A Simple Proof of QBF Hardness

Olaf Beyersdorff, Joshua Blinkhorn

Friedrich-Schiller-Universität Jena, Jena, Germany

Abstract

We provide a simple and direct proof of the exponential hardness of the KBKF formulas in the proof system Q-Resolution.

Keywords: proof complexity, QBF, Q-Resolution, lower bounds

1. Introduction

The main objective in proof complexity is to obtain sharp bounds on the proof size of formulas in different formal proof systems. Traditionally, proof complexity has focused on propositional logic [1]. In the last decade there has been intense research on proof complexity of quantified Boolean formulas (QBF). This has been mainly driven by huge advances in the development of QBF solvers [2], which successfully tackle numerous applications [3], but has also uncovered deep connections to circuit complexity [4, 5] and bounded arithmetic [4].

Among the proof systems studied in proof complexity, the resolution calculus takes centre stage, both in the propositional and in the QBF setting. Propositional resolution [6, 7] is one of the simplest and best-analysed proof systems [1, 8], and gained further importance through its tight connections to CDCL solving [9], established in [10, 11]. Propositional resolution was generalised to QBF in the early 1990s with the system Q-Resolution (Q-Res) [12]. Again this is arguably the simplest and best-studied QBF proof system, which as in the SAT case underpins QCDCL solving [13, 1].

There are a number of families of QBFs that frequently appear throughout the QBF literature. Arguably the most prominent among these are the

1There are many extensions of Q-Res and different QBF solving approaches, with the precise relations between QBF solving models and QBF resolution calculi subject to ongoing research [14].
formulas of Kleine Büning, Karpinski, and Flögel, termed the KBKF formulas after their inventors, and introduced in the same work [12] in which Q-Res was developed. For QBF proof complexity, they occupy a similarly central role as the pigeonhole formulas for propositional proof complexity [15]. The KBKF formulas (and easy modifications thereof) permeate the QBF proof complexity literature (e.g. [16, 17, 18, 19, 20, 21, 22, 23, 24]) and give rise to many lower bounds and separations of proof systems.

In their original form, the KBKF formulas were introduced as the first hard formulas for Q-Res. This was stated in [12], however no formal proof was given for the claimed exponential lower bound of KBKF in Q-Res. The paper [12] contains a proof, but there is general consensus in the QBF community that this proof sketch only serves as intuition for their hardness and does not constitute a formal lower bound argument.

The first formal proof of KBKF hardness for Q-Res was only given some 20 years later [20], but this was shown as a lower bound for the more powerful QBF resolution system IR [26], a calculus based on expansion of universal variables [27]. The system IR simulates Q-Res [26] and hence the lower bound of [20] implies the lower bound for Q-Res stated in [12]. However, the proof in [20] is technically very complex and specifically tailored towards KBKF and IR.

A second, more elegant proof was given in [21]. This used a semantic size-cost-capacity technique, developed in that paper as a general lower bound method for QBF calculi. However, this technique is neither directly applicable to KBKF nor to Q-Res. For that reason [21] proved a lower bound for a modification of KBKF in the stronger system of QU-Resolution, which then by a separate argument entails the KBKF lower bound in Q-Res.

A third proof was provided in [24], again using a general technique of formula weight. As with the second proof, this technique does not apply directly to Q-Res, but to the stronger expansion system IR, already figuring in the first proof.

Hence, none of the previous proofs directly works on Q-Res, but all make detours to stronger proof systems. In addition, they are either very complex (first proof) or use sophisticated general lower bound techniques, not

---

3 For completeness, we mention a fourth proof [22]. This proof through Prover-Delayer games is again quite complex and only yields lower bounds in the weaker system of tree-like Q-Resolution, thereby not implying the result stated in [12].
Our contribution in this paper is to give a simple and direct proof of the exponential hardness of KBKF in Q-Res. The proof uses restrictions of Q-Res proofs by partial assignments together with a simple counting argument.

As explained above, the result itself is not new, but given the importance of the KBKF formulas in the QBF literature, we believe that our simple and self-contained argument should be of value to the community. The proof idea itself is potentially applicable to further formulas.

