


# Semi-Algebraic Proof Systems for QBF

Olaf Beyersdorff  

Friedrich Schiller University Jena, Germany

Ilario Bonacina  

UPC Universitat Politècnica de Catalunya, Barcelona, Spain

Kaspar Kasche  

Friedrich Schiller University Jena, Germany

Meena Mahajan  

The Institute of Mathematical Sciences (A CI of Homi Bhabha National Institute), Chennai, India

Luc Nicolas Spachmann  

Friedrich Schiller University Jena, Germany

---

## Abstract

We introduce new semi-algebraic proof systems for Quantified Boolean Formulas (QBF) analogous to the propositional systems Nullstellensatz, Sherali-Adams and Sum-of-Squares. We transfer to this setting techniques both from the QBF literature (strategy extraction) and from propositional proof complexity (size-degree relations and pseudo-expectation). We obtain a number of strong QBF lower bounds and separations between these systems, even when disregarding propositional hardness.

**2012 ACM Subject Classification** Theory of computation → Proof complexity; Theory of computation → Complexity theory and logic

**Keywords and phrases** QBF, Proof Complexity, Sums-of-Squares, Nullstellensatz, Sherali-Adams, Semi-Algebraic Proof Systems

**Digital Object Identifier** 10.4230/LIPIcs.SAT.2025.5

**Funding** *Olaf Beyersdorff*: Carl-Zeiss Foundation and DFG grant BE 4209/3-1.

*Ilario Bonacina*: This author was funded by the AEI with the grant number PID2022-138506NB-C22.

*Kaspar Kasche*: Carl-Zeiss Foundation.

*Meena Mahajan*: Supported in part by the J. C. Bose Fellowship of SERB, ANRF.

**Acknowledgements** The authors would like to thank the Oberwolfach Research Institute for Mathematics: the idea for this work started during the Oberwolfach workshop 2413 “Proof Complexity and Beyond”, and the Schloss Dagstuhl – Leibniz Center for Informatics: part of this work has been done during the Dagstuhl Seminar 24421 “SAT and Interactions”.

## 1 Introduction

Two key results in algebraic and semi-algebraic geometry are the Nullstellensatz and the Positivstellensatz. The first can be seen as an algebraic identity certifying that a set of polynomial equations is unsatisfiable while the second as an algebraic identity certifying that a system of polynomial *inequalities* is unsatisfiable. In other words, both the Nullstellensatz and the Positivstellensatz naturally give rise to proof systems and in recent years intense research was performed on the proof complexity of such systems. In particular, the proof system *Sum-of-Squares*, a special case of Positivstellensatz, starting from [7], has received a lot of attention for its connection with algorithms based on hierarchies of SDP relaxations (see for instance [45, 47]). For similar reasons, the even more restrictive *Sherali-Adams* proof system has been investigated, named after its connection with the Sherali-Adams hierarchy of linear programming since its original definition (see for instance [36, 50]).



© Olaf Beyersdorff, Ilario Bonacina, Kaspar Kasche, Meena Mahajan, and Luc Nicolas Spachmann; licensed under Creative Commons License CC-BY 4.0

28th International Conference on Theory and Applications of Satisfiability Testing (SAT 2025).

Editors: Jeremias Berg and Jakob Nordström; Article No. 5; pp. 5:1–5:19

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

In this work, we devise a simple and natural way to extend the proof systems Nullstellensatz (NS), Sum-of-Squares (SOS) and Sherali-Adams (SA) from the context of propositional existentially quantified variables to existentially and universally quantified variables. In other words, we show how to define proof systems for quantified Boolean formulas (QBF) inspired by the propositional proof systems above.

The study of propositional and QBF proof systems is motivated both by theoretical reasons and also by connections to SAT and QBF solving [10, 22, 28]. While for SAT-solvers conflict-driven clause learning (CDCL) is the ruling paradigm, which by the seminal work of [1, 48] is essentially equivalent to the propositional proof system *Resolution* (Res), there are several competing approaches in QBF, with CDCL-based [53] and *expansion*-based solving [43] among the main paradigms. To model the strength of QBF-solvers several (often incomparable) QBF proof systems have been introduced and analysed [14, 39, 43]. Of most relevance to this work is QU-Resolution (QU-Res) [44, 52]. QU-Res adds to propositional Resolution the  $\forall$ -reduction rule that allows to eliminate universal variables from clauses. In [16] it has been shown that this approach of augmenting a propositional proof system by a  $\forall$ -reduction rule taking care of universal quantifiers also works for other common inference-based proof systems such as various Frege systems [16, 32], *Cutting Planes* [19, 33] – a proof system modelling geometric reasoning related to Chvátal-Gomory cuts – and *Polynomial Calculus* [21, 31], modelling algebraic reasoning related to Gröbner bases computations.

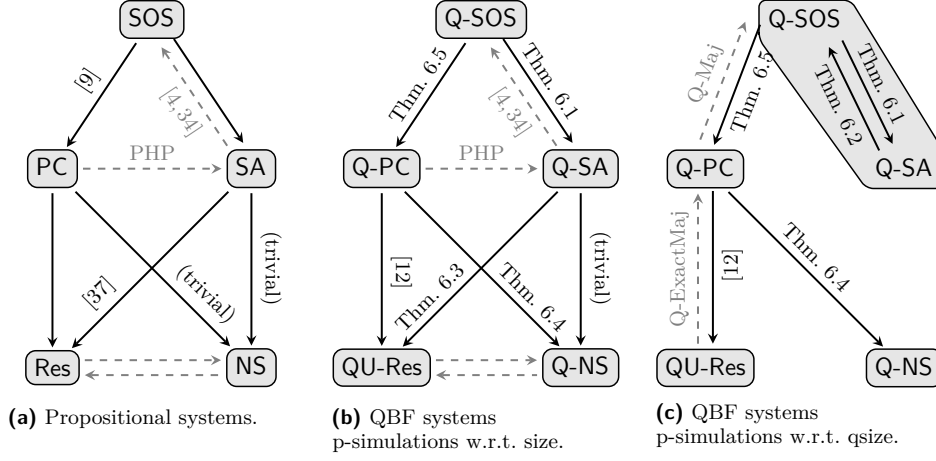
A common feature of all the propositional proof systems above is that they are *inference*-based, unlike the static systems NS/SA/SOS where a proof is just an algebraic identity of some specific form depending on the system at hand. This has posed quite some problems to adapt such systems to the QBF setting, and it was not clear at all whether an approach similar to a  $\forall$ -reduction rule was even viable. Recently there has been a suggestion to define QBF analogues of NS based on  $\forall$ -expansion [29], but these differ considerably from our approach here and the  $\forall$ -reduction paradigm discussed above.

We show that an approach similar to a  $\forall$ -reduction rule *does* allow to **define QBF versions of NS/SA/SOS**, which we call Q-NS/Q-SA/Q-SOS respectively. We argue that our definitions are quite natural: they add to the algebraic equations of NS/SA/SOS simple polynomials that strongly resemble  $\forall$ -reduction and meet the same technical condition on variable dependence.

We begin the systematic study of these QBF proof systems in terms of **lower and upper bounds, strategy extraction, and simulations**. Concerning the latter, Figure 1a recalls the relations between propositional NS/SA/SOS and further propositional proof systems such as Resolution (Res) and Polynomial Calculus (PC). In Figure 1b, we depict our results on the new QBF systems Q-NS/Q-SA/Q-SOS and how they relate to QU-Res and Q-PC. The figures are virtually identical: what changes is that proofs of the simulations, although mimicking those in the propositional setting, require extra care. Figure 1c depicts the simulation order when we factor out the propositional complexity and consider *genuine* QBF hardness stemming from quantifier alternations – a framework that has become standard in QBF proof complexity (cf. [20, 30] for background). We call the “genuine” size measure *qsize*, which only counts monomial size in the new  $\forall$ -reduction polynomials. Lower bounds on *qsize* are tighter and trivially imply lower bounds on the traditional size measure that counts all monomials. Hence, lower bounds and separations in *qsize* are harder to obtain. In fact, Q-SA and Q-SOS become equivalent w.r.t. *qsize* while they are separated w.r.t. *size*.

The fact that the systems we define fit so nicely into the lattice of QBF proof systems using the  $\forall$ -reduction approach suggests that the definitions we give are natural analogues of  $\forall$ -reduction in this context. The analogy with the  $\forall$ -reduction rule of QU-Res gets even

clearer when using the language of weighted clauses and Resolution to describe NS and SA [25]. For simplicity (and length constraints) we describe Q-NS and Q-SA using the usual algebraic language instead of the language of weighted clauses.



■ **Figure 1** Simulations and separations between algebraic proof systems in the propositional and the QBF setting. By  $P \rightarrow Q$  we indicate that proof system  $P$  polynomially simulates  $Q$ , while  $P \dashrightarrow Q$  means that the proof system  $P$  does not polynomially simulate  $Q$ . We omit polynomial (non-)simulations implied by those displayed.

For lower and upper bounds we develop and adapt techniques that originate both from propositional and QBF proof complexity.

Regarding the **transfer of propositional techniques**, we show how to lift common techniques for SOS from the propositional setting to Q-SOS: we establish a **size-degree relation** analogous to the propositional one [2], and show how to adapt the notion of **pseudo-expectation**, the prime lower-bound method for semi-algebraic systems [40] to the QBF setting. Both adaptations require interesting modifications and do not just replicate the propositional techniques (see Lemma 3.11 and Definition 5.1 with the discussion thereafter). We use pseudo-expectations to show an exponential lower bound for Q-SOS for the Equality QBFs [11] with respect to the tighter qsize measure (Theorem 5.3).

Regarding **QBF techniques**, we develop **strategy extraction** for Q-SOS. Strategy extraction has become the predominant technique to analyse QBF proof systems (see [12, 16, 17] for instance) and is also of tremendous practical importance for QBF solving and verification [5, 22, 39]. Specifically, we show that Q-SOS allows strategy extraction by polynomial threshold functions and develop a new score game interpretation. Interestingly, this score game allows to characterise genuine proof size in Q-SOS and Q-NS (Theorem 3.6). We also use it to elegantly show completeness of the new systems and a linear upper bound for the Q-Majority QBFs, which are known to be hard for Q-PC [21], yielding the separation depicted in Figure 1c.

**Structure of the paper.** Section 2 contains preliminaries and notation. Section 3 defines our new semi-algebraic QBF systems and shows their soundness and completeness together with the size-degree relation for Q-SOS. Section 4 contains the strategy extraction for Q-SOS and some consequences. In Section 5 we develop the lower bound technique of pseudo-expectations for Q-SOS and show an exponential lower bound. Section 6 we compare the QBF systems via p-simulations. We conclude in Section 7 with some open problems.

