Proof Complexity Meets Algebra*

Albert Atserias[1] and Joanna Ochremiak[2]

1 **Universitat Politècnica de Catalunya, Barcelona, Spain**
`atserias@cs.upc.edu`
2 **Université Paris Diderot – Paris 7, Paris, France**
`joanna.ochremiak@gmail.com`

Abstract

We analyse how the standard reductions between constraint satisfaction problems affect their proof complexity. We show that, for the most studied propositional and semi-algebraic proof systems, the classical constructions of pp-interpretability, homomorphic equivalence and addition of constants to a core preserve the proof complexity of the CSP. As a result, for those proof systems, the classes of constraint languages for which small unsatisfiability certificates exist can be characterised algebraically. We illustrate our results by a gap theorem saying that a constraint language either has resolution refutations of bounded width, or does not have bounded-depth Frege refutations of subexponential size. The former holds exactly for the widely studied class of constraint languages of bounded width. This class is also known to coincide with the class of languages with Sums-of-Squares refutations of sublinear degree, a fact for which we provide an alternative proof. We hence ask for the existence of a natural proof system with good behaviour with respect to reductions and simultaneously small size refutations beyond bounded width. We give an example of such a proof system by showing that bounded-degree Lovász-Schrijver satisfies both requirements.

1998 ACM Subject Classification F.1.3 Complexity Measures and Classes, F.4.1 Mathematical Logic, F.2.2 Nonnumerical Algorithms and Problems

Keywords and phrases Constraint Satisfaction Problem, Proof Complexity, Reductions, Gap Theorems

Digital Object Identifier 10.4230/LIPIcs.ICALP.2017.110

1 Introduction

The notion of efficient reduction is at the heart of all subareas of computational complexity. However, in some subareas such as proof complexity, even though the concept exists, it is much less developed. The study of the lengths of proofs has developed mostly by studying combinatorial statements, each somewhat in isolation. There is little theory, for instance, explaining why the best studied families of propositional tautologies are encodings of the pigeonhole principle or those derived from systems of linear equations over the 2-element field. Whether there is any connection between the two is an even less explored mystery.

Luckily this fact is subject to revision, especially if proof complexity exports its methods to the study of problems beyond universal combinatorial statements. Consider the NP-hard optimization problem called MAX-CUT. The objective is to find a partition of the vertices

* Both authors partially funded by European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme, grant agreement ERC-2014-CoG 648276 (AUTAR). First author partially funded by MINECO through TIN2013-48031-C4-1-P (TASSAT2). Part of this work was done while the authors were in residence at the Simons Institute for the Theory of Computing.

44th International Colloquium on Automata, Languages, and Programming (ICALP 2017).
Editors: Ioannis Chatzigiannakis, Piotr Indyk, Fabian Kuhn, and Anca Muscholl;
Article No. 110; pp. 110:1–110:14

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

of a given graph which maximizes the number of edges that cross the partition. The best efficient approximation algorithm known for this problem relies on certifying a bound on the optimum of its semidefinite programming relaxation. Once the certificate for the relaxation is in place, a rounding procedure gives an approximate integral solution: at worst 87% of the optimum in this case [12].

In the example of the previous paragraph, the problem that is subject to proof complexity analysis is that of certifying a bound on the optimum of an arbitrary MAX-CUT instance. The celebrated Unique Games Conjecture (UGC) can be understood as a successful approach to explaining why current algorithms and proof complexity analyses stop being successful where they do, and reductions play an important role there [26]. One of the interesting open problems in this area is whether the analysis of the Sums-of-Squares semidefinite programming hierarchy of proof systems (SOS) could be used to improve over the 87% approximation ratio for MAX-CUT. Any improvement on this would improve the approximation status of all problems that reduce to it, and refute the UGC [16]. For the constraint satisfaction problem, in which all constraints must be satisfied, the analogue question was resolved very recently also by exploiting the theory of reducibility: in that arena, low-degree SOS unsatisfiability proofs exist only for problems of *bounded width* [11, 25].

The goal of this paper is to develop the standard theory of reductions between constraint satisfaction problems in a way that it applies to many of the proof systems from the literature, including but not limited to SOS. Doing this requires a good amount of tedious work, but at the same time has some surprises to offer that we discuss next.

Consider a constraint language B given by a finite domain of values, and relations over that domain. The instances of the constraint satisfaction problem (CSP) over B are given by a set of variables and a set of constraints, each of which binds some tuple of the variables to take values in one of the relations of B. The literature on CSPs has focussed on three different types of conditions that, if met by two constraint languages, give a reduction from the CSP of one language to the CSP of the other. These conditions are a) *pp-interpretability*, b) *homomorphic equivalence*, and c) *addition of constants to the core* (see [9, 5]). What makes these three types of reductions important is that they correspond to classical algebraic constructions at the level of the *algebras of polymorphisms* of the constraint languages. Indeed, pp-interpretations correspond to taking homomorphic images, subalgebras and powers. The other two types of reductions put together ensure that the algebra of the constraint language is idempotent. Thus, for any fixed algorithm, heuristic, or method $\mathcal{M}$ for deciding the satisfiability of CSPs, if the class of constraint languages that are solvable by $\mathcal{M}$ is closed under these notions of reducibility, then this class admits a purely algebraic characterization in terms of identities.

Our first result is that, for most proof systems P in the literature, each of these methods of reduction preserves the proof complexity of the problem with respect to proofs in P. Technically, what this means is that if B is obtained from B' by a finite number of constructions a), b) and c), then, for an appropriate fixed encoding scheme of the statement that an instance is unsatisfiable, efficient proofs of unsatisfiability in P for instances of B' translate into efficient proofs of unsatisfiability in P for instances of B. The propositional proof systems for which we prove this include DNF-resolution with terms of bounded size, bounded-depth Frege, and Frege. The semi-algebraic proof systems for which we prove it include Sherali-Adams, Lasserre/SOS, and Lovász-Schrijver of bounded and unbounded degree.

Our second main result is an application: we obtain unconditional gap theorems for the proof complexity of CSPs. Building on the bounded-width theorem for CSPs [4, 8], the

known correspondance between local consistency algorithms, existential pebble games and bounded width resolution [17, 2], the lower bounds for propositional and semi-algebraic proof systems [1, 19, 6, 7, 13, 10], and a modest amount of additional work to fill in the gaps, we prove the following strong gap theorem:

▶ **Theorem 1.** *Let B be a finite constraint language. Then exactly one of the following holds:*

1. *B has resolution refutations of bounded width and hence polynomial size,*
2. *B has neither Frege refutations of bounded depth and subexponential size, nor Lasserre/SOS refutations of sublinear degree.*

Moreover, case *1.* in Theorem 1 happens precisely if B has bounded width. As noted earlier, the collapse of Lasserre/SOS to bounded width was already known; here we give a different proof. As an immediate corollary we get that resolution is also captured by algebra, despite the fact that our methods fall short to prove that it is closed under reductions.

