Electronic Colloquium on Computational Complexity, Report No. 5 (2016)

Extension Variables in QBF Resolution

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

[1] School of Computing, University of Leeds, United Kingdom
[2] Microsoft Research, Cambridge, United Kingdom

Abstract. We investigate two QBF resolution systems that use extension variables: *weak extended Q-resolution*, where the extension variables are quantified at the innermost level, and *extended Q-resolution*, where the extension variables can be placed inside the quantifier prefix. These systems have been considered previously by Jussila et al. [13], who give experimental evidence that extended Q-resolution is stronger than weak extended Q-resolution.
Here we prove an exponential separation between the two systems, thereby confirming the conjecture of [13]. Conceptually, this separation relies on showing strategy extraction for weak extended Q-resolution by bounded-depth circuits. In contrast, we show that this strong strategy extraction result fails in extended Q-resolution.

1 Introduction

Using extension variables to abbreviate possibly complex formulas is a well known and powerful concept in proof complexity and solving. In Tseitin transformations, extension variables are used to encode arbitrary propositional formulas in CNF. More generally, allowing the extension rule in proofs is known to shorten proof size drastically for many examples. This makes extension variables also very interesting in the context of solving, and indeed modern proof checking formats such as RAT for SAT-solvers [11] and QRAT for QBF solvers [12] incorporate the use of extension variables.

When augmenting the classical resolution system with the extension rule, allowing to introduce a new variable v to abbreviate a disjunction $\neg x \vee \neg y$, we arrive at *extended resolution* [21], cf. also [16]. Although resolution itself is considered a weak proof system with many known lower bounds (cf. [20]), extended resolution is an extremely powerful system. Extended resolution is equivalent to extended Frege systems [7,15], one of the strongest proof systems considered today. Showing any non-trivial lower bounds for extended Frege constitutes an extremely challenging problem with even hard candidate formulas currently lacking.

In QBF solving and proof complexity, using extension variables was first considered by Jussila et. al. [13], where they augment Q-resolution, a QBF analogue of resolution [14], to an extended Q-resolution system. In comparison to the propositional case, extension variables in QBF present one additional challenge. We cite the relevant passage from [13]:

"In adapting the extension rule to the QBF setting, the crucial question is where to 'put' new variables, e.g., how defined variables are ordered with respect to variables that already occur in the formula. It seems intuitive that new variables can only be existential. It is also clear that they cannot be moved further out than the innermost variable on which they depend. In the experimental section we show that we actually need this freedom to move defined variables as far out as possible. Keeping them in the innermost existential scope, as for instance in the Tseitin encoding of a non-CNF QBF formula, is insufficient."

The main contribution of this work is to underline this experimental observation with a rigorous theoretical argument. For this we consider two systems: weak extended Q-resolution, where extension variables are quantified at the innermost level, and extended Q-resolution,

ISSN 1433-8092

where extension variables are quantified immediately after the innermost variable on which they depend.

Our main result is an exponential separation between these two versions. We show that QPARITY formulas recently introduced in [5] have short proofs in extended Q-resolution, but require exponential-size proofs in weak extended Q-resolution.

The lower bound uses the strategy extraction technique, recently introduced for Q-resolution in [5] and further developed for stronger systems in [3]. Here we show that weak extended Q-resolution admits strategy extraction in AC^0, i.e., from each refutation of a false QBF we can extract a winning strategy for the universal player that can be computed by constant-depth circuits. This allows to transfer Håstad's circuit lower bound for parity [10] to a proof size lower bound for the QPARITY formulas in weak extended Q-resolution.

2 Preliminaries

We recall some definitions on QBFs and proof systems.