## 2 Preliminaries

**QBF preliminaries.** We consider Quantified Boolean Formulas (QBF) of the form  $\mathcal{Q}.\varphi$ , where  $\varphi$  is a CNF formula and  $\mathcal{Q}$  is the quantifier prefix. Both the variables of  $\varphi$  and the variables of  $\mathcal{Q}$  range over a set of Boolean variables  $V$ . Let  $\text{vars}_{\forall}(\mathcal{Q})$  (resp.  $\text{vars}_{\exists}(\mathcal{Q})$ ) be the set of universally (resp. existentially) quantified variables in  $\mathcal{Q}$ .

The evaluation of a QBF formula  $\mathcal{Q}.\varphi$  can be seen as a game (the *evaluation game*) between two players: the existential  $\exists$ -player and the universal  $\forall$ -player, where the  $\exists$ -player's goal is to satisfy the formula  $\varphi$  and the  $\forall$ -player's goal is to falsify it. The players take turns according to the order of the quantifiers in  $\mathcal{Q}$ . We call this game the evaluation game to distinguish it from a new game, the *score game*, which we introduce in Section 3.1.

A very well-studied QBF proof system is QU-Res [6, 44, 52], which can be seen as a natural extension of the propositional proof system Resolution [24, 49] to the QBF setting.

The QBF proof system QU-Res refutes a false QBF  $\mathcal{Q}.\varphi$  inferring the empty clause  $\perp$  from the clauses in  $\varphi$  using the resolution rule  $\frac{C \vee v}{C \vee D} \frac{D \vee \neg v}{C \vee D}$ , but also using a  $\forall$ -reduction rule  $\frac{C \vee u}{C}$ , where all the variables in  $C$  must be on the left of  $u$  in  $\mathcal{Q}$ . The *size* of a QU-Res refutation  $\pi$  ( $\text{size}(\pi)$ ) is the number of applications of rules in  $\pi$ , while  $Q$ -size ( $\text{qsize}(\pi)$ ) is the number of applications of the  $\forall$ -reduction rule.

**Algebraic proof systems.** Given a set of Boolean variables  $V$ , let  $\bar{V}$  be the set of new formal variables  $\bar{v}$  for  $v \in V$ . We consider polynomials with rational coefficients and variables in  $V \cup \bar{V}$ , i.e. polynomials in the ring  $\mathbb{Q}[V \cup \bar{V}]$ . Given a polynomial  $p$  and an assignment  $\alpha$  of its variables, we denote with  $p|_{\alpha}$  the evaluation of  $p$  in  $\alpha$ .

In this work we encode clauses and CNF formulas into polynomials using the so-called *twin-variables encoding*. A clause  $C = \bigvee_{v \in P} v \vee \bigvee_{v \in N} \neg v$  is encoded as the set of polynomials

$$\text{enc}(C) = \left\{ \prod_{v \in P} \bar{v} \prod_{v \in N} v \right\} \cup \{v^2 - v, v + \bar{v} - 1 : v \in P \cup N\}.$$

A CNF  $\varphi = \bigwedge_{j=1}^m C_j$  is encoded as a set of polynomials  $\text{enc}(\varphi) = \bigcup_{j=1}^m \text{enc}(C_j)$ . The formula  $\varphi$  is satisfiable if and only if the set of polynomial equalities  $\{p = 0 : p \in \text{enc}(\varphi)\}$  is satisfiable.

► **Fact 2.1.** Given a polynomial  $r \in \mathbb{Q}[V \cup \bar{V}]$ , if  $r$  evaluates to 0 over every Boolean assignment satisfying  $\varphi$  (and setting  $v + \bar{v}$  to 1), then  $r$  is in the ideal generated by  $\text{enc}(\varphi)$ , i.e. there are polynomials  $q_p$  such that  $r = \sum_{p \in \text{enc}(\varphi)} q_p p$ .

A refutation of an unsatisfiable CNF  $\varphi$  in variables  $V$  in the system Nullstellensatz, NS, (resp. Sherali-Adams, SA, or Sum-of-Squares, SOS) is an algebraic identity  $\pi$  of the form

$$\sum_{p \in \text{enc}(\varphi)} q_p p + q + 1 = 0, \tag{1}$$

where all the polynomials  $q_p, q$  are in  $\mathbb{Q}[V \cup \bar{V}]$ , and for NS  $q$  is identically 0 (resp. for SA  $q$  is a polynomial with non-negative coefficients, and for SOS  $q = \sum_{s \in S} s^2$ , that is  $q$  is a sum of squares). The *size* of the NS/SA/SOS refutation  $\pi$ ,  $\text{size}(\pi)$ , is the number of monomials (counted with repetition) in  $q_p$  and  $q$ . The *degree* of  $\pi$ ,  $\text{deg}(\pi)$ , is the maximum degree of any of the polynomials  $q_p p$ , and  $q$ .

► **Remark 2.2 (On variations of NS, SA and SOS).** The proof system NS has been considered also for polynomials over arbitrary fields [27]. In this paper we focus only on polynomials with rational coefficients. The proof systems NS, SA and SOS have been also studied using

a different encoding of CNF formulas: the encoding  $\text{enc}'(C)$ , which is the same as  $\text{enc}(C)$  but with each  $\bar{v}$  variable substituted by  $1 - v$ . The systems NS, SA and SOS under the  $\text{enc}'$  encoding are exponentially weaker than the corresponding system under the encoding  $\text{enc}$  [38]. In this paper we focus only on polynomials using the encoding  $\text{enc}$ . The proof system SOS has also been studied recently on Boolean variables representing the Boolean values as  $\pm 1$  instead of  $0/1$  [51], i.e. using instead of the polynomials  $v^2 - v$  the polynomials  $v^2 - 1$ . In this paper we focus only on polynomials using  $0/1$ -valued variables.

Another well-studied algebraic propositional proof system is *Polynomial Calculus* (PC) [31]. A Polynomial Calculus (over  $\mathbb{Q}$ ) refutation of the set of polynomials  $\text{enc}(\varphi)$ , for an unsatisfiable CNF formula  $\varphi$ , is a sequence of polynomials showing that 1 can be derived from  $\text{enc}(\varphi)$  using the inference rules  $\frac{p}{p+q}$  for polynomials  $p, q$ , and  $\frac{p}{vp}$  where  $v$  is a variable or  $v \in \mathbb{Q}$ . The *degree* and (monomial) *size* of the refutation are respectively the largest degree of a polynomial in it and the number of monomials in it (counted with multiplicity).

In [16, 21], the authors showed how to extend the proof system PC to the QBF context. This resulted in QBF proof system *Q-Polynomial Calculus* (Q-PC). Q-PC refutes a QBF  $\mathcal{Q}.\varphi$  analogously to the system PC, i.e. showing that the polynomial 1 can be derived from the polynomials in  $\text{enc}(\varphi)$  using the inference rules  $\frac{p}{p+q}$  for polynomials  $p, q$ , and  $\frac{p}{vp}$  where  $v$  is a variable or  $v \in \mathbb{Q}$ , but also using a  $\forall$ -reduction rule  $\frac{p}{p|_{u=b}}$ , for  $b \in \{0, 1\}$  where all the variables in  $p$  distinct from  $u$  must be left of  $u$  in  $\mathcal{Q}$ . The size of a Q-PC refutation is the number of monomials in the refutation (counted with repetition), while the *qsize* is the number of monomials in the polynomials involved in the  $\forall$ -reduction steps (again counted with repetition). The reason to study *qsize* and not just *size* is to factor out the propositional hardness of the principles and focus on genuine QBF hardness (cf. [20, 30]).

### 3 Algebraic systems for QBFs

We introduce new QBF proof systems inspired by propositional NS/SA/SOS. We call them Q-NS/Q-SA/Q-SOS. As their propositional counterparts they are static proof systems: a refutation of a false QBF  $\mathcal{Q}.\varphi$  over variables  $V$  in Q-Nullstellensatz, Q-NS, (resp. Q-Sherali-Adams, Q-SA, and Q-Sum-of-Squares, Q-SOS) is an algebraic identity  $\pi$  of the form

$$\sum_{p \in \text{enc}(\varphi)} q_p p + \sum_{u \in \text{vars}_{\forall}(\mathcal{Q})} q_u (1 - 2u) + q + 1 = 0, \quad (2)$$

where all the polynomials  $q_p, q_u, q$  are in  $\mathbb{Q}[V \cup \bar{V}]$ , the variables in  $q_u$  are all quantified before  $u$  in  $\mathcal{Q}$  (i.e. on the left of  $u$ ), and for Q-NS  $q$  is identically 0 (resp. for Q-SA  $q$  is a polynomial with non-negative coefficients, and for Q-SOS  $q = \sum_{s \in S} s^2$ , that is  $q$  is a sum of squares). We call the expression in eq. (2) a Q-NS-refutation of  $\mathcal{Q}.\varphi$  (resp. Q-SA-refutation/Q-SOS-refutation).

► **Definition 3.1** (size, degree, *qsize* and *qdeg*<sub>∃</sub>). *The size of a Q-NS/Q-SA/Q-SOS refutation  $\pi$  ( $\text{size}(\pi)$ ) is the number of monomials (counted with repetition) in  $q_p, q_u$  and  $q$ . The degree of  $\pi$  ( $\text{deg}(\pi)$ ) is the maximum degree of any of the polynomials  $q_p p, q_u(1 - 2u)$ , and  $q$ .*

*The Q-size of  $\pi$  ( $\text{qsize}(\pi)$ ) is defined analogously to the size but accounts only for the monomials in the polynomials  $q_u$ . The existential Q-degree of  $\pi$  ( $\text{qdeg}_{\exists}(\pi)$ ) is the maximum existential degree of any  $q_u$ , where the existential degree is the highest number of existentially quantified variables in any monomial.*

The definitions of size and degree for Q-NS/Q-SA/Q-SOS are completely analogous to the definitions in the propositional setting, while Q-size and Q-degree factor out propositional hardness and therefore give measures more appropriate to study principles where the hardness

stems from quantification. The definition of Q-size also aligns with genuine QBF hardness measures defined in [20] and analysed e.g. in [13, 21] for QU-Resolution and Q-PC, where only universal reduction steps are counted. In a sense, the polynomial  $q_u$  in (2) can be understood as a universal reduction step on  $u$ . In particular, on QBFs without universal variables, Q-NS/Q-SA/Q-SOS are equivalent to their propositional counterparts NS/SA/SOS.