▶ **Corollary 2.** *Let B be a finite constraint language. Then B has resolution refutations of subexponential size if and only if B has resolution refutations of polynomial size, if and only if B has resolution refutations of bounded width.*

Our third main result is about proof systems that operate with polynomial inequalities beyond Lasserre/SOS. Theorem 1 raises a question of identifying a proof system that can surpass bounded width. In other words: is there a natural proof system for which the class of languages that have efficient unsatisfiability proofs is closed under the standard reducibility methods for CSPs, and that at the same time has efficient unsatisfiability proofs beyond bounded width? By the bounded-width theorem for CSPs, one way, and indeed the only way, of surpassing bounded width is by having efficient proofs of unsatisfiability for systems of linear equations over some finite Abelian group. In view of the limitations of certain semi-algebraic proof systems that are imposed by Theorem 1, it is perhaps a surprise that, as we show, bounded degree Lovász-Schrijver (LS) is such a proof system.

▶ **Theorem 3.** *Unsatisfiable systems of linear equations over the 2-element group have LS refutations of bounded degree and polynomial size.*

Proving this amounts to showing that Gaussian elimination over $\mathbb{Z}_2$ can be simulated by reasoning with low-degree polynomial inequalities over $\mathbb{R}$. The proof of this counter-intuitive fact relies on earlier work in proof complexity for reasoning about gaps of the type $(-\infty, c] \cup [c+1, +\infty)$, for $c \in \mathbb{Z}$, through quadratic polynomial inequalities [15].

We want to close by pointing out that another proof system that can efficiently solve CSPs of bounded width, and that at the same time goes beyond bounded width, is the proof system that operates with ordered binary decision diagrams from [3]. Although it looks unlikely that our methods could be used for this proof system, whether it is closed under the standard CSP reducibilities is something that was not checked, neither in [3], nor here.

2 Preliminaries

2.1 Propositional logic and proofs

A literal is a variable X or the negation of a variable $\overline{X}$. We think of $\wedge$ and $\vee$ as commutative, associative and idempotent. Negation is allowed only on literals, so formulas are in negation normal form. If A is a formula, we define its complement $\overline{A}$ by exchanging $\vee$ and $\wedge$ and negating literals. The size of a formula A is the number of symbols in it.

We work with a Tait-style proof system for propositional logic that we call *Frege*. Its rules are *axiom*, *cut*, *introduction of conjunction*, and *weakening*:

$$\frac{}{A \vee \overline{A}} \qquad \frac{C \vee A \quad D \vee \overline{A}}{C \vee D} \qquad \frac{C \vee A \quad D \vee B}{C \vee D \vee (A \wedge B)} \qquad \frac{C}{C \vee A}. \tag{1}$$

In these rules, C and D could be the empty formula 0 or its complement 1, and A is a formula. A *Frege proof* of A from a set of formulas H is a sequence of formulas ending with A each of which is either in H, or follows from previous formulas in the sequence by one of the inference rules. The proof is called a *refutation* of H if the last formula is the empty formula 0. As a proof system, Frege is sound and implicationally complete. If $\mathcal{C}$ is a class of formulas, a $\mathcal{C}$-Frege proof is one that has all its formulas in the class $\mathcal{C}$. The size of a proof is the sum of the sizes of the formulas in it.

A k-term is a conjunction of at most k literals and a k-clause is a disjunction of at most k literals. A k-DNF is a disjunction of k-terms and a k-CNF is a conjunction of k-clauses. We define the classes of $\Sigma_{t,k}$- and $\Pi_{t,k}$-formulas inductively. For $t = 1$, these are just the classes of k-DNF and k-CNF formulas, respectively. For $t \geq 2$, a formula is $\Sigma_{t,k}$ if it is a disjunction of $\Pi_{t-1,k}$-formulas, and it is $\Pi_{t,k}$ if it is a conjunction of $\Sigma_{t-1,k}$-formulas. We write Σ_t and Π_t for $\Sigma_{t,1}$ and $\Pi_{t,1}$, respectively. The t and the k in $\Sigma_{t,k}$ and $\Pi_{t,k}$ are called the *depth* and the *bottom fan-in*, respectively.

Observe that Σ_1-Frege is essentially resolution, and $\Sigma_{1,k}$-Frege is the system R(k) introduced by Krajicek [18], also known as Res(k), k-DNF resolution, and k-DNF Frege. This proof system is important for us because it is the weakest for which we can prove closure under reductions. It is a sound and implicationally complete proof system for proving k-DNFs from k-DNFs. A resolution proof has *width* k if all clauses in it are k-clauses.

In this paper, we use the expression *Frege proof of depth d and bottom fan-in k* to mean a $\Sigma_{d,k}$-Frege proof. *Bounded-depth Frege* means Σ_d-Frege for some d. This coincides with other definitions in the literature. Again, Frege of depth d and bottom fan-in k, as a proof system, is sound and implicationally complete for proving $\Sigma_{d,k}$-formulas from $\Sigma_{d,k}$-formulas.

2.2 Polynomials and algebraic proofs

Let $X_1, \ldots, X_n$ be n algebraic commuting variables ranging over $\mathbb{R}$. We define proof systems for inequalities $P \geq 0$, where P is a polynomial in $\mathbb{R}[X_1, \ldots, X_n]$. We think of equations $P = 0$ as two inequalities $P \geq 0$ and $-P \geq 0$. For our purposes it will suffice to have the variables range over $\{0, 1\}$. Accordingly, we introduce *twin* variables $\bar{X}_1, \ldots, \bar{X}_n$ with the meaning that $\bar{X}_i = 1 - X_i$ for $i = 1, \ldots, n$.

In all proof systems, the following axioms will be imposed on these variables:

$$X_i^2 - X_i = 0 \qquad \bar{X}_i^2 - \bar{X}_i = 0 \qquad X_i + \bar{X}_i - 1 = 0, \tag{2}$$

$$X_i \geq 0 \qquad \bar{X}_i \geq 0 \qquad 1 - X_i \geq 0 \qquad 1 - \bar{X}_i \geq 0 \qquad 1 \geq 0. \tag{3}$$

Observe that $X_i\bar{X}_i = 0$ follows from these axioms: multiply $X_i + \bar{X}_i - 1 = 0$ by X_i and use $X_i^2 - X_i = 0$. This sort of reasoning is captured by the proof systems we are about to define.

Let P and Q denote polynomials. In addition to the axioms in (2), we consider rules of inference for deriving polynomial inequalities: from $P \geq 0$ and $Q \geq 0$, derive $P + Q \geq 0$, and from $P \geq 0$ and $Q \geq 0$ derive $PQ \geq 0$. Also we allow square inequalities for free: $P^2 \geq 0$. These are called *addition*, *multiplication* and *positivity of squares*.

If H denotes a system of polynomial inequalities $P_1 \geq 0, \ldots, P_r \geq 0$, a *semi-algebraic proof* of $P \geq 0$ from H is a sequence of polynomial inequalities ending with $P \geq 0$ each of

which is either in H, or is an axiom inequality from (2) and (3), or follows from previous inequalities in the sequence by one of the inference rules. The semi-algebraic proof is called a *refutation* of H if the last inequality is $-1 \geq 0$. As a proof system for inequalities evaluated over $\{0,1\}$, this is sound and implicationally complete (we note, however, that without some restrictions on the domain of evaluation, completeness is not true).