2. Background

In this section, we cover all the necessary background for the lower-bound proof in the following section.

Propositional logic. $U$ is a countable set of Boolean variables. A literal is a variable $z$ in $U$ or its negation $\overline{z}$, with $\text{var}(z) = \text{var}(\overline{z}) = z$. The literals $z$ and $\overline{z}$ are complementary. A clause is a disjunction $C = a_1 \lor \cdots \lor a_k$ of pairwise non-complementary literals, with $\text{vars}(C) := \{\text{var}(a_i) : i \in [k]\}$. A subclause of $C$ is a disjunction of a subset of its disjuncts. A conjunctive normal form formula (CNF) is a conjunction $F := C_1 \land \cdots \land C_k$ of clauses, with $\text{vars}(F) := \bigcup_{i=1}^{k} \text{vars}(C_i)$.

An assignment $\sigma$ to a set $Z$ of Boolean variables is a function from $Z$ into the set of Boolean constants $\{0, 1\}$. The set of all assignments to $Z$ is denoted $\langle Z \rangle$. A partial assignment to $Z$ is an assignment to a subset $Z' \subseteq Z$, called a subassignment of $\sigma$ when it agrees with $\sigma$ on $Z'$. We consider the constant 0 synonymous with the so-called empty clause, i.e. the disjunction of arity zero.

The restriction of a literal, clause, or CNF $\phi$ by $\sigma$, denoted $\phi[\sigma]$, is the result of substituting each variable $z$ in $Z$ by $\sigma(z)$, followed by applying the standard simplifications for Boolean constants, i.e. $\overline{0} \mapsto 1$, $\overline{1} \mapsto 0$, $C \lor 0 \mapsto C$, $C \lor 1 \mapsto 1$, $F \land 1 \mapsto F$, and $F \land 0 \mapsto 0$. We say that $\sigma$ satisfies $\phi$ when $\phi[\sigma] = 1$, and falsifies $\phi$ when $\phi[\sigma] = 0$.

Quantified Boolean formulas. A quantified Boolean formula (QBF) is a formula of the form $Q := P \cdot F$, where $P := \forall U_1 \exists X_1 \cdots \forall U_d \exists X_d$ is called the quantifier prefix and $F$ is a CNF called the matrix. The $U_i$ and $X_i$ are pairwise-disjoint sets of Boolean variables called the blocks of $Q$. Curly braces are omitted from blocks when writing a QBF.
The sets \( \text{vars}_e(Q) := \bigcup_{i=1}^d X_i \) and \( \text{vars}_u(Q) := \bigcup_{i=1}^d U_i \) are referred to as the \textit{existential variables} and \textit{universal variables} of \( Q \), respectively, and their union \( \text{vars}(Q) \) as the \textit{variables} of \( Q \). We deal only with \textit{closed} QBFs, i.e. those for which \( \text{vars}(F) \subseteq \text{vars}(Q) \). The \textit{restriction} of \( Q \) by an assignment \( \sigma \) is \( Q[\sigma] := P[\sigma] \cdot F[\sigma] \), where \( P[\sigma] \) is obtained from \( P \) by deleting each variable in \( \text{vars}(\sigma) \) and any redundant quantifiers.

QBF semantics are defined in terms of the \textit{two-player evaluation game}. Two players, named \textit{universal} and \textit{existential}, assign the variables of a QBF in the order of the prefix, each player assigning only the variables of his designated quantification type. If the assignment falsifies the matrix, the universal player wins, otherwise the existential player wins. A QBF \( Q \) is called \textit{false} when it has a \textit{winning strategy} for the universal player; that is, the universal player can choose assignments to win the evaluation game, regardless of how the existential player chooses his assignments.

The \textbf{KBKF formulas}. A QBF family is an infinite sequence of QBFs. The following family, named after its creators Kleine Büning, Karpinski and Flögel [12], is arguably one of the most famous.

