cdots (1 - l_t) \leq 0.$$ 

The reverse inequality of (2.1) is trivial. □

**Corollary 3.1.** For any $d \in \{2, 3, \ldots, \infty\}$, $\text{LS}^d$ polynomially simulates $\text{LS}^\infty$ (and, hence, $\text{LS}^\infty$ polynomially simulates polynomial calculus).

**Corollary 3.2.** $\text{LS}^\infty$ polynomially simulates the Positivstellensatz calculus.

**Remark 3.1.** Note that there is a linear lower bound [Gri01a] on the degree of the Positivstellensatz calculus refutation of the symmetric knapsack problem $m - x_1 - x_2 - \cdots - x_n = 0$ (where $m \notin \mathbb{Z}$, $3n/4 > m > n/4$). However, by the completeness
of LS [LS91, Theorem 1.4], there is an LS (i.e., of degree two) refutation of this problem.

It turns out that the converse of Lemma 3.1 is also true. In particular, this means that there is an $\overline{LS}^k$ refutation of every unsatisfiable 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

\[(l_1 + \cdots + l_i - 1)(1 - l_{i+1}) \cdots (1 - l_t) \geq 0 \quad (3.1)\]

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

\[(l_1 + \cdots + l_m + l_{m+1} - 1 - l_1 l_{m+1} - \cdots - l_m l_{m+1})(1 - l_{m+2}) \cdots (1 - l_t) \geq 0.\]

Adding $l_j l_{m+1}(1 - l_{m+2}) \cdots (1 - l_t) \geq 0$ (which easily follows from the axioms) for $j = 1, \ldots, m$, we obtain (3.1) for $i = m + 1$. □

**Corollary 3.3.** For any $d \in \{2, 3, \ldots, \infty\}$, $\overline{LS}^d$ polynomially simulates $LS^d$.

**Corollary 3.4.** There is an $LS^k$ refutation of every formula in $k$-CNF.

**Theorem 3.1.** There is an $LS^{2k}$ 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 as follows. Consider a monomial $m = uv$ of degree at least two, where $u$ and $v$ are variables (possibly coinciding). We replace $uv$ by a new variable $x_{uv}$ and add the following three inequalities to the system:

\[x_{uv} \leq u,\]
\[x_{uv} \leq v,\]
\[x_{uv} \geq u + v - 1.\]

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. We 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 variable corresponding to a monomial $m$ by $x_m$ (note that $x_m$ may be defined not uniquely, but this is not important for our argument).

According to [LS91, Theorem 1.4], there is an LS (i.e., of degree two) refutation of $S'$. For every added variable $x_m$, we replace $x_m$ by $m$ in this refutation. Thus we obtain a “proof” of $S$ using only old variables.

Now, we 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. In (2.9), we replace multiplication by a new variable $x_{u_1 u_2 \ldots u_s}$ with multiplication by the (old) variables $u_1, u_2, \ldots, u_s$. 


We also have to replace the steps (2.9) that involve multiplication of \( f \geq 0 \) by 
\((1 - x u_1 u_2 ... u_s)\). Instead, we multiply 
\( f \geq 0 \) by 
\( (1 - x) \); we also multiply 
\( f \geq 0 \) by 
\( u_1 \) and by 
\( (1 - u_2) \), \( f \geq 0 \) by 
\( u_1, u_2 \), and \( (1 - u_3) \), etc. Summing all the obtained 
inequalities, we get 
\( f(1 - x u_1 u_2 ... u_s) \geq 0 \).

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 obtain 
a valid LS\(^2k\) refutation of the system \( S \).

\[\square\]

4. Short LS + 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 LS + CP\(^2\) but has only exponential-size refutations in CP.

The set of inequalities we use is close to that used by Pudlák to prove an exponential lower bound for CP [Pud97]. Pudlák’s bound remains valid for this system. Therefore, to prove the theorem, it is sufficient to show that this set of inequalities has polynomial-size refutations in LS\(^4\) and LS + CP\(^2\).

**Clique-coloring tautologies.** Given a graph \( G \) on \( n \) vertices, we try to color it 
with \( m - 1 \) colors, 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 \( \{1, \ldots, m\} \) 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 the vertices with \( m - 1 \) colors. The assignment of a color \( \ell \) to a 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 a coloring is expressed by
\[
\sum_{\ell=1}^{m-1} r_{i\ell} \leq 1 \quad \text{(4.4)}
\]
for each \( i = 1, \ldots, n \).

To make sure that each node is colored, we write
\[
\sum_{\ell=1}^{m} r_{i\ell} \geq 1 \quad \text{(4.2)}
\]
for each \( i = 1, \ldots, n \).

Then, every label of a clique is mapped to at least one vertex of \( G \), i.e.,
\[
\sum_{i=1}^{n} q_{ki} \geq 1 \quad \text{(4.3)}
\]
for each \( k = 1, \ldots, m \).

Next, the mapping encoded by \( q_{ki} \) is injective:
\[
\sum_{k=1}^{m} q_{ki} \leq 1 \quad \text{(4.4)}
\]
for each \( i = 1, \ldots, n \).
Finally, to ensure that we indeed have a clique, we write
\[ q_{ki} + q_{k'i}j \leq p_{ij} + 1 \quad (4.5) \]
for all \( i, j, k, k' \) satisfying \( k \neq k' \) and \( 1 \leq i < j \leq n \).

**Weak clique-coloring tautologies.** Inequalities (4.1)–(4.5) are the original inequalities from [Pud97]. We add one more family of inequalities to this system while retaining the applicability of [Pud97, Corollary 7], that is, any CP refutation of the new system still involves at least \( 2^\Omega((n/\log n)^{1/3}) \) steps. Namely, we add
\[ \sum_{i=1}^{n} q_{ki} \leq 1 \quad (4.6) \]
for all \( k = 1, \ldots, m \). This inequality means that the \( k \)-th vertex of the clique is mapped to no more than one vertex of \( G \).

**The PHP interpretation of weak clique-coloring tautologies.** The condition that the \( i \)-th vertex of \( G \) is the \( k \)-th vertex of the clique and is colored with color \( \ell \) is encoded as \( q_{ki}r_{i\ell} \geq 1 \), and the condition that the \( k \)-th vertex of the clique has color \( \ell \) 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 (2.18) and (2.19) hold for \( x_{k\ell} \)'s; moreover, there are short LS\(^4\), as well as LS + CP\(^2\), derivations of these inequalities.

There is a polynomial-size CP refutation for PHP [CCT87]. In our notation (note that \( x_{k\ell} \) denotes a quadratic polynomial), such a refutation translates into an LS + 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 use the following technical statement.

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

**Proof.** The assertion concerning CP is established in the proof of Proposition 7 in [CCT87]. (It is proved by induction: adding up the two inequalities \( a_1 + \sum_{i \in F} a_i \leq 1 \) and \( a_2 + \sum_{i \in F} a_i \leq 1 \) for \( F \subset \{1 \ldots N\} - \{1, 2\} \) and applying \( a_1 + a_2 \leq 1 \), we derive \( a_1 + a_2 + \sum_{i \in F} a_i \leq 3/2 \). Rounding down of the right-hand side of the last inequality completes the proof of the induction step.)