The main complexity measures for semi-algebraic proofs are size and degree. Polynomials are typically represented as explicit sums of monomials, or as algebraic formulas or circuits. Using formulas or circuits as representations requires some additional technicalities that we want to avoid (see [22, 14]). For all our examples below, we use the representation of an explicit sum of monomials; its size includes the sizes of the coefficients.

The proofs in the *Lovász-Schrijver* (LS) proof system are semi-algebraic proofs for which the following restrictions apply: 1) the polynomial Q in the multiplication rule is either a positive real or a variable, and 2) the positivity-of-squares is not allowed. When it is allowed, the system is called *Positive Semidefinite Lovász-Schrijver* and is denoted LS$^+$. Originally the Lovász-Schrijver proof system was defined to manipulate quadratic polynomials only (see [21, 23]). We follow [15] and consider the extension to arbitrary degree. For LS- and LS$^+$-proofs, an important complexity measure originally studied by Lovász and Schrijver is its *rank*, which is the maximum nesting depth of multiplication by a variable in the proof. Note that, due to possible cancellations, the degree of an LS-proof could in principle be much smaller than its rank.

We define two additional proof systems called *Sherali-Adams* (SA) and *Lasserre/Sums-of-Squares* (SOS). One way to do that is by thinking of them as subsystems LS and LS$^+$ proof systems, respectively, with the additional restriction that all applications of the multiplication rule must *precede* all applications of the addition rule. Due to the structural restriction in which multiplications precede additions, we can think of a proof of $P \geq 0$ from H as a polynomial identity of the form

$$\sum_{i=1}^{r} c_i \cdot P_i \cdot \prod_{j \in J_i} X_j \prod_{k \in K_i} \bar{X}_k = P, \tag{4}$$

where $c_1, \ldots, c_r$ are non-negative real numbers, and $P_1, \ldots, P_r$ are polynomials such that either the inequality $P_i \geq 0$ is in the set of hypothesis H, or they are axiom polynomials from (2) and (3), or they are squares of polynomials, when these are allowed. Note that the size of an SA or SOS proof thought of as a semi-algebraic proof is polynomially related to the sum of the sizes of the non-zero c_i's in (4).

We close this section by noting the relationships between LS and SA proofs on one hand, and LS$^+$ and SOS proofs on the other. Clearly, each SA proof of degree d is also an LS proof of degree d. The converse is certainly not true, but what is true is that every LS proof of degree d and rank k can be converted into an SA proof of degree $d + k$, where the rank is the complexity measure for LS proofs that we defined earlier. The same relationships hold between LS$^+$ and SOS: every SOS-proof of degree d is an LS$^+$ of degree d, and every LS$^+$ proof of degree d and rank k can be converted into an SOS-proof of degree $d + k$. The conversions go by swapping the order in which the addition and the multiplication rules are applied in LS proofs, when they appear in the *wrong* order. See [20] for a related discussion.

2.3 Constraint satisfaction problem

There are many equivalent definitions of the constraint satisfaction problem. Here we use the definition in terms of homomorphisms. Below we introduce the necessary terminology.

A *relational vocabulary* L is a set of symbols, each symbol has an associated arity. A *structure* $\mathbb{B}$ over L is a set B, called a *domain* together with a set of relations over B. For each $R \in L$ or arity r, there is a relation $R(\mathbb{B}) \subseteq B^r$ sometimes called an *interpretation* of R in $\mathbb{B}$. We say that a relational structure is finite if its domain is finite and it has finitely many non-empty relations. For two structures $\mathbb{B}$ and $\mathbb{B}'$ over the same vocabulary L, a *homomorphism* from $\mathbb{B}$ to $\mathbb{B}'$ is a function $h\colon B \to B'$, which preserves all the relations, that is, if $(b_1, \ldots, b_r) \in R(\mathbb{B})$, then $(h(b_1), \ldots, h(b_r)) \in R(\mathbb{B}')$, for each $R \in L$.

For a fixed L-structure $\mathbb{B}$ over a relational vocabulary L, the constraint satisfaction problem of $\mathbb{B}$, denoted CSP($\mathbb{B}$), is the following computational problem: given a finite L-structure $\mathbb{A}$, decide whether there exists a homomorphism from $\mathbb{A}$ to $\mathbb{B}$. In the context of CSP the structure $\mathbb{B}$ is often called a *constraint language*. We usually assume that the constraint language $\mathbb{B}$ is finite.

To reason about propositional proof systems for CSP we use the following fixed encoding. By CNF($\mathbb{A}, \mathbb{B}$) we denote the CNF formula which has clauses

1. $\bigvee_{b \in B} X(a, b)$ for each $a \in A$,
2. $\overline{X(a, b_0)} \vee \overline{X(a, b_1)}$ for each $a \in A$ and $(b_0, b_1) \in B^2$ with $b_0 \neq b_1$,
3. $\overline{X(a_1, b_1)} \vee \cdots \vee \overline{X(a_r, b_r)}$ for each natural number r, each $R \in L$ of arity r, each $(a_1, \ldots, a_r) \in R(\mathbb{A})$, and each $(b_1, \ldots, b_r) \in B^r \setminus R(\mathbb{B})$.

It is not difficult to see that the formula CNF($\mathbb{A}, \mathbb{B}$) is satisfiable if and only if there is a homomorphism from $\mathbb{A}$ to $\mathbb{B}$.

To reason about semi-algebraic proof systems in the context of CSP we use the following fixed encoding. By INEQ($\mathbb{A}, \mathbb{B}$) we denote the system of linear inequalities defined as follows:

1. $\sum_{b \in B} X(a, b) - 1 \geq 0$ for each $a \in A$,
2. $\bar{X}(a, b_0) + \bar{X}(a, b_1) - 1 \geq 0$ for each $a \in A$ and $(b_0, b_1) \in B^2$ with $b_0 \neq b_1$,
3. $\sum_{i=1}^{r} \bar{X}(a, b_i) - 1 \geq 0$ for each natural number r, each $R \in L$ of arity r, each $(a_1, \ldots, a_r) \in R(\mathbb{A})$, and each $(b_1, \ldots, b_r) \in B^r \setminus R(\mathbb{B})$.

It is easy to see that the above system of linear inequalities has a solution satisfying the axioms from (2) and (3) if and only if there is a homomorphism from $\mathbb{A}$ to $\mathbb{B}$.

The existential k-pebble game is played on two relational structures $\mathbb{A}$ and $\mathbb{B}$ over the same vocabulary by two players called Spoiler and Duplicator. The players are given two corresponding sets of pebbles $\{a_1, \ldots, a_k\}$ and $\{b_1, \ldots, b_k\}$. In each round Spoiler picks one of the k pebbles $a_1, \ldots, a_k$, say a_i, and puts it on an element of the structure $\mathbb{A}$. Duplicator responds by picking the corresponding pebble b_i and placing it on some element of the structure $\mathbb{B}$. For simplicity, in any given configuration of the game let us identify a pebble with the element of the structure that it is placed on. Spoiler wins if at any point during the game the partial function $f : A \to B$ defined by $f(a_i) = b_i$, for each pebbled element a_i of $\mathbb{A}$, is either not well defined or is not a partial homomorphism. Otherwise, the Duplicator wins.