Any lower bound on Q-size immediately implies the same lower bound on size. The reason to consider the *existential* Q-degree is a connection between Q-size and existential Q-degree similar to the inequality between size and width in resolution [13] (see Section 3.3).

As a first result we prove that Q-NS, Q-SA, Q-SOS are sound QBF proof systems.

► **Theorem 3.2 (soundness).** *If there exists a Q-NS- or Q-SA- or Q-SOS-refutation of  $\mathcal{Q}.\varphi$ , then  $\mathcal{Q}.\varphi$  is false.*

**Proof.** Suppose, for a contradiction, that  $\mathcal{Q}.\varphi$  is a true QBF, so the  $\exists$ -player has a winning strategy  $\sigma$ , but at the same time there is a refutation of  $\mathcal{Q}.\varphi$  of the form as in eq. (2) where all the variables in polynomials  $q_u$  are on the left of  $u$  and  $q$  is identically zero (Q-NS), or a polynomial with non-negative coefficients (Q-SA), or a sum of squares (Q-SOS).

For every strategy  $\tau$  of the  $\forall$ -player, the game proceeds following the strategies  $\sigma$  and  $\tau$  and constructs a total Boolean assignment  $\alpha_{\sigma,\tau}$  satisfying the matrix  $\varphi$ . That is  $\sum_{p \in \text{enc}(\varphi)} q_p p$  evaluates to 0 under every assignment  $\alpha_{\sigma,\tau}$ . For a universal variable  $u$ , we write  $\tau_{<u}$  for the part of  $\tau$  on variables to the left of  $u$  and  $\tau_{\geq u}$  for the rest of  $\tau$ . Taking a uniform probability distribution over all universal strategies  $\tau$ , for every universal variable  $u$  it holds that:

$$\mathbb{E}_{\tau} [q_u(1 - 2u)] \stackrel{(\star)}{=} \mathbb{E}_{\tau_{<u}} [q_u \mathbb{E}_{\tau_{\geq u}} [1 - 2u]] = \mathbb{E}_{\tau_{<u}} [q_u \cdot 0] = 0,$$

where in the equality  $(\star)$  we used the fact that all the polynomials  $q_u$  only depend on variables on the left of  $u$ . Hence, evaluating both sides of eq. (2) on  $\alpha_{\sigma,\tau}$  and taking  $\mathbb{E}_{\tau}$ , the LHS equals  $\mathbb{E}_{\tau} [q|_{\alpha_{\sigma,\tau}} + 1]$ , which is always at least 1, while the RHS is 0. Contradiction. ◀

► **Remark 3.3 (Q-NS over arbitrary fields).** The definition of Q-NS from eq. (2) can be trivially adapted from polynomials over  $\mathbb{Q}$  to arbitrary fields of characteristic different from 2. In characteristic 2 it gives an unsound system since all the terms  $(1 - 2u)$  are identically 1. Indeed, in characteristic 2 every formula with at least one universal variable could be “refuted” by setting all  $q_p = 0$  and a single  $q_u = 1$ .

► **Remark 3.4 (unary vs binary coefficients).** Unlike in the propositional setting where the unary versions of NS/SA/SOS give rise to non-trivial (and interesting) proof systems [41], in the QBF setting imposing unary (i.e.  $\pm 1$ ) coefficients in Q-NS/Q-SA/Q-SOS refutations seems to give rise to very weak systems. For instance, unary Q-SOS cannot even efficiently refute a false QBF formula as simple as  $\forall u_1 \forall u_2 \cdots \forall u_n. \bigvee_{i=1}^n u_i$ . We omit the argument as it is similar to the one used to prove Theorem 3.2 above.

### 3.1 Completeness via a score game

To show completeness of Q-NS/Q-SA/Q-SOS, we introduce a new *score* game. We call it *score* game to distinguish it from the *evaluation* game used for the QBF semantics (cf. Sec. 2).

The *score* game, as the evaluation game, is played between a universal and an existential player on a QBF  $\mathcal{Q}.\varphi$ , building a total Boolean assignment. As in the evaluation game, the players take turns according to the quantifier prefix  $\mathcal{Q}$  and the existential player can freely decide on the value of existential variables. For the universal variables the score game differs from the usual evaluation game: the universal player gives a preference for the universal

variable  $u$  in the form of a number  $s_u \in \mathbb{Q}$ . Then, the existential player sets  $u$  to  $b \in \{0, 1\}$  and the universal player scores  $s_u(2b - 1)$  points. There are two variants of this game that differ in the winning condition:

**variant 1** the universal player wins if  $\varphi$  is falsified or the total score is strictly positive;

**variant 2** the universal player wins if  $\varphi$  is falsified or the total score equals 1.

Clearly every winning strategy of VARIANT 2 is also a winning strategy of VARIANT 1. The intuition behind the universal preferences is that the sign of  $s_u$  encodes the preferred assignment (if the preferred assignment is  $u = 0$  then the universal player sets  $s_u > 0$ , and  $s_u < 0$  for  $u = 1$ ) and the absolute value encodes the magnitude of this preferred choice. If the existential player follows the choice, the universal player loses  $|s_u|$  points; otherwise he gains the same amount.

Our interest in the score game is that the universal winning strategies can be transformed into Q-NS/Q-SOS refutations.

► **Proposition 3.5.** *A QBF  $\mathcal{Q}.\varphi$  is false if and only if the universal player has a winning strategy in the score game for  $\mathcal{Q}.\varphi$  (in either variant).*

**Proof.** Let the QBF  $\mathcal{Q}.\varphi$  be false. Then there exists a winning strategy  $\tau = (\tau_u)_{u \in \text{vars}_\forall(\mathcal{Q})}$  for the universal player in the evaluation game. In the score game, on the universal variable  $u$  the universal player plays depending on the total score  $S$  up to this point and  $\tau$ . The preferred choice of the universal player is  $\tau_u$  and he assigns to  $u$  score

$$s_u = \begin{cases} 0 & \text{if } S = 1, \\ (1 - 2\tau_u)(1 - S) & \text{otherwise.} \end{cases}$$

If in each step of the game the universal player gets always his preference  $\tau_u$ , then the matrix  $\varphi$  is falsified (since  $\tau$  is a winning strategy in the evaluation game). Otherwise, let  $u^*$  be the first variable where the universal player does not get his preference and  $S^*$  the total score before deciding the value for  $u$ . Since, by assumption the universal player does not get his preference but the value  $1 - \tau_{u^*}$  instead, then, after setting  $u^*$ , the total score is

$$S^* + s_{u^*}(2(1 - \tau_{u^*}) - 1) = 1. \quad (3)$$

At this moment the universal player has essentially just won since he can set all following scores to 0 and the final total score of the game will be 1.

For the other direction, if the universal player has a winning strategy in the score game on  $\mathcal{Q}.\varphi$  then he wins also against the case when the existential player makes the scores negative in each moment of the game. In this case the resulting assignment must falsify the matrix  $\varphi$  since the universal player is using a winning strategy. As such, this strategy is also a winning strategy for the universal player in the usual evaluation game and the QBF  $\mathcal{Q}.\varphi$  is false. ◀

We require the universal strategy for each universal variable  $u$  to be expressed as a polynomial in all variables to the left of  $u$  in the quantifier prefix. The *size* of a universal strategy in the score game is then the sum of the number of monomials in all the  $s_u$ .

► **Theorem 3.6.** *Let  $\pi$  be a shortest Q-SOS (resp. Q-NS) refutation of  $\mathcal{Q}.\varphi$  with respect to its Q-size. Then  $\text{qsize}(\pi)$  equals the size of the shortest universal winning strategy in the score game in VARIANT 1 (resp. VARIANT 2) on  $\mathcal{Q}.\varphi$ .*



**Proof.** Let  $U = \text{vars}_\forall(\mathcal{Q})$ , let  $S$  be the size of the shortest universal winning strategy in the score game on  $\mathcal{Q}.\varphi$ , and let  $\pi$  be the LHS of a shortest Q-SOS (resp. Q-NS) refutation written as

$$\sum_{p \in \text{enc}(\varphi)} q_p p + \sum_{u \in \text{vars}_\forall(\mathcal{Q})} q_u (1 - 2u) + q = -1. \quad (4)$$

To show that  $\text{qsize}(\pi) \geq S$  consider the universal strategy setting  $s_u = q_u$ . This is a winning strategy in the score game, i.e. for every total assignment  $\alpha$  the universal player wins the score game. Indeed, if  $\alpha$  falsifies  $\varphi$  then the universal player wins automatically (in both versions of the game). Assume then that  $\alpha$  satisfies  $\varphi$ , that is for every  $p \in \text{enc}(\varphi)$ ,  $p|_\alpha = 0$ . Therefore,  $\pi$  evaluated at  $\alpha$  is the same as  $\sum_{u \in U} q_u (1 - 2u) + q$  evaluated at  $\alpha$ . The expression  $\sum_{u \in U} q_u (1 - 2u)$  evaluates under  $\alpha$  to  $-1$  if  $\pi$  is a Q-NS refutation or to  $\leq -1 < 0$  if  $\pi$  is a Q-SOS refutation. Therefore the total score when playing the game given the total assignment  $\alpha$  is

$$\sum_{u \in U} s_u (2u - 1) = \left( \sum_{u \in U} q_u (2u - 1) \right) \Big|_\alpha = - \left( \sum_{u \in U} q_u (1 - 2u) \right) \Big|_\alpha$$

and this latter sum equals 1 if  $\pi$  is a Q-NS refutation or it is  $> 0$  if  $\pi$  is a Q-SOS refutation. In other words the universal player in such cases wins using the scores.

To prove  $\text{qsize}(\pi) \leq S$ , we consider the cases where  $\pi$  is a Q-NS or Q-SOS refutation.

**Case 1:  $\pi$  is a Q-NS refutation.** Let  $(s_u)_{u \in U}$  be a shortest universal winning strategy for the score game in VARIANT 2 on  $\mathcal{Q}.\varphi$  and let  $q_u$  be the polynomial computing  $s_u$  as a function of the variables left of  $u$  in  $\mathcal{Q}$ . In particular, on all Boolean assignments  $\alpha$  satisfying the matrix  $\varphi$ , the universal player wins because the total score is 1, i.e.  $(\sum_{u \in U} q_u (1 - 2u))|_\alpha = -1$  and therefore  $\sum_{u \in U} q_u (1 - 2u) + 1$  is in the ideal generated by the polynomials in  $\text{enc}(\varphi)$  (this follows from Fact 2.1). This gives a Q-NS refutation of  $\mathcal{Q}.\varphi$  with a Q-size of at most  $S$ .