The assertion concerning LS is implied by Lemma 1 of [Pud99], where the case \( N = 3 \) is considered, and the argument used in the proof of Proposition 1 of [Pud99].

\[ \square \]

Below we show that there is a polynomial-size derivation of (2.18)–(2.19) from (4.1)–(4.6) in LS\(^4\), as well as in LS + CP\(^2\).
Deriving PHP from weak clique-coloring tautologies. Let us derive (2.18). For each \( i \), we multiply both sides of (4.2) by \( q_{ki} \) and sum the resulting inequalities over \( i \). We obtain
\[
\sum_{i=1}^{n} \sum_{\ell=1}^{m-1} q_{ki} r_{i\ell} \geq \sum_{i=1}^{n} q_{ki}.
\]
Adding (4.3) to this inequality yields (2.18).

Proof. Multiplying both sides of (4.2) by \( q_{ki} \) and, applying the rounding rule, obtain
\[
q_{ki} + q_{k'j} + r_{i\ell} + r_{j\ell} \leq 3, \quad 1 \leq i < j \leq n, \ 1 \leq \ell \leq m-1, \ 1 \leq k \neq k' \leq m. \quad (4.7)
\]
Using \( q_{ki}^2 \leq q_{ki} \) and similar inequalities for \( q_{k'j}, r_{i\ell} \) and \( r_{j\ell} \), we rewrite (4.7) 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, we simplify this inequality to
\[
2q_{ki} r_{i\ell} + 2q_{k'j} r_{j\ell} \leq 3,
\]
and, applying the rounding rule, obtain
\[
q_{ki} r_{i\ell} + q_{k'j} r_{j\ell} \leq 1, \quad 1 \leq i < j \leq n, \quad 1 \leq \ell \leq m-1, \quad 1 \leq k \neq k' \leq m. \quad (4.8)
\]
Alternatively, we can derive (4.8) in \( S^4 \) using the following lemma.

Lemma 4.3. In \( S^4 \), 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 \( b = b^2 \), we obtain \( ab - a/2 \leq 0 \) (respectively, \( a - ab \leq 3/2 - 3/2b \)). Adding these two inequalities yields \( a/2 + 3b/2 \leq 3/2 \). The inequality multiplied by \( b \) and \( b^2 = b \) imply \( ab \leq 0 \). \( \square \)

Using \( q_{ki} r_{i\ell} \leq q_{ki} \) and (4.6), we obtain
\[
(x_{\ell}) = \sum_{i=1}^{n} q_{ki} r_{i\ell} \leq 1, \quad 1 \leq \ell \leq m-1, \quad 1 \leq k \leq m. \quad (4.9)
\]
Now, let us add (4.4) to 0 \( \leq q_{k'i} \) for each \( k'' \) different from \( k \) and \( k' \). We obtain \( q_{ki} + q_{k'i} \leq 1 \). After multiplying this inequality by \( r_{i\ell} \) and adding \( r_{i\ell} \) to the result, we obtain
\[
q_{ki} r_{i\ell} + q_{k'i} r_{i\ell} \leq 1. \quad (4.10)
\]
Relations (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 bounds we can easily derive $S \leq 1$ either in LS$^4$ or in LS + CP$^2$ by using Lemma 4.1. As $S = x_{k\ell} + x_{k'\ell}$, (2.19) holds, which proves the assertion for LS + CP$^2$.

For LS$^4$, it remains to show that all the $x_{k\ell}$’s are Boolean. Multiplying both sides of (4.9) by $x_{k\ell}$, we obtain $x_{k\ell}^2 \leq x_{k\ell}$. On the other hand, $x_{k\ell}^2 = x_{k\ell} + \sum_{i \neq j} q_{ki}r_{i\ell}q_{kj}r_{j\ell} \geq x_{k\ell}$, because $q_{ki}r_{i\ell}q_{kj}r_{j\ell} \geq 0$ can be derived in LS$^4$ for each $i$ and $j$.

5. Reasoning about integers

In this section, we explain how various versions of Lovász–Schrijver calculi can be used for reasoning about integers. The following lemma introduces the basic primitive for such a reasoning, the family of quadratic inequalities $f_d(Y) \geq 0$. The lemma shows that there are short proofs that an integer linear combination of variables is either at most $d - 1$ or at least $d$ for any integer $d$. It follows that there are short LS$^3$ (as well as LS$^3_{0/1\text{-split}}$) proofs of the symmetric knapsack problem, and that CP$^2$ with polynomially bounded coefficients can be simulated in LS$^3$ (as well as in LS$^3_{0/1\text{-split}}$).

**Lemma 5.1.** Suppose that
- $Y = \sum_{i=1}^n a_i x_i$,
- $f_d(Y) = (Y - (d - 1))(Y - d)$,
- $a_i$ are integers,
- $x_i$ are variables.

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

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

**Proof.** Without loss of generality, we rewrite $Y$ as $\sum_{i=1}^l s_i x_{l_i}$, where $s_i \in \{-1, 1\}$ and $l_i = l_j$ is allowed. We derive the inequalities $f_c(Y_i) \geq 0$ by induction on $j$ for $Y_j = \sum_{i=1}^j s_i x_i$, and for each $c \in [d - t + j, \ldots, d + t - j]$. The base ($j = 1$) is trivial. Suppose that the required inequalities are already derived for $j \leq k$. Let us derive $(Y_{k+1} - (c - 1))(Y_{k+1} - c) \geq 0$ for every $c \in [d - t + k + 1, \ldots, d + t - k - 1]$. 1. If $s_{k+1} = 1$, we multiply $f_{c-1}(Y_k) \geq 0$ by $x_{k+1}$ and $f_c(Y_k) \geq 0$ by $(1 - x_{k+1})$ and sum the obtained inequalities. The left-hand side of the resulting inequality is

\[
\begin{align*}
  f_{c-1}(Y_k)x_{k+1} &+ f_c(Y_k)(1 - x_{k+1}) \\
  &= (f_c(Y_k) + 2(Y_k - (c - 1)))x_{k+1} + f_c(Y_k)(1 - x_{k+1}) \\
  &= f_c(Y_k) + 2(Y_k - (c - 1))x_{k+1} \\
  &= Y_k^2 - (2c - 1)Y_k + c(c - 1) + 2Y_kx_{k+1} - (2c - 1)(Y_k + x_{k+1}) + c(c - 1).
\end{align*}
\]

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

Otherwise if $s_{k+1} = -1$, we multiply $f_{c+1}(Y_k) \geq 0$ by $x_{k+1}$ and $f_c(Y_k) \geq 0$ by $(1 - x_{k+1})$ and sum the obtained inequalities. The left-hand side of the resulting
The above arguments show (it suffices to substitute 0 or 1 for $r = 0$) before multiplying by $(2 - c)x_{k+1}$.

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

2. The proof in LS$_{0/1}$-split follows from the proof in LS$^3$ given above. However, before multiplying by $x_{k+1}$ and $1 - x_{k+1}$, we make the assumption $x_{k+1} = r$ for $r = 0, 1$ (thus the multiplication by constants and do not increase the degree).

The above arguments show (it suffices to substitute 0 or 1 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 the assumption $x_{k+1} = 0$, because $f_{c+1}(Y_k) \geq 0$ under the assumption $x_{k+1} = s_{k+1}$ and $f_{c-1}(Y_k) \geq 0$ under the assumption $x_{k+1} = -s_{k+1}$).

The following lemma is a general fact unrelated to integers; it says that we can substitute equalities into inequalities.