A finite relational structure $\mathbb{B}$ has *width* k if, for every finite structure $\mathbb{A}$ of the same vocabulary as $\mathbb{B}$, if there is no homomorphism from $\mathbb{A}$ to $\mathbb{B}$, then Spoiler wins the existential k-pebble game on $\mathbb{A}$ and $\mathbb{B}$. The structure $\mathbb{B}$ has *bounded width* if it has width k for some k. Structures of bounded width are exactly those structures for which CSP($\mathbb{B}$) can be solved by a local consistency algorithm [17].

3 Closure under reductions

There are three types of reductions often considered in the context of CSPs: a) pp-interpretability b) homomorphic equivalence c) addition of constants to a core.

Let $\mathbb{B}$ and $\mathbb{B}'$ be finite relational structures over finite vocabularies L and L'. The structure $\mathbb{B}'$ is *pp-definable* in $\mathbb{B}$ if is has the same domain and for every relation symbol $T \in L'$ the relation $T(\mathbb{B}')$ is definable in $\mathbb{B}$ by a *pp-formula*, i.e., a first order formula using only symbols from L, conjunction, equality, and existential quantification. Formally, for every relation symbol $T \in L'$ there exists a pp-formula $\phi_T(x_1, \ldots, x_r)$, where r is the arity of T, such that $T(\mathbb{B}') = \{(b_1, \ldots, b_r) \in B^r : \mathbb{B} \models \phi_T(x_1/b_1, \ldots, x_r/b_r)\}$.

Pp-interpretability is a generalization of pp-definability which allows for changing the domain of a CSP language. Given two relational structures $\mathbb{B}$ and $\mathbb{B}'$, we say that $\mathbb{B}'$ is *pp-interpretable* in $\mathbb{B}$ if there exist a positive integer n and a surjective partial function $f\colon B^n \to B'$ such that the preimages of all relations in $\mathbb{B}'$ (including the equality relation) and the domain of f are pp-definable in $\mathbb{B}$. One of the fundamental results of the *algebraic approach* to the constraint satisfaction problem is that, whenever $\mathbb{B}'$ is pp-interpretable in $\mathbb{B}$, the CSP of the language $\mathbb{B}'$ is not harder than the CSP of the language $\mathbb{B}$ [9].

Structures $\mathbb{B}$ and $\mathbb{B}'$ over a vocabulary L are *homomorphically equivalent* if there exist homomorphisms from $\mathbb{B}$ to $\mathbb{B}'$ and from $\mathbb{B}'$ to $\mathbb{B}$. Obviously, if L-structures $\mathbb{B}$ and $\mathbb{B}'$ are homomorphically equivalent, then any L-structure $\mathbb{A}$ maps homomorphically to $\mathbb{B}$ if and only if it maps homomorphically to $\mathbb{B}'$. So the CSP problems over both languages are the same.

Homomorphic equivalence allows us to focus on studying constraint satisfaction problems of well-behaved structures which in this context turn out to be those exhibiting little symmetry. A finite relational structure is called a *core* if all its endomorphisms are surjective. It is known that every relational structure has a homomorphically equivalent substructure that is a core. Core structures can be extended by one-element unary relations which we refer to as *constants*, without increasing the complexity of the language [9].

It has been shown recently [5] that any class of constraint languages that is closed under the constructions a), b) and c) has an algebraic characterization in terms of identities of height 1. Here we show that DNF Frege, bounded-depth Frege, Frege, Sherali-Adams, Sums-of-Squares and Lovász-Schrijver proof systems behave well with respect to those three types of reductions.

Let us fix relational structures $\mathbb{B}$ and $\mathbb{B}'$ such that $\mathbb{B}'$ is obtained from $\mathbb{B}$ by a finite sequence of constructions a), b) and c). There is a known polynomial-time computable transformation that maps instances $\mathbb{A}'$ of CSP($\mathbb{B}'$) to instances $\mathbb{A}$ of CSP($\mathbb{B}$) such that $\mathbb{A}$ is satisfiable if and only if $\mathbb{A}'$ is satisfiable, and the size of $\mathbb{A}$ is linear in the size of $\mathbb{A}'$. We prove that this transformation satisfies the following:

▶ **Theorem 4.** *For any positive integers t, k and s, and any instance $\mathbb{A}'$, if there is a Frege refutation of* CNF($\mathbb{A}, \mathbb{B}$) *of depth t, bottom fan-in k, and size s, then there is a Frege refutation of* CNF($\mathbb{A}', \mathbb{B}'$) *of depth t, bottom fan-in polynomial in k, and size polynomial in the size of $\mathbb{A}'$ and s.*

▶ **Theorem 5.** *For any positive integers k and s, and any instance $\mathbb{A}'$, if there is a Sherali-Adams, Sums-of-Squares or Lovász-Schrijver refutation of* INEQ($\mathbb{A}, \mathbb{B}$) *of degree k and size s, then there is, respectively, a Sherali-Adams, Sums-of-Squares or Lovász-Schrijver refutation of* INEQ($\mathbb{A}', \mathbb{B}'$) *of degree linear in k and size polynomial in the size of $\mathbb{A}'$ and s.*

We point out that Theorem 5 in the case of the Sherali-Adams and Sums-of-Squares proof systems can be extracted from [24] and [25]. We include it here to illustrate the broad applicability of the systematic proof-complexity approach.

The main idea in proving the above theorems for all the proof systems under consideration is the same. The refutation for an instance $\mathbb{A}$ of CSP($\mathbb{B}$) is transformed into a refutation for an instance $\mathbb{A}'$ of CSP($\mathbb{B}'$) by substituting the variables of CNF($\mathbb{A}, \mathbb{B}$) or INEQ($\mathbb{A}, \mathbb{B}$) by

DNFs with bounded terms and a bounded number of terms or by polynomials with bounded degree, a bounded number of monomials and coefficients from a fixed, finite set, respectively. The additional condition we need to ensure in order to control the growth of the size and depth/degree of the refutations is that each formula from $\mathrm{CNF}(\mathbb{A},\mathbb{B})$ and every polynomial inequality from $\mathrm{INEQ}(\mathbb{A},\mathbb{B})$ after applying the substitution is a logical consequence of a bounded number of formulas/inequalities from $\mathrm{CNF}(\mathbb{A}',\mathbb{B}')$ or $\mathrm{INEQ}(\mathbb{A}',\mathbb{B}')$, respectively.

4 Upper bound

We say that a finite relational structure $\mathbb{B}$ has *resolution refutations of bounded width* if there is a positive integer k such that, for every finite structure $\mathbb{A}$ over the same vocabulary, if there is no homomorphism from $\mathbb{A}$ to $\mathbb{B}$, then $\mathrm{CNF}(\mathbb{A},\mathbb{B})$ has a resolution refutation of width k. The goal of this section is to prove the following:

▶ **Theorem 6.** *Let $\mathbb{B}$ be a finite relational structure. The following are equivalent:*
1. *$\mathbb{B}$ has bounded width,*
2. *$\mathbb{B}$ has resolution refutations of bounded width.*

In preparation for the proof we revisit the characterization of resolution width in terms of existential pebble games from [2].

