# Understanding Cutting Planes for QBFs

**Olaf Beyersdorff[1], Leroy Chew[1], Meena Mahajan[2], and Anil Shukla[2]**

1 **School of Computing, University of Leeds, United Kingdom**
2 **The Institute of Mathematical Sciences, HBNI, Chennai, India**

**Abstract**

We define a cutting planes system CP+∀red for quantified Boolean formulas (QBF) and analyse the proof-theoretic strength of this new calculus. While in the propositional case, Cutting Planes is of intermediate strength between resolution and Frege, our findings here show that the situation in QBF is slightly more complex: while CP+∀red is again weaker than QBF Frege and stronger than the CDCL-based QBF resolution systems Q-Res and QU-Res, it turns out to be incomparable to even the weakest expansion-based QBF resolution system ∀Exp+Res.

Technically, our results establish the effectiveness of two lower bound techniques for CP+∀red: via strategy extraction and via monotone feasible interpolation.

**1998 ACM Subject Classification** F.2.2 Nonnumerical Algorithms and Problems: Complexity of proof procedures

**Keywords and phrases** proof complexity, QBF, cutting planes, resolution, simulations

## 1 Introduction

The main problem of *proof complexity* is to understand the minimal size of proofs for natural classes of formulas in important proof systems. Proof complexity deeply connects to a number of other areas, most notably computational complexity, circuit complexity, first-order logic, and practical solving. Recently the connection to practical solving has been a main driver for the field. Modern SAT solvers routinely solve huge industrial instances of the NP-hard SAT problem with even millions of variables. Because runs of the solver on unsatisfiable formulas can be interpreted as proofs for unsatisfiability in a system corresponding to the solver, proof complexity provides the main theoretical tool for an understanding of the power and limitations of these algorithms.

During the last decade there has been great interest and research activity to extend the success of SAT solvers to the more expressive *quantified Boolean formulas (QBF)*. Due to its PSPACE completeness (even for restricted versions [2]), QBF is far more expressive than SAT and thus applies to further fields such as formal verification or planning [5, 21, 35].

Triggered by this exciting development in QBF solving, *QBF proof complexity* has seen a stormy development in past years. A number of resolution-based systems have been designed with the aim to capture ideas in QBF solving. Broadly, these systems can be classified into two types corresponding to two principal approaches in QBF solving: proof systems modelling *conflict driven clause learning (CDCL):* Q-resolution Q-Res [7, 29], universal resolution QU-Res [39], long-distance resolution [3], and their extensions [4]; and proof systems modelling *expansion solving*: ∀Exp+Res [28] and their extensions [7]. Proof complexity research of these systems resulted in a complete understanding of the relative complexity of QBF resolution systems [4, 8], and the transfer of classical techniques to QBF systems was thoroughly assessed [9–11]. In addition, stronger QBF Frege and Gentzen systems were defined and investigated [6, 12, 20].

Most SAT and QBF solvers use resolution as their underlying proof system. Resolution is a weak proof systems for which a wealth of lower bounds and in fact lower bound techniques are known (cf. [16, 38]). This raises the question – often controversially discussed within the proof complexity and solving communities – whether it would be advantageous to build solvers on top of more powerful proof systems. While Frege systems appear too strong and proof search is hindered by non-automatisability results [14, 32], a natural system of intermediate strength is Cutting Planes first defined in [19].

Using ideas from integer linear programming [17, 25], Cutting Planes works with linear inequalities, allowing addition of inequalities as well as multiplication and division by positive integers as rules. Translating propositional clauses into inequalities, Cutting Planes derives the contradiction $0 \geq 1$, thereby demonstrating that the original set of inequalities (and hence the corresponding clause set) has no solution. As mentioned, Cutting Planes is a proof system of intermediate strength: it simulates resolution, but allows short proofs for the famous pigeonhole formulas hard for resolution [27], while it is simulated by and strictly weaker than Frege [24, 34].

## Our contributions

For QBFs a similar Cutting Planes system based on integer linear programming has been missing. It is the aim of this paper to define a natural Cutting Planes system for QBF and give a comprehensive analysis of its proof complexity.

**1. Cutting Planes for QBF.** We introduce a complete and sound QBF proof system CP+∀red that works with quantified linear inequalities, where each variable is either quantified existentially or universally in a quantifier prefix. The system CP+∀red extends the classical Cutting Planes system with one single ∀-reduction rule allowing manipulation of universally quantified variables. The definition of the system thus naturally aligns with the QBF resolution systems Q-Res [29] and QU-Res [39] and the stronger QBF Frege systems [6] that likewise add universal reduction to their classical base systems.

Inspired by the recent work on semantic Cutting Planes [23] we also define a stronger system semCP+∀red where in addition to universal reduction all semantically valid inferences between inequalities are allowed (Section 7).

**2. Lower bound techniques for CP+∀red.** We establish two lower bound methods for CP+∀red: strategy extraction (Section 4) and feasible interpolation (Section 5).

*Strategy extraction* as a lower bound technique was first devised for Q-Res [8] and subsequently extended to QBF Frege systems [6, 12]. The technique applies to calculi that allow to efficiently extract winning strategies for the universal player from a refutation (or alternatively Skolem functions for the existential variables from a proof of a true QBF). Here we show that CP+∀red admits strategy extraction in $\mathsf{TC}^0$, thus establishing an appealing link between CP+∀red proofs (which can count) and the counting circuit class $\mathsf{TC}^0$ (Theorem 8). For each function $f \in \mathsf{PSPACE/poly}$ we construct false QBFs $Q_{\mathrm{qbf}}\text{-}f_n$ where each winning strategy forces the universal player to compute $f$. Thus assuming the existence of $f \in \mathsf{PSPACE/poly} \setminus \mathsf{TC}^0$ we obtain lower bounds for $Q_{\mathrm{qbf}}\text{-}f_n$ in CP+∀red (Corollary 9) and even semCP+∀red (Corollary 21).

*Feasible interpolation* is another classical technique transferring circuit lower bounds to proof size lower bounds; however, here we import lower bounds for monotone arithmetic circuits [34] and hence the connection between the circuits and the lines in the proof system is less direct than in strategy extraction. Feasible interpolation holds for classical resolution [31] and Cutting Planes [34], and indeed was shown to be effective for all QBF resolution systems [9].

Following the approach of [34] we establish this technique for CP+∀red (Theorem 12) and in fact for the stronger semCP+∀red (Theorem 22).

It is interesting to note that while feasible interpolation is the only technique known for classical Cutting Planes, we have two conceptually different lower bound methods – and hence more (conditionally) hard formulas in QBF. This is in line with recent findings in [12] showing that lower bounds for QBF Frege either stem from circuit lower bounds (for $\mathsf{NC}^1$) or from classical Frege lower bounds. Our results here illustrate the same paradigm for CP+∀red: lower bounds arise either from $\mathsf{TC}^0$ lower bounds (via strategy extraction) or via classical lower bound methods for Cutting Planes (feasible interpolation).

**3. Relations to other QBF proof systems.** We compare our new system CP+∀red with previous QBF resolution and Frege systems. In contrast to the classical setting, the emerging picture is somewhat more complex: while CP+∀red is strong enough to simulate the core CDCL QBF resolution systems Q-Res and QU-Res and indeed is exponentially stronger than these systems (Theorem 17), CP+∀red is incomparable (under a natural circuit complexity assumption) to even the base system ∀Exp+Res of the expansion resolution systems (Theorem 18). Conceptually, this means that in contrast to the SAT case, QBF solvers based on linear programming and corresponding to CP+∀red will not encompass the full strength of current resolution-based QBF solving techniques.

On the other hand, CP+∀red turns out to be simulated by Frege+∀red, and Frege+∀red is exponentially more powerful than CP+∀red (Theorem 19). While this separation could be achieved by lifting the classical separation [34] to QBF by considering purely existentially quantified formulas, we highlight that our separation also holds for natural QBFs expressing the clique-co-clique principle, which is not known to have a succinct propositional representation.

## 2 Notation and preliminaries

**Quantified Boolean Formulas.** A literal is a Boolean variable or its negation. We say a literal $x$ is complementary to the literal $\neg x$ and vice versa. A *clause* is a disjunction of literals and a *term* is a conjunction of literals. The empty clause is denoted by $\Box$, and is semantically equivalent to false. A formula in *conjunctive normal form* (CNF) is a conjunction of clauses. For a literal $l = x$ or $l = \neg x$, we write $\mathrm{var}(l)$ for $x$ and extend this notation to $\mathrm{var}(C)$ for a clause $C$. Let $\alpha$ be any partial assignment. For a clause $C$, we write $C|_\alpha$ for the clause obtained after applying the partial assignment $\alpha$ to $C$.

Quantified Boolean Formulas (QBFs) extend propositional logic with Boolean quantifiers with the standard semantics that $\forall x.F$ is satisfied by the same truth assignments as $F|_{x=0} \wedge F|_{x=1}$ and $\exists x.F$ as $F|_{x=0} \vee F|_{x=1}$. We assume that QBFs are in *closed prenex form* with a CNF matrix, i.e., we consider the form $\mathcal{Q}_1 x_1 \cdots \mathcal{Q}_n x_n . \phi$ where each $\mathcal{Q}_i$ is either $\exists$ or $\forall$, and $\phi$ is a quantifier-free CNF formula, called the matrix, in the variables $x_1, \ldots, x_n$. Any QBF can be efficiently (in polynomial time) converted to an equivalent QBF in this form (using PSPACE-completeness of such QBFs). We denote such formulas succinctly as $\mathcal{Q} . \phi$. The *index* $\mathrm{ind}(y)$ of a variable $y$ is its position in the prefix $\mathcal{Q}$; for each $i \in [n]$, $\mathrm{ind}(x_i) = i$. If $\mathrm{ind}(x) < \mathrm{ind}(y)$, we say that $x$ occurs *before* $y$, or *to the left of* $y$. The *quantification level* $\mathrm{lv}(y)$ of a variable $y$ in $\mathcal{Q} . \phi$ is the number of alternations of quantifiers to the left of $y$ in the quantifier prefix of $\mathcal{Q} . \phi$. For instance, in the QBF $\exists x_1 \forall x_2 \forall x_3 \exists x_4 \phi$, $\mathrm{lv}(x_1) = 1$, $\mathrm{lv}(x_2) = \mathrm{lv}(x_3) = 2$, and $\mathrm{lv}(x_4) = 3$.

Often it is useful to think of a QBF $\mathcal{Q}_1 x_1 \cdots \mathcal{Q}_n x_n . \phi$ as a game between two players: *universal* ($\forall$) and *existential* ($\exists$). In the $i$-th step of the game, the player $\mathcal{Q}_i$ assigns a value to the variable $x_i$. The existential player wins if $\phi$ evaluates to 1 under the assignment constructed in the game. The universal player wins if $\phi$ evaluates to 0. A *strategy for $x_i$* is a function from all variables of index $< i$ to $\{0, 1\}$. A *strategy* for the universal player is a collection of strategies, one for each universally quantified variable. Similarly, a *strategy* for the existential player is a collection of strategies, one for each existentially quantified variable. A strategy for the universal player is a winning strategy if using this strategy to assign values to variables, the universal player wins any possible game, irrespective of the strategy used by the existential player. Winning strategies for the existential player are similarly defined. For any QBF, exactly one of the two players has a winning strategy. A QBF is false if and only if there exists a *winning strategy* for the universal player ( [26], [1, Sec. 4.2.2], [33, Chap. 19]).

**Proof systems.** Following notation from [18], a *proof system* for a language $\mathcal{L}$ is a polynomial-time onto function $f : \{0, 1\}^* \to \mathcal{L}$. Each string $\phi \in \mathcal{L}$ is a *theorem*, and if $f(\pi) = \phi$, then $\pi$ is a *proof* of $\phi$ in $f$. Given a polynomial-time function $f : \{0, 1\}^* \to \{0, 1\}^*$ the fact that $f(\{0, 1\}^*) \subseteq \mathcal{L}$ is the *soundness property* for $f$ and the fact that $f(\{0, 1\}^*) \supseteq \mathcal{L}$ is the *completeness property* for $f$.

Proof systems for the language of propositional unsatisfiable formulas (UNSAT) are called *propositional proof systems* and proof systems for the language of false QBFs are called *QBF proof systems*. These are *refutational* proof systems. Equivalently, propositional proof systems and QBF proof systems can be defined respectively for the languages of true propositional formulas (TAUT) and of true QBFs. Since any QBF $\mathcal{Q} . \phi$ can be converted in polynomial time to another QBF $\mathcal{Q}' . \phi'$ such that exactly one of $\mathcal{Q} . \phi$ and $\mathcal{Q}' . \phi'$ is true, it suffices to consider only refutational QBF proof systems.

Given two proof systems $f_1$ and $f_2$ for the same language $L$, we say that $f_1$ simulates $f_2$, if there exists a function $g$ and a polynomial $p$ such that $f_1(g(w)) = f_2(w)$ and $|g(w)| \leq p(|w|)$ for all $w$. Thus $g$ translates a proof $w$ of $x \in L$ in the system $f_2$ into a proof $g(w)$ of $x \in L$ in the system $f_1$, with at most polynomial blow-up in proof-size. If there is such a $g$ that is also polynomial-time computable, then we say that $f_1$ p-simulates $f_2$.