\textbf{Definition 1} (KBKF family [12]). \textit{The KBKF family is the QBF family whose \( n \)th instance is}

\[
\text{KBKF}_n := \exists x_1 y_1 \forall u_1 \ldots \exists x_n y_n \forall u_n \exists z_1 \cdots z_n \cdot \text{kbkf}_n,
\]

\textit{where \text{kbkf}_n is the conjunction of the clauses}

\[
(x_i \lor u_i), \quad (y_i \lor u_i), \quad (y_i \lor u_i), \quad (x_i \lor u_i), \quad (x_i \lor u_i), \quad (y_i \lor u_i), \quad (y_i \lor u_i), \quad (u_i \lor z_i), \quad (u_i \lor z_i), \quad \text{for } i \in [n-1],
\]

\[
(x_{n+1} \lor y_{n+1}), \quad (x_{n+1} \lor y_{n+1}), \quad (y_{n+1} \lor z_{n+1}), \quad (y_{n+1} \lor z_{n+1}), \quad (z_i \lor z_i), \quad (z_i \lor z_i), \quad \text{for } i \in [n].
\]

\textit{The four sets } \( X_n := \{x_1, \ldots, x_n\} \), \( Y_n := \{y_1, \ldots, y_n\} \), \( U_n := \{u_1, \ldots, u_n\} \), \textit{and } \( Z_n := \{z_1, \ldots, z_n\} \textit{partition the variables of } \text{KBKF}_n.\)

We remark that the formulas are stated slightly differently in [12], containing a further existential variable \( y_0 \) that occurs positively in the first clause of \text{kbkf}_n above and in an additional unit clause \((y_0)\). This is easily
transformed into the definition above, and the two formulations have the same proof complexity.

Each instance KBKF \(_n\) is a false QBF. The universal player can win the evaluation game on KBKF \(_n\) with this simple strategy.

**Strategy 1.** For each \(i \in [n]\), assign \(u_i\) to the same value as \(x_i\) was assigned by the existential player.

Let us give some intuition on this strategy. The existential player starts by setting one of \(x_1\) and \(y_1\) to 0, otherwise he falsifies \((\overline{x_1} \lor \overline{y_1})\) and loses immediately. Assume that the existential chooses \(x_1 = 0\) and \(y_1 = 1\). If the universal player tries to win, he will counter with \(u_1 = 0\), thus forcing the existential player again to set one of \(x_2\) and \(y_2\) to 0. This continues for \(n\) rounds, leaving in each round a choice of \(x_i = 0\) or \(y_i = 0\) to the existential player, to which the universal counters by setting \(u_i\) accordingly. Finally, the existential player is forced to set one of \(z_1, \ldots, z_n\) to 0. This will falsify either of the clauses \((u_i \lor z_i)\) or \((\overline{u_i} \lor z_i)\) for some \(i \in [n]\), and the universal player wins.

It is clear from this explanation that the existential player has exponentially many choices, and that the universal player needs to counter all of these choices in any winning strategy. We will exploit this intuition for a formal proof of hardness in the proof system Q-resolution, which we introduce next.

**The Q-resolution proof system.** Q-resolution (Q-Res, \[12\]) is a refutational QBF proof system, i.e. a formal calculus that demonstrates the falsity of a given QBF.

**Definition 2 (Q-Res \[12\]).** A Q-Res refutation of a QBF \(P \cdot F\) is a sequence \(C_1, \ldots, C_k\) of clauses in which \(C_k\) is the empty clause and each \(C_i\) is derived by one of the following rules:

- **A** Axiom: \(C_i\) is a clause in the matrix \(F\).
- **R** Resolution: \(C_i = A \lor B\), where \(C_r = A \lor z\) and \(C_s = B \lor \overline{z}\) for some \(r, s < i\) and some existential variable \(z\).
- **U** Universal reduction: \(C_i = C_r \lor a\) for some \(r < i\) and universal literal \(a\), where \(\text{var}(a)\) is quantified in \(P\) after each existential variable in \(C\).