Let $L = \{R_0, \ldots, R_q\}$ be a finite relational vocabulary consisting of $q+1$ symbols of arity q. Let $\mathbb{S}_q$ be an L-structure with two-element domain $\{0,1\}$, where each relation $R_i(\mathbb{S}_q)$ encodes the set of valuations that satisfy a q-clause with i negated variables. More precisely, for $0 \leq i \leq q$, let $R_i(\mathbb{S}_q) = \{0,1\}^q \setminus \{(x_1,\ldots,x_q)\}$ where $(x_1,\ldots,x_q) \in \{0,1\}^q$ is the vector defined by $x_j = 0$ for $j > i$ and $x_j = 1$, otherwise. Now for every q-CNF F, we define an L-structure $\mathbb{A}_F$. Its domain is the set of variables in F, and $R_i(\mathbb{A}_F)$ is the set of all tuples $(X_1,\ldots,X_q)$ such that the clause $\overline{X_1} \vee \ldots \vee \overline{X_i} \vee X_{i+1} \vee \ldots \vee X_q$ belongs to F. We allow the variables in the clauses to repeat, so the definition covers clauses with less than q literals. Observe that partial homomorphisms from $\mathbb{A}_F$ to $\mathbb{S}_q$ correspond to partial truth assignments to the variables of F that do not falsify any clause from F. Hence, for every q-CNF F, it holds that F is satisfiable if and only if there is a homomorphism from $\mathbb{A}_F$ to $\mathbb{S}_q$.

▶ **Theorem 7** ([2])**.** *Let k and q be positive integers such that $k \geq q$ and let F be q-CNF. Then F has a resolution refutation of width k if and only if Spoiler wins the existential $(k+1)$-pebble game on $\mathbb{A}_F$ and $\mathbb{S}_q$.*

We use the above theorem to establish a similar correspondence between existential pebble games on structures $\mathbb{A}$ and $\mathbb{B}$ and bounded width resolution refutations of $\mathrm{CNF}(\mathbb{A},\mathbb{B})$.

▶ **Lemma 8.** *Let $\mathbb{A}$ and $\mathbb{B}$ be relational structures over the same vocabulary of maximum arity r, let $q = |B|$, and let k be an integer such that $k \geq q$ and $k \geq r$. Then:*
1. *if Spoiler wins the existential $(k+2)$-pebble game on $\mathbb{A}$ and $\mathbb{B}$, then $\mathrm{CNF}(\mathbb{A},\mathbb{B})$ has a resolution refutation of width $k+q$,*
2. *if Duplicator wins the existential $(k+2)$-pebble game on $\mathbb{A}$ and $\mathbb{B}$, then $\mathrm{CNF}(\mathbb{A},\mathbb{B})$ does not have a resolution refutation of width $k+1$.*

Proof of Theorem 6. For the implication 1 to 2, assume that $\mathbb{B}$ has bounded width, say l. Let $k = \max\{q, r, l\}$, where $q = |B|$ and r is the maximum arity of the vocabulary of $\mathbb{B}$. Let $\mathbb{A}$ be a structure over the same vocabulary and assume that there is no homomorphism from $\mathbb{A}$ to $\mathbb{B}$. Then Spoiler wins the existential l-pebble game on $\mathbb{A}$ and $\mathbb{B}$, and hence also the existential $(k+2)$-pebble game on $\mathbb{A}$ and $\mathbb{B}$, since $k+2 \geq l$. The hypotheses of Lemma 8

hold, so by part *1* CNF$(\mathbb{A},\mathbb{B})$ has a resolution refutation of width $k+q$. This shows that $\mathbb{B}$ has resolution refutations of width $k+q$, and hence resolution refutations of bounded width.

For the implication 2 to 1, assume that $\mathbb{B}$ has resolution refutations of width l. Again let $k=\max\{q,r,l\}$. Let $\mathbb{A}$ be a structure over the same vocabulary as $\mathbb{B}$ and assume that there is no homomorphism from $\mathbb{A}$ to $\mathbb{B}$. Then CNF$(\mathbb{A},\mathbb{B})$ has a resolution refutation of width l, and hence of width $k+1$ since $k+1\geq l$. The hypotheses of Lemma 8 hold, so by part *2* in that lemma, Spoiler wins the existential $(k+2)$-pebble game on $\mathbb{A}$ and $\mathbb{B}$. This shows that $\mathbb{B}$ has width $k+2$, and hence bounded width. ◀

5 Lower bounds

Let $d(n)$ and $s(n)$ be functions. We say that a finite relational structure $\mathbb{B}$ has Frege refutations of depth $d(n)$ and size $s(n)$ if, for every finite structure $\mathbb{A}$ over the same vocabulary, if there is no homomorphism from $\mathbb{A}$ to $\mathbb{B}$, then CNF$(\mathbb{A},\mathbb{B})$ has a Frege refutation of depth $d(|A|)$ and size $s(|A|)$. We say that $\mathbb{B}$ has Frege refutations of bounded depth and subexponential size if there exist $d(n)=O(1)$ and $s(n)=2^{n^{o(1)}}$ such that $\mathbb{B}$ has Frege refutations of depth $d(n)$ and size $s(n)$.

Similarly, we say that a finite relational structure $\mathbb{B}$ has Sums-of-Squares refutations of degree $d(n)$ if, for every finite structure $\mathbb{A}$ over the same vocabulary, if there is no homomorphism from $\mathbb{A}$ to $\mathbb{B}$, then INEQ$(\mathbb{A},\mathbb{B})$ has a Sums-of-Squares refutation of degree $d(|A|)$. We say that $\mathbb{B}$ has Sums-of-Squares refutations of sublinear degree if there exists $d(n)=o(n)$ such that $\mathbb{B}$ has Sums-of-Squares refutations of degree $d(n)$. We prove:

▶ **Theorem 9.** *Let $\mathbb{B}$ be a finite relational structure. The following are equivalent:*
1. *$\mathbb{B}$ has bounded width,*
2. *$\mathbb{B}$ has Frege refutations of bounded depth and subexponential size,*
3. *$\mathbb{B}$ has Sums-of-Squares refutations of sublinear degree.*

The equivalence of *1* and *3* is known [11, 25]. Here we provide an alternative proof. The implication *1* to *2* follows from Theorem 6: every resolution refutation is a Frege refutation of depth one, and if the refutation has bounded width, then it has polynomial size and hence subexponential size. The implication *1* to *3* follows from Theorem 6 via the fact that bounded-degree SA simulates bounded-width resolution: bounded-width resolution is simulated by bounded-degree SA, which implies Sums-of-Squares refutations of a constant, and hence sublinear, degree.

For both implications *2* to *1* and *3* to *1* we use an algebraic characterization of unbounded width. We begin with some definitions.