**QBF resolution calculi.** *Resolution* (Res), introduced by Blake [13] and Robinson [37], is a refutational proof system for formulas in CNF form. The lines in the Res proofs are clauses. The only inference (resolution) rule is $\frac{C \vee x \qquad D \vee \neg x}{C \cup D}$ where $C, D$ denote clauses and $x$ is a variable. A Res refutation derives the empty clause $\square$.

*Q-resolution* (Q-Res) [29] is a resolution-like calculus operating on QBFs in prenex form with a CNF matrix. The lines in the Q-Res proofs are clauses. It uses the propositional resolution rule above with the side conditions that variable $x$ is existential and if $z \in C$, then $\neg z \notin D$. In addition Q-Res has the universal reduction rule $\frac{C \vee u}{C}$ and $\frac{C \vee \neg u}{C}$ ($\forall$-Red), where variable $u$ is universal and every existential variable $x \in C$ has $\mathrm{lv}(x) < \mathrm{lv}(u)$. If resolution is also permitted on universal variables, then we get the calculus QU-Res [39].

*Expansion-based* calculi are another type of resolution systems significantly different from Q-Res. In this paper, we will briefly refer to one such calculus, the $\forall$Exp+Res from [28].

**Frege systems.** Frege proof systems are the 'textbook' proof systems for propositional logic based on axioms and rules [18]. A Frege system comprises a finite set of axiom schemes and rules. A *Frege proof* is a sequence of formulas (using $\wedge$, $\vee$, $\neg$) where each formula is either a substitution instance of an axiom, or can be inferred from previous formulas by a valid inference rule. Frege systems are required to be sound and implicationally complete.

A refutation of a false QBF $\mathcal{Q} . \phi$ in the system Frege+$\forall$red [6] is sequence of lines $L_1, \ldots, L_\ell$ where each line is a formula, $L_1 = \phi$, $L_\ell = \bot$ and each $L_i$ is inferred from previous lines $L_j$, $j < i$, using the inference rules of Frege or using the reduction rule

$\frac{L_j}{L_j[u/B]}$ ($\forall$**Red**), where $u$ is the rightmost (highest index) variable among the variables of $L_j$, $B$ is a formula containing only variables left of $u$, and $L_j[u/B]$ is the formula obtained from $L_j$ by replacing each occurrence of $u$ in $L_j$ by $B$.

**Circuit classes.** We recall the definitions of some standard circuit classes (cf. [40]). The class $\mathsf{TC}^0$ contains all languages recognisable by polynomial-size circuits using $\neg$, $\vee$, $\wedge$ and threshold gates with bounded depth and unbounded fan-in. Stronger classes are obtained by using $\mathsf{NC}^1$ circuits of polynomial size and logarithmic depth with bounded fan-in $\neg$, $\vee$, $\wedge$ gates, and by $\mathsf{P/poly}$ circuits of polynomial size. We use non-uniform classes throughout.

**Decision lists [36].** A *decision list* is a list $L$ of pairs $(t_1, v_1), \ldots, (t_r, v_r)$, where each $t_i$ is a term and $v_i$ is a value in $\{0, 1\}$, and the last term $t_r$ is the constant term **true** (i.e., the empty term). A decision list $L$ defines a Boolean function as follows: for any assignment $\alpha$, $L(\alpha)$ is defined to be equal to $v_j$ where $j$ is the least index such that $t_j|_\alpha = 1$. (Such an item always exists, since the last term always evaluates to 1). In [6], this definition has been generalised to $\mathcal{C}$-decision lists (for some circuit class $\mathcal{C}$), where instead of terms one can use circuits from $\mathcal{C}$. A $\mathcal{C}$-decision list yields the circuit $f(x) = \vee_{i=1}^{r} (v_i \wedge C_i(x) \wedge \wedge_{j<i} \neg C_j(x))$. Thus a polynomial-sized $\mathsf{TC}^0$-decision list yields a $\mathsf{TC}^0$ circuit.

## 3 The CP+∀red proof system

In this section we define a QBF analogue of the classical Cutting Planes proof system by augmenting it with a reduction rule for universal variables. We denote this system by CP+∀red. Consider a false quantified set of inequalities $\mathcal{F} \equiv \mathcal{Q}_1 x_1 \ldots \mathcal{Q}_n x_n.\ F$, where $F$ is a set of linear inequalities of the form $\sum x_i a_i \geq A$ for integers $a_i$ and $A$, and $F$ includes the set of inequalities $B = \{x_i \geq 0, -x_i \geq -1 \mid i \in [n]\}$. The inequalities in $B$ are called the Boolean axioms, because they force any integer-valued assignment $\bar{a}$ to the variables, satisfying $F$, to take only $0, 1$-values. We point out that classical Cutting Planes proof systems (only existential variables) can refute any inconsistent set of linear inequalities over integers. However, once universal quantification is allowed, dealing with an unbounded domain is more messy. Since our primary goal in defining this proof system is to refute false QBFs, and since QBFs have only Boolean variables, we only consider sets of inequalities that contain $B$.

▶ **Definition 1** (CP+∀red proofs for inequalities)**.** Consider a set of quantified inequalities $\mathcal{F} \equiv \mathcal{Q}_1 x_1 \ldots \mathcal{Q}_n x_n.\ F$, where $F$ also contains the Boolean axioms. A CP+∀red refutation $\pi$ of $\mathcal{F}$ is a quantified sequence of linear inequalities $\mathcal{Q}_1 x_1 \ldots \mathcal{Q}_n x_n.[I_1, I_2, \ldots, I_l]$ where the quantifier prefix is the same as in $\mathcal{F}$, $I_l$ is an inequality of the form $0 \geq C$ for some positive integer $C$, and for every $j \in \{1, \ldots, l\}$, either $I_j \in F$, or $I_j$ is derived from earlier inequalities in the sequence via one of the following inference rules:

1. **Addition**: From $\sum_k c_k x_k \geq C$ and $\sum_k d_k x_k \geq D$, derive $\sum_k (c_k + d_k) x_k \geq C + D$.
2. **Multiplication**: From $\sum_k c_k x_k \geq C$, derive $\sum_k d c_k x_k \geq dC$, where $d \in \mathbb{Z}^+$.
3. **Division**: From $\sum_k c_k x_k \geq C$, derive $\sum_k \frac{c_k}{d} x_k \geq \left\lceil \frac{C}{d} \right\rceil$, where $d \in \mathbb{Z}^+$ divides each $c_k$.
4. **∀-red**: From $\sum_{k \in [n] \setminus \{i\}} c_k x_k + h x_i \geq C$, derive $\begin{cases} \sum_{k \in [n] \setminus \{i\}} c_k x_k \geq C & \text{if } h > 0; \\ \sum_{k \in [n] \setminus \{i\}} c_k x_k \geq C - h & \text{if } h < 0. \end{cases}$

   This rule can be used provided variable $x_i$ is universal, and provided all existential variables with nonzero coefficients in the hypothesis are to the left of $x_i$ in the quantification prefix.

(That is, if $x_j$ is existential, then $j > i \Rightarrow c_j = 0$.) Observe that when $h > 0$, we are replacing $x_i$ by 0, and when $h < 0$, we are replacing $x_i$ by 1. We say that the universal variable $x_i$ has been reduced.

Each inequality $I_j$ is a line in the proof $\pi$. Note that proof lines are always of the form $\sum_k c_k x_k \geq C$ for integer-valued $c_k, C$. The length of $\pi$ (denoted $|\pi|$) is the number of lines in it, and the size of $\pi$ (denoted size($\pi$)) is the bit-size of a representation of the proof (this depends on the number of lines and the binary length of the numbers in the proof).

In order to use CP+∀red as a refutational system for QBFs in prenex form with CNF matrix, we must translate QBFs into quantified sets of inequalities.

▶ **Definition 2** (Encoding QBFs as inequalities)**.** We first describe how to encode a CNF formula $F$ over variables $x_1, \ldots, x_n$ as a set of linear inequalities. Define $R(x) = x$, $R(\bar{x}) = 1 - x$. A clause $C \equiv (l_1 \vee \cdots \vee l_k)$ is translated into the inequality $R(C) \equiv \sum_{i=1}^{k} R(l_i) \geq 1$. A CNF formula $\phi = C_1 \wedge \cdots \wedge C_m$ is represented as the set of inequalities $F_\phi = \{R(C_1), R(C_2), \ldots, R(C_m)\} \cup B$, where $B$ is the set of Boolean axioms $x \geq 0, -x \geq -1$ for each variable $x$. We call this the standard encoding. For a QBF $\mathcal{Q}_1 x_1 \ldots \mathcal{Q}_n x_n .\ \phi$ with a CNF matrix $\phi$, the encoding is the quantified set of linear inequalities $\mathcal{Q}_1 x_1 \ldots \mathcal{Q}_n x_n .\ F_\phi$.

We say that a 0, 1-assignment $\alpha$ satisfies the inequality $I \equiv \sum_{i=1}^{n} a_i x_i \geq b$ (i.e., $I|_\alpha = 1$), if $\sum_{i=1}^{n} a_i \alpha_i \geq b$. For any clause $C$, an assignment satisfies $C$ if and only if it satisfies $R(C)$. Since the standard encoding includes all Boolean axioms, we obtain the following:

▶ **Proposition 3.** *Let $\mathcal{Q} . \phi$ be a QBF in closed prenex CNF, and let $\mathcal{F} = \mathcal{Q} .\ F_\phi$ be its encoding as a quantified set of linear inequalities. Then $\mathcal{Q} . \phi$ is false if and only if $\mathcal{F}$ is false.*

As for QBFs, we can play the 2-player game on the encoding $\mathcal{F}$ of a QBF. Players choose 0-1 values for their variables in the order defined in the prefix. The ∀ player wins if the assignment so constructed violates some inequality in $F$. As before, when $\mathcal{F}$ is false, the universal player has a winning strategy; otherwise the existential player has a winning strategy.

▶ **Definition 4** (CP+∀red proofs for QBFs)**.** Let $\mathcal{Q} . \phi = \mathcal{Q}_1 x_1 \cdots \mathcal{Q}_n x_n . \phi$ be a false QBF in prenex CNF, and let $\mathcal{F}$ be its encoding as a quantified set of linear inequalities. A CP+∀red (refutation) proof of $\mathcal{Q} . \phi$ is a CP+∀red proof of $\mathcal{F}$ as defined in Definition 1.

It is worth noting that a CP+∀red proof for inequalities, as in Definition 1, can start with encodings of QBFs, but can also start with quantified sets of inequalities that contain the Boolean axioms but do not correspond to any QBF, since the initial non-Boolean inequalities can have arbitrary integer coefficients.

Observe that in the ∀-red step of CP+∀red, if $u$ is the universal variable being reduced, then $u$ need not be the rightmost variable with a non-zero coefficient. There may be universal variables to the right of $u$ with non-zero coefficients. This is analogous to the conditions in QU-Res. However, in the Frege+∀red proof system defined in [6], the variable being reduced from a formula is required to be the rightmost in the formula. We show below that imposing such a condition in CP+∀red does not affect the strength of the proof system. That is, if we call a proof where the ∀-red steps are applied only to the rightmost universal variables with non-zero coefficients a **normal-form** proof, then any CP+∀red proof can be efficiently converted to one in normal form. In later sections we often assume this normal form.

▶ **Lemma 5.** *Any CP+∀red proof can be converted into normal form in polynomial time.*

**Proof.** (Sketch.) To reduce a variable $u$, first reduce all universal variables to the right of $u$, then reduce $u$, then re-introduce the previously reduced variables using Boolean axioms. ◀

Now we show that CP+∀red is a complete and sound proof system for false QBFs.

▶ **Theorem 6.** *CP+∀red is a complete and sound proof system for false QBFs. That is, if $\varphi$ is a false QBF, then there exists a CP+∀red refutation of $\varphi$ (completeness), and if there exists a CP+∀red refutation of $\varphi$, then $\varphi$ is false (soundness).*

**Proof.** (Sketch.) Completeness: We show that CP+∀red p-simulates QU-Res; given a QU-Res proof $\pi$, for each $C \in \pi$ we can derive $R(C)$ in CP+∀red. (The resolution rule is simulated by the CP part as in the classicial case, and the ∀-Red rule of QU-Res is also present in CP+∀red.) Since QU-Res is known to be complete, it follows that CP+∀red is complete.

Soundness: Let $\mathcal{F} = \mathcal{Q}.\ F$ be the standard encoding of $\varphi$, and let $\pi = \mathcal{Q}.[I_1, I_2, \ldots, I_l]$ be a normal form CP+∀red refutation of $\mathcal{F}$. We show that the following is valid for each $j \in [l]$: $\mathcal{Q}.\ [F \wedge I_1 \wedge \cdots \wedge I_{j-1}] \implies \mathcal{Q}.\ [F \wedge I_1 \wedge \cdots \wedge I_{j-1} \wedge I_j]$. Thus if $\mathcal{F} = \mathcal{Q}.F$ is true, then so is $\mathcal{Q}.\ [F \wedge I_1 \wedge \cdots \wedge I_{l-1} \wedge I_l]$. However, $I_l$ is not satisfied by any assignment, so this statement is false. Hence $\mathcal{F}$ is false, and by Proposition 3, $\varphi$ is also false. ◀

Note that for false quantified inequalities, the soundness of CP+∀red follows from the same proof, but completeness will require an additional argument.