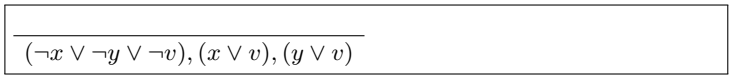
Quantified Boolean formulas. A (closed prenex) *quantified Boolean formula* (QBF) is a formula in quantified propositional logic where each variable is quantified at the beginning of the formula, using either an existential or universal quantifier. We denote such formulas as $\mathcal{Q}\,.\,\phi$, where ϕ is a propositional Boolean formula in conjunctive normal form (CNF), called *matrix*, and $\mathcal{Q}$ is its *quantifier prefix*. The *quantification level* $\mathsf{lv}(y)$ of a variable y in $\mathcal{Q}\,.\,\phi$ is the number of alternations of quantifiers y has on its left in the quantifier prefix of $\mathcal{Q}\,.\,\phi$. Given a variable y, we will sometimes refer to the variables with quantification level lower than $\mathsf{lv}(y)$ as variables *left* of y; analogously the variables with quantification lever higher than $\mathsf{lv}(y)$ will be *right* of y.

Often it is useful to think of a QBF $\mathcal{Q}_1 X_1 \dots \mathcal{Q}_k X_k\,.\,\phi$ 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 [9], [1, Sec. 4.2.2], [17, Chap. 19].

Classical resolution. *Resolution*, introduced by Blake [6] and Robinson [19], is a refutational proof system manipulating unsatisfiable CNFs as sets of clauses. The only inference rule is $\dfrac{C \vee x \qquad D \vee \neg x}{C \cup D}$ where C, D denote clauses and x is a variable. A resolution refutation derives the empty clause $\bot$.

QBF resolution calculi. *Q-resolution* by Kleine Büning, Karpinski, and Flögel [14] is a resolution-like calculus that operates on QBFs in prenex form where the matrix is a CNF. It uses the propositional resolution rule above with the side conditions that variable x is existential and if $z \in C$, then $\neg z \notin D$. We do this to prevent tautological clauses, which we also forbid from being introduced in the proof system via axiom. In addition Q-resolution has a universal reduction rule

$$\frac{C \vee u}{C} \qquad \frac{C \vee \neg u}{C}\ (\forall\text{-Red})$$



where:
x, y are variables already in the formula
v is a fresh variable,
v is inserted into prefix as existentially quantified,
weak extension: insert v at the end of the prefix
general extension: insert v after x and y in the prefix

Fig. 1. Two versions of *extension rule*

where variable u is universal and all other existential variables $x \in C$ are left of u in the quantifier prefix.

Q-resolution is not the only QBF resolution system; for further calculi cf. e.g. [4].

3 Two versions of extended Q-resolution

Extended resolution for propositional resolution [21], enables adding clauses expressing the equality $v \Leftrightarrow (\neg x \vee \neg y)$, for a fresh variable v. We follow this idea in the context of Q-resolution. Here, we need to decide the position of the fresh variable in the prefix. Two versions are considered. A weak one and a general one.

Figure 1 defines the two forms of the extension rule, which gives us two flavors of extended Q-resolution.

Definition 1. Weak extended Q-resolution *is the calculus of Q-resolution enhanced with the extension rule in its weak form.*

Definition 2. Extended Q-resolution *is the calculus of Q-resolution enhanced with the extension rule in its general form.*

Extended resolution and circuits. Semantically, introducing a fresh variable via the extension rule, corresponds to defining $v = x \,\mathsf{nand}\, y$. This enables expressing any Boolean functions in a circuit form by a sequence of extension rules. Consider for instance $x \vee y$. Introduce fresh variables x^{n} and y^{n} to denote the negation of x and y, respectively, by setting $x^{\mathrm{n}} = x \,\mathsf{nand}\, x$. Subsequently, use those to define the final output o by setting $o = x^{\mathrm{n}} \,\mathsf{nand}\, y^{\mathrm{n}}$.

In the following text, whenever it is obvious that a formula is expressible in a circuit form, we omit the intermediate definitions. In particular, in proofs, we enable writing extension clauses where x and y may be literals rather than just variables.

For instance, the extension clauses $x \vee \neg y \vee \neg v$, $\neg x \vee \neg v$, $y \vee \neg v$ are realized by the introduction of a variable x^n corresponding to the negation of x, introduction of v via the extension rule and finally replacing x^n with $\neg x$ by extra resolutions steps.