Let $G=(G,+,0)$ be a finite Abelian group. For each $g\in G$ and every $(z_1,\ldots,z_k)\in\mathbb{Z}^k$, we define a relation $R_{(g,z_1,\ldots,z_k)}=\{(g_1,\ldots,g_k)\in G^k : z_1g_1+\ldots+z_kg_k=g\}$, where z_ig_i is a shortcut for the sum of $|z_i|$ copies of $\mathrm{sign}(z_i)g_i$. Let $\sim$ be the equivalence relation on the set $G\times\mathbb{Z}^k$ that identifies tuples defining the same relation. Since there are only finitely many k-ary relations on the finite set G, the equivalence relation $\sim$ has finitely many equivalence classes. Let $L(G,k)$ be the relational vocabulary that for every equivalence class $[(g,z_1,\ldots,z_k)]$ has one k-ary relation symbol $E_{[(g,z_1,\ldots,z_k)]}$, and let $\mathbb{B}(G,k)$ be the $L(G,k)$-structure that has domain G and where each relation symbol $E_{[(g,z_1,\ldots,z_k)]}$ is interpreted as $R_{(g,z_1,\ldots,z_k)}$. The CSP of $\mathbb{B}(G,k)$ is called kLIN(G). Instances of kLIN(G) are systems of linear equations over the group G with k variables per equation.

▶ **Theorem 10** ([4, 8])**.** *Let $\mathbb{B}$ be a finite relational structure. The following are equivalent:*

1. $\mathbb{B}$ *does not have bounded width,*
2. *there exists a non-trivial finite Abelian group* G *such that* $\mathbb{B}(G,3)$ *is pp-interpretable in* $\mathbb{B}^+$*, where* $\mathbb{B}^+$ *is the expansion of the core of* $\mathbb{B}$ *with all constants.*

Thus, in view of Theorems 4 and 5, in order to prove that *2* implies *1*, and that *3* implies *1* in Theorem 9, it suffices to prove lower bounds for $3\mathrm{LIN}(G)$, for every non-trivial finite Abelian group G.

For bounded-depth Frege we appeal to the lower bound for the pigeonhole principle [1, 6, 19]. To use that we need to be able to encode the pigeonhole principle as an unsatisfiable system of equations over an arbitrary Abelian group G. In [7], such a reduction was obtained for the so-called *Tseitin formulas*, that encode a certain system of linear equations over $\mathbb{Z}_2$ that is derived from an expander graph. Here we adapt the formulas to encode systems of linear equations over arbitrary finite Abelian groups and then show that the reduction in [7] can be adapted to our formulas. For Sums-of-Squares, unlike for bounded-depth Frege, we do not need to adapt an existing lower bound proof from the literature for $\mathbb{Z}_2$ to all finite Abelian groups because this was already done. The lower bound that we need to complete the proof of Theorem 9 is the following.

▶ **Theorem 11** ([10]). *For every non-trivial finite Abelian group* G *there exists a positive* δ *such that for every sufficiently large integer* n *there is an* n*-variable unsatisfiable instance* $\mathbb{A}$ *of* $3\mathrm{LIN}(G)$ *such that every SOS refutation of* $\mathrm{INEQ}(\mathbb{A}, \mathbb{B}(G,3))$ *has degree at least* δn*.*

The exact statement from [10] is Theorem G.8 from Appendix G, which differs from the version above. However, the original one implies the variant that we need.

6 Upper bounds in Lovász-Schrijver

In this section we show that all unsatisfiable instances of $3\mathrm{LIN}(\mathbb{Z}_2)$ have LS refutation of degree 6 and size polynomial in the number of variables. Indeed, the argument to get polynomial-size upper bound in constant degree works equally well for $3\mathrm{LIN}(\mathbb{Z}_p)$, when p is prime, with some inessential complications. We focus on $\mathbb{Z}_2$ for simplicity.

6.1 Initial remarks on the encoding

We identify the elements of the two-element field $\mathbb{Z}_2$ with $\{0,1\}$. Let $\mathbb{E}$ be an instance of $k\mathrm{LIN}(\mathbb{Z}_2)$ with n variables. In the encoding $\mathrm{INEQ}(\mathbb{E}, \mathbb{B}(\mathbb{Z}_2,k))$ of $\mathbb{E}$ as a system of linear inequalities, there are four variables $X(a,0), X(a,1), \bar{X}(a,0), \bar{X}(a,1)$ for each variable a in $\mathbb{E}$. Note, however, that they are restricted to satisfy $X(a,0) = \bar{X}(a,1)$ and $\bar{X}(a,0) = X(a,1)$ by the inequality $X(a,0) + X(a,1) - 1 \geq 0$ from INEQ and the default equations in (2), which in this case read $X(a,0)^2 - X(a,0) = X(a,1)^2 - X(a,1) = 0$ and $X(a,0) + \bar{X}(a,0) - 1 = X(a,1) + \bar{X}(a,1) - 1 = 0$. Consequently, in the following we will ignore the variables of the type $X(a,0)$ and their twins and keep only the variables $X(a,1)$ and $\bar{X}(a,1)$. In order to simplify the notation even further, we will assume that the variables of $\mathbb{E}$ are called $X_1, \ldots, X_n$, and that those of INEQ are called $X_1, \ldots, X_n$ and $\bar{X}_1, \ldots, \bar{X}_n$.

We interpret the variables $X_1, \ldots, X_n$ as ranging over $\mathbb{Z}_2$ or $\mathbb{Q}$ depending on the context. Let E be an equation of $\mathbb{E}$, say $E : a_1X_1 + \cdots + a_nX_n = b$, where $a_1, \ldots, a_n \in \mathbb{Z}_2$ and $b \in \mathbb{Z}_2$. Without loss of generality we can assume that there are exactly k many a_i's that are 1. In INEQ, the encoding of this equation is given by the following inequalities:

$$\sum_{i \in T} \bar{X}_i + \sum_{i \in I \setminus T} X_i - 1 \geq 0 \qquad \text{for all } T \subseteq I \text{ such that } |T| \equiv 1 - b \mod 2,$$

where $I = \{i \in [n] : a_i \neq 0\}$. Note that $|I| = k$. We write $\mathcal{S}(E)$ to denote this set of inequalities; it has exactly 2^{k-1} many inequalities, and all of them are satisfied in $\mathbb{Q}$ by a $\{0,1\}$-assignment if and only if the equation E is satisfied in $\mathbb{Z}_2$ by the same assignment. Let $\mathcal{S}(\mathbb{E})$ be the union of all $\mathcal{S}(E)$ as E ranges over the equations in $\mathbb{E}$. Observe that, except for the small detail that only half of the variables are used, INEQ is basically the same as $\mathcal{S}(\mathbb{E})$.

