Proof Complexity of Resolution-based QBF Calculi

Olaf Beyersdorff[1], Leroy Chew[1], and Mikoláš Janota[2]

1 School of Computing, University of Leeds, UK
2 INESC-ID, Lisbon, Portugal

Abstract

Proof systems for quantified Boolean formulas (QBFs) provide a theoretical underpinning for the performance of important QBF solvers. However, the proof complexity of these proof systems is currently not well understood and in particular lower bound techniques are missing. In this paper we exhibit a new and elegant proof technique for showing lower bounds in QBF proof systems based on strategy extraction. This technique provides a direct transfer of circuit lower bounds to lengths of proofs lower bounds. We use our method to show the hardness of a natural class of parity formulas for Q-resolution and universal Q-resolution. Variants of the formulas are hard for even stronger systems as long-distance Q-resolution and extensions. With a completely different lower bound argument we show the hardness of the prominent formulas of Kleine Büning et al. [34] for the strong expansion-based calculus IR-calc. Our lower bounds imply new exponential separations between two different types of resolution-based QBF calculi: proof systems for CDCL-based solvers (Q-resolution, long-distance Q-resolution) and proof systems for expansion-based solvers (∀Exp+Res and its generalizations IR-calc and IRM-calc). The relations between proof systems from the two different classes were not known before.

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

Keywords and phrases proof complexity, QBF, lower bound techniques, separations

Digital Object Identifier 10.4230/LIPIcs.STACS.2015.76

1 Introduction

Proof complexity studies the complexity of theorem proving in various formal systems, providing both sharp lower and upper bounds for the size of proofs of important combinatorial statements. One motivation for this research comes from its close connection to fundamental questions in computational complexity, and this connection has been present since the very beginnings of the field [20]. Another motivation is the tremendous success of SAT solvers, which today solve huge industrial instances of the NP-hard SAT problem with even millions of variables. Proof complexity provides the main theoretical tool for an understanding of the power and limitations of these algorithms. As most modern SAT solvers are based on resolution, this proof system has received a key attention; and many ingenious techniques have been devised to understand the complexity of resolution proofs (cf. [40, 17] for surveys).

During the last decade there has been a 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 [38, 7, 21]. As for SAT solvers, runs of QBF solvers produce witnesses of unsatisfiability (proofs), and there has been a lot of interest in the correspondence between the formal systems and solvers.

In particular, Kleine Büning et al. [34] define a resolution-like calculus called *Q-resolution* (Q-Res). There are several extensions of Q-Res; notably *long-distance Q-resolution* (LD-Q-

32nd Symposium on Theoretical Aspects of Computer Science (STACS 2015).
Editors: Ernst W. Mayr and Nicolas Ollinger; pp. 76–89
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

SYMPOSIUM ON THEORETICAL ASPECTS OF COMPUTER SCIENCE

Res) [3], which is more powerful than the standard Q-Res [22]. Q-Res and its extensions are important as they model QBF solving based on CDCL [24]. While Q-Res can only resolve on existential variables, the proof system *QU-Res*, introduced by Van Gelder [43], also allows to resolve on universal variables. Combining universal and long-distance Q-resolution, Balabanov et al. [4] recently considered the system LQU^{+}-Res. Apart from CDCL, another main approach to QBF-solving is through *expansion of quantifiers* [14, 6, 28]. Recently, a proof system ∀Exp+Res was introduced with the motivation to trace expansion-based QBF solvers [29]. ∀Exp+Res also uses resolution, but is conceptually very different from Q-Res.

In the recent work [8] two further proof systems *IR-calc* and *IRM-calc* are introduced, which unify the CDCL and expansion based approaches in the sense that IR-calc simulates both Q-Res and ∀Exp+Res. The system IRM-calc enhances IR-calc and additionally simulates long-distance Q-resolution. While IR-calc and IRM-calc are quite powerful, they still preserve the property of strategy extraction, which is important for verifying runs of QBF solvers.

In general, it is fair to say that the complexity and relations between QBF proof systems are not well understood. In particular, in sharp contrast to propositional proof complexity, we currently lack lower bound techniques for QBF proof systems.[1]

Our contributions

In this paper we aim towards a significantly better understanding of proof complexity of QBF proof systems. Our main contributions are the following:

1. A new lower bound method based on strategy extraction. We exhibit a new method to obtain lower bounds to the proof size in QBF proof systems, which directly allows to transfer circuit lower bounds to size of proof lower bounds. This method is based on the property of *strategy extraction*, which is known to hold for many resolution-based QBF proof systems. A QBF proof system has strategy extraction if given a refutation of a false QBF φ it is possible to efficiently compute a winning strategy for the universal player for φ.

The basic idea of our method is both conceptually simple and elegant: If we know that a family φ_n of false QBFs requires large winning strategies, then proofs of φ_n must be large in all proof systems with feasible strategy extraction. Now we need suitable formulas φ_n. Starting with a language L – for which we know (or conjecture) circuit lower bounds – we construct a family of false QBFs φ_n such that every winning strategy of the universal player for φ_n will have to compute L for inputs of length n. Consequently, a circuit lower bound for L directly translates into a lower bound for the winning strategy and therefore the proof size.

This immediately implies conditional lower bounds. However, if carefully implemented, our method also yields *unconditional lower bounds*. For Q-Res (and QU-Res) it is known that strategy extraction is computationally easy [3]; it is in fact possible in AC^0 as we verify here. Using the hardness of parity for AC^0 we can therefore construct formulas $\mathrm{QP{\small ARITY}}_n$ that require exponential-size proofs in Q-Res (and QU-Res).

Conceptually, our lower bound method via strategy extraction is similar to the feasible interpolation technique [35], which is one of the most successful techniques in classical proof complexity. In feasible interpolation, circuit lower bounds are also translated into proof size lower bounds. However, feasible interpolation only works for formulas of a special syntactic

[1] We note the very recent game technique for tree-like Q-Res [9], inspired by [10, 11, 12]. Further, [5] introduces a technique that lifts *known* hardness results for Q-Res to stronger systems by modifying the formula. We use that idea in Sec. 5.