4 The QParity formulas

We recall the QParity formulas from [5]. Let $\mathrm{xor}(o_1, o_2, o)$ 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 equal to $o_1 \oplus o_2$. Define

QPARITY$_n$ as

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

The auxiliary variables t_i express the prefix sums $x_1 \oplus \cdots \oplus x_i$, and hence t_n computes the parity $x_1 \oplus \cdots \oplus x_n$ of the x variables. Therefore, the formulas express that there exists an assignment to the x variables such that $x_1 \oplus \cdots \oplus x_n$ is neither 0 nor 1, an obvious contradiction. The crucial feature of QPARITY$_n$ is that the only strategy of the universal player to win on this formula is to play $z = x_1 \oplus \cdots \oplus x_n$, i.e., the strategy has to compute parity.

In [5] the QPARITY formulas are shown to require exponential-size Q-Res refutations. Here we will show that they in fact provide an exponential separation of weak extended Q-resolution and extended Q-resolution.

5 Short proofs for QParity in extended Q-resolution

We show that QPARITY is easy for extended Q-resolution.

Theorem 3. *The formulas* QPARITY$_n$ *have linear-size proofs in extended Q-resolution.*

Proof. We define extension variable $s_2 = (x_1 \vee x_2) \wedge (\bar{x}_1 \vee \bar{x}_2)$. In clausal form this introduces the following clauses:

$$s_2 \vee \bar{x}_1 \vee x_2 \quad s_2 \vee x_1 \vee \bar{x}_2 \quad \bar{s}_2 \vee x_1 \vee x_2 \quad \bar{s}_2 \vee \bar{x}_1 \vee \bar{x}_2$$

For $2 < i \leq n$, we define extension variables $s_i = s_{i-1} \oplus x_i = (s_{i-1} \vee x_i) \wedge (\bar{s}_{i-1} \vee \bar{x}_i)$.
In clausal form this introduces the following clauses:

$$s_i \vee \bar{x}_i \vee s_{i-1} \quad s_i \vee x_i \vee \bar{s}_{i-1} \quad \bar{s}_i \vee x_i \vee s_{i-1} \quad \bar{s}_i \vee \bar{x}_i \vee \bar{s}_{i-1}$$

The main part of this short proof is to show that we can easily substitute s_i for t_i. We will show this by induction on i. The shortness comes from the fact that s_n literals are left of z. This allows us to reduce z literals "early" and get a contradiction.

Induction Claim: Clauses $s_i \vee \bar{t}_i$ and $t_i \vee \bar{s}_i$ (that show $s_i = t_i$) are provable in $O(i)$ size proofs.

Base Case: Let $i = 2$,

$$\dfrac{\dfrac{\dfrac{s_2 \vee \bar{x}_1 \vee x_2 \quad \bar{t}_2 \vee \bar{x}_1 \vee \bar{x}_2}{s_2 \vee \bar{t}_2 \vee \bar{x}_1} \quad \dfrac{s_2 \vee x_1 \vee \bar{x}_2 \quad \bar{t}_2 \vee x_1 \vee x_2}{s_2 \vee \bar{t}_2 \vee x_1}}{s_2 \vee \bar{t}_2}$$

$$\dfrac{\dfrac{\dfrac{t_2 \vee \bar{x}_1 \vee x_2 \quad \bar{s}_2 \vee \bar{x}_1 \vee \bar{x}_2}{t_2 \vee \bar{s}_2 \vee \bar{x}_1} \quad \dfrac{t_2 \vee x_1 \vee \bar{x}_2 \quad \bar{s}_2 \vee x_1 \vee x_2}{t_2 \vee \bar{s}_2 \vee x_1}}{t_2 \vee \bar{s}_2}$$

Inductive Step: we assume from induction hypothesis that we have for some $i \leq n$, $s_{i-1} \vee \bar{t}_{i-1}$ and $t_{i-1} \vee \bar{s}_{i-1}$

Firstly we use the clauses that express $s_{i-1} = t_{i-1}$ to substitute s_{i-1} for t_{i-1} .