**Lemma 5.2.** Let $f$ be a polynomial in variables $v_1, \ldots, v_n$, and let $X$ and $Y$ be polynomials in variables $v_2, \ldots, v_n$. Suppose that $g(v_2, \ldots, v_n) = f(X, v_2, \ldots, v_n)$ and $h(v_2, \ldots, v_n) = f(Y, v_2, \ldots, v_n)$. If the degrees of $g$ and $h$ are 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

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

where $p_i$ and $n_i$ are polynomials in $v_2, \ldots, v_n$ consisting only of positive monomials and $c$ does not depend on $X$. Then, we multiply the equality $Y - X = 0$ by $p_i$ (i.e., multiply it by all monomials in $p_i$ and sum the results with the same coefficients as in $p_i$) and by $n_i$. The sum of the obtained two equalities is $(Y - X)(p_i - n_i) = 0$.

We multiply this equality 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

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

Now, we represent $(p_i - n_i)Y$ as a difference $p_i' - n_i'$ of two polynomials containing only positive monomials and repeat the procedure. After $d$ repetitions, we obtain the required derivation.

It follows that there are short LS$^3$ (as well as LS$_{0/1}$-split) refutations of the symmetric knapsack problem.
Theorem 5.1. There is a polynomial-size \( \text{LS}^3 \) (and \( \text{LS}_{*,0/1}\text{-split} \)) refutation of
\[
m - x_1 - x_2 - \cdots - x_n = 0, \tag{5.2}
\]
where \( m \notin \mathbb{Z} \).

Proof. Using Lemma 5.2, substitute (5.2) into \( f_m(\sum_{i=1}^n x_i) \geq 0 \) of Lemma 5.1. \( \Box \)

To show that \( \text{LS}_{*,\text{split}} \) and \( \text{LS}^3 \) polynomially simulate \( \text{CP} \), we first (equivalently) redefine \( \text{CP} \) so that it will manipulate linear inequalities of form \( A \geq a \), where \( A = a_1 x_1 + \cdots + a_n x_n \), \( x_1, \ldots, x_n \) are (integer) variables and \( a_1, \ldots, a_n, a \) are integers. The rounding rule (2.8) transforms into
\[
\sum_i a_i x_i \geq c \tag{5.3}
\]
where \( d \in \mathbb{N} ; \ d \mid a_1, \ldots, a_n \).

We define \( \text{CP} \) with polynomially bounded coefficients (cf. \([BPR95]\)) by the requirement that the absolute values of \( a_i \) are bounded by a polynomial in the length of a \( \text{CP} \) refutation.

Theorem 5.2. The following systems polynomially simulate \( \text{CP} \) with polynomially bounded coefficients:

1. \( \text{LS}_{*,\text{split}} \), 2. \( \text{LS}^3 \).

Proof. We fix a \( \text{CP} \) refutation and simulate it rule by rule. Rule (2.7) is simulated word for word as in \( \text{LS} \), so we need to simulate only the rule (5.3). By Lemma 5.1 we can derive the inequality \( f_c(A/d) \geq 0 \) for \( c = [a/d] \) in \( \text{LS}_{*,0/1}\text{-split} \) (as well as in \( \text{LS}^3 \)).

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

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

Remark 5.1. The hypotheses \( f > 0, -f \geq 0 \) used for the \( \text{LS}_{*,\text{split}} \) derivations in the proof of Theorem 5.2 are linear.

6. Short proof of Tseitin’s tautologies in \( \text{LS}^d \)

We recall the construction of Tseitin’s tautologies. Let \( G = (V, E) \) be a graph with an odd number \( n \) of vertices. To each edge \( e \in E \) we attach 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 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 equalities whose PC translation provided by Lemmas 3.1 and 3.2 is
\[
\prod_{e \in S'_c} x_e \cdot \prod_{e \notin S'_c} (1 - x_e) = 0 \tag{6.1}
\]
(for each vertex \( v \) and each subset \( S'_e \) of even cardinality of the set \( S_e \) of edges incident to \( v \)). There are \( 2d-1 \) 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.** We set \( Y_i = y_{v_1} + \cdots + y_{v_i} \), where \( v_1, \ldots, v_i \) are pairwise distinct vertices of \( G \) and \( y_e = \sum_{e \ni v_i} x_e \). For every \( c \in \{0, \ldots, i(d-1)/2\} \), we shall prove by induction that \( f_c(Y_i/2) \geq 0 \) 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 basis \((i = n)\) 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 pass from step \( i + 1 \) to step \( i \) of the refutation, we set \( Y = Y_{i+1} \) 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 \( c \in \{0, \ldots, i(d-1)/2\} \).

Fix some subset \( S \subseteq S_{v_{i+1}} \) of odd size. We put \( t = |S|, c' = c + (t-1)/2 \in [c, \ldots, c + (d-1)/2] \subseteq [0, \ldots, (i+1)(d-1)/2] \). Consider

\[
P(S) = \prod_{e \in S} x_e \prod_{e \notin S} (1-x_e).
\]

Since we have \( f_c((Y-1)/2) \geq 0 \) by the induction hypothesis, \((2.9)\) implies

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

which can be rewritten as

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

Axioms \((2.10)\) and rules \((2.9)\) directly imply

\[
yP(S) = tP(S). \tag{6.3}
\]

By Lemma 5.2, we can substitute \((6.3)\) into \((6.2)\) and obtain

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

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

\[
1 = \sum_{S \subseteq S_e, |S| \text{ is odd}} P(S).
\]

This equality is the sum of equalities \((6.1)\) for a fixed vertex \( v \), because we can write \( 1 = x + (1-x) = xy + (1-x)y + x(1-y) + (1-x)(1-y) = \cdots \) for any collection of variables \( x, y, \ldots \). \( \square \)
Remark 6.1. Sometimes, Tseitin’s tautologies are formulated in a different way. We take \( G \) with an arbitrary (not necessarily odd) number of vertices, assign weight \( w_v \in \{0, 1\} \) to each vertex \( v \), and write Boolean formulas expressing \( \bigoplus_{v \in V} x_v = w_v \). If \( \bigoplus_{v \in V} w_v = 1 \), this set of formulas is contradictory. Note that our technique applies to this kind of Tseitin’s tautologies as well.

Remark 6.2 (A. Kojevnikov). The degree of the proof of Tseitin’s tautologies can be reduced if one allows to apply the rounding rule (2.8) to higher-degree inequalities. For example, there is a short proof of sixth-degree tautologies in the “LS\(^6\)+CP\(^3\)” proof system. First, note that \( (y_e - 1)(y_e - 3)(y_e - 5) = 0 \), because this is an integer linear combination of equalities (6.1). Then, we sum 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 the Lovász–Schrijver rank

In this section we prove two lower bounds on the Lovász–Schrijver rank. There is a series of lower bounds on the Lovász–Schrijver rank in the literature (see, e.g., [CD01], [GT01] and the references therein). 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 (Section 7.2) a linear lower bound on the LS\(^+\)-rank (and a logarithmic lower bound on the LS\(^+\),\(^*\)-rank) of the symmetric knapsack problem by reducing it to a lower bound on the degree of the Positivstellensatz calculus refutation [Gri01a] (see also Theorem 8.1 below). However, this system of inequalities is not a translation of a propositional formula, and thus lower bounds for it cannot be directly used in the propositional proof theory.