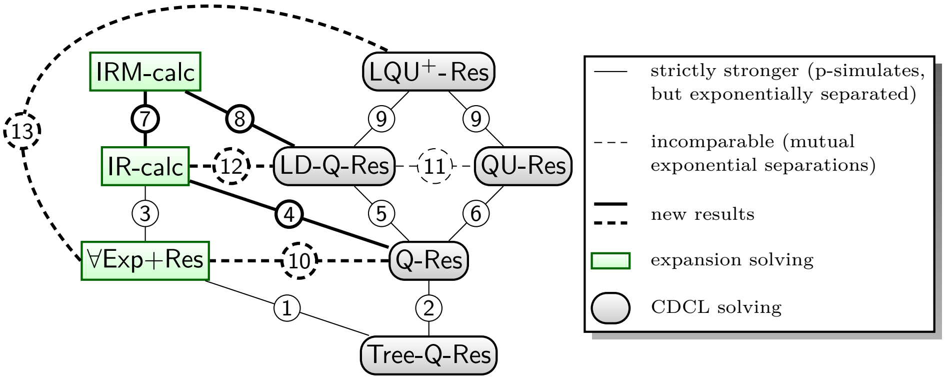

Figure 1 The simulation order of QBF resolution systems (references in the table below).

form, while our technique directly applies to arbitrary languages. It is a long-standing belief in the proof complexity community that there exists a direct connection between progress for showing lower bounds in circuit complexity and for proof systems (cf. [19]). For QBF proof systems our technique makes such a connection very explicit.

2. Lower bounds for QBF proof systems. Our new lower bound method directly gives a new lower bound for Q-Res for the parity formulas. In addition, we transfer this lower bound to the stronger systems LD-Q-Res and QU-Res by arguing that neither long-distance nor universal resolution gives any advantage on a suitable modification of the parity formulas.

For the strong system IR-calc from [8] we show that the strategy extraction method is not directly applicable (at least for unconditional bounds in the way we use it here). However, we use a completely different lower bound argument to obtain an exponential lower bound for the well-known formulas KBKF(t) of Kleine Büning, Karpinski and Flögel [34] in IR-calc. In the same work [34], where Q-Res was introduced, these formulas were suggested as hard formulas for Q-Res. In fact, a number of further separations of QBF proof systems builds on this [22, 4]. Here we show in a technically involved counting argument that the formulas are even hard for IR-calc. As IR-calc simulates Q-Res [8] we obtain as a by-product a formal proof of the hardness of KBKF(t) in Q-Res.

	Simulation/Separation			Incomparable
1	[31]	[31]	10	[30], Cor. 16
2	by Def.	[16]	11	[4]
3	[8]	[30], [8]	12	Cor. 8, Cor. 24
4	[8]	Cor. 16	13	Cor. 8, Cor. 24
5	by Def.	[22]		
6	by Def.	[43]		
7	by Def.	[8], Cor. 8		
8	[8]	Cor. 24		
9	by Def.	[4]		

3. Separations between QBF proof systems. Our lower bounds imply a number of new separations and incomparability results. The two main new results are: *(i) IR-calc does not simulate LD-Q-Res; (ii) LQU$^+$-Res does not simulate ∀Exp+Res.* Both are in fact exponential separations. Item (i) is obtained from the lower bound for KBKF(t), while (ii) follows from the lower bound on a variant of the parity formulas. In contrast to separations by KBKF(t), all separations derived from (ii) even hold for formulas of bounded quantifier complexity. Together with previous simulation results these imply many further separations.

Figure 1 depicts the simulation order of QBF resolution systems together with the separations. Combined with previous simulations and separations (cf. the table accompanying Fig. 1) this yields an almost complete understanding of the simulation order of QBF resolution systems.

2 Preliminaries

A *literal* is a Boolean variable or its negation. If l is a literal, $\neg l$ denotes the complementary literal, i.e. $\neg\neg x = x$. A *clause* is a disjunction of literals and a *term* is a conjunction of literals. The empty clause is denoted by $\bot$, which 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.

Quantified Boolean Formulas (QBFs) [33] extend propositional logic with quantifiers with the standard semantics that $\forall x.\, \Psi$ is satisfied by the same truth assignments as $\Psi[0/x] \wedge \Psi[1/x]$ and $\exists x.\, \Psi$ as $\Psi[0/x] \vee \Psi[1/x]$. Unless specified otherwise, we assume that QBFs are in *closed prenex* form with a CNF *matrix*, i.e., we consider the form $\mathcal{Q}_1 X_1 \ldots \mathcal{Q}_k X_k.\, \phi$, where X_i are pairwise disjoint (ordered) sets of variables; $\mathcal{Q}_i \in \{\exists, \forall\}$ and $\mathcal{Q}_i \neq \mathcal{Q}_{i+1}$. The formula ϕ is in CNF and is defined only on variables $X_1 \cup \ldots \cup X_k$. The propositional part ϕ is called the *matrix* and the rest the *prefix*. If $x \in X_i$, we say that x is at *level* i and write $\mathrm{lv}(x) = i$; we write $\mathrm{lv}(l)$ for $\mathrm{lv}(\mathrm{var}(l))$. In contrast to the level, the *index* $\mathrm{ind}(x)$ provides the more detailed information on the actual position of x in the prefix, i.e. all variables are indexed by $1, \ldots, n$ from left to right.

$$\frac{}{C}\ (\text{Axiom}) \qquad \frac{D \cup \{u\}}{D}\ (\forall\text{-Red}) \qquad \frac{D \cup \{u^*\}}{D}\ (\forall\text{-Red}^*)$$

C is a clause in the matrix. Literal u is universal and $\mathrm{lv}(u) \geq \mathrm{lv}(l)$ for all $l \in D$.

$$\frac{C_1 \cup U_1 \cup \{x\} \qquad C_2 \cup U_2 \cup \{\neg x\}}{C_1 \cup C_2 \cup U}\ (\text{Res})$$

We consider four instantiations of the Res-rule:
S∃R: x is existential.
If $z \in C_1$, then $\neg z \notin C_2$. $U_1 = U_2 = U = \emptyset$.
S∀R: x is universal. Otherwise same conditions as S∃R.
L∃R: x is existential.
If $l_1 \in C_1, l_2 \in C_2$, $\mathrm{var}(l_1) = \mathrm{var}(l_2) = z$ then $l_1 = l_2 \neq z^*$. U_1, U_2 contain only universal literals with $\mathrm{var}(U_1) = \mathrm{var}(U_2)$. $\mathrm{ind}(x) < \mathrm{ind}(u)$ for each $u \in \mathrm{var}(U_1)$.
If $w_1 \in U_1, w_2 \in U_2$, $\mathrm{var}(w_1) = \mathrm{var}(w_2) = u$ then $w_1 = \neg w_2$, $w_1 = u^*$ or $w_2 = u^*$. $U = \{u^* \mid u \in \mathrm{var}(U_1)\}$.
L∀R: x is universal. Otherwise same conditions as L∃R.

Figure 2 The rules of CDCL-based proof systems.

$$\frac{}{\left\{l^{[\tau]} \mid l \in C, l \text{ exist.}\right\} \cup \{\tau(l) \mid l \in C, l \text{ univ.}\}}\ (\text{Ax})$$

C is a clause from the matrix and τ is an assignment to all universal variables.

$$\frac{C_1 \vee x^{\tau} \qquad C_2 \vee \neg x^{\tau}}{C_1 \cup C_2}\ (\text{Res})$$

Figure 3 The rules of ∀Exp+Res [31].