**Case 2:  $\pi$  is a Q-SOS refutation.** Let  $(s_u)_{u \in U}$  be a shortest universal winning strategy for the score game in VARIANT 2 on  $\mathcal{Q}.\varphi$  and let  $q_u$  be the polynomial computing  $s_u$  as a function of the variables left of  $u$  in  $\mathcal{Q}$ . For an assignment  $\alpha$ , let  $\text{score}(\alpha) = \sum_{u \in U} s_u (2u - 1)|_\alpha$ . For every Boolean assignment  $\alpha$  satisfying the matrix  $\varphi$ , since  $(s_u)_u$  is a winning strategy, we have  $\text{score}(\alpha) > 0$ . That is for  $c = \frac{1}{2} \min_{\alpha \models \varphi} \text{score}(\alpha)$  we have

$$\sum_{u \in U} \frac{s_u}{c} (1 - 2u) = - \frac{\text{score}(\alpha)}{c} < -1. \quad (5)$$

In this way, for every  $\alpha$  satisfying  $\varphi$ ,  $1 - \frac{\text{score}(\alpha)}{c} < 0$ . Let  $q = - \sum_{\alpha \models \varphi} \left(1 - \frac{\text{score}(\alpha)}{c}\right) \chi_\alpha(\mathbf{v})$ , where  $\chi_\alpha(\mathbf{v})$  is the monomial which evaluates to 1 if the variables  $\mathbf{v}$  are set according to  $\alpha$ , and 0 on any other Boolean assignment. Modulo the polynomials  $v^2 - v$ ,  $q$  is a sum of squares, hence to conclude it is enough to notice that the polynomial  $\sum_{u \in U} \frac{1}{c} q_u (1 - 2u) + q + 1$  evaluates to 0 on every assignment satisfying  $\text{enc}(\varphi)$ , hence it belongs to the ideal generated by the polynomials in  $\text{enc}(\varphi)$  (this follows from Fact 2.1). This gives a Q-SOS refutation of  $\mathcal{Q}.\varphi$  having the same qsize as the strategy  $(s_u)_u$ . ◀

► **Corollary 3.7** (completeness). Q-NS/Q-SA/Q-SOS are complete.

**Proof.** Proposition 3.5 and Theorem 3.6 immediately imply the completeness of Q-NS. As Q-NS refutations are special cases of Q-SA and Q-SOS refutations their completeness also follows. ◀



### 3.2 Upper bounds in Q-SOS via the score game

Due to Theorem 3.6, the score game can be used to obtain bounds on the qsize of Q-SOS refutations. The advantage is being able to argue directly on countermodels (without reference to the syntactic representation of the matrix). To that end, we use QBFs  $Q-C_n$  from [16], which are defined via their countermodel computed by a family of circuits  $C_n$ .

► **Definition 3.8** ( $Q-C_n$  [16]). *Let  $n$  be an integer and  $C_n$  be a circuit with inputs  $x_1, \dots, x_n$  and a single output. We define*

$$Q-C_n = \exists x_1 \dots \exists x_n \forall u \exists t_1 \dots \exists t_m. (u \leftrightarrow C_n(x_1, \dots, x_n)) ,$$

where the additional variables  $t_i$  are used for a Tseitin-encoding of the circuit  $C_n$  into CNF (the  $i^{\text{th}}$  node in  $C_n$  is represented by variable  $t_i$ , and if, e.g., node  $i$  is an  $\wedge$ -gate between nodes  $j$  and  $k$ , then we have clauses encoding  $t_i \leftrightarrow (t_j \wedge t_k)$ , and similarly for  $\vee$  and  $\neg$  gates).

For the  $Q-C_n$  formulas, the only countermodel sets  $u$  to  $C_n(x_1, \dots, x_n)$ . Here, we are specifically interested in choosing circuits  $C_n$  that compute  $\text{Majority}_n$ . A circuit calculating  $\text{Majority}_n$  evaluates to true, if and only if at least half of the  $n$  input variables are set to true. We show that  $Q\text{-Majority}_n$  has short Q-SOS refutations in the qsize measure.

► **Proposition 3.9.**  *$Q\text{-Majority}_n$  has Q-SOS refutations of linear qsize.*

**Proof.** In the score game for  $Q\text{-Majority}_n$ , set  $s_u = -x_1 - \dots - x_n + \frac{n}{2} - \frac{1}{4}$ . The choice of the constant  $\frac{1}{4}$  is somewhat arbitrary, but should be between 0 and  $\frac{1}{2}$ . As there is only a single universal variable, this defines a complete strategy for the universal player. We show that  $s_u$  is a winning strategy. For an arbitrary assignment  $\alpha$ ,  $s_u|_\alpha < 0$  if and only if at least half of the existential  $x_i$  variables are set to 1, otherwise  $s_u|_\alpha > 0$ . As such, the total score of the score game on  $\alpha$  is  $(-x_1 - \dots - x_n + \frac{n}{2} - \frac{1}{4})(2u - 1)|_\alpha$ . This is negative only if either  $u = 1$  and at least half of the  $x_i$  equal 1 or  $u = 0$  and less than half of the  $x_i$  equal 1, i.e. if the matrix is satisfied, the score is positive.

This strategy has size  $n + 1$  and degree 1, hence, by Theorem 3.6, there exists a Q-SOS refutation of  $Q\text{-Majority}_n$  with a qsize linear in  $n$ . ◀

It is known that  $Q\text{-Majority}_n$  requires Q-PC refutations of exponential qsize [21], therefore the previous result yields the exponential separation between Q-PC and Q-SOS in Figure 1.

### 3.3 From existential Q-degree to Q-size

In various proof systems, strong enough lower bounds on the degree/width of proofs immediately imply non-trivial lower bounds on proof size. This happens for instance in propositional proof systems such as Resolution [8], Polynomial Calculus [31], Sherali-Adams and Sum-of-Squares [2]; and in QBF proof systems as well, for instance in QU-Resolution [13], and Q-PC [21]. It turns out that a very similar statement holds in Q-SOS between the existential Q-degree ( $\text{qdeg}_\exists(\cdot)$ , see Definition 3.1) and Q-size ( $\text{qsize}(\cdot)$ , see Definition 3.1).

► **Theorem 3.10.** *Let  $Q.\varphi$  be a false QBF with  $n$  variables that has a Q-SOS refutation of qsize  $s$ . Then it has a Q-SOS refutation of  $\text{qdeg}_\exists O(\sqrt{n \log s})$ .*

The argument is similar to the proof of the analogous size-width inequality for Resolution from [8]. The main difference is the proof of the lemma below showing how to combine a proof of  $\text{qdeg}_\exists k - 1$  of  $Q.\varphi|_{x=1}$  and a proof of  $\text{qdeg}_\exists k$  of  $Q.\varphi|_{x=0}$  into a proof of  $\text{qdeg}_\exists k$  of  $Q.\varphi$ . This is done using the score game from the previous section.

► **Lemma 3.11.** *Let  $Q.\varphi$  be a false QBF and  $x \in \text{vars}_\exists(Q)$ . If there is a Q-SOS refutation  $\pi_1$  of  $Q.\varphi|_{x=1}$  with  $\text{qdeg}_\exists(\pi_1) \leq k-1$ , and a Q-SOS refutation  $\pi_0$  of  $Q.\varphi|_{x=0}$  with  $\text{qdeg}_\exists(\pi_0) \leq k$ , then there is a Q-SOS refutation  $\pi$  of  $Q.\varphi$  with  $\text{qdeg}_\exists(\pi) \leq k$ .*

**Proof.** We consider the equivalent representation of the proofs as universal strategies in the score game. Let  $q_1$  be the final score in  $\pi_1$  and  $q_0$  be the final score in  $\pi_0$ . Let  $c$  be the maximum of  $|q_0| + 1$  over all assignments, and  $d$  be the smallest *positive* value that  $q_1$  can take (or 1 if  $q_1$  does not take positive values). For each  $u \in \text{vars}_\forall(Q)$ , let  $q_u = x \cdot q_u^1 + \frac{d}{c}q_u^0$ , where  $q_u^0$  and  $q_u^1$  are the polynomials for  $u$  in  $\pi_0$  and  $\pi_1$ . Combining these  $q_u$  yields a strategy  $\pi$  with final score  $q = x \cdot q_1 + \frac{d}{c}q_0$  and  $\text{qdeg}_\exists(\pi) \leq k$ .

We still need to argue that  $\pi$  is a universal winning strategy, i.e. that on every assignment  $\alpha$  satisfying  $\varphi$  we have  $q(\alpha) > 0$ . If  $\alpha$  sets  $x = 0$ , then it satisfies  $\varphi|_{x=0}$ , so  $q_0(\alpha) > 0$  due to the correctness of  $\pi_0$ . But if  $x = 0$  then  $q = 0 \cdot q_1 + \frac{d}{c}q_0 > 0$ . If  $\alpha$  sets  $x = 1$ , then it satisfies  $\varphi|_{x=1}$ , so  $q_1(\alpha) > 0$  due to the correctness of  $\pi_1$ . By the definitions of  $c$  and  $d$ , we have  $c > -q_0(\alpha)$  and  $d \leq q_1(\alpha)$ . This means that  $\frac{d}{c}q_0 > -d \geq -q_1(\alpha)$  and  $q = 1 \cdot q_1 + \frac{d}{c}q_0 > 0$ . ◀

► **Lemma 3.12.** *Let  $d, n, b \in \mathbb{N}^{\geq 0}$  and  $Q.\varphi$  be a false QBF. Let  $\pi$  be a Q-SOS refutation of  $Q.\varphi$  so that its  $q_u$  polynomials contain, in total, fewer than  $(1 - \frac{d}{2n})^{-b}$  monomials of existential degree  $> d$ . Then there is a Q-SOS refutation  $\pi'$  of  $Q.\varphi$  with  $\text{qdeg}_\exists(\pi') \leq d + b$ .*

The proof of this lemma is virtually identical to the proof of [8, Theorem 3.5]. Informally, the proof is by an inductive argument on  $n$  and  $b$ , considering the *high-degree* monomials to be the ones with  $\text{qdeg}_\exists$  at least  $d$ . By a counting argument there will be a literal  $x$  appearing in at least a  $\frac{d}{2n}$  fraction of them. Restricting by  $x = 0$  and  $x = 1$ , we have that the first restriction eliminates at least  $\frac{d}{2n}$  of the high-degree monomials, while the second eliminates one variable. Then using the inductive hypothesis and Lemma 3.11 concludes the argument.

Given the two lemmas above it is immediate to prove Theorem 3.10.