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

7.1. More definitions. Below, we 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

\[
x_0 \geq 0, \quad Ax \leq x_0 b.
\]

(7.1)

Then, we denote the set of feasible points of (7.1) by \( K \) and the cone generated by all 0-1 vectors in \( K \) by \( K_f \). We 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 the \( j \)-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 \( Y \) such that

(i) \( Y = Y^T \).
The iterated operators \(N_0 \) and \(N_+ \) are defined naturally as \(N_0(K) := K \) and \(N_+(K) := N_+(N_-^{r-1}(K)) \).

It is shown in [LS91] that
\[
K_1 \subseteq N_0^{n}(K) \subseteq N_0^{n-1}(K) \subseteq \cdots \subseteq N_0^{k}(K) \subseteq \cdots \subseteq N_{(+)}^{r}(K) \subseteq K. \tag{7.2}
\]

The LS-rank (respectively, LS\(_+-\)rank) of a system of linear inequalities \(Ax \leq b\) is the minimal \(k\) in (7.2) such that \(N_k(K) = K_1\) (respectively, \(N_k^+(K) = K_1\)), where \(K = K(A, b)\), as above.

Alternative definitions of Lovász–Schrijver ranks in proof systems terms are as follows. A proof in a Lovász–Schrijver proof system is a directed acyclic graph such that its vertices correspond to the derived inequalities, and there is an edge between \(f \geq 0\) and \(g \geq 0\) if and only if \(g\) is derived from \(f\) (and, maybe, something else) in one step. Now, we drop the edges corresponding to rule (2.7). The rank of a refutation is the length of the longest path from an axiom to a 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. The LS\(_-\)- and LS\(_+-\)-ranks are defined similarly. Note that this definition can be generalized smoothly to LS\(_d\), LS\(_d^+\), LS\(_d^*\), and LS\(_d^+\_\_\).
Next, we replace the first rule of \((2.9)\) by multiplication by \(x = (x - x^2) + x^2\) providing the representation

\[
f x = \left( \sum (x_i - x_i^2) u_i x + (x - x^2) \sum v_j^2 + \left( m - \sum x_i \right) u_0 x \right) + \sum (v_j x)^2,
\]

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

At the end of the derivation in \(\text{LS}_+\) of \(\text{LS}_+\)-rank \(k_+\), we get a representation of the form

\[-1 = \sum (x_i - x_i^2) \bar{u}_i + (m - \sum x_i) \bar{u}_0 + \sum \bar{v}_j^2,
\]

where \(\deg(x_i - x_i^2) \bar{u}_i\), \(\deg(m - \sum x_i) \bar{u}_0\), and \(\deg \bar{v}_j^2 \leq 2k_+\) by recursion. This provides a Positivstellensatz calculus refutation of the knapsack problem with degree less than or equal to \(2k_+\). Applying \([\text{Gri01a}]\) (see also Theorem \(8.1\)), we conclude that \(2k_+ \geq n/2\); thus the \(\text{LS}_+\)-rank of \(K\) is at least \(n/4\).

2. We fix an \(\text{LS}_+, \ast\)-refutation of \(K\) and, arguing as above, observe that, if two derived polynomials \(f\) and \(g\)

\[
g = \sum (x_i - x_i^2) u'_i + \left( m - \sum x_i \right) u'_0 + \sum (v'_j)^2
\]

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

\[
\deg(x_i - x_i^2) u_i, \quad \deg \left( m - \sum x_i \right) u_0, \quad \deg v_j^2, \quad \deg(x_i - x_i^2) u'_i, \quad \deg \left( m - \sum x_i \right) u'_0, \quad \deg(v'_j)^2 \leq 2^k,
\]

then their product

\[
f g = \left( \sum (x_i - x_i^2) u_i g + \sum (x_i - x_i^2) u'_i \sum v_j^2 + \left( m - \sum x_i \right) u_0 g \right) + \left( m - \sum x_i \right) u'_0 \sum v_j^2 + \sum (v_j v'_j)^2
\]

can be written again in the desired form \((7.3)\) where the degrees of the polynomials are bounded by \(2^{k+1}\). This allows us to replace rule \((2.12)\). By recursion, at the end of the derivation in \(\text{LS}_+, \ast\) of \(\text{LS}_+, \ast\)-rank \(k_+\), we obtain a representation

\[-1 = \sum (x_i - x_i^2) \bar{u}_i + (m - \sum x_i) \bar{u}_0 + \sum \bar{v}_j^2
\]

with \(\deg(x_i - x_i^2) \bar{u}_i\), \(\deg(m - \sum x_i) \bar{u}_0\), and \(\deg \bar{v}_j^2 \leq 2^{k_+}\). As above, applying \([\text{Gri01a}]\) (or Theorem \(8.1\)), we conclude that \(2^{k_+} \geq n/2\) and, thereby, the \(\text{LS}_+, \ast\)-rank of \(K\) is at least \(\log_2 n - 1\).

**Remark 7.1.** Similarly to the bound in Theorem \(7.1(2)\), a logarithmic lower bound on the \(\text{LS}_+, \ast\)-rank can be obtained for the parity principle and for Tseitin’s tautologies relying on \([\text{Gri01b}]\).
7.3. The LS-rank of PHP. Let $e_k$ denote the all-1 vector of length $k$.

$Q_n \subset \mathbb{R}^n$ denotes the $n$-dimensional 0-1 hypercube, and $P_{m-1}$ is the feasible set of system (2.18)--(2.19)), i.e., 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, the LS-rank of $P_{m-1}$ is at least $m-2$.

This theorem follows from Lemma 7.2 below.

We write $x \in \bar{N}^r(m-1)$ to denote that $(1, x) \in N^r(P_{m-1})$. We also identify $\bar{N}^o(m-1)$ with $P_{m-1}$ itself.

Let $x \in \bar{N}^o(m-1)$. We define $w_{ab}^x = w_{ab}^x(x) \in Q_{m+1}$, where $1 \leq a \leq m+1$ and $1 \leq b \leq m$, as follows.

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

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

**Proof.** The statement for $r = 0$ is trivial.

Arguing by induction, we assume that, for any $x$ and any $t < r$, $x \in \bar{N}^t(m-1)$ implies $w_{ab}^x(x) \in \bar{N}^t(m)$. Without loss of generality, we suppose that $a = b = 1$.

Take a particular basis $(e_1, \ldots, e_{m(m-1)})$ in $\mathbb{R}^{m(m-1)}$ with respect to which $x$ is written as

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

(This basis only determines ordering of variables particularly convenient for our purposes.) In such a basis, $w_{11}^x(x) = (1, 0, \ldots, 0, x)$.

Assume that $x \in \bar{N}^r(m-1)$. Then there exists a matrix $Y = \begin{pmatrix} 1 & x^T \\ x & Y' \end{pmatrix} \in M(N^{r-1}(P_{m-1}))$. Consider

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

where $0_{s,q}$ denotes the 0-matrix of size $s \times q$. Let us show that $\bar{Y} \in M(N^{r-1}(P_m))$, which implies the statement of the lemma.

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

Note that if $Y_{0,j} = 0$, then $\bar{Y}e_j = 0$, as $P_{m-1} \subseteq Q_{m(m-1)}$. Hence $\bar{Y}_{0,j} = 0$ implies $\bar{Y}e_j = 0$. Thus if $\bar{Y}e_j \neq 0$, then we can take the normalization $\frac{1}{\bar{Y}_{0,j}} \bar{Y}e_j$. By the induction hypothesis applied to $x = Ye_j$, we have $\frac{1}{\bar{Y}_{0,j}} \bar{Y}e_j \in N^{r-1}(P_m)$ for all $j$ such that $\bar{Y}_{0,j} \neq 0$. Hence $\bar{Y}e_j \in N^{r-1}(P_m)$ for all $j$. 