Often it is useful to think of a QBF $\mathcal{Q}_1 X_1 \ldots \mathcal{Q}_k X_k.\, \phi$ as a *game* between the *universal* and the *existential player*. In the i-th step of the game, the player $\mathcal{Q}_i$ assigns values to all the variables X_i. The existential player wins the game iff the matrix ϕ evaluates to 1 under the assignment constructed in the game. The universal player wins iff the matrix ϕ evaluates to 0. Given a universal variable u with index i, a *strategy for* u is a function from all variables of index $< i$ to $\{0, 1\}$. A QBF is false iff there exists a *winning strategy* for the universal player, i.e. if the universal player has a strategy for all universal variables that wins any possible game [25][1, Sec. 4.2.2][37, Chap. 19].

A *proof system* [20] for a language L over Γ is a poly-time computable function $f : \Gamma^\star \to \Gamma^\star$ with $rng(f) = L$. If $f(x) = y$ then x is called an f-proof for y. For $L =$ QBF we speak of a *QBF proof system*. In our systems here, proofs are sequences of clauses; a *refutation* is a proof deriving $\bot$. A proof system S for L *simulates* a proof system P for L if there exists a polynomial p such that for all P-proofs π of x there is an S-proof π' of x with $|\pi'| \leq p(|\pi|)$.

Resolution-based calculi for QBF. We now give a brief overview of the main existing resolution-based calculi for QBF. We start by describing the proof systems modelling *CDCL-based QBF solving*; their rules are summarized in Figure 2. The most basic and important system is *Q-resolution (Q-Res)* by Kleine Büning et al. [34]. It is a resolution-like calculus that operates on QBFs in prenex form with CNF matrix. In addition to the axioms, Q-Res comprises the resolution rule S∃R and universal reduction ∀-Red (cf. Fig. 2).

$$\frac{}{\left\{x^{[\tau]} \mid x \in C, x \text{ is existential}\right\}}\ (\text{Ax})$$

C is a non-tautological clause from the matrix.
$\tau = \{0/u \mid u \text{ is universal in } C\}$, where the notation $0/u$ for literals u is shorthand for $0/x$ if $u = x$ and $1/x$ if $u = \neg x$.

$$\frac{x^\tau \vee C_1 \qquad \neg x^\tau \vee C_2}{C_1 \cup C_2}\ (\text{Resolution})$$

$$\frac{C}{\mathsf{inst}(\tau, C)}\ (\text{Instantiation})$$

τ is an assignment to universal variables with $\mathsf{rng}(\tau) \subseteq \{0, 1\}$.

Figure 4 The rules of IR-calc [8].

Long-distance resolution (LD-Q-Res) appears originally in the work of Zhang and Malik [44] and was formalized into a calculus by Balabanov and Jiang [3]. It merges complementary literals of a universal variable u into the special literal u^*. These special literals prohibit certain resolution steps. In particular, different literals of a universal variable u may be merged only if $\text{lv}(x) < \text{lv}(u)$, where x is the resolution variable. LD-Q-Res uses the rules L∃R, ∀-Red and ∀-Red*.

QU-resolution (QU-Res) [43] removes the restriction from Q-Res that the resolved variable must be an existential variable and allows resolution of universal variables. The rules of QU-Res are S∃R, S∀R and ∀-Red. *LQU$^+$-Res* [4] extends LD-Q-Res by allowing short and long distance resolution pivots to be universal, however, the pivot is never a merged literal z^*. LQU$^+$-Res uses the rules L∃R, L∀R, ∀-Red and ∀-Red*.

The second type of calculi models *expansion-based QBF solving*. These calculi are based on *instantiation* of universal variables: ∀Exp+Res [31], IR-calc, and IRM-calc [8]. All these calculi 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. $\neg x^{0/u_1 1/u_2}$. For any annotated literal l^σ, the substitution σ must not make assignments to variables at a higher quantification level than l, i.e. if $u \in \mathsf{dom}(\sigma)$, then u is universal and $\text{lv}(u) < \text{lv}(l)$. To preserve this invariant, we use the *auxiliary notation* $l^{[\sigma]}$, which for an existential literal l and an assignment σ to the universal variables filters out all assignments that are not permitted, i.e. $l^{[\sigma]} = l^{\{c/u \in \sigma \mid \text{lv}(u) < \text{lv}(l)\}}$.

Axiom and instantiation rules as in IR-calc in Figure 4.

$$\frac{x^{\tau \cup \xi} \vee C_1 \qquad \neg x^{\tau \cup \sigma} \vee C_2}{\mathsf{inst}(\sigma, C_1) \cup \mathsf{inst}(\xi, C_2)}\ (\text{Res})$$

$\mathsf{dom}(\tau)$, $\mathsf{dom}(\xi)$ and $\mathsf{dom}(\sigma)$ are mutually disjoint. $\mathsf{rng}(\tau) = \{0, 1\}$

$$\frac{C \vee b^\mu \vee b^\sigma}{C \vee b^\xi}\ (\text{Merging})$$

$\mathsf{dom}(\mu) = \mathsf{dom}(\sigma)$.
$\xi = \{c/u \mid c/u \in \mu, c/u \in \sigma\} \cup$
$\{*/u \mid c/u \in \mu, d/u \in \sigma, c \neq d\}$

Figure 5 The rules of IRM-calc [8].

The simplest instantiation-based calculus we consider is the calculus $\forall$Exp+Res, whose rules are presented in Figure 3. The system IR-calc extends $\forall$Exp+Res by enabling partial assignments in annotations. To do so, we utilize the auxiliary operations of *completion* and *instantiation*. For assignments τ and μ, we write $\tau \veebar \mu$ for the assignment σ defined as follows: $\sigma(x) = \tau(x)$ if $x \in \mathsf{dom}(\tau)$, otherwise $\sigma(x) = \mu(x)$ if $x \in \mathsf{dom}(\mu)$. The operation $\tau \veebar \mu$ is called *completion* because μ provides values for variables not defined in τ. The operation is associative and therefore we can omit parentheses. For an assignment τ and an annotated clause C the function $\mathsf{inst}(\tau, C)$ returns the annotated clause $\left\{l^{[\sigma \veebar \tau]} \mid l^{\sigma} \in C\right\}$. The system IR-calc is defined in Figure 4.

The calculus IRM-calc further extends IR-calc by enabling annotations containing $*$. The rules of the calculus IRM-calc are presented in Figure 5. The symbol $*$ may be introduced by the merge rule, e.g. by collapsing $x^{0/u} \vee x^{1/u}$ into $x^{*/u}$. The calculus IR-calc p-simulates $\forall$Exp+Res as well as Q-Res. The calculus IRM-calc p-simulates IR-calc as well as LD-Q-Res [8].