$$\frac{\bar{t}_i \vee \bar{x}_i \vee \bar{t}_{i-1} \quad t_{i-1} \vee \bar{s}_{i-1} \quad t_i \vee x_i \vee \bar{t}_{i-1}}{\bar{t}_i \vee \bar{x}_i \vee \bar{s}_{i-1} \quad t_i \vee x_i \vee \bar{s}_{i-1}}$$

$$\frac{\bar{t}_i \vee x_i \vee t_{i-1} \quad s_{i-1} \vee \bar{t}_{i-1} \quad t_i \vee \bar{x}_i \vee t_{i-1}}{\bar{t}_i \vee x_i \vee s_{i-1} \quad t_i \vee \bar{x}_i \vee s_{i-1}}$$

We can use that the clauses that define s_i and t_i are structurally the same to derive $s_i = t_i$.

$$\frac{\dfrac{s_i \vee \bar{x}_i \vee s_{i-1} \quad \bar{t}_i \vee \bar{x}_1 \vee \bar{s}_{i-1}}{s_i \vee \bar{t}_i \vee \bar{x}_i} \qquad \dfrac{s_i \vee x_i \vee \bar{s}_{i-1} \quad \bar{t}_i \vee x_i \vee s_{i-1}}{s_i \vee \bar{t}_i \vee x_1}}{s_i \vee \bar{t}_i}$$

$$\frac{\dfrac{t_i \vee \bar{x}_i \vee s_{i-1} \quad \bar{s}_i \vee \bar{x}_i \vee \bar{s}_{i-1}}{t_i \vee \bar{s}_i \vee \bar{x}_i} \qquad \dfrac{t_i \vee x_i \vee \bar{s}_{i-1} \quad \bar{s}_i \vee x_1 \vee s_{i-1}}{t_i \vee \bar{s}_i \vee x_i}}{t_i \vee \bar{s}_i}$$

Since we only add a constant number of clauses, the induction argument allows us to keep a $O(i)$ size proof up until $s_n \vee \bar{t}_n$ and $t_n \vee \bar{s}_n$.

$$\frac{s_n \vee \bar{t}_n \quad z \vee t_n}{s_n \vee z} \qquad \frac{t_n \vee \bar{s}_n \quad \bar{z} \vee \bar{t}_n}{\bar{s}_n \vee \bar{z}_n}$$

Because s_n is defined only on x_i variables and so universal reduction is available

$$\frac{\dfrac{s_n \vee z}{s_n} \qquad \dfrac{\bar{s}_n \vee \bar{z}_n}{\bar{s}_n}}{\bot}$$

This completes the short refutation in extended Q-resolution.

6 Strategy extraction and hardness of QParity in weak extended Q-resolution

We now complement the upper bound from the previous section with a lower bound for the same formulas in weak extended Q-resolution. The lower bound argument rests on strategy extraction, which is a widely used paradigm in QBF solving and proof systems. Strategy extraction as a lower bound technique was introduced in [5] and further developed in [3].

The idea is to show that from refutations of false formulas it is possible to efficiently extract winning strategies for the universal player. For Q-resolution it is known [2] that strategies can be extracted in a very simple model, namely decision lists.

Definition 4 (Rivest [18]). *A* decision list *is a finite sequence of pairs (t_i, c_i) where t_i is a term and $c_i \in \{0, 1\}$ is a Boolean constant. Additionally, the last term is the empty term, semantically equivalent to true. For an assignment μ, a decision list $D = (t_1, c_1), \ldots, (t_n, c_n)$ evaluates to c_i if i is the least index such that $\mu \models t_i$. We say that (t_i, c_i)* triggers *under μ if this condition is satisfied.*

Now we take a look at how decision lists are translated into bounded-depth Boolean circuits.

Lemma 5 (Beyersdorff, Chew, Janota [5]). *If the function f can be represented as a polynomial-size decision list D, then f can be computed by polynomial-size circuits of depth 3.*

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 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 $f_S = \bigvee_{i \in S} f_i$. The function f_S is equal to f_D and can be computed in depth 3 as all t_i are just terms.

Balabanov and Jiang [2] showed that Q-resolution allows strategy extraction in decision lists. Here we show that the same remains true in weak extended Q-resolution. In comparison to [2] we provide a simplified proof.