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

**Lemma 7.2.** \( \frac{1}{m-1}e_{m(m-1)} \in \bar{N}^{m-3}(m-1) \) for \( m \geq 3 \).

**Proof.** The case of \( m = 3 \) is trivial. Denote \( x_k = \frac{1}{k} e_{k(k+1)} \).

Arguing by induction, we assume that \( x_k \in \bar{N}^{k-2}(k) \) for all \( 1 < k < m-1 \). Let \( Y \) be the matrix with columns \((1, x_{m-1}), \frac{1}{m-1}(1, w^{11}(x_{m-2})), \frac{1}{m-1}(1, w^{12}(x_{m-2})), \ldots, \frac{1}{m-1}(1, w^{m,m-1}(x_{m-2}))\). Then \( Y^T \bar{Y} \) and \( Y_{0,j} = Y_{jj} \).

By the induction hypothesis and Lemma 7.1, \( Y_{e_j} \in N^{m-4}(P_{m-1}) \) for each \( j > 0 \).

Next, observe that

\[
Y e_0 = \sum_{p=1}^{m-1} Y e_{(q,p)} \quad \text{for any } 1 \leq q \leq m \tag{7.4}
\]

(here we identify \((q, p)\) with \( j \)). Hence \( Y e_0 \in N^{m-4}(P_{m-1}) \).

Finally, from (7.4), we have \( Y(e_0 - e_{(q,p)}) = \sum_{s=1, s \neq q}^{m-1} Y e_{(q,s)} \). Thus \( Y \in M(N^{m-4}(P_{m-1})) \), which proves the statement. □

8. A linear lower bound on the “Boolean degree” of the Positivstellensatz calculus refutations of the knapsack

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

We define the Boolean degree \( B\text{deg}(t) \) of a monomial \( t \) as \( \text{deg}(t) \), i.e., as the number of its variables; then we extend the notion of \( B\text{deg} \) to polynomials as \( B\text{deg}(f) = \text{max } B\text{deg}(t_i) \), where the maximum is taken over all nonzero monomials \( t_i \) in \( f \). Thereby, we define the \( B\text{deg} \) of a derivation in PC and, subsequently, in the Positivstellensatz and Positivstellensatz calculus as the maximum \( B\text{deg} \) of all polynomials in the derivation (in the Positivstellensatz and Positivstellensatz calculus, these include the polynomials \( h_n^2 \); see the definitions in Section 2.2).

The following lemma extends the argument used in the proof of Theorem 5.1 of [IPS99] from \( \text{deg} \) to \( B\text{deg} \).

**Lemma 8.1.** Let \( f(x_1, \ldots, x_n) = c_1 x_1 + \cdots + c_n x_n - m \), where \( c_1, \ldots, c_n \in \mathbb{R}\setminus\{0\} \). If \( q \) is deducible in PC from the knapsack problem \( f = 0 \) with \( B\text{deg} \leq ((n-1)/2) \), then

\[
q = \sum_{i=1}^{n} (x_i - x_i^2)g_i + fg,
\]

where \( \text{deg}(fg) \leq B\text{deg}(q) \).

**Proof.** Similarly to Theorem 5.1 in [IPS99], the lemma is proved by induction along a (fixed) deduction in PC. Assume (8.1) and consider a polynomial \( qx_1 \) obtained
from \( q \) by multiplying it by the variable \( x_1 \). Without loss of generality, we can suppose that \( g \) is reduced. Then \( \frac{r}{x_1} = \frac{f}{x_1}x_1 \); set \( h = \frac{r}{x_1} \) and \( d = \deg(h) - 1 \). We need to verify that \( d + 2 = \deg(fh) \leq \Bdeg(qx_1) \). Taking into account that

\[
d + 1 = \deg(h) \leq \deg(g) + 1 = \deg(fg) \leq \Bdeg(q) \leq \Bdeg(qx_1),
\]

we see that the only case to be brought to a contradiction is \( \Bdeg(qx_1) = \Bdeg(q) = \deg(g) + 1 = d + 1 \).

Let us write \( g = p + x_1p_1 \), where all terms of \( g \) not containing \( x_1 \) are gathered in \( p \). Clearly, \( \deg(p) \leq \deg(g) = d \). Moreover, \( \deg(p) = d \), because \( \deg(p) < d \) implies \( d + 1 = \deg(h) \leq \Bdeg(qx_1) \leq \max(\Bdeg(x_1p), \Bdeg(x_1^2p_1)) \leq d \).

On the other hand, \( d = \Bdeg(q) - 1 \leq \lceil (n - 1)/2 \rceil - 1 \). Therefore, Lemma 5.2 from [IPS99] applied to the instance \( c_2x_2 + \cdots + c_nx_n \) of symmetric knapsack gives

\[
\deg((c_2x_2 + \cdots + c_nx_n)p) = \deg(p) + 1 = d + 1
\]

(the condition that \( p \) is reduced should be added to the formulation of Lemma 5.2 in [IPS99]).

Hence there exists a monomial \( x'^J = \prod_{j \in J} x_j \) occurring in \( p \) with a certain \( J \subseteq \{2, \ldots, n\} \), where \( |J| = d \), and there exists an \( i \in \{2, \ldots, n\} \) such that the monomial \( x_ix'^J \), being of degree \( d + 1 \), occurs in the polynomial \( (c_2x_2 + \cdots + c_nx_n)p \);

in particular, \( i \notin J \).

Because of this, the monomial \( T = x_1x'^Jx_1 \) with \( \deg(T) = d + 2 \) occurs in

\[
p' = (c_2x_2 + \cdots + c_nx_n)px_1.
\]

Furthermore, \( T \) occurs in

\[
\frac{r}{x_1} = \frac{(c_2x_2 + \cdots + c_nx_n) + (c_1x_1 - m))(p + x_1p_1)x_1},
\]

since after opening the parenthesis in the right-hand side of this expression, we obtain only \( p' \) and the two subexpressions

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

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 \( \frac{r}{x_1} = \frac{r}{x_1} \), we conclude that \( \Bdeg(qx_1) \geq \deg(\frac{r}{x_1}) = \deg(\frac{r}{x_1}) \geq d + 2 \); the achieved contradiction proves the induction hypothesis for the case of the rule of multiplication by a variable (note that the second rule in (2.2) can be replaced by 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 \( \deg(fu) \leq \Bdeg(r) \). Then, making use of (8.1), we obtain \( v + u = \frac{r}{v} \), where \( v = g + u \). The inequality

\[
\deg(v) \leq \max\{\deg(g), \deg(u)\} \leq \max\{\Bdeg(q), \Bdeg(r)\} - 1
\]

\[
\leq \lceil (n - 1)/2 \rceil - 1 \leq \lfloor n/2 \rfloor - 1
\]
enables us to apply Lemma 5.2 from [IPS99] to $v$, which gives $\deg(fv) = \deg(v) + 1 = \deg(fv)$. Therefore, $B\deg(r + q) \geq \deg(r + q) = \deg(fv)$. \hfill \Box

The next corollary extends Theorem 5.1 from [IPS99].