Since we will refer to the p-simulation of QU-Res by CP+∀red later, we state it as a separate lemma; the proof is in the completeness part of the proof of Theorem 6.

▶ **Lemma 7.** *CP+∀red p-simulates QU-Res.*

## 4 Strategy extraction for CP+∀red

*Strategy extraction* is an important paradigm in QBF, also very desirable in practise (cf. [3, 7, 22, 26]). Winning strategies for the universal player can be very complex. But a QBF proof system has the strategy extraction property for a particular class of circuits $\mathcal{C}$ whenever we can efficiently extract, from every refutation $\pi$ of a false QBF $\varphi$, a winning strategy for the universal player where the strategies for individual universal variables are computable in circuit class $\mathcal{C}$.

In this section we show how to extract, from a refutation in CP+∀red, winning strategies computable by bounded depth circuits with threshold gates.

▶ **Theorem 8** (Strategy Extraction Theorem)**.** *Given a false QBF $\varphi = \mathcal{Q}.\ \phi$, with $n$ variables, and a CP+∀red refutation $\pi$ of $\varphi$ of size $m$, it is possible to extract from $\pi$ a winning strategy where for each universal variable $u \in \varphi$, the strategy $\sigma_u$ can be computed by Boolean circuits of $(m+n)^{O(1)}$ size, constant depth, with unbounded fanin AND, OR, NOT gates as well as threshold gates. In particular, if $\varphi$ can be refuted in CP+∀red in $n^{O(1)}$ size, then the winning strategies can be computed in $\mathsf{TC}^0$.*

**Proof.** (Sketch.) We adapt the technique from [6]. Let $\mathcal{Q}.\ F$ be the standard encoding of $\varphi$, and let $\pi = \mathcal{Q}.\ [I_1, \ldots, I_l]$ be a normal-form CP+∀red proof of $\mathcal{Q}.\ F$ of length $l$ and size $m \geq l$. For $j \in \{0, 1, \ldots, l\}$, define $\pi_j = \mathcal{Q}.\ [I_{j+1}, \ldots, I_l]$ and $F_j = F \cup \{I_1, \ldots, I_j\}$. By downward induction on $j$, from $\pi_j$ we show how to compute, for each universal variable $u$, a Boolean function $\sigma_u^j$ that maps each assignment to the variables quantified before $u$ to a bit $\{0, 1\}$. These functions satisfy the property that in a 2-player game played on the formula $\mathcal{Q}.\ F_j$, if the universal player uses strategy $\sigma_u^j$ for each universal variable $u$, then finally some inequality in $F_j$ is falsified. We describe the functions $\sigma_u^j$ by decision lists of size $O(l)$, where each condition is checkable by a constant-depth polynomial-in-$m$ sized threshold circuit.

Since all axioms are included in $F$, we can skip the axiom download steps in the proof.

The strategy is as follows: $\sigma_u^l = 0$ for all $u$. For $j \le l$, if $I_j$ is obtained by a classical rule, then $\sigma_u^{j-1} = \sigma_u^j$ for every universal variable $u$. If $I_j$ is derived using a $\forall$-red rule; that is $I_j = I_k|_{u=b_j}$ for some $k < j$, then for all $u' \neq u$, $\sigma_{u'}^{j-1} = \sigma_{u'}^j$. For $u$, if $I_k|_{u=b_j}(\vec{a}) = 0$, then $\sigma_u^{j-1}(\vec{a}) = b_j$, else $\sigma_u^{j-1}(\vec{a}) = \sigma_u^j(\vec{a})$. (The value $I_k|_{u=b_j}(\vec{a})$ can be determined since variables to the right of $u$ have zero coefficient in $I_k$.) It is easy to see that these functions so defined have the desired property. ◀

Theorem 8 yields the following conditional lower bound for CP+∀red proof size.

▶ **Corollary 9.** *If* PSPACE/poly $\not\subseteq$ TC$^0$*, then there exists a family of false QBFs* $Q_{qbf}$-$f_n$ *that requires super-polynomial size proofs in CP+∀red.*

**Proof.** Let $f_n \in$ PSPACE/poly $\setminus$ TC$^0$. Consider the following false sentence based on $f_n$:

$$\exists x_1 \dots x_n \forall z. \left[ f(\vec{x}) \neq z \right].$$

Since $f_n$ is in PSPACE/poly and QBF is PSPACE-complete, the value of $f_n$ can be compactly expressed by a QBF. That is, $f_n(\vec{x}) \equiv \mathcal{Q}_1 y_1 \dots \mathcal{Q}_r y_r . \psi_n(\vec{x}, \vec{y})$ where $r$ is polynomial in $n$ and $\psi_n(\vec{x}, \vec{y})$ is in P/poly. Thus we have the false sentence

$$\exists x_1 \dots x_n \forall z. \Big[ \overbrace{(\mathcal{Q}_1 y_1 \dots \mathcal{Q}_r y_r . \psi_n(\vec{x}, \vec{y}))}^{f_n(\vec{x})} \leftrightarrow \neg z \Big].$$

We now choose circuits $C_n$ computing $\psi_n$ and use additional variables $\vec{s}$ and $\vec{t}$ to represent the gate values in the P/poly circuits $C_n$ and $\neg C_n$, respectively. We obtain the QBF

$$\exists x_1 \dots x_n \forall z \mathcal{Q}_1 y_1 \dots \mathcal{Q}_r y_r \bar{\mathcal{Q}}_1 w_1 \dots \bar{\mathcal{Q}}_r w_r \exists \vec{s}, \vec{t}.\ \left[ (C_n(\vec{x}, \vec{y}, \vec{s}) \vee z) \wedge \left( \neg C_n(\vec{x}, \vec{w}, \vec{t}) \vee \neg z \right) \right]$$

where $\bar{\mathcal{Q}} = \exists$ if $\mathcal{Q} = \forall$ and vice versa. We call this formula $Q_{qbf}$-$f_n$ and remark that it is a false prenex QBF with CNF matrix. ($C_n$ can be expressed as a CNF; then adding the literal $z$ to each clause expresses $C_n \vee z$. Similarly for $\neg C_n \vee \neg z$.)

In the two-player game on $Q_{qbf}$-$f_n$ or on its standard encoding, the only winning strategy for the universal variable $z$ is the function $f_n(\vec{x})$ itself. Therefore if there exists a polynomial size CP+∀red proof for $Q_{qbf}$-$f_n$, then from Theorem 8, $f_n \in$ TC$^0$, a contradiction. ◀

## 5 Feasible (monotone) interpolation for CP+∀red

In this section we show that CP+∀red admits feasible monotone interpolation. We adapt the technique first used by Pudlák [34] to re-prove and generalise the result of Krajíček [31].

Consider a false QBF of the form

$$\varphi = \exists \vec{p} \mathcal{Q} \vec{q} \mathcal{Q} \vec{r} . \left[ A'(\vec{p}, \vec{q}) \wedge B'(\vec{p}, \vec{r}) \right]$$

where $\vec{p}$, $\vec{q}$, and $\vec{r}$ are mutually disjoint sets of propositional variables, $A'(\vec{p}, \vec{q})$ is a set of clauses using only the $\vec{p}$ and $\vec{q}$ variables, and $B'(\vec{p}, \vec{r})$ is a set of clauses using only the $\vec{p}$ and $\vec{r}$ variables. Thus $\vec{p}$ are the common variables between them. The $\vec{q}$ and $\vec{r}$ variables can be quantified arbitrarily, with any number of quantification levels. Since $\varphi$ is false, on any assignment $\vec{a}$ to the variables in $\vec{p}$, either $\varphi_{\vec{a},0} = \mathcal{Q}\vec{q}.\ A'(\vec{a}, \vec{q})$ or $\varphi_{\vec{a},1} = \mathcal{Q}\vec{r}.\ B'(\vec{a}, \vec{r})$ (or both) must be false. An interpolant for $\varphi$ is a Boolean function that, given $\vec{a}$, indicates which of $\varphi_{\vec{a},0}$, $\varphi_{\vec{a},1}$ is false. As defined in [9], a QBF proof system $S$ admits feasible interpolation if from an $S$-proof $\pi$ of such a QBF $\varphi$, we can extract a Boolean circuit $C_\pi$ computing an interpolant for $\varphi$, such that, the size of $C_\pi$ is polynomially related to the size of $\pi$. If, whenever the $\vec{p}$ variables occur only positively in $A'$ or only negatively in $B'$, the polynomial sized (with respect to the size of $\pi$) interpolating circuit for $\varphi$ is monotone, then we say that $S$ admits monotone feasible interpolation.

Cutting Planes naturally gives rise to arithmetic rather than Boolean circuits, as in the classical case in [34]. Generalising this to the case of QBFs, we have the following definitions.

▶ **Definition 10.** [34] A monotone real circuit is a circuit which computes with real numbers and uses arbitrary non-decreasing real unary and binary functions as gates.

We say that a monotone real circuit computes a Boolean function (uniquely determined by the circuit), if for all inputs of 0's and 1's the circuit outputs 0 or 1.

▶ **Definition 11.** A QBF proof system $S$ admits *monotone real feasible interpolation* if for any false QBF $\varphi$ of the form $\exists\vec{p}\mathcal{Q}\vec{q}\mathcal{Q}\vec{r}.\big[A'(\vec{p},\vec{q}) \wedge B'(\vec{p},\vec{r})\big]$ where the $\vec{p}$ variables occur only positively in $A'$ or only negatively in $B'$, and for any $S$-proof $\pi$ of $\varphi$, we can extract from $\pi$ a monotone real circuit $C$ of size polynomial in the length of $\pi$ and the number $n$ of $\vec{p}$ variables, such that $C$ computes a Boolean function, and on every $0,1$ assignment $\vec{a}$ for $\vec{p}$,

$$C(\vec{a}) = 0 \implies \mathcal{Q}\vec{q}.A'(\vec{a},\vec{q}) \text{ is false, and}$$
$$C(\vec{a}) = 1 \implies \mathcal{Q}\vec{r}.B'(\vec{a},\vec{r}) \text{ is false.}$$

Such a $C$ is called a monotone real interpolating circuit for $\varphi$.

We prove that the CP+∀red proof system for false QBFs has this property:

▶ **Theorem 12.** *CP+∀red for false QBFs admits monotone real feasible interpolation.*

To prove this, we will actually prove a stronger theorem, about interpolants for all false quantified sets of inequalities (not just those arising from false QBFs).

▶ **Theorem 13.** *CP+∀red for inequalities admits monotone real feasible interpolation. That is, let $\mathcal{F}$ be any false quantified set of inequalities of the form $\exists\vec{p}\mathcal{Q}\vec{q}\mathcal{Q}\vec{r}.\big[A(\vec{p},\vec{q}) \wedge B(\vec{p},\vec{r})\big]$ where $A \cup B$ includes all Boolean axioms, and where the coefficients of $\vec{p}$ are either all non-negative in $A$ or are all non-positive in $B$. If $\mathcal{F}$ has a CP+∀red-proof $\pi$, of length $l$, then we can extract a monotone real circuit $C$ of size polynomial in $l$ and the number $n$ of $\vec{p}$ variables in $\mathcal{F}$, such that $C$ computes a Boolean function, and on any $0,1$ assignment $\vec{a}$ to $\vec{p}$,*

$$C(\vec{a}) = 0 \implies \mathcal{Q}\vec{q}.A(\vec{a},\vec{q}) \text{ is false, and}$$
$$C(\vec{a}) = 1 \implies \mathcal{Q}\vec{r}.B(\vec{a},\vec{r}) \text{ is false.}$$

*Such a $C$ is called a monotone real interpolating circuit for $\mathcal{F}$.*

**Proof.** (Sketch.) Let $\pi = \exists\vec{p}\mathcal{Q}\vec{q}\mathcal{Q}\vec{r}.\ [I_1,\dots,I_l]$ be a CP+∀red refutation of $\mathcal{F}$. The idea, as in [34], is to associate with each inequality

$$I \equiv \sum_k e_k p_k + \sum_i f_i q_i + \sum_j g_j r_j \geq D$$

in $\pi$, two inequalities

$$I_0 \equiv \sum_i f_i q_i \geq D_0, \quad I_1 \equiv \sum_j g_j r_j \geq D_1$$

depending on the Boolean assignment $\vec{a}$ to the $\vec{p}$ variables, in such a way that

- $I_0$ and $I_1$ together imply $I|_{\vec{a}}$. (It suffices to ensure $D_0 + D_1 \geq D - \sum_k e_k a_k$.)

- $I_0$ can be derived solely from the $\mathcal{Q}\vec{q}.A(\vec{a},\vec{q})$ part in CP+∀red.
- $I_1$ can be derived solely from the $\mathcal{Q}\vec{r}.B(\vec{a},\vec{r})$ part in CP+∀red.