6.2 Some technical lemmas

For every linear form $L(X_1, \ldots, X_n) = \sum_{i=1}^n a_i X_i$ with rational coefficients $a_1, \ldots, a_n$ and every integer c, let $D_c(L) = (L - c)(L - c + 1)$, which is a quadratic polynomial. In words, the inequality $D_c(L) \geq 0$ states that L does not fall in the open interval $(c - 1, c)$. Such statements have short proofs of low degree:

▶ **Lemma 12** ([15]). *For every integer c and for every linear form $L(X_1, \ldots, X_n) = \sum_{i=1}^n a_i X_i$ with integer coefficients $a_1, \ldots, a_n$, there is a LS proof of the inequality $D_c(L) \geq 0$ (from nothing) of degree 3 and size polynomial in $\max\{|a_i| : i = 1, \ldots, n\}$, $|c|$ and n.*

In the following, for $I \subseteq [n]$ and $T \subseteq I$, let $M_T^I(X_1, \ldots, X_n) := \prod_{i \in T} X_i \prod_{i \in I \setminus T} \bar{X}$. As usual, $M_\emptyset^I(X_1, \ldots, X_n) = 1$. Such polynomials are called *extended monomials*.

▶ **Lemma 13.** *For every $I \subseteq [n]$, there is an LS proof of $\sum_{T \subseteq I} M_T^I - 1 = 0$ (from nothing) of degree $|I|$ and size polynomial in $2^{|I|}$, and for every $T \subseteq I \subseteq [n]$, there is an LS proof of $\left(\sum_{i \in I} X_i - |T|\right) M_T^I = 0$ (from nothing) of degree $|I| + 1$ and size polynomial in $|I|$.*

6.3 Simulating Gaussian elimination

Now we prove the main result of this section.

▶ **Theorem 14.** *Let $\mathbb{E}$ be an instance of $3\mathrm{LIN}(\mathbb{Z}_2)$ with n variables and m equations. If $\mathbb{E}$ is unsatisfiable, then $\mathcal{S}(\mathbb{E})$ has an LS refutation of degree 6 and size polynomial in n and m.*

Proof. Write $\mathbb{E}$ in matrix form $AX = b$, where X is a column vector of n variables, A is a matrix in $\mathbb{Z}_2^{m \times n}$, and b is a vector in $\mathbb{Z}_2^m$. Let $a_{j,1}, \ldots, a_{j,n}$ be the j-th row of A, so the j-th equation of $\mathbb{E}$ is $E_j : a_{j,1}X_1 + \cdots + a_{j,n}X_n = b_j$. Assume $\mathbb{E}$ is unsatisfiable over $\mathbb{Z}_2$. Then b cannot be expressed as a $\mathbb{Z}_2$-linear combination of the columns of A, so the $\mathbb{Z}_2$-rank of the matrix $[\, A \mid b \,]$ exceeds the $\mathbb{Z}_2$-rank of A. Since the rank of A is at most n, this means that there exists a subset of at most n rows J such that, with arithmetic in $\mathbb{Z}_2$, we have $\sum_{j \in J} a_{j,i} = 0$ for every $i \in [n]$, and at the same time $\sum_{j \in J} b_j = 1$. In order to simplify the notation, we assume without loss of generality that $J = \{1, \ldots, |J|\}$.

For every $k \in \{0, \ldots, |J|\}$, define the linear form

$$L_k(X_1, \ldots, X_n) := \frac{1}{2}\left(\sum_{j=1}^{k}\sum_{i=1}^{n} a_{j,i}X_i + \sum_{j=k+1}^{|J|} b_j\right).$$

In this definition of L_k, the coefficients $a_{j,i}$ and b_j are interpreted as rationals. We provide proofs of $D_c(L_k) \geq 0$ for every $c \in R_k := \{0, \ldots, (k+1)n\}$ by reverse induction on $k \in \{0, \ldots, |J|\}$.

The base case $k = |J|$ is a special case of Lemma 12. To see why note that the condition $\sum_{j \in J} a_{j,i} = 0$ over $\mathbb{Z}_2$ means that, if arithmetic were done in $\mathbb{Q}$, then $\sum_{j \in J} a_{j,i}$ is an even natural number. But then all the coefficients of

$$L_{|J|}(X_1, \ldots, X_n) = \frac{1}{2}\sum_{j=1}^{|J|}\sum_{i=1}^{n} a_{j,i}X_i = \sum_{i=1}^{n}\left(\frac{1}{2}\sum_{j=1}^{|J|} a_{j,i}\right)X_i$$

are integers. Hence Lemma 12 applies.

Suppose now that $0 \leq k \leq |J| - 1$ and that we have a proof of $D_d(L_{k+1}) \geq 0$ available for every $d \in R_{k+1}$. Fix $c \in R_k$; our immediate goal is to give a proof of $D_c(L_k) \geq 0$. As k is fixed, write L in place of L_{k+1}, and let the $(k+1)$-st equation E_{k+1} be written as $\sum_{i \in I} X_i = b$, where $I = \{i \in [n] : a_{k+1,i} = 1\}$. Note that $L = L_k + \ell/2$ where $\ell := -b + \sum_{i \in I} X_i$. Fix $T \subseteq I$ such that $|T| \equiv b \bmod 2$, and let $d = c + (t - b)/2$ where $t = |T|$. Note that $d \in R_{k+1}$ as $c \in R_k$ and $0 \leq t \leq n$ and $0 \leq b \leq 1$ are such that $t - b$ is even. Multiplying $D_d(L) \geq 0$ by the extended monomial M_T^I we get $(L - d)(L - d + 1)M_T^I \geq 0$. Replacing $L = L_k + \ell/2$ in the factor $(L - d)$ and recalling $d = c + (t - b)/2$, this inequality can be written as

$$(L_k - c)(L - d + 1)M_T^I + (L - d + 1)\tfrac{1}{2}A \geq 0, \tag{5}$$

where $A := (\ell + b - t)M_T^I$. By the second part of Lemma 13 we have a proof of $A = 0$, and hence of $(L - d + 1)A/2 = 0$. Composing with (5) we get a proof of $(L_k - c)(L - d + 1)M_T^I \geq 0$. The same argument applied to the factor $(L - d + 1)$ of this inequality gives $(L_k - c)(L_k - c + 1)M_T^I \geq 0$. This is precisely $D_c(L_k)M_T^I \geq 0$. Adding up over all $T \subseteq I$ with $|T| \equiv b \bmod 2$ we get

$$D_c(L_k) \sum_{\substack{T \subseteq I \\ |T| \equiv b}} M_T^I \geq 0. \tag{6}$$

Now note that for each $T \subseteq I$ such that $|T| \equiv 1 - b \mod 2$, the inequality $-M_T^I \geq 0$ is the multiplicative encoding of one of the inequalities in $\mathcal{S}(E)$. Thus, it is not difficult to show that it has an SA derivation from this inequality of size polynomial in $|I|$ and degree $|I| + 1$. Therefore, we get proofs of $-M_T^I \geq 0$, and hence of $M_T^I = 0$, for every $T \subseteq I$ such that $|T| \equiv 1 - b \bmod 2$. But then also of $D_c(L_k)M_T^I = 0$ for every such T. Adding up and composing with (6) we get

$$D_c(L_k) \sum_{T \subseteq I} M_T^I \geq 0. \tag{7}$$

From Lemma 13 we get $1 - \sum_{T \subseteq I} M_T^I = 0$, and hence $D_c(L_k) - D_c(L_k) \sum_{T \subseteq I} M_T^I \geq 0$, from which $D_c(L_k) \geq 0$ follows from addition with (7).