Theorem 6. *Given a refutation π of QBF ϕ in weak extended Q-resolution, there exists a winning strategy for the universal player for ϕ such that for each universal variable u of ϕ the winning strategy can be represented as a Boolean function f_u that is expressible as a decision list whose size is polynomial in $|\pi|$.*

Proof. We first review the proof of the strategy extraction theorem for Q-resolution and then explain at the end how it applies to weak extended Q-resolution.

Let $\pi = (L_1, \ldots, L_\ell)$ be a resolution refutation of the false QBF $\mathcal{Q} \,.\, \phi$ and let

$$\pi_i = \begin{cases} \emptyset & \text{if } i = \ell, \\ (L_{i+1}, \ldots, L_\ell) & \text{otherwise.} \end{cases}$$

We show, by reverse induction on i, that from π_i it is possible to construct in linear time (w.r.t. $|\pi_i|$) a winning strategy σ^i for the universal player for the QBF formula $\mathcal{Q} \,.\, \phi_i$, where

$$\phi_i = \begin{cases} \phi & \text{if } i = 0, \\ \phi \wedge L_1 \wedge \cdots \wedge L_i & \text{otherwise,} \end{cases}$$

such that for each universal variable u in $\mathcal{Q} \,.\, \phi$, there exists a decision list D_u^i computing σ_u^i as a function of the variables in $\mathcal{Q}$ left of u, having size $O(|\pi_i|)$.

The statement of the theorem corresponds to the case when $i = 0$. The base case of the induction is for $i = \ell$. In this case σ^ℓ is trivial since ϕ_ℓ contains the line $L_\ell = \bot$, and we can define all the D_u^ℓ as $u \leftarrow 0$.

We show now how to construct σ_u^{i-1} and D_u^{i-1} from σ_u^i and D_u^i:

- If L_i is derived by resolution, then for each universal variable u we set $\sigma_u^{i-1} = \sigma_u^i$ and $D_u^{i-1} = D_u^i$.
- Suppose L_i is the result of an application of a $\forall$red rule on clause L_j, that is $L_j = L_i \vee u^c$ with $c \in \{0, 1\}$, where u is the rightmost variable in L_j, and u^0 stands for $\neg u$ and u^1 for u. Let $\boldsymbol{x}_{u'}$ denote the variables on the left of u' in the quantifier prefix of $\mathcal{Q} \,.\, \phi$. Then we define

$$\sigma_{u'}^{i-1}(\boldsymbol{x}_{u'}) = \begin{cases} \sigma_{u'}^i(\boldsymbol{x}_{u'}) & \text{if } u' \neq u, \\ 1 - c & \text{if } u' = u \text{ and } L_i(\boldsymbol{x}_u) = 0, \\ \sigma_u^i(\boldsymbol{x}_u) & \text{if } u' = u \text{ and } L_i(\boldsymbol{x}_u) = 1. \end{cases}$$

Moreover for each $u' \neq u$ we set $D_{u'}^{i-1} = D_{u'}^i$ and we set D_u^{i-1} as follows:

$\texttt{if } \neg L_i(\boldsymbol{x}_u) \texttt{ then } u \leftarrow 1 - c\texttt{;}$
$\texttt{else } D_i^u(\boldsymbol{x}_u)\texttt{.}$

We now check that for each u', $\sigma_{u'}^{i-1}$ respects all the properties of the inductive claim.

It is clear that $\sigma_{u'}^{i-1}$ and $D_{u'}^{i-1}$ are well defined and constructed in linear time w.r.t. $|\pi_{i-1}|$. Also, by construction $D_{u'}^{i-1}$ computes $\sigma_{u'}^{i-1}$.

To verify that σ^{i-1} is a winning strategy for $\mathcal{Q}\,.\,\phi_{i-1}$ we fix an assignment ρ to the existential variables of ϕ. Let τ_i be the complete assignment to existential and universal variables, constructed in response to ρ under the strategy σ^i. By induction hypothesis τ_i falsifies ϕ_i. We need to show that τ_{i-1} falsifies ϕ_{i-1}. To show this we distinguish again two cases.