Then the inequalities corresponding to the last step of the proof, $I_l$, are $0 \geq D_0$ and $0 \geq D_1$, with $D_0 + D_1 \geq 1$. Hence $D_0 > 0 \implies \vec{Q}\vec{q}.A(\vec{a},\vec{q})$ is false, and $D_1 > 0 \implies \vec{Q}\vec{r}.B(\vec{a},\vec{r})$ is false. Note that we only need to compute one of the values $D_0$, $D_1$ to identify a false part of $\mathcal{F}$. Furthermore, we will show that if all the coefficients $e_k$ in $B(\vec{p},\vec{r})$ are non-positive, then $D_1$ can be computed by a real monotone circuit of size $O(nl)$. If all the coefficients $e_k$ in $A(\vec{p},\vec{q})$ are non-negative, then we will show that $-D_0$ can be computed by a real monotone circuit of size $O(nl)$. (The inputs to the circuit are an assignment $\vec{a}$ to the $\vec{p}$ variables.) Applying the unary non-decreasing threshold function $D_1 > 0$? or $-D_0 \geq 0$? to its output will then give a monotone real interpolating circuit for $\mathcal{F}$. ◀

Using monotone interpolation (Theorem 12), we now prove an unconditional lower bound for the CP+∀red proof system, which is based on the false clique-co-clique formulas from [9].

▶ **Definition 14.** Fix positive integers $k, n$ with $k \leq n$. $\textsc{CliqueCoClique}_{n,k}$ is the class of QBFs of the form $\exists\vec{p}\mathcal{Q}\vec{q}\mathcal{Q}\vec{r}.\ [A_{n,k}(\vec{p},\vec{q}) \wedge B_{n,k}(\vec{p},\vec{r})]$ where

- $\vec{p}$ is the set of variables $\{p_{uv} \mid 1 \leq u < v \leq n\}$. An assignment to $\vec{p}$ picks a set of edges, and thus an $n$-vertex graph that we denote $G_{\vec{p}}$.
- $\mathcal{Q}\vec{q}.\ A_{n,k}(\vec{p},\vec{q})$ is a QBF expressing the property that $G_{\vec{p}}$ has a clique of size $k$.
- $\mathcal{Q}\vec{r}.\ B_{n,k}(\vec{p},\vec{r})$ is a QBF expressing the property that $G_{\vec{p}}$ has no clique of size $k$.

Any QBF in $\textsc{CliqueCoClique}_{n,k}$ expresses the clique-co-clique principle (there is a graph both containing and not containing a $k$-clique) and is obviously false. In [9], a particular QBF $\varphi_n \in \textsc{CliqueCoClique}_{n,n/2}$ of size polynomial in $n$ is described. It can be easily generalised to QBFs $\varphi_{n,k} \in \textsc{CliqueCoClique}_{n,k}$ of size polynomial in $n$.

Let $\Phi_{n,k}$ be any QBF in $\textsc{CliqueCoClique}$, and suppose that it has a CP+∀red proof of length $l$. From Theorem 12, we obtain a monotone real circuit $C$ of size $O(l + n^2)$ computing a Boolean function, such that for every $0, 1$ input vector $\vec{a}$ of length $\binom{n}{2}$ encoding a graph $G$, $C(\vec{a}) = 1 \iff G$ has a $k$ clique.

In [34], Pudlák showed the following exponential lower bound on the size of real monotone circuits interpolating the famous "clique-color" encodings.

▶ **Theorem 15** ( [34]). *Suppose that the inputs for a monotone real circuit $C$ are $0, 1$ vectors of length $\binom{n}{2}$ encoding in the natural way graphs on an $n$-element set. Suppose that $C$ outputs $1$ on all cliques of size $k$ and outputs $0$ on all complete $(k-1)$-partite graphs, where $k = \lfloor \frac{1}{8}(n/\log n)^{2/3} \rfloor$. Then the size of the circuit is at least $2^{\Omega((n/\log n)^{1/3})}$.*

(In some earlier literature, clique-color has been referred to as clique-co-clique. However, this is misleading because the clique-color encoding is weaker than $\Phi_{n,k}$ in the following sense. The clique-color encoding says that there exists a graph which has a $k$-clique and is complete $(k-1)$-partite (maximal $(k-1)$-colorable). A graph may neither have a $k$-clique nor be complete $(k-1)$-partite, so both parts of the clique-color formula may be false. Our clique-co-clique formulas, on the other hand, always have exactly one true part.)

Since complete $(k-1)$-partite graphs have no $k$-clique, the real monotone interpolating circuit $C$ we obtain from a CP+∀red proof of $\Phi_{n,k}$ also satisfies the premise of Theorem 15. Hence, $C$ must have size exponential in $n$. But $C$'s size is polynomially related to the length of the CP+∀red proof of $\Phi_{n,k}$. We have thus obtained the following:

▶ **Corollary 16.** *For $k = \lfloor \frac{1}{8}(n/\log n)^{2/3} \rfloor$, any false QBF $\Phi_{n,k} \in \textsc{CliqueCoClique}_{n,k}$ requires proofs of length exponential in $n$ in the CP+∀red proof system. In particular, the QBF $\varphi_{n,k}$ from Definition 14 requires proofs of length exponential in $|\varphi_{n,k}|$ in CP+∀red.*

## 6 Relative power of CP+∀red and other QBF proof systems

In this section we relate the power of CP+∀red with other well known QBF proof systems.

▶ **Theorem 17.** *CP+∀red is exponentially stronger than Q-Res and QU-Res.*

**Proof.** By Lemma 7, CP+∀red p-simulates QU-Res (and hence Q-Res), and is thus at least as strong as them. From classical proof complexity we know that false CNF formulas based on the pigeonhole principle are easy for Cutting Planes proof system [19] but hard for resolution [27]. Therefore CP+∀red is exponentially more powerful than any QBF proof system based on resolution (Q-Res, QU-Res, etc); these systems cannot simulate CP+∀red. ◀

▶ Remark. Note that the separating QBFs have only existential quantification. However, there are also separating QBFs using universal quantifiers (cf. the appendix).

This means that CP+∀red is stronger than the classical CDCL proof systems. However, as we show next, is is weaker than even the base system of expansion solving.

▶ **Theorem 18.** *CP+∀red and ∀Exp+Res are incomparable unless* P/poly = $\mathsf{TC}^0$*, i.e.,*

- *∀Exp+Res cannot simulate CP+∀red.*
- *If* P/poly $\not\subseteq$ $\mathsf{TC}^0$ *then CP+∀red cannot simulate ∀Exp+Res.*

**Proof.** In [28], Janota and Marques-Silva show that there exists a family of false QBFs which are hard for ∀Exp+Res but easy to refute in Q-Res. As CP+∀red p-simulates Q-Res (Lemma 7), we conclude that ∀Exp+Res cannot simulate CP+∀red.

For the second claim let $f_n \in$ P/poly $\setminus$ $\mathsf{TC}^0$ be computed by circuit family $C_n$ of size $l(n) \in n^{O(1)}$. We use $C_n$ to express the obviously false sentence $\exists x_1 \cdots x_n \forall z. f(\vec{x}) \neq z$. Associate a variable $t_i$ with each gate $g_i$ in $C_n$, and consider the QBF

$$Q\text{-}f_n \equiv \exists x_1 \cdots x_n \forall z \exists t_1 \cdots t_l . (t_l \neq z) \wedge \bigwedge_{i=1}^{l} (t_i \text{ is consistent with the inputs to gate } i).$$

The inner formula can be written as an $O(l)$-sized CNF, so $Q\text{-}f_n$ has size $n^{O(1)}$. Note that $Q\text{-}f_n$ has a single universal variable $z$, and the (only) winning strategy for the universal player is $z = f(\vec{x})$. If $Q\text{-}f_n$ has a proof of size polynomial in $n$, then by Theorem 8, this strategy, and hence $f_n$, are in $\mathsf{TC}^0$, a contradiction. On the other hand, from [8, Proposition 28], we know that the formula $Q\text{-}f_n$ can be refuted in ∀Exp+Res in $O(n + l)$ steps. ◀

▶ **Theorem 19.** *Frege+∀red is exponentially stronger than CP+∀red: Frege+∀red p-simulates CP+∀red, whereas CP+∀red does not simulate Frege+∀red.*

**Proof.** (Sketch.) In the classical (propositional) setting, Cook, Coullard and Turán [19] first showed that Extended Frege p-simulates Cutting Planes. Then Goerdt [24] showed that even Frege p-simulates Cutting Planes. Using techniques from [15], [19], and [24], we show that the same simulation goes through with minor modifications for QBFs.

Since Frege is exponentially more powerful than Cutting Planes over propositional formulas (as witnessed by the clique-colour formulas [34], see also Section 5), the converse simulation fails, and CP+∀red and Frege+∀red are exponentially separated. ◀

There are also separating examples with non-trivial universal quantifiers. In Section 5, we described a class of QBF formulas expressing the clique-co-clique principle. By Corollary 16, none of them have short proofs in CP+∀red. We show that a particular member of this class (i.e., a particular way of encoding clique-co-clique) has short proofs in Frege+∀red.

▶ **Theorem 20.** *There is a* $\Phi_{n,k} \in \textsc{CliqueCoClique}_{n,k}$ *of size polynomial in* $n$*, with a Frege+∀red proof of size polynomial in* $n$*.*

## 7 Semantic cutting planes for QBFs

The classical Cutting Planes proof system can be extended to the semantic Cutting Planes proof system by allowing the following semantic inference rule: from inequalities $I'$, $I''$, we can infer $I$ in one step if every Boolean assignment satisfying both $I'$ and $I''$ also satisfies $I$. In [23], it is shown that semantic Cutting Planes is exponentially more powerful than Cutting Planes. We now augment the system semantic Cutting Planes with the ∀-reduction rule as defined for CP+∀red, to obtain a QBF version denoted semCP+∀red. In fact, in this system we need only two rules, semantic inference and ∀-reduction, since the addition, multiplication and division rules of Cutting Planes are also semantic inferences, and the Boolean axioms can be semantically inferred from any inequality.

It is clear that semCP+∀red is sound and complete. However it is not possible to verify the semantic rule efficiently (unless P= NP).

As in CP+∀red, we call a semCP+∀red proof $\pi$ a normal-form proof if ∀-red is applied only to the rightmost universal variable. Since one can use Boolean axioms in semCP+∀red; Lemma 5 is valid in semCP+∀red as well. That is one can convert any semCP+∀red proof $\pi$ into a normal form in polynomial time.

Clearly, SemCP+∀red is at least as powerful as CP+∀red. From classical proof complexity we known that semantic Cutting Planes is exponentially more powerful than Cutting Planes [23]. That is, in [23, Theorem 2], it has been shown that for every $n$, there exists a CNF formula $F_n$ which has a short semantic Cutting Planes refutation but needs $2^{n^{\Omega(1)}}$ lines to refute in Cutting Planes. Thus semCP+∀red is also exponentially more powerful than CP+∀red, as witnessed by these purely existentially quantified formulas.

In Theorem 8, we established strategy extraction from CP+∀red proofs. These results hold for semCP+∀red proofs as well; if $I_j$ is obtained by semantic inference, we do not change the strategy functions and let $\sigma_u^{j-1} = \sigma_u^j$ for every universal variable $u$. Thus all the conditional lower bounds on CP+∀red (Corollary 9, Theorem 18) continue to hold:

▶ **Corollary 21.** *1. If PSPACE $\not\subseteq$ TC$^0$, then for any $f_n \in$ PSPACE $\setminus$ TC$^0$, the false QBFs $Q_{qbf}$-$f_n$ require super-polynomial size proofs in semCP+∀red.*

*2. If P/poly $\not\subseteq$ TC$^0$, then semCP+∀red cannot simulate ∀Exp+Res. For any $f_n \in$ P/poly$\setminus$TC$^0$, the false QBFs $Q$-$f_n$ require super-polynomial size proofs in semCP+∀red.*

For obtaining unconditional lower bounds, we need an analogue of real monotone interpolation (Theorems 12, 13). For this, we adapt the corresponding proof technique used in the classical case from [23]. Using their technique for semantic inference, and handling axioms and ∀-reduction rules as in the proof of Theorem 13, everything goes through as desired.

▶ **Theorem 22.** *SemCP+∀red admits monotone real feasible interpolation for false QBFs.*

Using Theorem 22, we obtain an unconditional exponential lower bound for semCP+∀red, analogous to Corollary 16.

▶ **Corollary 23.** *For $k = \lfloor \frac{1}{8}(n/\log n)^{2/3} \rfloor$, any false QBF $\Phi_{n,k} \in$ CliqueCoClique$_{n,k}$ requires proofs of length exponential in $n$ in the semCP+∀red proof system. In particular, the QBFs $\varphi_{n,k}$ from Definition 14 require proofs of length exponential in $|\varphi_{n,k}|$ in semCP+∀red.*

**Acknowledgements.** This work was supported by the EU Marie Curie IRSES grant CORCON, grant no. 48138 from the John Templeton Foundation, EPSRC grant EP/L024233/1, and a Doctoral Training Grant from EPSRC (2nd author).