**Corollary 8.1.** Any PC deduction of the knapsack $f$ has $B\deg > \lfloor(n - 1)/2\rfloor$.

Now, we can formulate the following theorem extending the theorem of [Gri01a] from $\deg$ to $B\deg$. Let $\delta$ denote the step function which equals 2 outside the interval $(0, n)$ and $2k + 4$ on the intervals $(k, k + 1)$ and $(n - k - 1, n - k)$ for all integers $0 \leq k < n/2$.

**Theorem 8.1.** Any Positivstellensatz calculus refutation of the symmetric knapsack problem $f = x_1 + \cdots + x_n - m$ has $B\deg \geq \min\{\delta(m), \lfloor(n - 1)/2\rfloor + 1\}$.

Proof. We follow the line of the proof of the theorem from [Gri01a]. Suppose that, on the contrary, there is a Positivstellensatz calculus refutation with $B\deg < d := \min\{\delta(m), \lfloor(n - 1)/2\rfloor + 1\}$. First, we apply Lemma 8.1 to the deduction in PC being an ingredient of the deduction in Positivstellensatz calculus (see the definitions in 2.2). This provides a Positivstellensatz refutation of the form

$$1 + \sum_{j} h_j^2 = \sum_{i=1}^{n} (x_i - x_i^2)g_i + fg,$$

(8.2)

where $B\deg(fg) \leq \deg(h_j^2) < d$.

The rest of the proof follows the idea from [Gri01a] of applying the linear mapping $B$ to both sides of (8.2), where $B$ is defined as

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

(8.3)
on the monomials $x^I$ and extended by linearity on the rest of $\mathbb{R}[x_1, \ldots, x_n]$.

It is worth mentioning that the linear mapping $B$ is defined on the quotient algebra $\mathbb{R}[x_1, \ldots, x_n]/(x_1 - x_1^2, \ldots, x_n - x_n^2)$; thereby, the proof in [Gri01a] actually estimates $B\deg$ rather than just $\deg$.

We sketch here a streamlined version of this proof, invoking at some point the technique of the theory of association schemes (see, e.g., [BL84]).

**Lemma 8.2** (see [Gri01a, Lemma 1.3]). If $g_0 \in \mathbb{R}[x_1, \ldots, x_n]$ and $B\deg(g_0) < n$, then $B(fg_0) = 0$.

Proof. We have $B(fX^I) = 0$ for all the monomials $X^I$ of $g_0$, because $B$ satisfies the recurrence $(n - k)B_{k+1} = (m - k)B_k$. \hfill \Box

On (the coefficient space of) $\mathbb{R}[x_1, \ldots, x_n]/(x_1 - x_1^2, \ldots, x_n - x_n^2)$, we introduce a quadratic form $Q$ by setting $Q(x^I, x^J) = B(x^{I+J})$ and denote the restriction of $Q$ to the subspace of polynomials of degree at most $\ell$ by $Q_\ell$. In what follows we take the liberty of denoting the matrix of $Q_\ell$ also by $Q_\ell$. Interestingly, $Q$ is known as the moment matrix of $B$ (see, e.g., [Las01], [Lau01]). The “if” part of the following statement is Lemma 1.4 from [Gri01a]. The “only if” part demonstrates that the bound of Theorem 8.1 cannot be improved, at least along these lines.
Lemma 8.3 (see [Gri01a, Lemma 1.4]). The form $Q_\ell$ is positive semidefinite if and only if $\ell - 1 < m < n - \ell + 1$ and $\ell \leq \lfloor n/2 \rfloor$.

A proof for this lemma is given later on, and this is where the promised streamlining occurs. Below, we 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, because $B(fg) = 0$ due to Lemma 8.2 and $B((x_i - x_i^2)g_i) = B(x_ig_i) - B(x_i^2g_i) = 0$. The left-hand side then amounts to $C = 1 + \sum_j h_j^T Q h_j$, where $h_j$ stands for the vector of coefficients in the polynomial $h$. As the maximal degree of $h_j$ cannot be larger than the maximal degree of the right-hand side of (8.2), we have $h_j^T Q h_j = h_j^T Q t h_j$, where $\ell$ falls into the range covered by Lemma 8.3. Hence $h_j^T Q h_j \geq 0$ and thus $C > 0$, which gives the desired contradiction. \hfill \Box

Proof of Lemma 8.3. Let us order the subsets of \{1, \ldots, n\} by their sizes (i.e., by the degrees of the corresponding monomials), using an arbitrary (but fixed) order within each size, and accordingly order the rows and columns of $Q_\ell$. Let $Q_{\ell \ell}$ denote the principal submatrix of $Q_\ell$ corresponding to the $\ell$-element subsets of \{1, \ldots, n\} (so that $Q_{\ell \ell}$ occupies the south-east corner of $Q_\ell$).

We show that $Q_\ell$ has at least $T - \binom{n}{\ell}$ zero eigenvalues, where $T = \sum_{i=0}^{\ell} \binom{n}{i}$. To this end, let us exhibit a basis for a subspace of such a dimension in the nullspace $\ker Q_\ell$. The coefficient vectors of $f x^I$ lie in $\ker Q_\ell$ as long as $|I| < \ell$, as can be shown by applying Lemma 8.2 to $B(f x^I)$, where $|I| \leq \ell$. These $f x^I$ form the desired basis, as they are linearly independent. This can be seen by building a basis for the subspace they generate, adding first the vector of coefficients of $f x^I$, where $I$ is the greatest (with respect to 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 form $D x^I$ with $D \in \mathbb{R} - \{0\}$ appears in $f x^I$, which implies that the dimension increases and proves the assertion.

To this point, we followed [Gri01a] quite closely. Now comes the first shortcut. Namely, we claim that the positive definiteness of $Q_{\ell \ell}$ implies the positive semidefiniteness of $Q_\ell$. Indeed, let $\mu_1 \geq \cdots \geq \mu_{\binom{n}{\ell}}$ (respectively, $\lambda_1 \geq \cdots \geq \lambda_{\ell}$) be the sequence of the eigenvalues of $Q_{\ell \ell}$ (respectively, of $Q_\ell$). It is well-known (the result is 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 $1 \leq i \leq \binom{n}{\ell}$ (see, e.g., [H90, Theorem 4.3.15] or [Lüt96, 5.3.1(11)]). Therefore, the first $\binom{n}{\ell}$ eigenvalues of $Q_\ell$ are not smaller than the smallest eigenvalue of $Q_{\ell \ell}$; thus they are positive, as required.

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

To complete the proof for all 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 a few definitions first. By \( M = M_\ell(\mathbb{C}) \), we denote the algebra of the \((\ell_\prime \times \ell_\prime)\) 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 \( C_M(S) = \{ c \in M : cs = sc \text{ for any } s \in S \} \). Note that \( C_M(S) \) is a subalgebra of \( M \).

Let \( \rho \subseteq M \) be the permutation representation of the symmetric group \( S_n \) acting on the subsets of size \( \ell \). That is, each \( \pi \in S_n \) is taken to the permutation \( \pi' \) in \( S_\ell(\mathbb{C}) \) defined by \( \pi'(t_1, \ldots, t_\ell) = \{ \pi(t_1), \ldots, \pi(t_\ell) \} \), and then turned into a 0-1 matrix \( \rho(\pi) \) by setting \( \rho_{i,i'}(\pi) = 1 \) and \( \rho_{i,j}(\pi) = 0 \) for the remaining pairs of indices \( (I,J) \), \( J \neq \pi'(I) \). Then \( Q_{\ell J} \in C_M(\rho) \). The algebra \( C_M(\rho) \) is known under many different names (see [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 by the condition \( (A_i)_{i,i'} = 1 \) if \( |I - J| = i \) form its basis \((0 \leq i \leq \ell)\).