\(^4\)Note that \(A \lor B\) cannot contain complementary literals by our definition of clauses.
The size of a refutation is the number of clauses in the sequence.

Figure 1 shows a \texttt{Q-Res} refutation of \texttt{KBKF}, depicted conventionally as a directed acyclic graph. Note that the edges of the graph appoint specific antecedents for each clause, a choice left implicit in the refutation written as a sequence. We assume that refutations are in a normal form in which the graph representation has a \textit{unique sink}; that is, the empty clause is the only clause which is not an antecedent in the application of a \texttt{Q-Res} rule.

A \texttt{Q-Res} refutation $\pi$ can be restricted by an assignment $\varepsilon$, denoted $\pi[\varepsilon]$. The technical details of this restriction (i.e. the formal definition of $\pi[\varepsilon]$) are not important. We only require two folklore facts about it, in the case where the assignment is existential.

**Proposition 1** (folklore). \textit{Given a \texttt{Q-Res} refutation $\pi$ of a \texttt{QBF} $Q$, let $\varepsilon$ be a partial assignment to $\text{vars}_{\exists}(Q)$.}

(a) $\pi[\varepsilon]$ is a \texttt{Q-Res} refutation of $Q[\varepsilon]$.

(b) Each universal subclause in $\pi[\varepsilon]$ is a universal subclause in $\pi$.

As restricting resolution proofs by partial assignments is standard in proof
complexity, we omit the proof.\footnote{A rigorous proof of Proposition \textbf{1} along with the definition of $\pi[\varepsilon]$ appears in, for example, \cite{28} Chapter 5, Facts 5.8 and 5.9.}

We also make use of a simple property of refutations when the first block of the refuted QBF is universal. As this property is more specific to Q-\texttt{Res} we include a proof for completeness.

**Proposition 2** (folklore). Let $\pi$ be a Q-\texttt{Res} refutation of a QBF whose first block $U$ is universally quantified. Assume further that for all clauses in $\pi$ there exists a path to the unique sink, which is the empty clause. Then the disjunction of the $U$ literals appearing in $\pi$ is a subclause of some clause appearing in $\pi$.

**Proof.** If there are no $U$ literals appearing in $\pi$, the proposition holds vacuously, so let us assume that there are. Since the graph representation of $\pi$ has the empty clause at its unique sink, each $U$ literal must be universally reduced within $\pi$. Let $C$ be the first clause in $\pi$ to which a universal reduction on a $U$ literal is applied. Since $U$ is the first block, $C$ contains no existential literals. Hence, the only Q-\texttt{Res} steps applicable to $C$ form a sequence of universal reductions ending at the empty clause, the unique sink of $\pi$. This sequence of reductions must reduce each $U$ literal in $\pi$, and hence each such literal appears in $C$. \hfill $\Box$

3. A simple proof of hardness for $\text{KBKF}_n$

3.1. Evaluation game strategies for $\text{KBKF}_n$

The $\text{KBKF}_n$ family has some characteristic semantic properties. For example, Strategy \textbf{1} is not unique. Bad choices from the existential player early on, for example assigning both $x_1$ and $y_1$ to 0, would falsify a clause voluntarily and lose, immediately. From here, the universal player may choose any assignment and win.

Strategy \textbf{1} is unique on a particular subset of the possible games. These are the games characterised by the set of existential assignments

$$\mathbb{E} := \{ \varepsilon \in \langle X_n \cup Y_n \rangle : \text{for each } i \in [n], \varepsilon(x_i) \neq \varepsilon(y_i) \}.$$
In each such game $\varepsilon \in \mathbb{E}$, the universal player’s assignment according to Strategy 1 is given by

$$
\mu_\varepsilon(u_i) := \begin{cases} 
0 & \text{if } \varepsilon(x_i) = 0, \\
1 & \text{if } \varepsilon(y_i) = 0.
\end{cases}
$$

It is easy to see that the $\mu_\varepsilon$ form the set $U := \{\mu_\varepsilon : \varepsilon \in \mathbb{E}\} = \langle U_n \rangle$, and that $|\mathbb{E}| = |U| = 2^n$. Our lower-bound proof is centred on the analysis of games belonging to $\mathbb{E}$, and the role of the corresponding universal assignments $\mathbb{U}$.