3 A lower bound in IR-calc for the formulas of Kleine Büning et al.

Our first main result is a proof complexity analysis of a well-known family of formulas KBKF(t) first defined by Kleine Büning et al. [34]. Here we prove that the KBKF(t) formulas are hard for IR-calc, which is stronger than Q-Res (Cor. 16,[8, Thm 6]). This provides the first non-trivial lower bound for IR-calc, and further even separates the system from LD-Q-Res.

▶ **Definition 1** (Kleine Büning, Karpinski and Flögel [34]). The formula KBKF(t) has prefix $\exists y_0, y_{1,0}, y_{1,1}\, \forall x_1\, \exists y_{2,0}, y_{2,1}\, \forall x_2 \ldots \forall x_{t-1}\, \exists y_{t,0}, y_{t,1}\, \forall x_t\, \exists y_{t+1} \ldots y_{t+t}$ and matrix clauses

$$\begin{array}{rlrll}
C_- &= \{\neg y_0\} & C_0 &= \{y_0, \neg y_{1,0}, \neg y_{1,1}\} & \\
C_i^0 &= \{y_{i,0}, x_i, \neg y_{i+1,0}, \neg y_{i+1,1}\} & C_i^1 &= \{y_{i,1}, \neg x_i, \neg y_{i+1,0}, \neg y_{i+1,1}\} & \text{for } i \in [t-1] \\
C_t^0 &= \{y_{t,0}, x_t, \neg y_{t+1}, \ldots, \neg y_{t+t}\} & C_t^1 &= \{y_{t,1}, \neg x_t, \neg y_{t+1}, \ldots, \neg y_{t+t}\} & \\
C_{t+i}^0 &= \{x_i, y_{t+i}\} & C_{t+i}^1 &= \{\neg x_i, y_{t+i}\} & \text{for } i \in [t].
\end{array}$$

Let us verify that the KBKF(t) formulas are indeed false QBFs and – at the same time – provide some intuition about them. The existential player starts by playing $y_0 = 0$ because of clause C_-. Clause C_0 forces the existential player to set one of $y_{1,0}, y_{1,1}$ to 0. Assume the existential chooses $y_{1,0} = 0$ and $y_{1,1} = 1$. If the universal player tries to win, he will counter with $x_1 = 0$, thus forcing the existential player again to set one of $y_{2,0}, y_{2,1}$ to 0. This continues for t rounds, leaving in each round a choice of $y_{i,0} = 0$ or $y_{i,1} = 0$ to the existential player, to which the universal counters by setting x_i accordingly. Finally, the existential player is forced to set one of $y_{t+1}, \ldots, y_{2t}$ to 0. This will contradict one of the clauses $C_{t+1}^0, C_{t+1}^1, \ldots, C_{2t}^0, C_{2t}^1$, and the universal player wins.

It is clear from this explanation, that the existential player has exponentially many choices and the universal player likewise needs to uniquely counter to all these choices to win. The aim of this section is to show that IR-calc and therefore Q-Res in some sense need to go through all these exponentially many options in order to refute the formula, thus forcing IR-calc and Q-Res proofs of exponential size.

Syntactically, KBKF(t) are *existential Horn formulas*, i.e., they contain at most one positive existential literal per clause. In fact, they even have a stronger property: C_- is the only clause without a head (a positive existential literal). We will strengthen this in the next lemma by a simple modification such that now all clauses have a head.

▶ **Lemma 2.** *We can transform every IR-calc refutation π of* KBKF(t) *into a IR-calc proof π' of y_0 from* KBKF(t) $\setminus \{\neg y_0\}$. *We perform this by: (i) deleting every instance of the axiom*

$\{\neg y_0\}$; *(ii) for every clause without a positive existential literal we add the literal* y_0 *to the clause with the empty annotation.*

After this transformation, which preserves proof length, we can focus on proofs of y_0 from $\mathrm{KBKF}(t) \setminus \{\neg y_0\}$. Exploiting that all axioms now contain exactly one positive literal we show a number of invariants, which hold for all clauses in all IR-calc proofs of the formulas.

▶ **Lemma 3.** *Let* C *be an annotated clause in an IR-calc proof of* y_0 *from* $\mathrm{KBKF}(t) \setminus \{\neg y_0\}$*. Then the following invariants hold for* C*:*

1. C *has exactly one positive literal* $y^A_{h,a}$ *for* $h \leq t$ *or* y^A_h *for* $h > t$ *(or* y_0 *with no annotation). We call this unique literal the* head *of* C *and use the indices* h *and* a *also in the following invariants to denote its position as well as* A *for its annotation.*
2. *If, for some* $j \in [2t], b \in \{0,1\}$ *and* B *some annotation,* $\neg y^B_{j,b} \in C$ *(or* $\neg y^B_j \in C$*), then* $j > h$*. i.e. literals in the body are always at a higher quantification level than the head.*
3. *If* $\neg y^B_{j,b} \in C$ *(or* $\neg y^B_j \in C$*), then* $A \cup \{a/x_h\} \subseteq B$*, where all extra annotations in* B *are of the form* c_k/x_k *for* $k > h$*. This invariant acts vacuously for* $h > t$ *where the clauses contain no negative literals.*
4. *If* $\neg y^B_{j,b} \in C$ *(or* $\neg y^B_j \in C$*) then for all* k*,* $h \leq k < j$ *(or* $h \leq k \leq t$*, when* $j > t$*) there is* $c_k \in \{0,1\}$ *such that* $c_k/x_k \in B$*.*
5. *If* $\neg y^B_{j,b} \in C$ *with* $j \leq t$*, then for* $k \in [t], d \in \{0,1\}$ *and* D *some annotation, there is no* $\neg y^D_{k,d} \in C$ *nor* $\neg y^D_{t+k} \in C$ *such that* $B \cup \{b/x_j\} \subseteq D$*.*

We will now give the overall idea of our lower bound argument. For a clause C we define a set $\Sigma(C)$ of annotations associated with C. Our lower bound argument then rests on counting the set $\Sigma(C)$ as we progress through the proof. More precisely, we show that axioms have empty Σ and that instantiation steps do not change Σ at all. In a resolution step $\frac{D_1 \quad D_2}{C}$, the set $\Sigma(C)$ either equals $\Sigma(D_1) \cup \Sigma(D_2)$ or grows by exactly one new element. In some sense, we only make progress in the proof in the latter case, and we need exponentially many resolution steps of this kind. Putting everything together we find that by the end of the proof we must have collected all the exponentially many annotations in $\Sigma(y_0)$, implying an exponential lower bound to the proof length (Theorem 6).

We now just give the skeleton of the formal argument. We start with the definition of Σ.