If L_i is derived by the resolution rule, then $\sigma^{i-1} = \sigma^i$ and $\tau_{i-1} = \tau_i$. Hence by induction hypothesis, τ_i falsifies a conjunct from ϕ_i. To argue that τ_{i-1} also falsifies a conjunct from ϕ_{i-1} we only need to look at the case when the falsified conjunct is L_i. As L_i is false under τ_i and L_i is derived by resolution, by soundness of the resolution rule one of the parent formulas of L_i in the application of the resolution rule must be falsified as well. Hence τ_{i-1} falsifies ϕ_{i-1}.

Let now L_i be derived by $\forall\mathsf{red}$ from $L_j = L_i \vee u^c$ for some $j < i$. In this case, our strategy σ^{i-1} changes the assignment τ_i only when τ_i made the universal player win by falsifying L_i. As we set u to $1 - c$, the modified assignment τ_{i-1} falsifies L_j. Otherwise, if τ_i does not falsify L_i we keep $\tau_{i-1} = \tau_i$ and hence falsify one of the conjuncts of ϕ_{i-1} by induction hypothesis.

Let us now explain how the above applies to weak extended Q-resolution. Consider a refutation π of a QBF $\mathcal{Q}\boldsymbol{x}\,.\,\phi(\boldsymbol{x})$ in weak extended Q-resolution. We can view π as a Q-resolution refutation of the QBF $\mathcal{Q}\boldsymbol{x}\exists\boldsymbol{y}\,.\,\phi(\boldsymbol{x}) \wedge \psi(\boldsymbol{x},\boldsymbol{y})$, where suitable extension variables $\boldsymbol{y}$ together with their definitions $\psi(\boldsymbol{x},\boldsymbol{y})$ have been added.

We apply the argument above to construct decision lists computing a winning strategy for $\mathcal{Q}\boldsymbol{x}\exists\boldsymbol{y}\,.\,\phi(\boldsymbol{x}) \wedge \psi(\boldsymbol{x},\boldsymbol{y})$. By definition of the $\forall\mathsf{red}$ rule, no $\boldsymbol{y}$ variables are present in $\forall\mathsf{red}$ steps in π. Hence the decision list will also not use any of the extension variables and therefore in fact compute a winning strategy for the original formula $\mathcal{Q}\boldsymbol{x}\,.\,\phi(\boldsymbol{x})$.

This result enables us to show lower bounds for formulas that require hard strategies. An example of such formulas are the QPARITY formulas. As observed earlier, the only winning strategy of the universal player on the QPARITY formulas is to actually compute the PARITY function. However, PARITY is the classic example of a function hard for bounded-depth circuits (and hence by Lemma 5 for decision lists).

Theorem 7 (Furst, Saxe, Sipser [8], Håstad [10]). *Every non-uniform family of bounded-depth circuits computing* PARITY *is of exponential size.*

Using strategy extraction we can now immediately transfer this circuit lower bound to an exponential lower bound in weak extended Q-resolution.

Theorem 8. *Any refutation of* QPARITY_n *in weak extended Q-resolution is of exponential size.*

Proof. The unique winning strategy for the variable z in QPARITY_n is to compute $x_1 \oplus \cdots \oplus x_n$. By Theorem 6, there is a polynomial-time algorithm for constructing a decision list D_n from any refutation of QPARITY_n in weak extended Q-resolution. Such decision list can be converted in polynomial time into a depth-3 circuit by Lemma 5. Hence, the refutation must be of exponential size due to Theorem 7.

Theorem 8 together with the upper bound from the previous section imply the following exponential separation.

Corollary 9. *Weak extended Q-resolution does not simulate extended Q-resolution.*

This also has consequences for strategy extraction in extended Q-resolution.

Theorem 10. *Extended Q-resolution has strategy extraction in* P*, but does not admit strategy extraction in* AC^0*.*

Proof. Inspecting the proof of Theorem 6 it is clear that extended Q-resolution still has strategy extraction in polynomial time, and in fact for the original formula not involving extension variables: for this it suffices to perform the construction of the decision lists as in Theorem 6 and then replace extension variables by their definition. To keep the size polynomial, this requires reusing definitions of extensions variables and hence instead of formulas will lead to polynomial-size circuits. However, the substitutions will increase the depth and not result in AC^0 circuits.