At this point we proved $D_c(L_0) \geq 0$ for every $c \in R_0 = \{0, \ldots, n\}$. Recall now that $\sum_{j=1}^{|J|} b_j$ is odd, say $2q + 1$, and at most n. In particular $q + 1$ belongs to R_0 and $L_0 = q + 1/2$. Thus we have a proof of $D_{q+1}(L_0) \geq 0$ where $D_{q+1}(L_0) = -(1/2)(1/2) = -1/4$. Multiplying by 4 we get the contradiction $-1 \geq 0$. ◀

7 Conclusions and Open Questions

Theorems 4 and 5 imply that for the proof systems under consideration the class of constraint languages admitting efficient refutations can be characterised algebraically. For most of those proof systems such a characterisation follows from the fact that efficient proofs of unsatisfiability exist exactly for languages of bounded width. However, by Theorem 14 the class of constraint languages admitting efficient refutations in Lovász-Schrijver, and consequently also the class of constraint languages admitting efficient Frege refutations, exceed bounded width. At the same time both of those classes are shown to admit algebraic characterisations. Providing such characterisations is a natural open problem that arises from our work.

A related direction that is also suggested by our work is whether the proof complexity of approximating MAX CSPs is also preserved by reductions. On the one hand, it is known that pp-definability preserves *almost satisfiability*; i.e., if $\mathbb{B}'$ is pp-definable in $\mathbb{B}$, then if $\mathbb{A}'$ is

an instance of MAX CSP($\mathbb{B}'$) that is almost satisfiable, then its standard transformation into an instance $\mathbb{A}$ of MAX CSP($\mathbb{B}$) is also almost satisfiable. The question we raise is the following: For which proof systems is it also the case that if there are efficient proofs that $\mathbb{A}$ is far from satisfiable then there also are efficient proofs that $\mathbb{A}'$ is far from satisfiable? Depending on how the terms "almost satisfiable" and "far from satisfiable" are quantified, a positive answer for such questions could lead to an algebraic approach to the theory of approximability of MAX CSPs and the UGC.

References

1. M. Ajtai. The complexity of the pigeonhole principle. In *29th Annual IEEE Symposium on Foundations of Computer Science*, pages 346–355, 1988.
2. A. Atserias and V. Dalmau. A combinatorial characterization of resolution width. *J. Comput. Syst. Sci.*, 74(3):323–334, May 2008. A preliminary version appeared in CCC 2003. doi:10.1016/j.jcss.2007.06.025.
3. A. Atserias, Ph. G. Kolaitis, and M. Vardi. Constraint propagation as a proof system. In *10th International Conference on Principles and Practice of Constraint Programming*, volume 3258 of *Lecture Notes in Computer Science*, pages 77–91. Springer-Verlag, 2004.
4. L. Barto and M. Kozik. Constraint satisfaction problems solvable by local consistency methods. *J. ACM*, 61(1):3:1–3:19, January 2014. doi:10.1145/2556646.
5. L. Barto, J. Opršal, and M. Pinsker. The wonderland of reflections. *CoRR*, abs/1510.04521, 2015. URL: http://arxiv.org/abs/1510.04521.
6. P. Beame, R. Impagliazzo, J. Krajícek, T. Pitassi, P. Pudlák, and A. Woods. Exponential lower bounds for the pigeonhole principle. In *24th Annual ACM Symposium on the Theory of Computing*, pages 200–220, 1992.
7. E. Ben-Sasson. Hard examples for bounded depth frege. In *34th Annual ACM Symposium on the Theory of Computing*, pages 563–572, 2002.
8. A. Bulatov. Bounded relational width. Manuscript, 2009.
9. A. Bulatov, P. Jeavons, and A. Krokhin. Classifying the complexity of constraints using finite algebras. *SIAM Journal on Computing*, 34(3):720–742, 2005.
10. Siu On Chan. Approximation resistance from pairwise-independent subgroups. *J. ACM*, 63(3):27:1–27:32, August 2016. doi:10.1145/2873054.
11. A. Dawar and P. Wang. Lasserre lower bounds and definability of semidefinite programming. *CoRR*, abs/1602.05409, 2016. URL: http://arxiv.org/abs/1602.05409.
12. M. X. Goemans and D. P. Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *J. ACM*, 42(6):1115–1145, November 1995. doi:10.1145/227683.227684.
13. D. Grigoriev. Linear lower bound on degrees of positivstellensatz calculus proofs for the parity. *Theoretical Computer Science*, 259(1–2):613–622, 2001.
14. D. Grigoriev and E. A. Hirsch. Algebraic proof systems over formulas. *Theoretical Computer Science*, 303(1):83 – 102, 2003.
15. D. Grigoriev, E. A. Hirsch, and D. V. Pasechnik. Complexity of semi-algebraic proofs. *Moscow Mathematical Journal*, 4(2):647–679, 2002.
16. S. Khot, G. Kindler, E. Mossel, and R. O'Donnell. Optimal inapproximability results for max-cut and other 2-variable csps? *SIAM Journal on Computing*, 37(1):319–357, 2007.
17. Ph. G. Kolaitis and M. Y. Vardi. A game-theoretic approach to constraint satisfaction. In *Proceedings of the Seventeenth National Conference on Artificial Intelligence and Twelfth Conference on Innovative Applications of Artificial Intelligence*, pages 175–181. AAAI Press, 2000. URL: http://dl.acm.org/citation.cfm?id=647288.721266.

18 J. Krajícek. On the weak pigeonhole principle. *Fundamenta Mathematicæ*, 170(1–3):123–140, 2001.

19 J. Krajícek, P. Pudlák, and A. Woods. Exponential lower bound to the size of bounded depth Frege proofs of the pigeon hole principle. *Random Structures and Algorithms*, 7(1):15–39, 1995.

20 M. Laurent. A comparison of the Sherali-Adams, Lovász-Schrijver and Lasserre relaxations for 0-1 programming. *Mathematics of Operations Research*, 28:470–496, 2001.

21 L. Lovász and A. Schrijver. Cones of matrices and set-functions and 0-1 optimization. *SIAM Journal on Optimization*, 1(2):166–190, 1991.

22 T. Pitassi. Algebraic propositional proof systems. In N. Immerman and Ph. G. Kolaitis, editors, *Descriptive Complexity and Finite Models*, volume 31 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 68–96. American Mathematical Society, 1997.

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

24 J. Thapper and S. Živný. Sherali-adams relaxations for valued csps. In *Automata, Languages, and Programming - 42nd International Colloquium, ICALP 2015*, pages 1058–1069, 2015.

25 J. Thapper and S. Živný. The limits of SDP relaxations for general-valued csps. *CoRR*, abs/1612.01147, 2016. URL: `http://arxiv.org/abs/1612.01147`.

26 M. Tulsiani. CSP gaps and reductions in the Lasserre hierarchy. In *41st Annual ACM Symposium on Theory of Computing (STOC)*, pages 303–312, 2009.