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 \( \rho \) into a direct sum of \( \ell + 1 \) irreducible representations. By 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 to 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, since \( Q_{\ell J} = \sum_{i=0}^{\ell} B_{\ell+1} A_i \) (here \( B \) is as in (8.3)), the set of eigenvalues of \( Q_{\ell J} \) equals the set of eigenvalues of the \((\ell + 1) \times (\ell + 1)\) diagonal matrix \( \sum_{i=0}^{\ell} B_{\ell+1} \text{diag}(p_i(0), p_i(1), \ldots, p_i(\ell)) \).

To summarize, we state the following lemma, which uses the expressions for \( p_i(j) \) from the corollary to Theorem 3.2.9 in [BI84].

**Lemma 8.4.** The set of eigenvalues of \( Q_{\ell J} \) is given by

\[
s_j = \sum_{i=0}^{\ell} B_{\ell+1} p_i(j)
\]

where

\[
p_i(j) = \binom{\ell}{i} \binom{n-\ell}{j-i} \frac{\binom{\ell}{i} \binom{n-\ell}{j-i}}{\binom{n}{j}} 3F_2 \left( \begin{array}{c} -i, -j, -n-1+j ; 1 \\ -\ell, -n+\ell \end{array} \right)
\]

Here \( _rF_s \left( a_1, \ldots, a_r; b_1, \ldots, b_s; y \right) = \sum_{i \geq 0} \frac{(a_1)_{i} \cdots (a_r)_{i}}{(b_1)_{i} \cdots (b_s)_{i}} \frac{y^i}{i!} \) denotes the hypergeometric series and \((a)_t = a(a+1) \cdots (a+t-1); (a)_0 = 1 \).

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

\[
\frac{s_j}{B\ell} = \sum_{i \geq 0} \binom{\ell}{i} \binom{m-\ell}{i} \frac{\binom{\ell}{i} \binom{n-\ell}{j-i}}{\binom{n}{j}} 3F_2 \left( \begin{array}{c} -i, -j, -n-1+j ; 1 \\ -\ell, -n+\ell \end{array} \right) > 0 \quad \text{for} \quad 0 \leq j \leq \ell.
\]
Changing the order of summation, we obtain
\[
\frac{s_j}{B_t} = \sum_{i \geq 0} c_i \sum_{i \geq 0} (-i)_t \left(\begin{array}{c} \ell \\ i \end{array}\right) \frac{(m - \ell)}{i} \\
= \sum_{i \geq 0} c_i (-t)_t \left(\begin{array}{c} \ell \\ t \end{array}\right) \frac{m - \ell}{t} \frac{2F_1 (-m + \ell + t; t - \ell; 1)}{t + 1} \\
= \sum_{i \geq 0} c_i (-t)_t \left(\begin{array}{c} \ell \\ t \end{array}\right) \frac{m - \ell}{t} \frac{\Gamma(-t + 1 + m) t!}{\Gamma(1 + m - \ell)!} 
\]
for \( c_t = \binom{-j}t \binom{-n+j-1}{t} \). The equality in the second row is obtained by applying the procedure described in [PWZ96, Chapter 3] that identifies hypergeometric series to the inner sum in the first row. Note that the first nonvanishing term of this sum is the \( t \)-th one (i.e., with \( i = t \)), and it equals \( (-t)_t \binom{m - \ell}{t} \).

The equality in the third row is derived using the Gauss identity (see [PWZ96, Sec. 3.5]).

Next, we again use the above-mentioned procedure from [PWZ96, Chapter 3] to identify the sum \( \frac{s_j}{B_t} = \sum_{\ell \geq 0} \frac{f_{\ell+1}}{\Gamma(1+m-\ell)!} \) as a hypergeometric series. Factoring out the constant term \( \frac{1}{\Gamma(1+m-\ell)!} \), we see that 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
\[
\frac{f_{t+1}}{f_t} = \frac{(t-j)(t-n+j-1)(-t+m-\ell)\Gamma(m-t)}{(t-n+j)(t+1)\Gamma(m-t+1)} \\
= \frac{(t-j)(t-n+j-1)(t-m+\ell)}{(t-n+j)(t+1)(t-m)};
\]
the latter equality is obtained by using the identity \( \Gamma(x+1)/\Gamma(x) = x \). This readily identifies the series, and we obtain
\[
\frac{s_j}{B_t} \frac{\Gamma(1+m-\ell)}{\Gamma(1+m)} \ell! = \sum_{\ell} \binom{n-m+\ell}{-n+j-1} \frac{\Gamma(-m+\ell, -n+j-1, -j; 1)}{(n+\ell)!} = \binom{n+m}{j} \binom{-j}{j} \frac{(n+j+1)}{(n+\ell)!} \binom{m}{j} 
\]
Here the Saalschütz identity (see [PWZ96, Sec. 3.5]) is applied to the second expression for \( j > 0 \) to obtain the rightmost expression, which is also valid for \( j = 0 \) by the definition of ascending factorial.

We should determine the sign of \( R_j = \frac{(-n+m)}{(-n+j)} \), as the remaining multiplicative term is positive. Note that the factors of the denominator are always negative. On the other hand, all the factors in the numerator are 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, we conclude that if \( m > n - \ell + 1 \), then there exists a \( j \) such that \( R_j < 0 \). Finally, we observe that if \( m < \ell - 1 \), then \( B_t < 0 \). Thus if the condition of Lemma 8.3 on \( m \) is not satisfied, then \( Q_E \) has a negative eigenvalue. This implies that \( Q_E \) is not positive semidefinite, which completes the proof of Lemma 8.3 and, thereby, of Theorem 8.1. \( \Box \)
9. An exponential lower bound on the size of Positivstellensatz calculus and 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 Positivstellensatz calculus and static LS refutations of the symmetric knapsack. We follow the notation introduced in Sections 2.5 and 8. The Boolean degree of a static LS (LS+) refutation is the maximum Boolean degree of the polynomials $u_{i,t}$ defined in Section 2.5.

Let us fix for a while a certain (threshold) $d$.

**Lemma 9.1.** Let $M$ denote the number of monomials of Boolean degrees at least $d$ that occur in a Positivstellensatz calculus refutation of a system of equations $S$. Then there is a variable $x$ such that the result of substituting $x = 0$ in this refutation is a valid Positivstellensatz calculus refutation of the system $S|_{x=0}$ and contains at most $M(1 - d/n)$ (nonzero) monomials of Boolean degrees at least $d$.

**Proof.** Since the refutation contains at least $M$ monomials of Boolean degrees $d$ or more, there is a variable $x$ occurring in at least $Md/n$ of these monomials. Therefore, at least $Md/n$ monomials vanish after the substitution. □

**Lemma 9.2.** Let $M$ denote the number of $u_{i,t}$'s in (2.17) 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 $x = a$ in (2.17) contains at most $M(1 - d/(2n))$ nonzero polynomials $u_{i,t}|_{x=a}$ of Boolean degrees at least $d$. (Note that by substituting a value $a$ for $x$ in (2.17) we obtain a valid static LS+ refutation of the system $S|_{x=a}$.)