**Proof of Theorem 3.10.** Set  $b = d = \sqrt{2n \log s}$  and observe that  $s < (1 - \frac{d}{2n})^{-b}$ . The number of high-degree monomials in the refutation is smaller than its total number of monomials  $s$ , so we can apply Lemma 3.12 and get a refutation of  $\text{qdeg}_\exists(b + d) \in O(\sqrt{n \log s})$ . ◀

## 4 Lower bounds via strategy extraction in the evaluation game

In QBF proof systems, strategy extraction is a welcome and ubiquitous feature. Informally, given a refutation of a false QBF, strategy extraction allows to represent in some computational model a winning strategy of the universal player in the *evaluation* game. Different QBF proof systems give rise to strategy extraction in different computational models. For example, from QU-Res refutations we get *unified decision lists* [13] and from Frege+ $\forall$ -reduction refutations we get  $\text{NC}_1$  circuits [16].

In this section, we show that Q-SOS/Q-SA/Q-NS also admit strategy extraction, using *polynomial threshold functions* (PTF) as the computational model (Theorem 4.3). We use this fact to prove a lower bound in Q-SOS (Corollary 4.4) and a p-simulation of Q-SOS by Q-TC<sub>0</sub>-Frege (Corollary 4.5).

► **Definition 4.1** (polynomial threshold function). *A Boolean function  $f : \{0, 1\}^n \rightarrow \{\pm 1\}$  is computed by a polynomial threshold function (PTF), if there exists some  $n$ -variate polynomial  $p \in \mathbb{Q}[x]$  such that  $f(x) = \text{sign}(p(x))$ . The size of the PTF is the number of monomials in  $p$  and the degree of the PTF is the degree of  $p$ .*

► **Remark 4.2** (On the PTF degree of parity). It is well known that  $f(\mathbf{x}) = x_1 \oplus x_2 \oplus \dots \oplus x_n$  cannot be computed by PTFs of degree less than  $n$ . We recall briefly the argument (see also for instance [46]). Let  $f(\mathbf{x}) = \text{sign}(p(\mathbf{x}))$  with  $p$  a  $n$ -variate polynomial of degree  $d$ . Since  $f$  is symmetric, there exists a symmetric  $n$  variate polynomial  $p'$  such that  $f(\mathbf{x}) = \text{sign}(p'(\mathbf{x}))$  and  $\deg(p') \leq \deg(p) = d$ . Since  $p'$  is symmetric, there exists a univariate polynomial  $p''$  such that  $p'(x_1 + \dots + x_n) = p'(\mathbf{x})$  and  $\deg(p'') = \deg(p')$ . In other words,  $f(\mathbf{x}) = \text{sign}(p''(x_1 + \dots + x_n))$ . To conclude it is enough to notice that on  $0, 1, \dots, n$  the polynomial  $p''$  must be alternating signs and hence it must have at least  $n$  real roots; therefore  $d \geq \deg(p'') \geq n$ .

Given a Q-SOS/Q-SA/Q-NS refutation  $\sum_{p \in \text{enc}(\varphi)} q_p p + \sum_{u \in \text{vars}_\forall(\mathcal{Q})} q_u (1 - 2u) + q + 1 = 0$  of a false QBF  $\mathcal{Q}.\varphi$ , we claim that for every universal variable  $u$ ,  $\text{sign}(q_u)$  computes a strategy for  $1 - 2u$ .<sup>1</sup> This can then be easily transformed into a strategy for  $u$  through a linear output transformation mapping  $-1$  to  $1$  and  $1$  to  $0$ . Per definition, for every universal variable  $u$ ,  $\text{sign}(q_u)$  is a PTF. The size of the extracted strategy is the sum of the sizes of the PTFs and, as such, the Q-size of the refutation. Analogously, the degree of the extracted strategy, i.e. the maximum degree of the PTFs, equals the total Q-degree of the refutation.

► **Theorem 4.3.** *Let  $\sum_{p \in \text{enc}(\varphi)} q_p p + \sum_{u \in \text{vars}_\forall(\mathcal{Q})} q_u (1 - 2u) + q + 1 = 0$  be a Q-SOS/Q-SA/Q-NS proof of a false QBF  $\mathcal{Q}.\varphi$ . Then the universal strategy that maps each universal variable  $u \in \text{vars}_\forall(\mathcal{Q})$  to  $\frac{1 - \text{sign}(q_u)}{2}$  is a countermodel (i.e. falsifies  $\varphi$ ).*

**Proof.** The syntactic restriction of countermodels, i.e. that each variable only depends on variables left of it in the quantifier prefix  $\mathcal{Q}$ , holds by definition of  $q_u$ .

For every universal variable  $u$  played according to the strategy, we have  $q_u(1 - 2u) = q_u \text{sign}(q_u) \geq 0$ . As such,  $\sum_{u \in \text{vars}_\forall(\mathcal{Q})} q_u (1 - 2u) + q + 1 \geq 1$ . Hence,  $\sum_{p \in \text{enc}(\varphi)} q_p p \leq -1$ , which is only possible if the matrix  $\varphi$  is not satisfied (otherwise  $q_p p = 0$  for all  $p \in \text{enc}(\varphi)$ ). ◀

To exemplify the strategy extraction technique for Q-SOS, we use Remark 4.2 and Theorem 4.3 to prove that the Parity formulas [18]

$$\text{Parity}_n = \exists x_1 \dots \exists x_n \forall u \exists t_1 \dots \exists t_n. (t_1 \leftrightarrow x_1) \wedge (u \leftrightarrow t_n) \wedge \bigwedge_{i=2}^n (t_i \leftrightarrow t_{i-1} \oplus x_i).$$

are exponentially hard for Q-SOS. Notice that the only winning strategy for the universal player is to set  $u = x_1 \oplus \dots \oplus x_n$ .

► **Corollary 4.4.** *Every Q-SOS refutation of  $\text{Parity}_n$  requires Q-size  $\exp(\Omega(n))$ .*

**Proof.** Let  $d := \text{qdeg}_\exists(\pi)$  and apply strategy extraction (Theorem 4.3) to get a PTF of degree  $d$  that computes  $u = \bigoplus_{i=1}^n x_i$ . By Remark 4.2, its degree is at least  $n$ , so  $d \geq n$ . Let  $s := \text{qsize}(\pi)$  and apply Theorem 3.10 to obtain  $n \leq d = O(\sqrt{n \log s})$  and therefore  $s = \exp(\Omega(n))$ . Theorem 3.10 can be applied here, because  $\text{Parity}_n$  only has a single universal variable and, as such, its existential Q-degree equals its total Q-degree. ◀

As a second consequence of Theorem 4.3, strategy extraction can also be used to embed Q-SOS into more powerful systems, in this case Q-TC<sub>0</sub>-Frege. Q-TC<sub>0</sub>-Frege is the TC<sub>0</sub>-Frege system with an added universal reduction rule. The Q-size of a Q-TC<sub>0</sub>-Frege refutation is the sum of the number of symbols of all lines involved in a  $\forall$ -reduction step.

► **Corollary 4.5.** *Q-TC<sub>0</sub>-Frege  $p$ -simulates Q-SOS in the qsize measure.*

<sup>1</sup> We use the convention that  $\text{sign}(0) = +1$ .

## 5 Lower bounds via Q-pseudo-expectation

In the propositional setting, the notion of pseudo-expectation is the standard tool to obtain degree lower bounds for SOS, see for instance [40]. Thanks to the size-degree relation for SOS [2], degree lower bounds also give size lower bounds.

Inspired by the propositional notion of pseudo-expectation, we give a notion of pseudo-expectation for Q-SOS and use it to prove lower bounds on the  $\text{qdeg}_{\exists}$  of Q-SOS refutations. In particular, for a false QBF  $\mathcal{Q}.\varphi$  and a Q-SOS expression  $\pi$  of the form

$$\sum_{p \in \text{enc}(\varphi)} q_p p + \sum_{u \in \text{vars}_{\forall}(\mathcal{Q})} q_u (1 - 2u) + q + 1, \quad (6)$$

where all the variables in  $q_u$  are on the left of  $u$  in  $\mathcal{Q}$  and  $q$  is a sum of squares, we consider *witnesses* that  $\pi \neq 0$ , i.e. that  $\pi$  is not a Q-SOS refutation of  $\mathcal{Q}.\varphi$ . In analogy to the propositional case, we call the witnesses we construct *Q-pseudo-expectations*.

► **Definition 5.1** (Q-pseudo-expectation in Q-SOS). *Given  $\mathcal{Q}.\varphi$  and a Q-SOS expression  $\pi$  as in eq. (6), a Q-pseudo-expectation for  $\mathcal{Q}.\varphi$  and  $\pi$  is a linear function  $\tilde{\mathbb{E}}: \mathbb{Q}[V \cup \bar{V}] \rightarrow \mathbb{R}$  such that:*

1.  $\tilde{\mathbb{E}}[1] = 1$ ;
2.  $\tilde{\mathbb{E}}[q + \sum_{p \in \text{enc}(\varphi)} q_p p] \geq 0$ ;
3.  $\tilde{\mathbb{E}}[\sum_{u \in \text{vars}_{\forall}(\mathcal{Q})} q_u (1 - 2u)] \geq 0$ .

In the propositional context, a single pseudo-expectation for SOS typically targets a fixed degree  $d$  and has properties similar to 1.–3. above but for arbitrary  $q_p$  and sum-of-squares  $q$  such that the degree of  $q_p p$  and  $q$  are at most  $d$ . In this way, a single pseudo-expectation rules out the possibility of *any* small-degree SOS refutation. There are exceptions to this general approach, for instance the pseudo-expectations used in [42] that are targeting all SOS proofs over a certain set of monomials, *but* we are not aware of degree lower bounds in SOS proved by constructing a family of pseudo-expectations each tailored to a specific set of polynomials (i.e. as in Definition 5.1 but without the condition in item 3.). In the QBF context, this is what we do. To rule out small  $\text{qdeg}_{\exists}$  Q-SOS refutations we use a family of pseudo-expectations, each targeting *one* possible candidate Q-SOS proof, i.e. an expression as in eq. (6). We formalise this approach in Theorem 5.2 and exemplify it in Theorem 5.3.