Regarding uniqueness, the following can be readily verified by inspection: if the existential player plays according to some $\varepsilon \in \mathbb{E}$, at the first moment his opponent deviates from $\mu_\varepsilon$, the existential player would win the game by setting all remaining existential variables to 1. The resulting existential assignment does not belong to $\mathbb{E}$, but demonstrates that deviating from Strategy 1 at any point during a game in $\mathbb{E}$ would lose by force.

3.2. The formal proof

The proof uses two key observations, which we formulate as Lemma 1.

**Lemma 1.** Let $\pi$ be a $\text{Q-Res}$ refutation of $\text{KBKF}_n$ and let $\varepsilon \in \mathbb{E}$.

(a) Every universal variable in $U_n$ appears in $\pi[\varepsilon]$.

(b) For each $i \in [n]$ there exists a subassignment $\varepsilon'_i$ of $\varepsilon$ such that the $u_i$ literal satisfied by $\mu_\varepsilon$ does not appear in $\pi[\varepsilon'_i]$.

Consideration of these two facts, in combination with the folklore properties of $\text{Q-Res}$ refutations, leads straightforwardly to an exponential proof-size lower bound for $\text{KBKF}_n$. The lemma is proved afterwards.

**Theorem 1.** Any $\text{Q-Res}$ refutation of $\text{KBKF}_n$ has size at least $2^n$.

**Proof.** Let $n \in \mathbb{N}$, and let $\pi$ be a $\text{Q-Res}$ refutation of $\text{KBKF}_n$.

Let $\varepsilon \in \mathbb{E}$. We first show that all the literals falsified by $\mu_\varepsilon$ appear in $\pi[\varepsilon]$. Aiming for contradiction, assume otherwise. By Lemma 1(a), each variable in the domain $U_n$ of $\mu_\varepsilon$ appears in $\pi[\varepsilon]$. It follows that there appears in $\pi[\varepsilon]$ some literal $a$ satisfied by $\mu_\varepsilon$, with $\text{var}(a) = u_i$, say. By Lemma 1(b), there exist domain-disjoint assignments $\varepsilon'_i$ and $\varepsilon''_i$ with $\varepsilon = \varepsilon'_i \cup \varepsilon''_i$ such that $a$ does not appear in $\pi[\varepsilon'_i]$. Then there exists some universal subclause in
\[ \pi[\varepsilon] = \pi[\varepsilon'][\varepsilon''], \] one of whose disjuncts is \( a \), which is not a universal subclause in \( \pi[\varepsilon'] \). This is in direct contradiction to Proposition 1(b).

Now, by Proposition 1(a), \( \pi[\varepsilon] \) is a refutation of
\[ \text{KBKF}_n[\varepsilon] = \forall U_n \exists Z_n \cdot \text{kbkf}_n[\varepsilon], \]
a QBF whose first block is universal. Let \( C_\varepsilon \) be the disjunction of the literals falsified by \( \mu_\varepsilon \). By Proposition 2, \( C_\varepsilon \) is a subclause in \( \pi[\varepsilon] \). Hence \( C_\varepsilon \) is a subclause in \( \pi \), by Proposition 1(b).

If follows that \( \{C_\varepsilon : \varepsilon \in \mathbb{E}\} = \{C : \text{vars}(C) = U_n \} \) contains \( 2^n \) distinct clauses, each of which is a subclause of some clause in \( \pi \). Hence \( |\pi| \geq 2^n \). \( \square \)