▶ **Definition 4.** Let C be a clause in an IR-calc proof of y_0 from $\mathrm{KBKF}(t) \setminus \{\neg y_0\}$. We define the set $\Sigma(C)$ of complete annotations (to all x_i) by the following rules.

1. $\Sigma(C) = \emptyset$ when $C = \{y^B_{t+j}\}$ *(type-1 clause).*
   Assume now that C is not type-1 and has the head $y^A_{h,a}$.
2. $\Sigma(C) = \emptyset$ when some x_j, $j < h$ is not given a value in A *(type-2 clause).*
3. Otherwise *(type-3 clause)*, $\Sigma(C)$ is defined by the following process of adding and removing assignments according to C, which now has complete annotations for each literal by Invariant 4. We start by initialising $\Sigma(C)$ as all complete annotations X to $x_1, \dots, x_t$ such that $A \cup \{a/x_h\} \subseteq X$ (if y_0 is the head we add the complete set of annotations). For each $\neg y^B_{j,b} \in C$ with $j \leq t$ we remove from $\Sigma(C)$ all complete annotations X such that $B \cup \{b/x_j\} \subseteq X$. Invariant 5 ensures that annotations will not be deleted twice here. Finally, we remove annotations B for all $y^B_j \in C$ with $j > t$ (note that B is necessarily complete by Invariants 3 and 4).

For type-3 clauses C, $\Sigma(C)$ counts the complete annotations (and their corresponding literals) resolved away, negative literals are required to be removed and positive literals increase Σ because they can be used to remove a negative literal by resolving. It works by making each $y_{i,j}$ worth twice as much as $y_{i+1,k}$ because of the C_i^j axioms. Types 1 and 2 are special cases.

The next lemma is the key to our lower bound.

▶ **Lemma 5.** *Let C be a clause in an IR-calc proof from $\mathrm{KBKF}(t) \setminus \{\neg y_0\}$.*

1. *If C is the instantiation of an axiom, then $\Sigma(C) = \emptyset$.*
2. *If C is derived by instantiating D, then $\Sigma(C) = \Sigma(D)$.*
3. *Let C be derived by resolving D_1 and D_2. Let $\sqcup$ denote disjoint union. If D_1 is a type-3 clause that is resolved with the type-1 clause $D_2 = \{y_{t+j}^B\}$ for $j > 0$ and there is no $k > 0$, $k \neq j$ such that $\neg y_{t+k}^B \in D_1$, then $\Sigma(C) = \Sigma(D_1) \sqcup \Sigma(D_2) \sqcup \{B\} = \Sigma(D_1) \sqcup \{B\}$. Otherwise $\Sigma(C) = \Sigma(D_1) \sqcup \Sigma(D_2)$.*

We can now deduce that all proofs of $\mathrm{KBKF}(t)$ in IR-calc are of at least exponential size.

▶ **Theorem 6.** *All proofs of $\mathrm{KBKF}(t)$ in IR-calc have length at least 2^t.*

Since IR-calc simulates Q-Res [8], we get as a corollary the hardness of $\mathrm{KBKF}(t)$ for Q-Res as already stated in [34].

▶ **Corollary 7.** *All proofs of $\mathrm{KBKF}(t)$ in Q-Res are of at least exponential size.*

As the formulas $\mathrm{KBKF}(t)$ are easy for long-distance and universal resolution [22, 43] we obtain the following exponential separations.

▶ **Corollary 8.** *IR-calc does neither simulate LD-Q-Res nor QU-Res.*

4 Lower bounds for Q-Res and QU-Res via strategy extraction

This section shows a new and conceptually very different lower bound for QU-Res (and thus for Q-Res). This lower bound constitutes in fact a new lower bound technique that is widely applicable (cf. Sec. 6). We illustrate this technique here with an exponential lower bound for parity formulas in QU-Res. This provides a separation between QU-Res and ∀Exp+Res.

The lower bound argument hinges on strategy extraction, which is a widely used paradigm in QBF solving and proof systems. We recall that QU-Res admits strategy extraction via a computationally very restricted model, namely decision lists.

▶ **Definition 9** (decision list [39])**.** A *decision list* $D = (t_1, c_1), \ldots, (t_n, c_n)$ is a finite sequence of pairs where t_i is a term and $c_i \in \{0, 1\}$ is a Boolean constant. Additionally, the last term is the empty term (equivalent to true). For an assignment μ, a decision list D evaluates to c_i if i is the least index such that $\mu \models t_i$, in such case we say that (t_i, c_i) *triggers* under μ.

Winning strategies in form of decision lists can be efficiently extracted from QU-Res proofs:

▶ **Theorem 10** (Balabanov, Jiang, Widl [3, 4])**.** *Given a Q-Res or QU-Res refutation π of QBF ϕ, there exists a winning strategy for the universal player for ϕ, such that each of its strategies for the universal variables is computable by a decision list of size polynomial in $|\pi|$.*

Balabanov et al. use a different form than decision lists, but it is semantically equivalent. We deem decision lists as more intuitive for our purposes. Note that that under our definition, a strategy for a universal variable may take as input outputs of strategy functions of smaller index (similarly as in the strategy construction by Goultiaeva et al. [25]).

The general idea behind our lower bound technique is as follows. First, we observe that we can define a family of QBFs ϕ_f, such that every winning strategy of the universal player must compute a unique Boolean function f (Lemma 12). If we know that strategy extraction is possible by a weak computational model, say AC^0, we can carefully choose the Boolean formula ϕ_f such that the unique winning strategy f cannot be computed by AC^0 circuits. As the extracted strategy is polynomial in the proof, this implies a lower bound on the proof size. Thus we immediately turn circuit lower bounds to lower bounds for the proof size.

We will now implement this idea for the *parity function* $\textsc{Parity}(x_1, \ldots, x_n) = x_1 \oplus \cdots \oplus x_n$, which is the classical example of a function not computable in AC^0.

▶ **Theorem 11** (Furst, Saxe, Sipser [23], Håstad [26]). $\textsc{Parity} \notin \mathsf{AC}^0$. *In fact, every non-uniform family of bounded-depth circuits computing* $\textsc{Parity}$ *is of exponential size.*

We first observe how to construct a QBF that forces a unique winning strategy.