► **Theorem 5.2.** *Given a QBF  $\mathcal{Q}.\varphi$ , if for every Q-SOS expression  $\pi$  as in eq. (6) with  $\text{qdeg}_{\exists}(\pi) < d$  there is a pseudo-expectation for  $\mathcal{Q}.\varphi$  and  $\pi$ , then every Q-SOS refutation of  $\mathcal{Q}.\varphi$  has  $\text{qdeg}_{\exists}$  at least  $d$ .*

**Proof.** If there was a Q-SOS refutation  $\pi = 0$  of  $\mathcal{Q}.\varphi$  with  $\text{qdeg}_{\exists}(\pi) < d$ , then taking the pseudo-expectation  $\tilde{\mathbb{E}}$  for  $\mathcal{Q}.\varphi$  and  $\pi$  we get  $\tilde{\mathbb{E}}[\pi] = \tilde{\mathbb{E}}[0] = 0$ . Notice that necessarily  $\tilde{\mathbb{E}}[0] = 0$ , by linearity and the identity  $\tilde{\mathbb{E}}[0 + 0] = \tilde{\mathbb{E}}[0]$ . On the other hand, again by linearity, and the properties of  $\tilde{\mathbb{E}}$ , we get  $\tilde{\mathbb{E}}[\pi] \geq 1$ . ◀

We apply the Q-pseudo-expectation technique to show a  $\text{qdeg}_{\exists}$  lower bound on Q-SOS refutations of the **Equality<sub>n</sub>** formulas [11] where

$$\text{Equality}_n = \exists x_1 \cdots x_n \forall u_1 \cdots u_n \exists t_1 \cdots t_n. \bigwedge_{i=1}^n (t_i \rightarrow (x_i \leftrightarrow u_i)) \wedge \bigvee_{i=1}^n t_i.$$

For the  $\text{qdeg}_{\exists}$  lower bound we only use the fact that every assignment satisfying the matrix sets  $u_i \leftrightarrow x_i$  for some  $i$ .

$\text{Equality}_n$  is a quite simple QBF. Hardness for Q-SOS might suggest that the system is weak.  $\text{Equality}_n$  is also hard for QU-Res and Q-PC [11], but easy in Q-depth- $d$  Frege [11], so the hardness appears to only stem from the expressiveness of the objects used. Similarly, Q-SOS on depth- $d$  arithmetic circuits (instead of polynomials) would shortly prove  $\text{Equality}_n$ , but if polynomials are represented explicitly as sums of monomials,  $\text{Equality}_n$  becomes hard.

► **Theorem 5.3.** *Every Q-SOS refutation  $\pi$  of  $\text{Equality}_n$  has  $\text{qdeg}_\exists(\pi) \geq n$  and  $\text{qsize}(\pi) \geq \exp(\Omega(n))$ .*

**Proof.** Let  $\mathcal{Q}.\varphi$  be the QBF encoding of  $\text{Equality}_n$ . First notice that, thanks to Theorem 3.10, it is enough to prove the  $\text{qdeg}_\exists$  lower bound. (We comment that to do this, the strategy extraction technique from Section 4 would not work here.)

Assume, towards a contradiction, that there is a Q-SOS refutation of  $\mathcal{Q}.\varphi$  of  $\text{qdeg}_\exists(\pi) < n$ :

$$\sum_{p \in \text{enc}(\varphi)} q_p p + \sum_{u \in \text{vars}_\forall(\mathcal{Q})} q_u (1 - 2u) + q + 1 = 0. \quad (7)$$

Let  $\pi$  the LHS of eq. (7). We construct a Q-pseudo-expectation for  $\mathcal{Q}.\varphi$  and  $\pi$ . This, by Theorem 5.2, implies the wanted contradiction.

Given  $\alpha = (\alpha_1, \dots, \alpha_n) \in \{0, 1\}^n$ , let  $\mathbf{x} \mapsto \alpha$  be the Boolean assignment setting  $x_i$  to  $\alpha_i$  for each  $i \in [n]$ . We define analogously  $\mathbf{u} \mapsto \alpha$  and  $\mathbf{t} \mapsto \alpha$ . Given  $\alpha, \beta \in \{0, 1\}^n$ , let  $\alpha \oplus \beta$  be the vector whose  $i$ th entry is the sum  $\alpha_i + \beta_i \pmod{2}$ .

Let  $h = \sum_{u \in \text{vars}_\forall(\mathcal{Q})} q_u (1 - 2u)$ . We have that

$$\sum_{\alpha, \beta \in \{0, 1\}^n} h|_{\mathbf{x} \mapsto \alpha, \mathbf{u} \mapsto \beta} = 0. \quad (8)$$

Let  $\gamma \in \{0, 1\}^n$  be the assignment maximizing  $\sum_{\alpha \in \{0, 1\}^n} h|_{\mathbf{x} \mapsto \alpha, \mathbf{u} \mapsto \gamma}$ . By eq. (8),

$$\sum_{\alpha \in \{0, 1\}^n} h|_{\mathbf{x} \mapsto \alpha, \mathbf{u} \mapsto \gamma} \geq 0. \quad (9)$$

We define our candidate Q-pseudo-expectation as

$$\tilde{\mathbb{E}}(p) = 2^{-n} \sum_{\alpha \in \{0, 1\}^n} p|_{\mathbf{x} \mapsto \alpha, \mathbf{u} \mapsto \gamma, \mathbf{t} \mapsto \alpha \oplus \gamma},$$

and we prove that  $\tilde{\mathbb{E}}$  satisfies all the conditions of the definition of Q-pseudo-expectation. The definition of  $\tilde{\mathbb{E}}$  immediately implies that  $\tilde{\mathbb{E}}[1] = 1$ , and  $\tilde{\mathbb{E}}[h] \geq 0$  follows from eq. (9). Let  $g = q + \sum_{p \in \text{enc}(\varphi)} q_p p$ . To conclude the argument we need to prove that  $\tilde{\mathbb{E}}[g] \geq 0$ .

Since  $g = -h - 1$  and by construction  $h$  cannot contain  $t_i$  variables, the polynomial  $g$  contains only  $x_i$  and  $u_i$  variables. That is,

$$\tilde{\mathbb{E}}[g] = 2^{-n} \sum_{\alpha \in \{0, 1\}^n} g|_{\mathbf{x} \mapsto \alpha, \mathbf{u} \mapsto \gamma} \stackrel{(*)}{=} 2^{-n} \sum_{\alpha \in \{0, 1\}^n} g|_{\mathbf{x} \mapsto \alpha \oplus \gamma, \mathbf{u} \mapsto \gamma},$$

where the last equality  $(*)$  follows as  $\alpha \oplus \gamma$  ranges over all  $\{0, 1\}^n$  just in a different order.

Let  $g'$  be the polynomial such that for every  $\alpha \in \{0, 1\}^n$ ,  $g'|_{\mathbf{x} \mapsto \alpha} = g|_{\mathbf{x} \mapsto \alpha \oplus \gamma, \mathbf{u} \mapsto \gamma}$ . The polynomial  $g'$  is constructed from  $g|_{\mathbf{u} \mapsto \gamma}$  replacing every occurrence of  $x_i$  by  $1 - x_i$  (resp.  $x_i$ ) if  $\gamma_i = 1$  (resp.  $\gamma_i = 0$ ). Crucially,  $g'$  has degree at most  $n - 1$ , since  $\deg(g') \leq \deg_\exists(g) = \deg_\exists(-h - 1) \leq \text{qdeg}_\exists(\pi) \leq n - 1$ . That is, for each monomial  $m$  in  $g'$ , there is some variable  $x_i$  not appearing in it, and  $m$  gets the same value on every pair  $\alpha, \alpha'$  where  $\alpha \in \{0, 1\}^n$  and

$\alpha'$  is identical to  $\alpha$  except in position  $i$ . This implies  $\sum_{\alpha \in \{0,1\}^n} (-1)^{|\alpha|} m|_{x \mapsto \alpha} = 0$ , where  $|\alpha|$  denotes the 1-norm of  $\alpha$ , the sum of all 1s in it. Summing over all monomials in  $g'$ , we get

$$\begin{aligned}
0 &= \sum_{\alpha \in \{0,1\}^n} (-1)^{|\alpha|} g'|_{x \mapsto \alpha} \\
&= \sum_{\alpha \in \{0,1\}^n} g'|_{x \mapsto \alpha} + \sum_{\alpha \in \{0,1\}^n} ((-1)^{|\alpha|} - 1) g'|_{x \mapsto \alpha} \\
&= \sum_{\alpha \in \{0,1\}^n} g|_{x \mapsto \alpha \oplus \gamma, u \mapsto \gamma} + \sum_{\alpha \in \{0,1\}^n} ((-1)^{|\alpha|} - 1) g'|_{x \mapsto \alpha} \\
&= 2^n \tilde{\mathbb{E}}[g] + \sum_{\alpha \in \{0,1\}^n} ((-1)^{|\alpha|} - 1) g'|_{x \mapsto \alpha} .
\end{aligned}$$

Hence, to conclude that  $\tilde{\mathbb{E}}[g] \geq 0$  it is enough to show that

$$\sum_{\alpha \in \{0,1\}^n} ((-1)^{|\alpha|} - 1) g'|_{x \mapsto \alpha} \leq 0 . \quad (10)$$

For  $\alpha$ s such that  $|\alpha|$  is even, the coefficient in front of  $g'|_{x \mapsto \alpha}$  is 0, while for  $\alpha$ s such that  $|\alpha|$  is odd, the coefficient in front of  $g'|_{x \mapsto \alpha}$  is  $-2$ . That is, to prove eq. (10), it suffices to show that for  $\alpha$ s such that  $|\alpha|$  is odd,  $g'|_{x \mapsto \alpha} \geq 0$ . By construction  $g'|_{x \mapsto \alpha} = g|_{x \mapsto \alpha \oplus \gamma, u \mapsto \gamma}$ , and since there are no  $t_i$  variables in  $g$ ,  $g|_{x \mapsto \alpha \oplus \gamma, u \mapsto \gamma} = g|_{x \mapsto \alpha \oplus \gamma, u \mapsto \gamma, t \mapsto \alpha}$ .

Now, if  $|\alpha|$  is odd, in particular  $\alpha \neq \mathbf{0}$  and  $\alpha \oplus \gamma \neq \gamma$ . It is easy to check that the assignment  $x \mapsto \alpha \oplus \gamma, u \mapsto \gamma, t \mapsto \alpha$  sets to 0 (i.e. satisfies) all the polynomials  $p \in \text{enc}(\varphi)$ . Since  $q$  is always non-negative on every assignment, we can conclude that  $g|_{x \mapsto \alpha \oplus \gamma, u \mapsto \gamma, t \mapsto \alpha} \geq 0$  and therefore  $g'|_{x \mapsto \alpha} \geq 0$ .  $\blacktriangleleft$

## 6 Simulations

We now investigate how the algebraic QBF systems relate to each other and to other known QBF proof systems such as QU-Resolution and Q-PC and show the p-simulations of Figure 1.

► **Theorem 6.1.** Q-SOS  $p$ -simulates Q-SA *w.r.t. the size and qsize measures*.