## References


1 Sanjeev Arora and Boaz Barak. *Computational Complexity – A Modern Approach.* Cambridge University Press, 2009.

2 Albert Atserias and Sergi Oliva. Bounded-width QBF is PSPACE-complete. *J. Comput. Syst. Sci.*, 80(7):1415–1429, 2014.

3 Valeriy Balabanov and Jie-Hong R. Jiang. Unified QBF certification and its applications. *Formal Methods in System Design*, 41(1):45–65, 2012.

4 Valeriy Balabanov, Magdalena Widl, and Jie-Hong R. Jiang. QBF resolution systems and their proof complexities. In *SAT'14*, pages 154–169, 2014.

5 Marco Benedetti and Hratch Mangassarian. QBF-based formal verification: Experience and perspectives. *JSAT*, 5(1-4):133–191, 2008.

6 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. ACM, 2016.

7 Olaf Beyersdorff, Leroy Chew, and Mikoláš Janota. On unification of QBF resolution-based calculi. In *MFCS, II*, pages 81–93, 2014.

8 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.

9 Olaf Beyersdorff, Leroy Chew, Meena Mahajan, and Anil Shukla. Feasible interpolation for QBF resolution calculi. In *Proc. International Colloquium on Automata, Languages, and Programming (ICALP'15)*, pages 180–192. Springer, 2015.

10 Olaf Beyersdorff, Leroy Chew, Meena Mahajan, and Anil Shukla. Are short proofs narrow? QBF resolution is not simple. In *Proc. Symposium on Theoretical Aspects of Computer Science (STACS'16)*, 2016.

11 Olaf Beyersdorff, Leroy Chew, and Karteek Sreenivasaiah. A game characterisation of tree-like Q-resolution size. In *LATA*, pages 486–498. Springer, 2015.

12 Olaf Beyersdorff and Ján Pich. Understanding Gentzen and Frege systems for QBF. In *Proc. ACM/IEEE Symposium on Logic in Computer Science (LICS)*, 2016.

13 A. Blake. *Canonical expressions in boolean algebra.* PhD thesis, University of Chicago, 1937.

14 Maria Luisa Bonet, Carlos Domingo, Ricard Gavaldà, Alexis Maciel, and Toniann Pitassi. Non-automatizability of bounded-depth Frege proofs. *Computational Complexity*, 13(1–2):47–68, 2004.

15 Samuel R. Buss. Polynomial size proofs of the propositional pigeonhole principle. *J. Symb. Log.*, 52(4):916–927, 1987.

16 Samuel R. Buss. Towards NP-P via proof complexity and search. *Ann. Pure Appl. Logic*, 163(7):906–917, 2012.

17 Václav Chvátal. Edmonds polytopes and weakly hamiltonian graphs. *Math. Program.*, 5(1):29–40, 1973.

18 Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *The Journal of Symbolic Logic*, 44(1):36–50, 1979.

19 William J. Cook, Collette R. Coullard, and György Turán. On the complexity of cutting-plane proofs. *Discrete Applied Mathematics*, 18(1):25–38, 1987.

20 Uwe Egly. On sequent systems and resolution for QBFs. In *Theory and Applications of Satisfiability Testing (SAT'12)*, pages 100–113, 2012.

21 Uwe Egly, Martin Kronegger, Florian Lonsing, and Andreas Pfandler. Conformant planning as a case study of incremental QBF solving. In *Artificial Intelligence and Symbolic Computation (AISC'14)*, pages 120–131, 2014.

22 Uwe Egly, Florian Lonsing, and Magdalena Widl. Long-distance resolution: Proof generation and strategy extraction in search-based QBF solving. In *Logic for Programming, Artificial Intelligence, and Reasoning - 19th International Conference (LPAR)*, pages 291–308, 2013.

23 Yuval Filmus, Pavel Hrubes, and Massimo Lauria. Semantic versus syntactic cutting planes. In *33rd Symposium on Theoretical Aspects of Computer Science, STACS , Orléans, France*, pages 35:1–35:13, 2016.

24 Andreas Goerdt. Cutting plane versus Frege proof systems. In *Computer Science Logic, 4th Workshop, CSL '90, Heidelberg, Germany, October 1-5, Proceedings*, pages 174–194, 1990.

25 Ralph E. Gomory. Outline of an algorithm for integer solutions to linear programs. *Bulletin of the American Mathematical Society*, 64(5):275–278, 1958.

26 Alexandra Goultiaeva, Allen Van Gelder, and Fahiem Bacchus. A uniform approach for generating proofs and strategies for both true and false QBF formulas. In *IJCAI*, pages 546–553, 2011.

27 Amin Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297–308, 1985.

28 Mikolás Janota and Joao Marques-Silva. Expansion-based QBF solving versus Q-resolution. *Theor. Comput. Sci.*, 577:25–42, 2015.

29 Hans Kleine Büning, Marek Karpinski, and Andreas Flögel. Resolution for quantified Boolean formulas. *Inf. Comput.*, 117(1):12–18, 1995.

30 Jan Krajíček. *Bounded Arithmetic, Propositional Logic and Complexity Theory.* Cambridge University Press, 1995.

31 Jan Krajíček. Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic. *The Journal of Symbolic Logic*, 62(2):457–486, 1997.

32 Jan Krajíček and Pavel Pudlák. Some consequences of cryptographical conjectures for $S_2^1$ and $EF$. *Information and Computation*, 140(1):82–94, 1998.

33 Christos H. Papadimitriou. *Computational Complexity.* Addison-Wesley, 1994.

34 Pavel Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *J. Symb. Log.*, 62(3):981–998, 1997.

35 Jussi Rintanen. Asymptotically optimal encodings of conformant planning in QBF. In *AAAI*, pages 1045–1050. AAAI Press, 2007.

36 Ronald L. Rivest. Learning decision lists. *Machine Learning*, 2(3):229–246, 1987.

37 John Alan Robinson. A machine-oriented logic based on the resolution principle. *Journal of the ACM*, 12:23–41, 1965.

38 Nathan Segerlind. The complexity of propositional proofs. *Bulletin of Symbolic Logic*, 13(4):417–481, 2007.

39 Allen Van Gelder. Contributions to the theory of practical quantified Boolean formula solving. In *CP*, pages 647–663, 2012.

40 Heribert Vollmer. *Introduction to Circuit Complexity – A Uniform Approach.* Texts in Theoretical Computer Science. Springer Verlag, Berlin Heidelberg, 1999.

## Appendix

The appendix contains all proofs and details omitted from the main part of the paper due to space constraints.

## More details supplementing Section 2

*Expansion-based* calculi are another type of resolution systems significantly different from Q-Res. These calculi are based on *instantiation* of universal variables and operate on clauses that comprise only existential variables from the original QBF, which are additionally *annotated* by a substitution to some universal variables, e.g. $\neg x^{u/0,v/1}$. For any annotated literal $l^\sigma$, the substitution $\sigma$ must not make assignments to variables right of $l$, i.e. if $u \in \mathsf{dom}(\sigma)$, then $u$ is universal and $\mathrm{lv}(u) < \mathrm{lv}(l)$. To preserve this invariant, we use the *auxiliary notation* $l^{[\sigma]}$, which for an existential literal $l$ and an assignment $\sigma$ to the universal variables filters out all assignments that are not permitted, i.e. $l^{[\sigma]} = l^{\{u/c \in \sigma \mid \mathrm{lv}(u) < \mathrm{lv}(l)\}}$. We say that an assignment is complete if its domain is all universal variables. Likewise, we say that a literal $x^\tau$ is fully annotated if all universal variables $u$ with $\mathrm{lv}(u) < \mathrm{lv}(x)$ in the QBF are in $\mathsf{dom}(\tau)$, and a clause is fully annotated if all its literals are fully annotated.

The calculus ∀Exp+Res from [28] works with fully annotated clauses on which resolution is performed. For each clause $C$ from the matrix and an assignment $\tau$ to all universal variables, ∀Exp+Res can use the axiom $\left\{l^{[\tau]} \mid l \in C, l \text{ existential}\right\} \cup \{\tau(l) \mid l \in C, l \text{ universal}\}$. As its only rule it uses the resolution rule on annotated variables

$$\frac{C \vee x^\tau \qquad D \vee \neg x^\tau}{C \cup D} \text{ (Res)}.$$

**Frege systems.** Frege proof systems are the common 'textbook' proof systems for propositional logic based on axioms and rules [18]. The lines in a Frege proof are propositional formulas built from propositional variables $x_i$ and Boolean connectives $\neg$, $\wedge$, and $\vee$. A Frege system comprises a finite set of axiom schemes and rules, e.g., $\phi \vee \neg\phi$ is a possible axiom scheme. A *Frege proof* is a sequence of formulas where each formula is either a substitution instance of an axiom, or can be inferred from previous formulas by a valid inference rule. Frege systems are required to be sound and implicationally complete. The exact choice of the axiom schemes and rules does not matter as any two Frege systems are p-equivalent, even when changing the basis of Boolean connectives [18] and [30, Theorem 4.4.13].

Usually Frege systems are defined as proof systems where the last formula is the proven formula. We use here the equivalent setting of refutation Frege systems where we start with the negation of the formula that we want to prove and derive the contradiction $\bot$.

A refutation of a false QBF $\mathcal{Q}\,.\,\phi$ in the system Frege+∀red [6] is sequence of lines $L_1, \dots, L_\ell$ where each line is a formula, $L_1 = \phi$, $L_\ell = \bot$ and each $L_i$ is inferred from previous lines $L_j$, $j < i$, using the inference rules of Frege or using the reduction rule

$$\frac{L_j}{L_j[u/B]} \text{ } (\forall\textbf{Red}),$$

where $u$ is the rightmost (highest index) variable among the variables of $L_j$, $B$ is a formula containing only variables left of $u$, and $L_j[u/B]$ is the formula obtained from $L_j$ by replacing each occurrence of $u$ in $L_j$ by $B$.

## Missing proofs from Section 3

**Lemma 5.** *Any CP+∀red proof can be converted into normal form in polynomial time.*

**Proof.** (of Lemma 5) Let $\pi$ be any CP+∀red proof of a false QBF $\varphi$. We efficiently convert $\pi$ into a normal-form proof $\pi'$ using the Boolean axioms. Let inequality $I'$ be derived in $\pi$ from $I$ by a ∀-reduction step on $w$. If $w$ is the rightmost universal variable in $I$, then nothing needs to be done. Otherwise, in any case, no existential variable right of $w$ can have non-zero coefficient in $I$. Let $(w =)w_0, w_1, \ldots, w_k$ be the universal variables right of (including) $w$ with non-zero coefficients $h_0, h_1, \ldots, h_k$ in $I$. We obtain $I'$ from $I$ via the following $(3k+1)$ steps:
For $j = k$ down to 0, reduce $w_j$.
For $j = 1$ up to $k$, if $h_j > 0$ then add $h_j(w_j \geq 0)$, else add $(-h_j)(-w_j \geq -1)$.
Observe that this proof fragment is in normal-form. ◀

**Theorem 6.** *CP+∀red is a complete and sound proof system for false QBFs. That is, if $\varphi$ is a false QBF, then there exists a CP+∀red refutation of $\varphi$ (completeness), and if there exists a CP+∀red refutation of $\varphi$, then $\varphi$ is false (soundness).*

**Proof.** Completeness: We show that CP+∀red p-simulates QU-Res; given a QU-Res proof $\pi$, for each $C \in \pi$ we can derive $R(C)$ in CP+∀red.

We know that the rules of the classical cutting planes system can p-simulate the resolution rule [19]. Observe that the same simulation works independent of the quantifier prefix or the nature of the pivot variable. Now we show how CP+∀red simulates the ∀-red rule of QU-Res proof system. Consider a ∀-red step in QU-Res of the form $\frac{C \vee u}{C}$, where $u$ is universal and all existential variables in the clause $C$ come before $u$ in the prefix. By induction we have derived the inequality $R(C \vee u)$ for the clause $C \vee u$. Reducing $u$ from this inequality is valid. Clearly, the coefficient of $u$ in the inequality $R(C \vee u)$ is $+1$. Hence in the CP+∀red proof, using the ∀-red rule assigns $u = 0$ and hence derives $R(C)$. Similarly, for $\frac{C \vee \bar{u}}{C}$, the coefficient of $u$ in the inequality $R(C \vee \bar{u})$ is $-1$ (the variable $u$ contributes $(1-u)$ to $R(C \vee \bar{u})$), hence the ∀-red rule in CP+∀red sets $u = 1$ and again derives $R(C)$.

Since QU-Res is known to be complete, it follows that CP+∀red is complete.

Soundness: Let $\mathcal{Q} . \phi = \mathcal{Q}_1 x_1 \cdots \mathcal{Q}_n x_n . \phi$ be a QBF in closed prenex CNF form, and let $\mathcal{F} = \mathcal{Q}.\ F$ be its encoding as inequalities. Recall that $F$ also includes Boolean axioms. Let $\pi = \mathcal{Q}_1 x_1 \ldots \mathcal{Q}_n x_n . [I_1, I_2, \ldots, I_l]$ be any CP+∀red refutation (see Definition 1) of $\mathcal{F}$. We can assume (using Lemma 5) that $\pi$ is in normal form.