**Proof of Lemma 1.** For part (a), observe that the matrix \( \text{kbkf}_n[\varepsilon] \) is the CNF
\[
(b \lor \exists z_1 \lor \cdots \lor \exists z_n) \land (u_1 \lor z_1) \land (\overline{u_1} \lor z_1) \land \cdots \land (u_n \lor z_n) \land (\overline{u_n} \lor z_n),
\]
where \( b = u \) if \( \varepsilon(x_n) = 0 \), and \( b = \overline{u} \) if \( \varepsilon(y_n) = 0 \). Now, removing any pair of clauses \((u_i \lor z_i), (\overline{u_i} \lor z_i)\) from the matrix of \( \text{KBKF}_n[\varepsilon] \) yields a true QBF. Hence, at least one clause from each pair must appear as an axiom in \( \pi[\varepsilon] \), otherwise \( \pi[\varepsilon] \) would be a Q-\text{Res} refutation of a true QBF. Therefore, each variable in \( U_n \) appears in \( \pi[\varepsilon] \).

For part (b), let \( i \in [n] \), and consider the assignment \( \varepsilon_i' \) defined as the domain restriction of \( \varepsilon \) to the variable set \( X_i \cup Y_i = \{x_1, \ldots, x_i\} \cup \{y_1, \ldots, y_i\} \). We will show that \( c \), the \( u_i \) literal falsified by \( \mu_\varepsilon \), appears in \( \pi[\varepsilon_i'] \). Since clauses do not contain complementary literals, \( \overline{u} \) does not appear in \( \pi[\varepsilon_i'] \), by Proposition 2 and the claim (b) follows.

In the particular case \( i = n \), we have \( \varepsilon_i' = \varepsilon \) and \( c = b \). Removing \((b \lor \exists z_1 \lor \cdots \lor \exists z_n)\) from the matrix of \( \text{KBKF}_n[\varepsilon] \) yields a true QBF, hence \( b \) appears in \( \pi[\varepsilon_i'] \). In the remaining case \( i < n \), \( \text{KBKF}_n[\varepsilon_i'] \) is the QBF with prefix \( \forall u_i \exists x_{i+1} \exists y_{i+1} \forall u_{i+1} \cdots \exists x_n \exists y_n \forall u_n \exists Z_n \) and matrix consisting of the clauses
\[
\begin{align*}
(c \lor \overline{x_{i+1}} \lor \overline{y_{i+1}}), \\
(x_j \lor u_j \lor \overline{x_{j+1}} \lor \overline{y_{j+1}}), & \quad \text{for } i + 1 \leq j \leq n - 1, \\
(y_j \lor \overline{u_j} \lor \overline{x_{j+1}} \lor \overline{y_{j+1}}), & \quad \text{for } i + 1 \leq j \leq n - 1, \\
(x_n \lor u_n \lor \overline{x}_1 \lor \cdots \lor \overline{x}_n), \\
(y_n \lor \overline{u_n} \lor \overline{x}_1 \lor \cdots \lor \overline{x}_n), \\
(u_i \lor z_i), & \quad \text{for } i \in [n], \\
(\overline{u_i} \lor z_i), & \quad \text{for } i \in [n].
\end{align*}
\]

It is easy to see that removing \((c \lor \overline{x_{i+1}} \lor \overline{y_{i+1}})\) from the matrix yields a true QBF, hence \( c \) appears in \( \pi[\varepsilon_i'] \). \( \square \)
4. Conclusion

Comparing the original formulation in [12, Theorem 3.2] with Theorem 1 we remark that the former is stated existentially: there exist QBFs that are hard for Q-Resolution. This was a natural formulation in that paper since the authors claimed the first lower bound for Q-Resolution. On the other hand, 25 years later, we now already have many exponential lower bounds for Q-Resolution (cf. [20, 21]) and our aim here was to give a simple proof of the hardness of precisely the same formulas used in the existential statement of [12].

In retrospect, it is quite surprising that the authors of [12] had such good intuition on what would constitute an interesting family of QBFs, and these KBKF formulas (and versions thereof) have since influenced research in QBF proof complexity. For instance, they do not only provide hard instances for Q-Resolution, but also separate Q-Resolution and QU-Resolution, for which we provably need QBFs of unbounded quantifier complexity, a result that was only established very recently [5].

Acknowledgements

Research was supported by grants from the Carl Zeiss Foundation and the John Templeton Foundation (grant no. 60842).

References