**Proof.** Since there are at least $Md$ occurrences of $x_i$ or $1 - x_i$ in the polynomials $u_{i,t}$ of Boolean degrees at least $d$, there is a variable $x$ such that either $x_i$ or $1 - x_i$ occurs in at least $Md/(2n)$ of these polynomials. Therefore, after substituting the appropriate value for $x$, at least $Md/(2n)$ polynomials $u_{i,t}$ vanish from (2.17). □

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

$$
\begin{align*}
  f_0 &= x_1 + \cdots + x_n - m, \\
  f_i &= x_i - x_i^2 \quad (1 \leq i \leq n), \\
  f_i &= (s'_i)^2 \quad (n + 1 \leq i \leq n')
\end{align*}
$$

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

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

(9.1)

where

$$
\begin{align*}
  g_{i,t} &= \gamma_{i,t} \prod_{k \in G_{i,t}^+} x_k \cdot \prod_{k \in G_{i,t}^-} (1 - x_k), \\
  t_j &= \tau_j \prod_{k \in T_j^+} x_k \cdot \prod_{k \in T_j^-} (1 - x_k)
\end{align*}
$$
for appropriate multisets $G^{-}_{i,l}$, $G^{+}_{i,l}$, $T^{-}_{j}$, and $T^{+}_{j}$, a positive real $\tau_j$, and an arbitrary real $\gamma_{i,l}$.

**Lemma 9.3.** If $n/4 < m < 3n/4$, then the Boolean degree $D$ of any static $\text{LS}_+$ refutation of the symmetric knapsack problem is at least $n/4$.

**Proof.** Let us replace each occurrence of $x_i$ in $t_j$ by $f_i + x_i^2$ and each occurrence of $1-x_i$ by $f_i + (1-x_i)^2$, expand the factors obtained, 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, we obtain 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 $\text{Bdeg}(g_i), \text{Bdeg}(h_j^2) \leq D$ and, thereby a Positivstellensatz (and Positivstellensatz calculus) refutation of the symmetric knapsack of Boolean degree at most $D + 2$. Theorem 8.1 implies that $D \geq [(n-1)/2] - 1 \geq n/4$. \(\square\)

**Theorem 9.1.** For $m = (2n + 1)/4$, the number of monomials in any Positivstellensatz calculus refutation of (5.2) is $\exp(\Omega(n))$ (hence the size of such a refutation is exponential).

**Proof.** Now, we set $d = \lfloor n/8 \rfloor$ and apply Lemma 9.1 repeatedly $\kappa = \lfloor n/4 \rfloor$ times. The result of all the substitutions contains $n - \kappa$ variables. We denote the result of the substitutions applied to $f_0$ (where $f_0 = x_1 + \cdots + x_n - m$) by $f_0'$. Note that $f_0'$ is again an instance of the knapsack problem. Therefore, we can apply Theorem 8.1 to our refutation of $f_0'$. Since the free term in $f_0'$ is the same as in $f$ and falls into the interval $(\lfloor (n - \kappa)/4 \rfloor, 3\lfloor (n - \kappa)/4 \rfloor)$, the degree of this new refutation is at least $(n - \kappa)/4 > d$.

Let $M_0$ denote the number of monomials of the degree at least $d$ in the original refutation. By Lemma 9.1, the new refutation contains at most $M_0(1 - d/n)^\kappa \leq M_0(1 - 1/8)^{n/4}$ nonzero monomials of degrees at least $d$. Since this new refutation contains at least one monomial of such a degree, we have $M_0(1 - 1/8)^{n/4} \geq 1$, i.e., $M_0 \geq (8/7)^{n/4}$, which proves the theorem. \(\square\)

**Theorem 9.2.** For $m = (2n + 1)/4$, the number of $g_i$’s and $t_j$’s in (9.1) is $\exp(\Omega(n))$. Hence, any static $\text{LS}_+$ refutation of (5.2) for $m = (2n + 1)/4$ must have size $\exp(\Omega(n))$.

**Proof.** Now, we set $d = \lfloor n/8 \rfloor$ and apply Lemma 9.2 repeatedly $\kappa = \lfloor n/4 \rfloor$ times. We denote the result of all the substitutions in (9.1) by (9.1’); it contains $n - \kappa$ variables. Let $u_{i,l}'$ denote the polynomial obtained from $u_{i,l}$, and let $f_0''$ denote the result of substitutions applied to $f_0$. Note that, after all substitutions, we obtain again an instance of the knapsack problem. Since the free term $m'$ of $f_0''$ falls in the interval $[m - \kappa, m]$ and $(n - \kappa)/4 < m - \kappa < m < 3(n - \kappa)/4$, we can apply Lemma 9.3 to (9.1’). Thus, the degree of (9.1’) is at least $(n - \kappa)/4 > d$.

Let $M_0$ denote the number of $u_{i,l}$’s of degrees at least $d$ in (9.1). By Lemma 9.2, refutation (9.1’) contains at most $M_0(1 - d/(2n))^\kappa \leq M_0(1 - 1/16)^{n/4}$ nonzero
polynomials $u_{i,l}'$ of degrees at least $d$. Since there is at least one polynomial $u_{i,l}'$ of such a 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 tree-like $LS_+$ (or $LS_\infty$) refutation of (5.2) for $m = (2n + 1)/4$ must have size $\exp(\Omega(n))$.

**Proof.** The size of such a tree-like refutation (even the number 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 Theorems 9.1 and 9.2 and Corollary 9.1 can be changed to any noninteger value between $\lceil n/4 \rceil$ and $\lfloor 3n/4 \rfloor$ by a choice of 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) $LS$ (see 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 for a static semialgebraic proof system for tautologies in DNF. 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.

3. Suggest a candidate for a lower bound in $LS^d$ for an (arbitrarily large) constant $d$.

4. How precise is the logarithmic lower bound on the $LS_\ast$-rank for the knapsack problem from Section 7.2?

5. Can we relax the condition on the polynomial growth of the coefficients in Theorem 5.2?

6. Is it possible to simulate $LS$ (or static $LS_\infty$) by means of a suitable version of CP (e.g., by the R(CP) introduced in [Kra98])? In other words, does there exist a converse to Theorem 5.2?

**Acknowledgments.** The authors are grateful to Arist Kojevnikov, Akihiro Mune-masa, Alexander Razborov, and Hans van Maaren for useful discussions.

The research described in this publication was made possible in part by Award No. RM1-2409-ST-02 of the U. S. Civilian Research & Development Foundation for the Independent States of the Former Soviet Union (CRDF).

**References**


D. G.: IRMAR, Université de Rennes, Campus de Beaulieu, 35042 Rennes, Cedex, France.

E-mail address: dima@maths.univ-rennes1.fr
URL: http://www.maths.univ-rennes1.fr/~dima/

E. H.: Steklov Institute of Mathematics at St. Petersburg, 27 Fontanka, 191011 St. Petersburg, Russia. Work partially done while visiting Delft University of Technology.

E-mail address: hirsch@pdmi.ras.ru
URL: http://logic.pdmi.ras.ru/~hirsch/

D. P.: Department of Technical Mathematics and Informatics, Faculty ITS, Delft University of Technology, Mekelweg 4, 2628 CD Delft, The Netherlands, and Theoretische Informatik, Fachbereich Biologie und Informatik, J. W. Goethe-Universität, Robert-Mayer Str. 11-15, Postfach 11 19 32, 60054 Frankfurt(Main), Germany.

E-mail address: dima@thi.informatik.uni-frankfurt.de
URL: http://www.thi.informatik.uni-frankfurt.de/~dima/