**Proof.** It is well known that (degree  $2d$ ) SOS  $p$ -simulates (degree  $d$ ) SA (see for instance [40, Lemma 3.63]). The same argument works without change in the QBF setting: every variable  $v$  in a positive monomial can be substituted by  $v^2$  summing a suitable multiple of  $v^2 - v$ . In this way, every positive monomial  $\frac{a}{b}m$  with  $a, b \in \mathbb{N}$  can be converted into  $\frac{s_1^2 + s_2^2 + s_3^2 + s_4^2}{b^2}m^2$  where  $s_1, s_2, s_3, s_4$  are four integers that sum up to  $ab$  (they exist by Lagrange's Four Squares Theorem). This converts  $\frac{a}{b}m$  into a sum of at most four squares with rational coefficients.  $\blacktriangleleft$

In the argument above, notice that the only increment in degree is in the propositional part, hence, different from the propositional case, Q-SOS with  $\text{qdeg}_{\exists} d$   $p$ -simulates Q-SA with  $\text{qdeg}_{\exists} d$ . In the qsize measure, the converse also holds.

► **Theorem 6.2.** Q-SA  $p$ -simulates Q-SOS *w.r.t. the qsize measure*.

**Proof.** Every polynomial  $q$  that is non-negative on the Boolean assignments can be written as a (possibly exponentially large) sum of the form  $\sum_{\alpha} q|_{\alpha} \chi_{\alpha}(v)$ , where  $\chi_{\alpha}(v)$  is a monomial that evaluates to 1 when the variables are set according to the Boolean assignment  $\alpha$  and on any other Boolean assignment it is 0. In other words, every Q-SOS refutation can be written as a possibly exponentially larger Q-SA refutation. The exponential blow-up appears in the propositional part which is not accounted for in qsize.  $\blacktriangleleft$



► **Theorem 6.3.** Q-SA  $p$ -simulates QU-Res w.r.t. both size and qsize.

**Proof.** (sketch) The argument in [37, Proposition 1 and Corollary 2] showing that degree  $d$  SA  $p$ -simulates width  $d$  Resolution can be easily adapted to the QBF setting. An alternative proof could be using the characterization of SA as *weighted* Resolution [25, Theorem 5.7]. Weighted Resolution is a proof system handling weighted clauses, i.e. pairs  $(C, w)$  with  $C$  a clause and  $w \in \mathbb{Z}$  (or  $\mathbb{Q}$ ). Adding to weighted Resolution the rule  $\frac{(C \vee u, 2w)}{(C, w)}$ , where all the variables in  $C$  appear left of  $u$  in the quantifier prefix will result in a system  $p$ -equivalent to Q-SA. QU-Res is then  $p$ -equivalent to weighted Resolution augmented with the rule above where all weights in the proofs are non-negative. ◀

► **Theorem 6.4.** Q-PC  $p$ -simulates Q-NS w.r.t. the size and qsize measures.

**Proof.** Let  $\mathcal{Q}.\varphi$  be a false QBF with  $n$  variables and  $m$  clauses and  $\pi$  be a Q-NS refutation of  $\mathcal{Q}.\varphi$  of the form

$$\sum_{p \in \text{enc}(\varphi)} q_p p + \sum_{u \in \text{vars}_{\forall}(\mathcal{Q})} q_u (1 - 2u) + 1 = 0, \quad (11)$$

Lines in a Q-PC proof can be multiplied by arbitrary polynomials. Hence, we can obtain in Q-PC the sum  $\sum_{p \in \text{enc}(\varphi)} q_p p$  from the polynomials in  $\text{enc}(\varphi)$  in a polynomial number of steps. Let  $\text{vars}_{\forall}(\mathcal{Q})$  be  $u_1, u_2, \dots, u_n$ . Due to the symbolic equality in eq. (11), this sum equals  $-1 - \sum_{i=1}^n q_{u_i} (1 - 2u_i)$ . We then use the  $\forall$ -reduction on  $u_n$ , then  $u_{n-1}$  etc. In the first step, restricting by  $u_n = 1$  and  $u_n = 0$ , we get respectively

$$-1 - \sum_{i=1}^{n-1} q_{u_i} (1 - 2u_i) - q_{u_n} \quad \text{and} \quad -1 - \sum_{i=1}^{n-1} q_{u_i} (1 - 2u_i) + q_{u_n}.$$

Adding them, we get  $-1 - \sum_{i=1}^{n-1} q_{u_i} (1 - 2u_i)$ . We repeat this process until we get rid of all universal variables and only the  $-1$  remains. It is clear from the argument that this simulation only increases the size and qsize linearly. ◀

► **Theorem 6.5.** Q-SOS  $p$ -simulates Q-PC w.r.t. the size and qsize measures.

**Proof.** (sketch) The argument in [9, Lemma 3.1] showing that degree  $2d$  SOS  $p$ -simulates degree  $d$  PC adapts easily to the QBF setting. The idea is that given a Q-PC derivation  $p_1, \dots, p_s$  we derive an algebraic expression for  $-p_i^2$  which eventually for  $i = s$  will give a Q-SOS refutation of  $\mathcal{Q}.\varphi$ . This is done inductively on  $i$  and is based on the following algebraic identities:

- sum rule (from  $p$  and  $q$  deduce  $ap + bq$  with  $a, b \in \mathbb{Q}$ ):  
 $-(ap + bq)^2 = -2a^2p^2 - 2b^2q^2 + (ap - bq)^2;$
- product rule (from  $p$  deduce  $xp$ ):  
 $-(xp)^2 = -p^2 + (p - xp)^2 + 2p^2(x - x^2);$
- $\forall$ -reduction (from  $p + qu$  deduce  $p$ ):  
 $-p^2 = -2(p + qu)^2 + (p + q)^2 - (q^2 + 2pq)(1 - 2u) + 2q^2(u^2 - u);$
- $\forall$ -reduction (from  $p + qu$  deduce  $p + q$ ):  
 $-(p + q)^2 = -2(p + qu)^2 + p^2 - (q^2 + 2pq)(1 - 2u) + 2q^2(u^2 - u).$

► **Corollary 6.6.** Q-SOS  $p$ -simulates Q-NS and is exponentially stronger, w.r.t. the size and qsize measures.

**Proof.** The simulation follows from Theorem 6.5 and Theorem 6.4. The separation follows from Proposition 3.9 and Theorem 6.4 for the qsize measure, and from propositional separations [4, 34] for the size measure. ◀



## 7 Conclusion

In this work we defined semi-algebraic proof systems for QBF and initiated their proof complexity investigation. While our results already reveal an interesting picture in terms of simulations and lower and upper bounds, a number of questions remain that appear to be of interest for further research.

In the propositional setting Res and NS are incomparable proof systems. Are also Q-NS and QU-Res incomparable w.r.t. the qsize measure?

In Section 4 we showed how to express strategy extraction for Q-SOS using polynomial threshold functions. Although this suffices for lower bounds, it appears interesting to determine the correct computational model *characterizing* strategy extraction for Q-SOS and Q-NS in the same sense as the tight characterisations for QU-Res [13], Q-PC [21], and QBF Frege systems [16].

Finally, it would be interesting to determine the relationship of our new semi-algebraic QBF systems to the static expansion-based algebraic systems suggested in [29], which might turn out to be incomparable in strength.

---

## References

- 1 Albert Atserias, Johannes Klaus Fichte, and Marc Thurley. Clause-learning algorithms with many restarts and bounded-width resolution. *J. Artif. Intell. Res.*, 40:353–373, 2011. doi:10.1613/jair.3152.
- 2 Albert Atserias and Tuomas Hakoniemi. Size-Degree Trade-Offs for Sums-of-Squares and Positivstellensatz Proofs. In *34th Computational Complexity Conference (CCC 2019)*, volume 137, pages 24:1–24:20, 2019. doi:10.4230/LIPICS.CCC.2019.24.
- 3 Albert Atserias, Massimo Lauria, and Jakob Nordström. Narrow proofs may be maximally long. In *29th Conference on Computational Complexity (CCC 2014)*, pages 286–297, 2014. doi:10.1109/CCC.2014.36.
- 4 Albert Atserias, Massimo Lauria, and Jakob Nordström. Narrow proofs may be maximally long. *ACM Trans. Comput. Logic*, 17(3):19:1–19:30, 2016. A preliminary version of this work appeared as [3]. doi:10.1145/2898435.
- 5 Valeriy Balabanov and Jie-Hong R. Jiang. Unified QBF certification and its applications. *Form. Methods Syst. Des.*, 41(1):45–65, 2012. doi:10.1007/s10703-012-0152-6.
- 6 Valeriy Balabanov, Magdalena Widl, and Jie-Hong R. Jiang. QBF resolution systems and their proof complexities. In *Proc. Theory and Applications of Satisfiability Testing (SAT)*, pages 154–169, 2014. doi:10.1007/978-3-319-09284-3\_12.
- 7 Boaz Barak, Fernando G.S.L. Brandao, Aram W. Harrow, Jonathan Kelner, David Steurer, and Yuan Zhou. Hypercontractivity, sum-of-squares proofs, and their applications. In *44th Annual ACM Symposium on Theory of Computing (STOC 2012)*, pages 307–326, 2012. doi:10.1145/2213977.2214006.
- 8 Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow – Resolution made simple. *J. ACM*, 48(2):149–169, 2001. doi:10.1145/375827.375835.
- 9 Christoph Berkholz. The Relation between Polynomial Calculus, Sherali-Adams, and Sum-of-Squares Proofs. In *35th Symposium on Theoretical Aspects of Computer Science (STACS)*, volume 96, pages 11:1–11:14, 2018. doi:10.4230/LIPICS.STACS.2018.11.
- 10 Olaf Beyersdorff. Proof complexity of quantified Boolean logic – a survey. In Marco Benini, Olaf Beyersdorff, Michael Rathjen, and Peter Schuster, editors, *Mathematics for Computation (M4C)*, pages 353–391. World Scientific, Singapore, 2022.
- 11 Olaf Beyersdorff, Joshua Blinkhorn, and Luke Hindle. Size, cost, and capacity: A semantic technique for hard random QBFs. In *Proc. Conference on Innovations in Theoretical Computer Science (ITCS’18)*, pages 9:1–9:18, 2018. doi:10.4230/LIPICS.ITCS.2018.9.