To argue that extended Q-resolution does not admit AC^0 strategy extraction we use again the QParity formulas, which have short proofs in extended Q-resolution by Theorem 3, but require exponential-size strategies by Theorem 7.

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, grant no. 48138 from the John Templeton Foundation, and EPSRC grant EP/L024233/1. The second author was supported by a Doctoral Training Grant from EPSRC.

References

1. Arora, S., Barak, B.: Computational Complexity – A Modern Approach. Cambridge University Press (2009)
2. Balabanov, V., Jiang, J.H.R.: Unified QBF certification and its applications. Formal Methods in System Design 41(1), 45–65 (2012)
3. Beyersdorff, O., Bonacina, I., Chew, L.: Lower bounds: From circuits to QBF proof systems. In: Proc. ACM Conference on Innovations in Theoretical Computer Science (ITCS'16). pp. 249–260. ACM (2016)
4. Beyersdorff, O., Chew, L., Janota, M.: On unification of QBF resolution-based calculi. In: MFCS. pp. 81–93 (2014)
5. Beyersdorff, O., Chew, L., Janota, M.: Proof complexity of resolution-based QBF calculi. In: Proc. Symposium on Theoretical Aspects of Computer Science. pp. 76–89. LIPIcs series (2015)
6. Blake, A.: Canonical expressions in boolean algebra. Ph.D. thesis, University of Chicago (1937)
7. Cook, S.A., Reckhow, R.A.: The relative efficiency of propositional proof systems. The Journal of Symbolic Logic 44(1), 36–50 (1979)
8. Furst, M.L., Saxe, J.B., Sipser, M.: Parity, circuits, and the polynomial-time hierarchy. Mathematical Systems Theory 17(1), 13–27 (1984)
9. Goultiaeva, A., Van Gelder, A., Bacchus, F.: A uniform approach for generating proofs and strategies for both true and false QBF formulas. In: IJCAI. pp. 546–553 (2011)
10. Håstad, J.: Computational Limitations of Small Depth Circuits. MIT Press, Cambridge (1987)
11. Heule, M., Jr., W.A.H., Wetzler, N.: Verifying refutations with extended resolution. In: Automated Deduction - CADE-24 - 24th International Conference on Automated Deduction. pp. 345–359 (2013)

12. Heule, M., Seidl, M., Biere, A.: A unified proof system for QBF preprocessing. In: IJCAR. pp. 91–106 (2014)
13. Jussila, T., Biere, A., Sinz, C., Kröning, D., Wintersteiger, C.M.: A first step towards a unified proof checker for QBF. In: Marques-Silva, J., Sakallah, K.A. (eds.) SAT. vol. 4501, pp. 201–214. Springer (2007)
14. Kleine Büning, H., Karpinski, M., Flögel, A.: Resolution for quantified Boolean formulas. Inf. Comput. 117(1), 12–18 (1995)
15. Krajíček, J., Pudlák, P.: Some consequences of cryptographical conjectures for S_2^1 and EF. Information and Computation 140(1), 82–94 (1998)
16. Kullmann, O.: On a generalization of extended resolution. Discrete Applied Mathematics 96-97, 149–176 (1999), http://dx.doi.org/10.1016/S0166-218X(99)00037-2
17. Papadimitriou, C.H.: Computational Complexity. Addison-Wesley (1994)
18. Rivest, R.L.: Learning decision lists. Machine Learning 2(3), 229–246 (1987)
19. Robinson, J.A.: A machine-oriented logic based on the resolution principle. Journal of the ACM 12, 23–41 (1965)
20. Segerlind, N.: The complexity of propositional proofs. Bulletin of Symbolic Logic 13(4), 417–481 (2007)
21. Tseitin, G.S.: On the complexity of derivations in the propositional calculus. Studies in Constructive Mathematics and Mathematical Logic Part II, ed. A.O. Slisenko (1968)

ECCC ISSN 1433-8092

http://eccc.hpi-web.de