▶ **Lemma 12.** *Consider the QBF* $\exists x_1, \ldots, x_n \forall z. (z \vee \phi_f) \wedge (\neg z \vee \neg \phi_f)$*, where* ϕ_f *is a propositional formula depending only on the variables* $x_1, \ldots, x_n$*. Let* $f : 2^n \to \{0, 1\}$ *be a Boolean function that returns 1 iff* ϕ_f *evaluates to true. Then there is a unique strategy for the universal player for* z*, which is* $z \leftarrow f$*.*

We will now use this idea specifically for the parity function. Consider the QBF $\Phi = \exists X \forall z \exists T. \ (F^+ \wedge F^-)$ where F^+ is a CNF encoding of $z \vee \textsc{Parity}(X)$ and F^- encodes $\neg z \vee \neg\textsc{Parity}(X)$. Both F^+ and F^- use additional variables in T. More precisely, for $N > 1$ define $\text{Q}\textsc{Parity}_N$ as follows. Let $\text{xor}(o_1, o_2, o)$ be the set of clauses $\{\neg o_1 \vee \neg o_2 \vee \neg o, o_1 \vee o_2 \vee \neg o, \neg o_1 \vee o_2 \vee o, o_1 \vee \neg o_2 \vee o\}$, which defines o to be $o_1 \oplus o_2$. Define $\text{Q}\textsc{Parity}_N$ as

$$\exists x_1, \ldots, x_N \, \forall z \, \exists t_2, \ldots, t_N. \ \text{xor}(x_1, x_2, t_2) \cup \textstyle\bigcup_{i=3}^{N} \text{xor}(t_{i-1}, x_i, t_i) \cup \{z \vee t_N, \neg z \vee \neg t_N\}.$$

Note that since we want to encode parity in CNF, i.e. a bounded-depth formula, and $\textsc{Parity} \notin \mathsf{AC}^0$, we need to use further existential variables (recall that existential AC^0 characterises all of NP). Choosing existential variables t_i to encode the prefix sums $x_1 \oplus \cdots \oplus x_i$ of the parity $x_1 \oplus \cdots \oplus x_N$ provides the canonical CNF formulation of parity.

To use the lower bound of Theorem 11 we need to verify that QU-Res enables strategy extraction in AC^0. This holds as decision lists can be turned into bounded-depth circuits.

▶ **Lemma 13.** *If* f_D *can be represented as a polynomial-size decision list* D*, then* $f_D \in \mathsf{AC}^0$*.*

Proof. Let $S = \{i \mid (t_i, 1) \in D\}$ be the indices of all pairs in D with 1 as the second component. Observe that f_D evaluates to 1 under μ iff one of the t_i with $i \in S$ triggers under μ. For each t_i with $i \in S$ construct a function $f_i = t_i \wedge \bigwedge_{l=1}^{i-1} \neg t_l$. Construct a circuit for the function $\bigvee_{i \in S} f_i$, which is equal to f_D and is computable in AC^0 as all t_i are just terms. ◀

We can now put everything together and turn the circuit lower bound of Theorem 11 into a lower bound for proof size in QU-Res.

▶ **Theorem 14.** *Any QU-Res refutation of* $\text{Q}\textsc{Parity}_N$ *is of exponential size in* N*.*

Proof. By Lemma 12 there is a unique strategy for the variable z in $\text{Q}\textsc{Parity}_N$, which is the $\textsc{Parity}$ function on N variables. From Theorem 10, there is a polynomial-time algorithm for constructing a decision list D_N from any QU-Res refutation of $\text{Q}\textsc{Parity}_N$. Such decision list can be converted in polynomial time into a circuit with bounded depth by Lemma 13. Hence, the decision list must be of exponential size in N due to Theorem 11. ◀

In contrast to this lower bound, the parity formulas are easy in ∀Exp+Res.

▶ **Lemma 15.** *The formulas* $\text{Q}\textsc{Parity}_N$ *have polynomial-size ∀Exp+Res refutations.*

Proof sketch. Expand z in both polarities, which generates the clauses $\mathrm{xor}(x_1, x_2, t_2^{0/z}) \cup \bigcup_{i=3}^{N} \mathrm{xor}(t_{i-1}^{0/z}, x_i, t_i^{0/z}) \cup \{t_N^{0/z}\}$ and $\mathrm{xor}(x_1, x_2, t_2^{1/z}) \cup \bigcup_{i=3}^{N} \mathrm{xor}(t_{i-1}^{1/z}, x_i, t_i^{1/z}) \cup \{\neg t_N^{1/z}\}$.

Inductively, for $i = 2, \ldots, N$ derive clauses representing $t_i^{0/z} = t_i^{1/z}$. This lets us derive a contradiction using the clauses $t_N^{0/z}$ and $\neg t_N^{1/z}$. ◀

Theorem 14 together with Lemma 15 immediately give the following separations.

▶ **Corollary 16.** *Q-Res and QU-Res do not simulate ∀Exp+Res, IR-calc, IRM-calc.*

This also has consequences for the complexity of strategy extraction in ∀Exp+Res.

▶ **Corollary 17.** *Winning strategies for ∀Exp+Res cannot be computed in* AC^0*. This even holds when the system ∀Exp+Res is restricted to formulas with constant quantifier complexity.*

Note, however, that strategy extraction for IRM-calc is in P due to [8, Thm. 4].

5 Extending the lower bound to LD-Q-Res and LQU$^+$-Res

We now aim to extend the lower bound from the previous section to stronger QBF proof systems using long-distance resolution. For this we cannot directly use the strategy extraction method from the last section. However, we will slightly modify the parity formulas and then reduce the hardness of those in the stronger systems to the hardness of QParity in Q-Res. As the modified formulas remain easy for ∀Exp+Res, these lower bounds imply many new separations between the proof systems involved.

We start by extending the lower bound to LD-Q-Res, which will provide a separation of LD-Q-Res and ∀Exp+Res. For this we consider a variant of the parity formulas from the last section. Let $\mathrm{xor}_l(o_1, o_2, o, z)$ be the set of clauses $\{z \vee \neg o_1 \vee \neg o_2 \vee \neg o,\ z \vee o_1 \vee o_2 \vee \neg o,\ z \vee \neg o_1 \vee o_2 \vee o,\ z \vee o_1 \vee \neg o_2 \vee o\}$ (xor_l defines o to be equal to $o_1 \oplus o_2$ if $z = 0$). The formulas $\mathrm{LQParity}_N$ are constructed from $\mathrm{QParity}_N$ by replacing each occurrence of $\mathrm{xor}(\ldots)$ by two copies $\mathrm{xor}_l(\ldots, z)$ and $\mathrm{xor}_l(\ldots, \neg z)$. It is easy to verify that the same arguments as for QParity in Section 4 also apply to LQParity, yielding:

▶ **Proposition 18.** *The formulas* $\mathrm{LQParity}_N$ *have polynomial-size ∀Exp+Res refutations, but require exponential-size Q-Res refutations.*

We now want to show that LQParity is hard for LD-Q-Res by arguing that long-distance steps do not help to refute these formulas. In the next two lemmas we will show that this actually applies to all QBFs Φ meeting the following condition.

▶ **Definition 19.** We say that z is *completely blocked in a QBF* Φ, if all clauses of Φ contain the universal variable z and some existential literal l such that $\mathrm{lv}(z) < \mathrm{lv}(l)$.