- 12 Olaf Beyersdorff, Joshua Blinkhorn, and Luke Hinde. Size, cost, and capacity: A semantic technique for hard random QBFs. *Logical Methods in Computer Science*, 15(1), 2019. A preliminary version of this work appeared as [11]. doi:10.23638/LMCS-15(1:13)2019.
- 13 Olaf Beyersdorff, Joshua Blinkhorn, Meena Mahajan, and Tomás Peitl. Hardness characterisations and size-width lower bounds for QBF resolution. *ACM Trans. Comput. Log.*, 24(2):10:1–10:30, 2023. doi:10.1145/3565286.
- 14 Olaf Beyersdorff and Benjamin Böhm. Understanding the relative strength of QBF CDCL solvers and QBF resolution. *Log. Methods Comput. Sci.*, 19(2), 2023. doi:10.46298/lmcs-19(2:2)2023.
- 15 Olaf Beyersdorff, Ilario Bonacina, and Leroy Chew. Lower bounds: From circuits to QBF proof systems. In *Proc. ACM Conference on Innovations in Theoretical Computer Science (ITCS'16)*, pages 249–260, 2016. doi:10.1145/2840728.2840740.
- 16 Olaf Beyersdorff, Ilario Bonacina, Leroy Chew, and Jan Pich. Frege systems for quantified Boolean logic. *J. ACM*, 67(2):9:1–9:36, 2020. Preliminary versions of this work appeared as [15] and [23]. doi:10.1145/3381881.
- 17 Olaf Beyersdorff, Leroy Chew, and Mikoláš Janota. New resolution-based QBF calculi and their proof complexity. *ACM Transactions on Computation Theory*, 11(4):26:1–26:42, 2019. doi:10.1145/3352155.
- 18 Olaf Beyersdorff, Leroy Chew, and Mikoláš Janota. Proof complexity of resolution-based QBF calculi. In *Proc. Symposium on Theoretical Aspects of Computer Science (STACS'15)*, pages 76–89. LIPIcs, 2015. doi:10.4230/LIPIcs.STACS.2015.76.
- 19 Olaf Beyersdorff, Leroy Chew, Meena Mahajan, and Anil Shukla. Understanding cutting planes for QBFs. *Inf. Comput.*, 262:141–161, 2018. doi:10.1016/j.ic.2018.08.002.
- 20 Olaf Beyersdorff, Luke Hinde, and Ján Pich. Reasons for hardness in QBF proof systems. *ACM Transactions on Computation Theory*, 12(2):10:1–10:27, 2020. doi:10.1145/3378665.
- 21 Olaf Beyersdorff, Tim Hoffmann, Kaspar Kasche, and Luc Nicolas Spachmann. Polynomial calculus for quantified boolean logic: Lower bounds through circuits and degree. In *49th International Symposium on Mathematical Foundations of Computer Science (MFCS)*, volume 306, pages 27:1–27:15, 2024. doi:10.4230/LIPIcs.MFCS.2024.27.
- 22 Olaf Beyersdorff, Mikoláš Janota, Florian Lonsing, and Martina Seidl. Quantified Boolean formulas. In Armin Biere, Marijn Heule, Hans van Maaren, and Toby Walsh, editors, *Handbook of Satisfiability, 2nd edition*, Frontiers in Artificial Intelligence and Applications. IOS press, 2021. doi:10.3233/FAIA201015.
- 23 Olaf Beyersdorff and Ján Pich. Understanding Gentzen and Frege systems for QBF. In *Proc. ACM/IEEE Symposium on Logic in Computer Science (LICS)*, 2016. doi:10.1145/2933575.2933597.
- 24 A. Blake. *Canonical expressions in boolean algebra*. PhD thesis, University of Chicago, 1937.
- 25 Ilario Bonacina, Maria Luisa Bonet, and Jordi Levy. Weighted, circular and semi-algebraic proofs. *J. Artif. Intell. Res.*, 79:447–482, 2024. A preliminary version of this work appeared as [26]. doi:10.1613/JAIR.1.15075.
- 26 Maria Luisa Bonet and Jordi Levy. Equivalence between systems stronger than resolution. In *23rd International Conference on Theory and Applications of Satisfiability Testing (SAT 2020)*, volume 12178, pages 166–181, 2020. doi:10.1007/978-3-030-51825-7\_13.
- 27 Sam Buss, Dima Grigoriev, Russell Impagliazzo, and Toniann Pitassi. Linear gaps between degrees for the polynomial calculus modulo distinct primes. *Journal of Computer and System Sciences*, 62(2):267–289, 2001. doi:10.1006/jcss.2000.1726.
- 28 Sam Buss and Jakob Nordström. Proof complexity and SAT solving. In Armin Biere, Marijn Heule, Hans van Maaren, and Toby Walsh, editors, *Handbook of Satisfiability*, Frontiers in Artificial Intelligence and Applications, pages 233–350. IOS Press, 2021. doi:10.3233/FAIA200990.

- 29 Sravanthi Chede, Leroy Chew, Balesh Kumar, and Anil Shukla. Understanding Nullstellensatz for QBFs. *Electron. Colloquium Comput. Complex.*, TR23-129, 2023. URL: <https://eccc.weizmann.ac.il/report/2023/129/>.
- 30 Hubie Chen. Proof complexity modulo the polynomial hierarchy: Understanding alternation as a source of hardness. *ACM Transactions on Computation Theory*, 9(3):15:1–15:20, 2017. doi:10.1145/3087534.
- 31 Matthew Clegg, Jeff Edmonds, and Russell Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *28th Annual ACM Symposium on the Theory of Computing (STOC)*, pages 174–183, 1996. doi:10.1145/237814.237860.
- 32 Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *The Journal of Symbolic Logic*, 44(1):36–50, 1979. doi:10.2307/2273702.
- 33 William Cook, Collette R. Coullard, and György Turán. On the complexity of cutting-plane proofs. *Discrete Applied Mathematics*, 18(1):25–38, 1987. doi:10.1016/0166-218X(87)90039-4.
- 34 Stefan S. Dantchev, Nicola Galesi, Abdul Ghani, and Barnaby Martin. Proof complexity and the binary encoding of combinatorial principles. *SIAM J. Comput.*, 53(3):764–802, 2024. A preliminary version appeared as [35]. doi:10.1137/20M134784X.
- 35 Stefan S. Dantchev, Abdul Ghani, and Barnaby Martin. Sherali-adams and the binary encoding of combinatorial principles. In *14th Latin American Symposium on Theoretical Informatics (LATIN 2020)*, volume 12118, pages 336–347, 2020. doi:10.1007/978-3-030-61792-9\_27.
- 36 Stefan S. Dantchev and Barnaby Martin. Rank complexity gap for lovász-schrijver and sherali-adams proof systems. *Comput. Complex.*, 22(1):191–213, 2013. doi:10.1007/S00037-012-0049-1.
- 37 Stefan S. Dantchev, Barnaby Martin, and Mark Nicholas Charles Rhodes. Tight rank lower bounds for the Sherali-Adams proof system. *Theor. Comput. Sci.*, 410(21-23):2054–2063, 2009. doi:10.1016/J.TCS.2009.01.002.
- 38 Susanna F. de Rezende, Massimo Lauria, Jakob Nordström, and Dmitry Sokolov. The power of negative reasoning. In *36th Computational Complexity Conference (CCC)*, volume 200, pages 40:1–40:24, 2021. doi:10.4230/LIPICS.CCC.2021.40.
- 39 Uwe Egly, Florian Lonsing, and Magdalena Widl. Long-distance resolution: Proof generation and strategy extraction in search-based QBF solving. In *Proc. Logic for Programming, Artificial Intelligence, and Reasoning (LPAR)*, pages 291–308, 2013. doi:10.1007/978-3-642-45221-5\_21.
- 40 Noah Fleming, Pravesh Kothari, and Toniann Pitassi. Semialgebraic proofs and efficient algorithm design. *Found. Trends Theor. Comput. Sci.*, 14(1-2):1–221, 2019. doi:10.1561/04000000086.
- 41 Mika Göös, Alexandros Hollender, Siddhartha Jain, Gilbert Maystre, William Pires, Robert Robere, and Ran Tao. Separations in proof complexity and TFNP. *J. ACM*, 71(4):26:1–26:45, 2024. doi:10.1145/3663758.
- 42 Tuomas Hakoniemi. Feasible interpolation for polynomial calculus and sums-of-squares. In *47th International Colloquium on Automata, Languages, and Programming (ICALP)*, volume 168, pages 63:1–63:14, 2020. doi:10.4230/LIPICS.ICALP.2020.63.
- 43 Mikolás Janota and Joao Marques-Silva. Expansion-based QBF solving versus Q-resolution. *Theor. Comput. Sci.*, 577:25–42, 2015. doi:10.1016/j.tcs.2015.01.048.
- 44 Hans Kleine Büning, Marek Karpinski, and Andreas Flögel. Resolution for quantified Boolean formulas. *Inf. Comput.*, 117(1):12–18, 1995. doi:10.1006/INCO.1995.1025.
- 45 Jean B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM J. Optim.*, 11(3):796–817, 2001. doi:10.1137/S1052623400366802.
- 46 Marvin Minsky and Seymour Papert. *Perceptrons – An introduction to computational geometry*. MIT Press, 1987. doi:10.7551/mitpress/11301.001.0001.

- 47 Ryan O'Donnell and Yuan Zhou. Approximability and proof complexity. In *Proceedings of the Twenty-Fourth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1537–1556. SIAM, 2013. doi:10.1137/1.9781611973105.111.
- 48 Knot Pipatsrisawat and Adnan Darwiche. On the power of clause-learning SAT solvers as resolution engines. *Artif. Intell.*, 175(2):512–525, 2011. doi:10.1016/j.artint.2010.10.002.
- 49 John Alan Robinson. A machine-oriented logic based on the resolution principle. *Journal of the ACM*, 12:23–41, 1965. doi:10.1145/321250.321253.
- 50 Hanif D. Sherali and Warren P. Adams. A hierarchy of relaxations between the continuous and convex hull representations for zero-one programming problems. *SIAM J. Discret. Math.*, 3(3):411–430, 1990. doi:10.1137/0403036.
- 51 Dmitry Sokolov. (semi)algebraic proofs over  $\pm 1$  variables. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, pages 78–90, 2020. doi:10.1145/3357713.3384288.
- 52 Allen Van Gelder. Contributions to the theory of practical quantified Boolean formula solving. In *Proc. Principles and Practice of Constraint Programming (CP)*, pages 647–663, 2012. doi:10.1007/978-3-642-33558-7\_47.
- 53 Lintao Zhang and Sharad Malik. Conflict driven learning in a quantified Boolean satisfiability solver. In *Proc. IEEE/ACM International Conference on Computer-aided Design (ICCAD)*, pages 442–449, 2002. doi:10.1145/774572.774637.