To prove soundness, we need to show that $\mathcal{Q} . \phi$ is false. From Proposition 3, it suffices to show that $\mathcal{F}$ is false. We do this by showing that the following is valid for each $j \in [l]$:

$$\mathcal{Q}_1 x_1 \ldots \mathcal{Q}_n x_n .\ [F \wedge I_1 \wedge \cdots \wedge I_{j-1}] \implies \mathcal{Q}_1 x_1 \ldots \mathcal{Q}_n x_n .\ [F \wedge I_1 \wedge \cdots \wedge I_{j-1} \wedge I_j],$$

where $I_j$ is derived from some inequalities before it via an inference rule of CP+∀red. Observe that the cases when $I_j$ is derived via Addition, Multiplication, or Division rules are straightforward, since every Boolean assignment satisfying $F \wedge I_1 \wedge \cdots \wedge I_{j-1}$ also satisfies $I_j$. We now concentrate on the ∀-red step.

Say $I_j$ is derived from $I_k$, $k < j$, via the ∀-red rule. Let $u = x_r$ be the universal variable reduced, and let $I_k$ be $\sum_s c_s x_s \geq C$ for some integers $c_1, \ldots, c_n, C$. Since $\pi$ is in normal form, for all $s > r$, $c_s = 0$.

Suppose the claimed statement is not valid. That is, $\mathcal{F}_{j-1} = \mathcal{Q} . F \wedge I_1 \wedge \cdots \wedge I_{j-1}$ is true but $\mathcal{F}_j = \mathcal{Q} . F \wedge I_1 \wedge \cdots \wedge I_j$ is false. The existential player has a winning strategy $\sigma_\exists$ for $\mathcal{F}_{j-1}$, while the universal player has a winning strategy $\sigma_\forall$ for $\mathcal{F}_j$. Let $\alpha$ be the assignment constructed when the players use these strategies for their variables. Then $\alpha$ satisfies $F \wedge I_1 \wedge \cdots \wedge I_{j-1}$, and in particular, $I_k$, but does not satisfy $I_j$. Define a new strategy $\sigma'_\forall$ for the universal player; it uses the same strategy as $\sigma_\forall$ for variables other than $x_r$, but flips the strategy of $\sigma_\forall$ for variable $x_r$. Let $\beta$ be the assignment constructed by strategies $\sigma_\exists$ and $\sigma'_\forall$. Then $\beta_s = \alpha_s$ for all $s < r$, and $\beta_r \neq \alpha_r$. These are the only values that matter for evaluating $I_k$. An examination of the $\forall$-red rule shows that it derives the tighter of the two inequalities $I_k|_{x_r=0}$ and $I_k|_{x_r=1}$ as $I_j$, and hence $I_k(\beta)$ equals $I_j(\alpha)$ and is false. Thus the existential player using strategy $\sigma_\exists$ does not win against the universal player using strategy $\sigma'_\forall$, and hence is not a winning strategy for $\mathcal{F}_{j-1}$, a contradiction.

Now let us assume that $\mathcal{F}$ is true, then we conclude that $\mathcal{Q}_1 x_1 \ldots \mathcal{Q}_n x_n.[I_1, I_2, \ldots, I_l]$ is also true. A contradiction, as the last inequality $I_l \equiv 0 \geq C$ is always false. ◀

## Missing proofs from Section 4

**Theorem 8 (Strategy Extraction Theorem).** *Given a false QBF $\varphi = \mathcal{Q}.\ \phi$, with $n$ variables, and a CP+∀red refutation $\pi$ of $\varphi$ of size $m$, it is possible to extract from $\pi$ a winning strategy where for each universal variable $u \in \varphi$, the strategy $\sigma_u$ can be computed by Boolean circuits of $(m+n)^{O(1)}$ size, constant depth, with unbounded fanin AND, OR, NOT gates as well as threshold gates. In particular, if $\varphi$ can be refuted in CP+∀red in $n^{O(1)}$ size, then the winning strategies can be computed in $\mathsf{TC}^0$.*

**Proof.** We adapt the technique from [6]. Let $\mathcal{Q}.\ F$ be the standard encoding of $\varphi$, and let $\pi = \mathcal{Q}.\ [I_1, \ldots, I_l]$ be a normal-form CP+∀red proof of $\mathcal{Q}.\ F$ of length $l$ and size $m \geq l$. For $j \in \{0, 1, \ldots, l\}$, define $\pi_j = \mathcal{Q}.\ [I_{j+1}, \ldots, I_l]$ and $F_j = F \cup \{I_1, \ldots, I_j\}$. By downward induction on $j$, from $\pi_j$ we show how to compute, for each universal variable $u$, a Boolean function $\sigma_u^j$ that maps each assignment to the variables quantified before $u$ to a bit $\{0, 1\}$. These functions satisfy the property that in a 2-player game played on the formula $\mathcal{Q}.\ F_j$, if the universal player chooses values for each universal variable $u$ according to $\sigma_u^j$, then finally some inequality in $F_j$ is falsified. We describe the functions $\sigma_u^j$ by decision lists of size $O(l)$, where each condition is checkable by a constant-depth polynomial-in-$m$ sized threshold circuit. In particular, when $m$ is polynomial in $n$, the functions $\sigma_u^j$ are computable in $\mathsf{TC}^0$.

Since all axioms are included in $F$, we can skip the axiom download steps in the proof.

**Base case:** When $j = l$, define $\sigma_u^l = 0$ for all $u$. Indeed $\sigma_u^l$ can take any Boolean value as $F_l$ contains $I_l$ which is the contradiction $0 \geq 1$.

**Induction hypothesis:** Assume that the claim is true at the $j^{th}$ step.

**Induction step:** For $j \leq l$, if $I_j$ is obtained by a classical rule, then $\sigma_u^{j-1} \equiv \sigma_u^j$ for every universal variable $u$. By induction, any strategy of the existential player, the assignment constructed by playing according to $\sigma_u^j$ falsifies some inequality in $F_j$. If it does not falsify $I_j$, then it must falsify an $I_k \in F_j$ with $k < j$, that is, an $I_k \in F_{j-1}$. Otherwise, since it falsifies $I_j$ and since the inference rules are sound, it also falsifies at least one of the hypotheses $I_k$, $k < j$.

If $I_j$ is derived using a ∀-red rule; that is $I_j = I_k|_{u=b_j}$ for some $k < j$, then for all $u' \neq u$, $\sigma_{u'}^{j-1} \equiv \sigma_{u'}^j$. For $u$, if $I_k|_{u=b_j}(\vec{a}) = 0$, then $\sigma_u^{j-1}(\vec{a}) = b_j$, else $\sigma_u^{j-1}(\vec{a}) = \sigma_u^j(\vec{a})$. (The value $I_k|_{u=b_j}(\vec{a})$ can be determined since variables to the right of $u$ have zero coefficient in $I_k$.)

By induction, against any strategy of the existential player, the assignment constructed by playing according to $\sigma_u^j$ falsifies some inequality in $F_j$. If does not falsify $I_j$, then it must falsify an $I_{k'} \in F_j$ with $k' < j$, that is, an $I_{k'} \in F_{j-1}$. In this case, we have defined $\sigma_u^{j-1} \equiv \sigma_u^j$, so playing according to $\sigma_u^{j-1}$ also falsifies $I_{k'} \in F_{j-1}$. Otherwise, since it falsifies

$I_j = I_k|_{u=b_j}$ and since in this case we have defined $\sigma_u^{j-1}(\vec{a}) = b_j$, so playing according to $\sigma_u^{j-1}$ also falsifies $I_k \in F_{j-1}$.

The decision list $D_u^{j-1}$ for $\sigma_u^{j-1}$ is constructed as follows: If $\neg(I_k|_{z=b_j}(\vec{x}))$ then $D_u^{j-1}(\vec{x}) = b_j$ else $D_u^{j-1}(\vec{x}) = D_u^j(\vec{x})$. Observe that $D_u^{j-1}(\vec{x})$ has just one more condition than $D_u^j(\vec{x})$. Since the bit-size of $I_k$ is at most $m$, and since addition and multiplication are in $\mathsf{TC}^0$, one can check the **if** condition by a bounded-depth threshold circuit with size polynomial in $m$. $\mathsf{TC}^0$.

The decision lists $D_u^0$ have length $O(l)$ and each condition is checkable by a constant-depth threshold circuit of size polynomial in $m$. The result follows. ◀

## Missing proofs from Section 5

We first show why Theorem 12 follows from Theorem 13.

**Theorem 12.** *CP+∀red for false QBFs admits monotone real feasible interpolation.*

**Proof.** (assuming Theorem 13.) Let $\varphi$ be the given false QBF. Encoding it as a quantified set of inequalities as per Definition 2, we get a quantified set of linear inequalities $\mathcal{F} = \mathcal{Q}.\ F$, of the form

$$\mathcal{F} = \exists\vec{p}\mathcal{Q}\vec{q}\mathcal{Q}\vec{r}.\big[A(\vec{p},\vec{q}) \cup B(\vec{p},\vec{r})\big]$$

Here, $A(\vec{p},\vec{q})$ contains inequalities $R(C)$ for all clauses $C \in A'$; these are of the form $\sum_k e_k p_k + \sum_i f_i q_i \geq b$. Similarly, $B(\vec{p},\vec{r})$ contains inequalities $R(C)$ for all $C \in B'$; these are of the form: $\sum_k e_k p_k + \sum_j g_j r_j \geq b$. The Boolean axioms corresponding to the $\vec{q}$ variables are included in $A$, those corresponding to the $\vec{r}$ variables are included in $B$. The Boolean axioms corresponding to the $\vec{p}$ variables also have to be included in $A \cup B$. They have both positive and negative coefficents. If $\vec{p}$ occurs only positively in $A'$, we include these in $B$, otherwise we include them in $A$.

Since $\varphi$ is false, so is $\mathcal{F}$. On any assignment $\vec{a}$ to the variables in $\vec{p}$, either $\mathcal{F}_{\vec{a},0} = \mathcal{Q}\vec{q}.\ A(\vec{a},\vec{q})$ or $\mathcal{F}_{\vec{a},1} = \mathcal{Q}\vec{r}.\ B(\vec{a},\vec{r})$ (or both) must be false. Furthermore, for $b \in \{0,1\}$, $\mathcal{F}_{\vec{a},b}$ is false exactly when $\varphi_{\vec{a},b}$ is false. Thus a monotone real interpolating circuit for $\mathcal{F}$ is also a monotone real interpolating circuit for $\varphi$.

Note that if $\vec{p}$ occurs only positively in $A'$, then the coefficients $e_k$ in all the inequalities in $A$ are non-negative. Similarly, if $\vec{p}$ occurs only negatively in $B'$, then the coefficients $e_k$ in all the inequalities in $B$ are non-positive. Hence, invoking Theorem 13 on $\mathcal{F}$, we obtain the desired monotone real interpolating circuit for $\mathcal{F}$ and for $\varphi$. ◀

**Theorem 13.** *CP+∀red for inequalities admits monotone real feasible interpolation. That is, let $\mathcal{F}$ be any false quantified set of inequalities of the form $\exists\vec{p}\mathcal{Q}\vec{q}\mathcal{Q}\vec{r}.\big[A(\vec{p},\vec{q}) \wedge B(\vec{p},\vec{r})\big]$ where $A \cup B$ includes all Boolean axioms, and where the coefficients of $\vec{p}$ are either all non-negative in $A$ or are all non-positive in $B$. If $\mathcal{F}$ has a CP+∀red-proof $\pi$, of length $l$, then we can extract a monotone real circuit $C$ of size polynomial in $l$ and the number $n$ of $\vec{p}$ variables in $\mathcal{F}$, such that $C$ computes a Boolean function, and on any $0,1$ assignment $\vec{a}$ to $\vec{p}$,*

$$C(\vec{a}) = 0 \implies \mathcal{Q}\vec{q}.A(\vec{a},\vec{q}) \text{ is false, and}$$
$$C(\vec{a}) = 1 \implies \mathcal{Q}\vec{r}.B(\vec{a},\vec{r}) \text{ is false.}$$

*Such a $C$ is called a monotone real interpolating circuit for $\mathcal{F}$.*

**Proof.** Let $\pi = \exists\vec{p}\mathcal{Q}\vec{q}\mathcal{Q}\vec{r}.\ [I_1, \ldots, I_l]$ be a CP+∀red refutation of $\mathcal{F}$. The idea, as in [34], is to associate with each inequality

$$I \equiv \sum_k e_k p_k + \sum_i f_i q_i + \sum_j g_j r_j \geq D$$

in $\pi$, two inequalities

$$I_0 \equiv \sum_i f_i q_i \geq D_0, \quad I_1 \equiv \sum_j g_j r_j \geq D_1$$

depending on the Boolean assignment $\vec{a}$ to the $\vec{p}$ variables, in such a way that

- $I_0$ and $I_1$ together imply $I|_{\vec{a}}$. (It suffices to ensure $D_0 + D_1 \geq D - \sum_k e_k a_k$.)
- $I_0$ can be derived solely from the $\mathcal{Q}\vec{q}.A(\vec{a},\vec{q})$ part in CP+∀red.
- $I_1$ can be derived solely from the $\mathcal{Q}\vec{r}.B(\vec{a},\vec{r})$ part in CP+∀red.