▶ **Lemma 20.** *Let Φ be a QBF and z be completely blocked in Φ. Let further C be a clause derived from Φ by LD-Q-Res. If C contains some existential literal l such that* $\mathrm{lv}(z) < \mathrm{lv}(l)$*, then $z \in C$ or $\neg z \in C$, or $z^* \in C$.*

▶ **Lemma 21.** *Let Φ be a QBF such that z is completely blocked in Φ and let π be a refutation of Φ such that the variable z is ∀-reduced as early as possible. Then the derivation of the empty clause in π does not contain z^* in any of its clauses.*

This enables us to prove the hardness of LQParity in LD-Q-Res.

▶ **Theorem 22.** *Any refutation of* $\mathrm{LQParity}_N$ *in LD-Q-Res is exponential in N.*

Proof. Any LD-Q-Res refutation π can be in polynomial time translated into a refutation π' such that $\forall$-reductions are carried out as soon as possible (such a refutation has clauses that are equal to the clauses of π or some universal literals are missing). From Lemma 21, the derivation of $\perp$ in π' contains no occurrences of the merged literal z^*, hence any such clauses can be removed from the refutation. Therefore π' is in fact also a Q-Res refutation. Hence, π must be exponential in N due to Proposition 18. ◀

Our next goal is to extend the lower bound for the parity formulas for the system LQU$^+$-Res, which enables both long-distance and universal resolution. For such we again modify the formula QParity, using a similar technique as in [4]. The trick is essentially to double the universal literals so they form tautological clauses when resolved. This way resolution on universal variables does not give any advantage.

We define formulas QUParity$_N$ from LQParity$_N$ as follows: replace the universal quantifier $\forall z$ by two new quantifiers $\forall z_1 \forall z_2$ and replace all occurrences of the literal z by $z_1 \vee z_2$ and likewise of $\neg z$ by $\neg z_1 \vee \neg z_2$. It is clear that these formulas are false as the universal player should play both z_1 and z_2 as they would z in QParity. In a similar argument as for LQParity we now show that neither long-distance nor universal resolution steps help to refute QUParity

▶ **Theorem 23.** QUParity$_N$ *require exponential-size refutations in LQU$^+$-Res.*

As QUParity$_N$ still remains easy for $\forall$Exp+Res in a proof similar to Lemma 15 we get the following separations.

▶ **Corollary 24.** *LQU$^+$-Res does not simulate $\forall$Exp+Res, IR-calc, and IRM-calc.*

6 Strategy extraction as a general lower bound technique

The results of Sect. 4 can be vastly generalised. We say that a QBF proof system P has *strategy extraction in complexity class* C if from each proof π of a QBF φ, a winning strategy for the universal player, i.e. strategies for all universal variables, can be computed from π in C.

Let L be a language in Σ^p_k/poly for some $k \geq 0$. Let $L = \{x \in \Sigma^\star \mid \exists y_1 \forall y_2 \dots Q y_k. A(x,y)\}$, where A is a predicate computable in P/poly. We can thus compute A by a sequence of polynomial-size circuits A_n. The computation of each such circuit A_n can be described by a CNF $C_n(\bar{x}, \bar{y}, \bar{w})$, where $\bar{x}$ are the propositional variables associated with the input x, $\bar{y}_1, \dots, \bar{y}_k$ are the propositional variables for the witnesses $y_1, \dots, y_k$, and $\bar{w}$ are auxiliary propositional variables describing the gates of the circuit A_n.

Now let $\Phi_{L,n}(\bar{x}, \bar{y}_1, \dots, \bar{y}_k, z, \bar{w}) = \exists \bar{x} \forall z \exists \bar{y}_1 \forall \bar{y}_2 \dots Q \bar{y}_k \exists \bar{w}. (z \leftrightarrow C_n(\bar{x}, \bar{y}_1, \dots, \bar{y}_k, \bar{w}))$. Clearly, this is a false QBF as it expresses that x is both in and outside L. Moreover, from the construction of the formula it is clear that the only winning strategy for the universal player is to play $z = 1 - \chi_L(x)$, where χ_L is the characteristic function of L, and to supply arbitrary values for the remaining universal variables $\bar{y}_2$ etc. Therefore each winning strategy for the universal player for Φ_L will have to compute the characteristic function of L. This immediately yields conditional lower bounds for proof systems with strategy extraction:

▶ **Theorem 25.** *Let P be QBF proof system with strategy extraction in* P/poly*. Then P is not polynomially bounded, unless* PH $\subseteq$ P/poly.

Note that the assumption PH $\not\subseteq$ P/poly is considered very weak. In fact, even NP$\cap$coNP $\subseteq$ P/poly is considered unlikely as factoring is in NP $\cap$ coNP. Also by the Karp-Lipton theorem [32], $\mathsf{NP} \subseteq \mathsf{P/poly}$ implies that the polynomial hierarchy collapses to the second level, and there are even stronger Karp-Lipton collapse consequences known (cf. [18, 13]).

Theorem 25 can be applied e.g. to IRM-calc, which has strategy extraction in P [8].

▶ **Corollary 26.** *IRM-calc is not polynomially bounded unless* $\mathsf{PH} \subseteq \mathsf{P/poly}$.

If the proof system allows for strategy extraction via weaker models, then we can improve the conditional lower bounds to unconditional lower bounds, possibly even exponential. We exemplify this paradigm in our next results.

▶ **Theorem 27.** *Let P be a QBF proof system.*

1. *Let P have strategy extraction in a complexity class C such that the non-uniform version of C is strictly weaker than $\mathsf{NP/poly}$. Then P is not polynomially bounded.*
2. *If P has strategy extraction in AC^0, then P requires exponential-size proofs, even for formulas of bounded quantifier complexity.*

Our previous Theorem 14 is an instance of item 2 of Theorem 27. In contrast, we can show that the method of strategy extraction is not effective for ∀Exp+Res (and therefore neither for IR-calc nor IRM-calc), because all formulas that are potentially hard via the strategy extraction method are easy for ∀Exp+Res, similarly as in Lemma 15.

▶ **Proposition 28.** *For every language $L \in \mathsf{P/poly}$ the formulas $\Phi_{L,n}$ have polynomial-size ∀Exp+Res refutations.*

We remark that the same method of constructing short ∀Exp+Res proofs does not work once we have further universal or existential variables in the formulas, i.e. if L is a language from a level Σ_i^{P} or Π_i^{P} with $i \geq 1$.

7 Conclusion

We have shown new lower bounds for Q-Res, IR-calc, LD-Q-Res and LQU$^+$-Res, and thereby settled the relative complexity of the main resolution-based QBF calculi. This reveals an almost complete picture of the simulation order of these proof systems (cf. Fig. 1). Most importantly, our results show striking separations between all proof systems modelling CDCL-based QBF solving vs. proof systems modelling expansion-based solving. This provides theoretical evidence that these two paradigms for QBF-solving are indeed complementary and should enhance the power of the solvers when carefully used in conjunction.

Two specific questions that remain open are to show explicit lower bounds for natural QBF formulas in IRM-calc and to fully explore the relationship of this system to universal resolution. With respect to lower bounds for IRM-calc we remark that it is easy to transfer classical resolution lower bounds to this system (e.g., use the existentially closed version of the pigeonhole principle) and thereby improve Corollary 26 to an unconditional lower bound. However, it would be interesting to find meaningful classes of QBFs that are hard for IRM-calc. Regarding the relationship to universal resolution we leave open whether IRM-calc can simulate LQU$^+$-Res (but conjecture incomparability of the systems).

A more general and challenging open problem is to determine the extent of the applicability of our new lower bound method via strategy extraction. Here we have shown that this method is very effective for ∃∀∃-formulas in Q-Res, but fails for exactly these formulas in expansion-based systems as ∀Exp+Res and stronger. Is it possible to use the technique for different types of QBFs even for unconditional lower bounds for stronger QBF proof systems? On open question remains how these techniques apply to the recent systems Q(D)-resolution [42] and QRAT [27].

Acknowledgments This work was partially supported by CMU-Portugal grant AMOS (CMUP-EPB/TIC/0049/2013), FCT grant POLARIS (PTDC/EIA-CCO/123051/2010), INESC-ID's multiannual PIDDAC funding PEst-OE/EEI/LA0021/2011, EPSRC grant EP/L024233/1, and a grant from the John Templeton Foundation. The second author was supported by a Doctoral Training Grant from EPSRC.

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 Sinz and Egly [41], pages 154–169.

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

6 Marco Benedetti. Evaluating QBFs via symbolic Skolemization. In Franz Baader and Andrei Voronkov, editors, *LPAR*, volume 3452, pages 285–300. Springer, 2004.

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

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

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

10 Olaf Beyersdorff, Nicola Galesi, and Massimo Lauria. A lower bound for the pigeonhole principle in tree-like resolution by asymmetric prover-delayer games. *Information Processing Letters*, 110(23):1074–1077, 2010.

11 Olaf Beyersdorff, Nicola Galesi, and Massimo Lauria. A characterization of tree-like resolution size. *Information Processing Letters*, 113(18):666–671, 2013.

12 Olaf Beyersdorff, Nicola Galesi, and Massimo Lauria. Parameterized complexity of DPLL search procedures. *ACM Transactions on Computational Logic*, 14(3), 2013.

13 Olaf Beyersdorff and Sebastian Müller. A tight Karp-Lipton collapse result in bounded arithmetic. *ACM Transactions on Computational Logic*, 11(4), 2010.

14 Armin Biere. Resolve and expand. In *SAT*, pages 238–246, 2004.

15 Armin Biere, Marijn Heule, Hans van Maaren, and Toby Walsh, editors. *Handbook of Satisfiability*, volume 185 of *Frontiers in Artificial Intelligence and Applications*. IOS Press, 2009.

16 Maria Luisa Bonet, Juan Luis Esteban, Nicola Galesi, and Jan Johannsen. On the relative complexity of resolution refinements and cutting planes proof systems. *SIAM J. Comput.*, 30(5):1462–1484, 2000.

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

18 Jin-Yi Cai. $S_2^p \subseteq ZPP^{NP}$. *Journal of Computer and System Sciences*, 73(1):25–35, 2007.

19 Stephen A. Cook and Phuong Nguyen. *Logical Foundations of Proof Complexity.* Cambridge University Press, 2010.

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

21 Uwe Egly, Martin Kronegger, Florian Lonsing, and Andreas Pfandler. Conformant planning as a case study of incremental QBF solving. *CoRR*, abs/1405.7253, 2014.

22 Uwe Egly, Florian Lonsing, and Magdalena Widl. Long-distance resolution: Proof generation and strategy extraction in search-based QBF solving. In McMillan et al. [36], pages 291–308.

23 Merrick L. Furst, James B. Saxe, and Michael Sipser. Parity, circuits, and the polynomial-time hierarchy. *Mathematical Systems Theory*, 17(1):13–27, 1984.

24 Enrico Giunchiglia, Paolo Marin, and Massimo Narizzano. Reasoning with quantified boolean formulas. In Biere et al. [15], pages 761–780.

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

26 Johan Håstad. *Computational Limitations of Small-depth Circuits.* MIT Press, Cambridge, MA, USA, 1987.

27 Marijn Heule, Martina Seidl, and Armin Biere. A unified proof system for QBF preprocessing. In *Automated Reasoning – 7th International Joint Conference, IJCAR*, volume 8562, pages 91–106. Springer, 2014.

28 Mikoláš Janota, William Klieber, João Marques-Silva, and Edmund M. Clarke. Solving QBF with counterexample guided refinement. In Alessandro Cimatti and Roberto Sebastiani, editors, *SAT*, volume 7317, pages 114–128. Springer, 2012.

29 Mikoláš Janota, Radu Grigore, and Joao Marques-Silva. On QBF proofs and preprocessing. In McMillan et al. [36], pages 473–489.

30 Mikoláš Janota and Joao Marques-Silva. ∀Exp+Res does not P-Simulate Q-resolution. International Workshop on Quantified Boolean Formulas, 2013.

31 Mikoláš Janota and Joao Marques-Silva. On propositional QBF expansions and Q-resolution. In M. Järvisalo and A. Van Gelder, editors, *SAT*, pages 67–82. Springer, 2013.

32 Richard M. Karp and Richard J. Lipton. Some connections between nonuniform and uniform complexity classes. In *Proc. 12th ACM Symposium on Theory of Computing*, pages 302–309. ACM Press, 1980.

33 Hans Kleine Büning and Uwe Bubeck. Theory of quantified boolean formulas. In Biere et al. [15], pages 735–760.

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

35 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.

36 Kenneth L. McMillan, Aart Middeldorp, and Andrei Voronkov, editors. *Logic for Programming, Artificial Intelligence, and Reasoning, LPAR.* Springer, 2013.

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

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

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

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

41 Carsten Sinz and Uwe Egly, editors. *Theory and Applications of Satisfiability Testing - SAT*, volume 8561. Springer, 2014.

42 Friedrich Slivovsky and Stefan Szeider. Variable dependencies and Q-resolution. In Sinz and Egly [41], pages 269–284.

43 Allen Van Gelder. Contributions to the theory of practical quantified Boolean formula solving. In Michela Milano, editor, *CP*, volume 7514, pages 647–663. Springer, 2012.

44 Lintao Zhang and Sharad Malik. Conflict driven learning in a quantified Boolean satisfiability solver. In *ICCAD*, pages 442–449, 2002.