Then the inequalities corresponding to the last step of the proof, $I_l$, are $0 \geq D_0$ and $0 \geq D_1$, with $D_0 + D_1 \geq 1$. Hence $D_0 > 0 \implies \vec{Q}\vec{q}.A(\vec{a},\vec{q})$ is false, and $D_1 > 0 \implies \vec{Q}\vec{r}.B(\vec{a},\vec{r})$ is false. Note that we only need to compute one of the values $D_0$, $D_1$ to identify a false part of $\mathcal{F}$. Furthermore, we will show that if all the coefficients $e_k$ in $B(\vec{p},\vec{r})$ are non-positive, then $D_1$ can be computed by a real monotone circuit of size $O(nl)$. If all the coefficients $e_k$ in $A(\vec{p},\vec{q})$ are non-negative, then we will show that $-D_0$ can be computed by a real monotone circuit of size $O(nl)$. (The inputs to the circuit are an assignment $\vec{a}$ to the $\vec{p}$ variables.) Applying the unary non-decreasing threshold function $D_1 > 0$? or $-D_0 \geq 0$? to its output will then give a monotone real interpolating circuit for $\mathcal{F}$.

We first describe the computation of $D_0$ and $D_1$ at each inequality. These are computed by two circuits, both of which have exactly the structure of $\pi$.

Consider the case when all $e_k$ in $B(\vec{p},\vec{r})$ are non-positive; the other case is analogous. All axioms are considered as either $A$-axioms or as $B$-axioms. The Boolean axioms concerning $\vec{p}$ variables are treated as $A$-axioms in this case.

The computation of $D_0$ and $D_1$ proceeds bottom-up as described below.

| How inequality $I$ is obtained | $D_0$ | $D_1$ |
|---|---|---|
| Axioms: | | |
| $p_k \geq 0$ | $-a_k$ | $0$ |
| $-p_k \geq -1$ | $a_k - 1$ | $0$ |
| $-q_i \geq -1$ | $-1$ | $0$ |
| $-r_j \geq -1$ | $0$ | $-1$ |
| $q_j \geq 0$ or $r_j \geq 0$ | $0$ | $0$ |
| $\sum_k e_k p_k + \sum f_i q_i \geq D$ | $D - \sum e_k a_k$ | $0$ |
| $\sum_k e_k p_k + \sum g_j r_j \geq D$ | $0$ | $D - \sum e_k a_k$ |
| Arithmetic: | | |
| Addition $I = I' + I''$ | $D_0' + D_0''$ | $D_1' + D_1''$ |
| Multiplication $I = hI'$, $h > 0$ | $h \times D_0'$ | $h \times D_1'$ |
| Division $I = I'/c$, $c > 0$ | $\left\lceil \frac{D_0'}{c} \right\rceil$ | $\left\lceil \frac{D_1'}{c} \right\rceil$ |
| Reduction: $I = I' \mid_{u=b}$; coefficient of $u$ in $I'$ is $h$. | | |
| $h > 0$ | $D_0'$ | $D_1'$ |
| $h < 0$ and $u$ is a $\vec{q}$ variable | $D_0' - h$ | $D_1'$ |
| $h < 0$ and $u$ is an $\vec{r}$ variable | $D_0'$ | $D_1' - h$ |

As in the proof argument from [34], a straightforward induction shows that with these computations, at each proof line $I$, the inequalities $I_0$ and $I_1$ together imply $I \mid_{\vec{a}}$, and that each $I_0$ can be derived from the $A$-axioms alone and each $I_1$ can be derived from the $B$-axioms alone.

All the operations required for the arithmetic and reduction steps compute non-decreasing functions. At the axioms, note that the dependence of the $D_1$ values on the assignment values $\vec{a}$ is always with non-negative coefficients $-e_k$; hence these functions are also non-decreasing. Thus we obtain a monotone real circuit for $D_1$, of size $O(nl)$. ◀

## Missing details and proofs from Section 6

**Example with universal quantifiers separating Q-Res, QU-Res from CP+∀red:** In [8] it has been shown that the false QBFs KBKF($t$), introduced in [29], are hard for Q-Res. However, they are known to have a polynomial-size proofs in QU-Res, and by Lemma 7 in CP+∀red as well; thus they separate Q-Res from CP+∀red.

Consider the family of false QBFs from [20], which we denote as Q-PHP$_n$. The formula is based on the pigeon hole principle but has universal quantifiers, and is shown in [20] to be hard for Q-Res. We observe that it is also hard for QU-Res, but easy for CP+∀red, providing another example separating QU-Res from CP+∀red.

The formula Q-PHP$_n$ is define as follows: let $\mathrm{CPHP}_n^{X_n}$ be the false CNF formula encoding pigeon hole principle on $n+1$ pigeon and $n$ holes, and over the variables in $X_n = \{x_1, \ldots, x_n\}$. To be precise,

$$\mathrm{CPHP}_n^{X_n} = \left( \bigwedge_{i=1}^{n+1} ( \bigvee_{j=1}^{n} x_{i,j}) \right) \wedge \left( \bigwedge_{j=1}^{n} \bigwedge_{1 \le i_1 < i_2 \le n+1} (\neg x_{i_1,j} \vee \neg x_{i_2,j}) \right)$$

Now define

$$\mathrm{DPHP}_n^{X_n} = \neg \mathrm{CPHP}_n^{X_n}$$

Clearly $\mathrm{DPHP}_n^{X_n} \in \mathrm{TAUT}$ and is in DNF. Consider the following formula:

$$\exists X_n \forall Y_n . \mathrm{DPHP}_n^{Y_n} \wedge \mathrm{CPHP}_n^{X_n}$$

with $Y_n \cap X_n = \emptyset$. This is a false QBF because $\mathrm{CPHP}_n^{X_n}$ is unsatisfiable. However the matrix of the formula is not in CNF. We define Q-PHP$_n$ to be the equivalent of the above formula where the matrix is in CNF form. In [20], the DNF formula $\mathrm{DPHP}_n^{Y_n}$ is encoded into an equivalent CNF formula $\mathrm{TPHP}_n^{Y_n, Z_n}$ using additional variables $\vec{Z}$, disjoint from $X_n$ and $Y_n$. To be precise,

$$\text{Q-PHP}_n = \exists X_n \forall Y_n \exists Z_n . \mathrm{TPHP}_n^{Y_n, \vec{Z}} \wedge \mathrm{CPHP}_n^{X_n}$$

with $\mathrm{DPHP}_n^{Y_n} \equiv \exists \vec{Z} . \mathrm{TPHP}_n^{Y_n, \vec{Z}}$ and $\mathrm{TPHP}_n^{Y_n, \vec{Z}}$ in CNF.

**Q-PHP$_n$ is hard for Q-Res and QU-Res [20], but easy for CP+∀red**: no resolution step is possible between the clauses from $\mathrm{TPHP}_n^{Y_n, \vec{Z}}$ and $\mathrm{CPHP}_n^{X_n}$, as the variable sets are disjoint. Also the refutation is possible only from the clauses of $\mathrm{CPHP}_n^{X_n}$, as $\forall Y_n \exists Z_n \mathrm{TPHP}_n^{Y_n, \vec{Z}}$ is true. Since all the variables in $X_n$ are existential, the claim follows directly from the hardness result of the pigeon hole principle for resolution [27], and the fact that the pigeon hole principle is easy for the Cutting-plane proof system [19, Proposition 7].

**Theorem 19.** *Frege+∀red is exponentially stronger than CP+∀red: Frege+∀red p-simulates CP+∀red, whereas CP+∀red does not simulate Frege+∀red.*

**Proof.** **Frege+∀red p-simulates CP+∀red**: Let $\varphi$ be a false formula $\varphi = \mathcal{Q}x_0 \cdots \mathcal{Q}x_{N-1}. [C_1 \wedge \cdots \wedge C_m]$, and let $\mathcal{F}$ denote its standard encoding as described in Definition 2. Fix any

CP+∀red proof $\pi = \mathcal{Q}x_0 \cdots \mathcal{Q}x_{N-1}.\ [I_1, I_2, \ldots, I_m]$ of $\mathcal{F}$. By Lemma 5, we can assume that $\pi$ is in normal form. We need to represent each inequality $I$ as a propositional formula $\text{Rep}(I)$, such that on each assignment $\alpha$ to the Boolean variables, $\text{Rep}(I)(\alpha)$ is 1 if and only if $I|_\alpha$ is 1. We do this almost exactly as in [24].

We know that integer arithmetic is in $\mathsf{NC}^1$. Thus, for a string of $(n+1)L$ Boolean variables $\tilde{y}$ representing the bits of $n+1$ signed integers $a_1, a_2, \ldots, a_n, b$ with bit length $L$ each, and $n$ Boolean variables $x_1, \ldots, x_n$, there is a formula $F$ of size polynomial in $n+L$ (and depth logarithmic in $nL$) such that on any assignment, $F$ is true exactly when the inequality $\sum_i a_i x_i \geq b$ is satisfied. To represent a specific inequality $I : \sum_i a_i x_i \geq b$, we append to the leaves of $F$ labeled from $\tilde{y}$ subformulas of the form $x \vee \bar{x}$ or $x \wedge \bar{x}$ depending on the bits of the $a_i$'s and $b$. The resulting formula has the variables $x_1, \ldots, x_n$ and is the representation $\text{Rep}(I)$.

Our simulating Frege+∀red proof will have the structure

$$\pi_1, \text{Rep}(I_1), \pi_2, \text{Rep}(I_2), \ldots, \pi_m, \text{Rep}(I_m), \pi_{m+1},\ \text{false}$$

where each $\pi_i$ is a sequence of formulas. That is, the simulating Frege+∀red proof is a sequence of formulas containing the subsequence

$$\text{Rep}(I_1), \text{Rep}(I_2), \ldots, \text{Rep}(I_m),\ \text{false}$$

For each axiom clause $C$, we need to derive the formula $\text{Rep}(R(C))$ by a short (polynomial in $n$) Frege+∀red proof. Furthermore, inside $\text{Rep}(R(C))$, there will be explicit sub-formulas representing the bits of each coefficient, $a_{ij}$ and $b_j$ for $i \in [n]$, $j \in [L]$. (To handle carry overflows, we pad each coefficient with 0s to length $\theta(L)$ as in [24].) There will also be explicit sub-formulas for each $a_{ij} \wedge x_i$.

We also need to derive each $\text{Rep}(I_t)$ from $\text{Rep}(I_j)$, $j < t$, via short (polynomial in the size of proof $\pi$) Frege+∀red proofs.

The addition rule, multiplication rule, and the division rule can be simulated as in the classical case [24]: since integer arithmetic is in $\mathsf{NC}^1$, we have small formulas $G$ expressing the coefficients of the resulting inequality $I$ from the used inequalities $I'$ and $I''$. A Frege style proof can describe how values from the subformulas in $\text{Rep}(I')$ and $\text{Rep}(I'')$ propagate through $G$ to bits equivalent to the corresponding input bits of $\text{Rep}(I)$.

Now we show the ∀-red step simulation.

Suppose the inequality $I_k$ is obtained from $I_j$ for some $j < k$ by applying the ∀-red rule, reducing universal variable $u$. Clearly, $u$ is the rightmost variable in $I_j$ with nonzero coefficient $h_u$. Inductively, we have already derived $\mathcal{F} \to \mathit{Rep}(I_j)$. Let $b_u = 0$ if $h_u > 0$, otherwise $b_u = 1$. We need to instantiate $u$ in $\text{Rep}(I_j)$ with $b_u$. But $u$ is not the rightmost variable in $\text{Rep}(I_j)$. However, for each variable $v$ to the right of $u$, we know that the coefficient $a_v$ of $v$ in $I_j$ is 0, and hence the sub-formulas evaluating to the bits $a_{vj}$, as well as the sub-formulas evaluating $a_{vj} \wedge v$, are all 0. In Frege+∀red, we can transform the pair of sub-formulas, $a_{vj} \wedge v$, and $a_{vj} \equiv 0$, to the subformula $a_{vj} \wedge 0$, and thus eliminate $v$ (note that $v$ does not figure anywhere else in the formula). Once this is done for all variables right of $u$, we have the formula $R$ in which the ∀-reduction step is valid in Frege+∀red. Performing this reduction gives the formula $R' = R\mid_{u=b_u}$. Now, a short Frege proof can allow us to derive $\text{Rep}(I_j \mid_{u=b_u}) = \text{Rep}(I_k)$. To see why such a proof exists, consider the case $b_u = 0$. Inside $R'$ we have subformulas for the bits $h_{uj}$ of the coefficient $h_u$ of $u$, and bits for $h_{uj} \wedge u$, and at $u$ we have attached a subformula evaluating to 0. What we want is subformulas where $u$ is still free, but the bits of the new coefficient of $u$ are all 0. That is, from $h_{uj} \wedge u$ and $u \equiv 0$, we want to derive $0 \wedge u$ (the reverse of what we did before the reduction for later variables

$v$). This is easy in Frege+∀red. The case when $b_u = 1$ is similar, with the added task of subtracting $h_u$ from the right-hand-side. This too can be tracked using an $\mathsf{NC}^1$ formula for subtraction.

**CP+∀red does not simulate Frege+∀red.** Since Frege is exponentially more powerful than Cutting Planes over propositional formulas (as witnessed by the clique-colour formulas [34], see also Section 5), CP+∀red cannot simulate Frege+∀red. ◀

**Theorem 20.** *There is a $\Phi_{n,k} \in \textsc{CliqueCoClique}_{n,k}$ of size polynomial in $n$, with a Frege+∀red proof of size polynomial in $n$.*

**Proof.** Fix positive integers $n$ (indicating the number of vertices of the graph) and $k \le n$ (indicating the size of the clique queried) and let $\vec{p}$ be the set of variables $\{p_{uv} \mid 1 \le u < v \le n\}$. An assignment to $\vec{p}$ picks a set of edges, and thus an $n$-vertex graph that we denote $G_{\vec{p}}$.

The formula $\mathcal{Q}\vec{q}.\ A_{n,k}(\vec{p},\vec{q})$ should express the property $\textsc{Clique}(n,k)$, that $G_{\vec{p}}$ has a clique of size $k$, and $\mathcal{Q}\vec{r}.\ B_{n,k}(\vec{p},\vec{r})$ should express the property co-$\textsc{Clique}(n,k)$.

Let $\vec{q}$ be the set of variables $\{q_{iu} \mid i \in [k], u \in [n]\}$. We use the following clauses.

$$\begin{aligned}
C_i &= q_{i1} \vee \cdots \vee q_{in} && \text{for } i \in [k]\\
D_{i,j,u} &= \neg q_{iu} \vee \neg q_{ju} && \text{for } i,j \in [k], i<j \text{ and } u \in [n]\\
E_{i,u,v} &= \neg q_{iu} \vee \neg q_{iv} && \text{for } i \in [k] \text{ and } u,v \in [n], u<v\\
F_{i,j,u,v} &= \neg q_{iu} \vee \neg q_{jv} \vee p_{uv} && \text{for } i,j \in [k], i<j \text{ and } u \ne v \in [n].
\end{aligned}$$

We can now express $\textsc{Clique}(n,k)$ as a polynomial-size QBF $\exists\vec{q}.A_{n,k}(\vec{p},\vec{q})$, where

$$A_{n,k}(\vec{p},\vec{q}) = \bigwedge_{i\in[k]} C_i \wedge \bigwedge_{i<j,u\in[n]} D_{i,j,u} \wedge \bigwedge_{i\in[k],u<v} E_{i,u,v} \wedge \bigwedge_{i<j,u\ne v} F_{i,j,u,v}.$$

Here the edge variables $\vec{p}$ appear only positively in $A_{n,k}(\vec{p},\vec{q})$.

Likewise co-$\textsc{Clique}(n,k)$ can be written as a QBF $\forall\vec{r}\exists\vec{t}.B_{n,k}(\vec{p},\vec{r},\vec{t})$ of polynomial size. In [9] one way of doing so is described. We describe here a somewhat different and more transparent encoding. This encoding can be used to obtain the results of [9] as well, and is more convenient for us here because it allows us to obtain a short Frege+∀red proof. For $\vec{r}$, we have a variable $r_{iu}$ for every variable $q_{iu}$ and we let the set of variables of $\vec{t}$ be $\{t_K \mid K \in A_{n,k}\} \cup \{t\}$. For each clause $K$ in $A_{n,k}(\vec{p},\vec{q})$, we include an equivalence $t_K \leftrightarrow K[r_{iu}/q_{iu}]$ in $B_{n,k}(\vec{p},\vec{r},\vec{t})$, which we represent as a set of clauses. We also introduce clauses for $t \leftrightarrow \bigwedge_{K\in A_{n,k}} t_K$, i.e., $t$ indicates whether the $\vec{r}$ variables encode a clique. Because we want to represent the co-clique formula we also include $\neg t$ in $B_{n,k}(\vec{p},\vec{r},\vec{t})$, which yields the CNF formula co-$\textsc{Clique}(n,k) = \forall\vec{r}\exists\vec{t}.B_{n,k}(\vec{p},\vec{r},\vec{t})$.

Our clique-co-clique formulas $\Phi_{n,k}$ are $\exists\vec{p}\exists\vec{q}\forall\vec{r}\exists\vec{t}.A_{n,k}(\vec{p},\vec{q}) \wedge B_{n,k}(\vec{p},\vec{r},\vec{t})$. We now show that these formulas are easy in Frege+∀red.

We use a result from [12, Theorem 8.1] which shows that a Frege+∀red super-polynomial lower bound must either come from a circuit lower bound or a classical Frege lower bound. More precisely, if false QBFs $\Phi_n$ do not admit polynomial-size Frege+∀red proofs, then either the universal player does not have $\mathsf{NC}^1$ winning strategies for the universal variables, or if small $\mathsf{NC}^1$ winning strategies exist, then the propositional formulas obtained by substituting the $\mathsf{NC}^1$ circuits for universal variables in $\Phi_n$ are hard for classical Frege.

In the case of the clique co-clique formulas $\Phi_{n,k}$ there exist short winning strategies for the universal player, namely $\vec{r} = \vec{q}$. To see this, we just need to consider the case where the existential player chooses a graph $\vec{p}$ that contains a $k$-clique exhibited in the $\vec{q}$-variables, because otherwise the universal player immediately wins on $A_{n,k}(\vec{p},\vec{q})$. In this case, choosing $\vec{r} = \vec{q}$ ensures that $B_{n,k}(\vec{p},\vec{r},\vec{t})$ fails as $\vec{r}$ indeed is a $k$-clique.

Substituting these winning strategies into $\Phi_{n,k}$, we obtain the false propositional formulas $A_{n,k}(\vec{p},\vec{q}) \wedge B_{n,k}(\vec{p},\vec{q},\vec{t})$, which admit short Frege refutations.

Using this intuition we can refute $\Phi_{n,k}$ in Frege+$\forall$red with short proofs. For this we first derive the tautology $\neg(A_{n,k}(\vec{p},\vec{q}) \wedge B_{n,k}(\vec{p},\vec{q},\vec{t}))$ by demonstrating a way to find a contradiction in $A_{n,k}(\vec{p},\vec{q}) \wedge B_{n,k}(\vec{p},\vec{q},\vec{t})$. To do this we observe that for any clause $K \in A_{n,k}(\vec{p},\vec{q})$, we have the equivalences $(t_K \leftrightarrow K) \in B_n(\vec{p},\vec{q},\vec{t})$, so we derive all $t_K$. Then, because $(t \leftrightarrow \bigwedge_{K\in A_{n,k}} t_K) \in B_{n,k}(\vec{p},\vec{q},\vec{t})$, we obtain $t$. This means that with $\neg t \in B_{n,k}(\vec{p},\vec{q},\vec{t})$ we have a contradiction, thus proving the negation $\neg(A_{n,k}(\vec{p},\vec{q}) \wedge B_{n,k}(\vec{p},\vec{q},\vec{t}))$.

Moving forward to the next step, we derive in (polynomially many) Frege steps the implication $\bigwedge_{i\in[k],j\in[\binom{n}{2}]}(q_{i,j} \leftrightarrow r_{i,j}) \rightarrow \neg(A_{n,k}(\vec{p},\vec{q}) \wedge B_n(\vec{p},\vec{r},\vec{t}))$, from which together with the axiom $A_n(\vec{p},\vec{q}) \wedge B_n(\vec{p},\vec{r},\vec{t})$ we derive the disjunction $\bigvee_{i\in[k],j\in[\binom{n}{2}]}(r_{i,j} \neq q_{i,j})$.

Now we perform $\forall$-reduction, starting with the rightmost universal variable $r_{i_1,j_1}$ and instantiating it with both 0 and 1. Thus we obtain two lines:

$$(0 \neq q_{i_1,j_1}) \vee \bigvee_{i\in[k],i\neq i_1,j\in[\binom{n}{2}],j\neq j_1} (r_{i,j} \neq q_{i,j})$$

$$(1 \neq q_{i_1,j_1}) \vee \bigvee_{i\in[k],i\neq i_1,j\in[\binom{n}{2}],j\neq j_1} (r_{i,j} \neq q_{i,j})$$

We then use the tautology $(q_{i_1,j_1} \leftrightarrow 0) \vee (q_{i_1,j_1} \leftrightarrow 1)$ and the two instantiations to remove the disjunct $(r_{i_1,j_1} \neq q_{i_1,j_1})$ from the disjunction. Continuing this iteratively, we remove all disjuncts and are left with the empty disjunct, hence refuting $\Phi_{n,k}$ in polynomial size. ◀

Note that if we changed the quantification and used formula $\exists\vec{p}\forall\vec{r}\exists\vec{t}\exists\vec{q}.A_{n,k}(\vec{p},\vec{q}) \wedge B_{n,k}(\vec{p},\vec{r},\vec{t})$ we would still be describing the same contradiction between clique and co-clique. However the above argument would not work for finding short Frege+$\forall$red proofs. This is because the strategies of the universal player cannot refer to the choices of $\vec{r}$ (since the universal player is restricted to using variables that appear left of the variable in question) but instead has to describe a $k$-clique expressed as the $\vec{r}$ variables whenever the existential player makes on in the graph variables. However the strategies that determine these clique are restricted to the $\vec{p}$ graph variable. Since cliques can be checked easily when found, they means that the universal strategies compute the NP-complete CLIQUE$(n,k)$ problem. So strategies are conjectured to be hard unless $\mathsf{NP} \subseteq \mathsf{NC}^1$. Because of the strategy extraction theorem from [6] $\mathsf{NP} \subseteq \mathsf{NC}^1$ will be a necessary condition for these modified formulas to have short proofs in Frege+$\forall$red.

## Missing proofs from Section 7

**Theorem 22.** *SemCP+$\forall$red admits monotone real feasible interpolation for false QBFs.*

**Proof.** Let $\varphi = \exists\vec{p}Q\vec{q}Q\vec{r}(A'(\vec{p},\vec{q}) \wedge B'(\vec{p},\vec{r}))$ be a false QBF formula. Without loss of generality, the $\vec{p}$ variables appear only negatively in $B'(\vec{p},\vec{r})$. Consider the standard encoding $\mathcal{F} = \exists\vec{p}Q\vec{q}Q\vec{r}(A(\vec{p},\vec{q}) \wedge B(\vec{p},\vec{r}))$ of $\varphi$ (see Definition 2). Clearly the coefficient of $\vec{p}$ variables in $B$ are non-positive. As discussed before it is sufficient to extract a monotone real feasible interpolation for $\mathcal{F}$. Let $\pi$ be any semCP+$\forall$red proof of $\mathcal{F}$, and as in the proof of Theorem 13, we construct a real monotone interpolating $C$ to detect whether $D_1 > 0$. Axioms and the $\forall$-reduction rule are handled exactly as in Theorem 13. Now suppose that the inequality

$I \equiv \sum_k e_k p_k + \sum_i f_i q_i + \sum_j g_j r_j \geq D$ is semantically inferred from $I'$ and $I''$. We define $I_0, I_1$ by defining $D_0$ and $D_1$.

$$D_0 = \min \left\{ \sum_i f_i q_i|_\gamma : \gamma \in \{0,1\}^{|\vec{q}|}, \gamma \text{ satisfies } I'_0, I''_0 \right\}$$
$$D_1 = \min \left\{ \sum_j g_j r_j|_\tau : \tau \in \{0,1\}^{|\vec{r}|}, \tau \text{ satisfies } I'_1, I''_1 \right\}$$

It suffices to show that $D_0 + D_1 \geq D - \sum_k e_k a_k$. For $D_0$, let the minimum be achieved at assignment $\gamma_0$, and for $D_1$, let the minimum be achieved at assignment $\tau_1$. Let $\rho$ be the assignment to the $\vec{q}$ and $\vec{r}$ variables setting $\vec{q}$ as in $\gamma_0$ and $\vec{r}$ as in $\tau_1$. Then $\rho$ satisfies $I'_0$, $I''_0$, $I'_1$, $I''_1$ (at $\vec{p} = \vec{a}$). Hence by induction, $\rho$ satisfies $I'$ and $I''$. Since $I$ is inferred semantically from $I'$ and $I''$, $\rho$ satisfies $I$ as well. Hence

$$D_0 + D_1 = \sum_i f_i q_i|_{\gamma_0} + \sum_j g_j r_j|_{\tau_1} = \left( \sum_i f_i q_i + \sum_j g_j r_j \right)|_\rho \geq D - \sum_k e_k a_k, \quad \text{as required.}$$

Since $\vec{p}$ appears only negatively in $B(\vec{p}, \vec{r})$, $D_1$ is a non-decreasing function of $D'_1$ and $D''_1$. (As the values of $D'_1$ and $D''_1$ increase, the set of assignments $\tau$ over which we take the minimum shrinks, and so the minimum value can only increase or stay the same.) ◀

The proof of Theorem 22 goes through even if the quantified set of linear inequalities $\mathcal{F}$ are of the form defined in Theorem 13, not just those arising from false QBFs. Therefore similar to Theorem 13, semCP+∀red also admits monotone real feasible interpolation for inequalities.