Lower bounds: from circuits to QBF proof systems

Olaf Beyersdorff\(^1\), Ilario Bonacina\(^2\) and Leroy Chew\(^1\)

\(^1\)School of Computing, University of Leeds, UK
\{o.beyersdorff,mm12lnc\}@leeds.ac.uk
\(^2\)Department of Computer Science, Sapienza University of Rome, Italy
bonacina@di.uniroma1.it

August 12, 2015

Abstract

A general and long-standing belief in the proof complexity community asserts that there is a close connection between progress in lower bounds for Boolean circuits and progress in proof size lower bounds for strong propositional proof systems. Although there are famous examples where a transfer from ideas and techniques from circuit complexity to proof complexity has been effective, a formal connection between the two areas has never been established so far. Here we provide such a formal relation between lower bounds for circuit classes and lower bounds for Frege systems for quantified Boolean formulas (QBF).

Starting from a propositional proof system \(P\) we exhibit a general method how to obtain a QBF proof system \(P + \forall\text{red}\), which is inspired by the transition from resolution to Q-resolution. For us the most important case is a new and natural hierarchy of QBF Frege systems \(\mathcal{C}^{\text{-Frege}} + \forall\text{red}\) that parallels the well-studied propositional hierarchy of \(\mathcal{C}^{\text{-Frege}}\) systems, where lines in proofs are restricted to a circuit class \(\mathcal{C}\).

Building on earlier work for resolution (Beyersdorff, Chew, and Janota, 2015a) we establish a lower bound technique via strategy extraction that transfers arbitrary lower bounds for the circuit class \(\mathcal{C}\) to lower bounds in \(\mathcal{C}^{\text{-Frege}} + \forall\text{red}\).

By using the full spectrum of state-of-the-art circuit lower bounds, our new lower bound method leads to very strong lower bounds for QBF Frege systems:

(i) exponential lower bounds and separations for \(\mathsf{AC}^0[p]^{\text{-Frege}} + \forall\text{red}\) for all primes \(p\);
(ii) an exponential separation of \(\mathsf{AC}^0[p]^{\text{-Frege}} + \forall\text{red}\) from \(\mathsf{TC}^0^{\text{-Frege}} + \forall\text{red}\);
(iii) an exponential separation of the hierarchy of constant-depth systems \(\mathsf{AC}^0[d]^{\text{-Frege}} + \forall\text{red}\) by formulas of depth independent of \(d\).

In the propositional case, all these results correspond to major open problems.

1 Introduction

Proof complexity investigates how difficult it is to prove theorems in different formal systems. The main question asks, given a formula \(\varphi\) and a proof system \(P\), typically comprised of axioms and rules, what is the size of the smallest proof of \(\varphi\) in \(P\). This question bears tight and fruitful relations to a number of further areas, in particular to computational complexity, where lower bounds to the size of proofs offer an approach towards the separation of complexity classes.
(Cook’s Programme), and to first-order logic (bounded arithmetic theories and their separations). More recently, the tremendous success of SAT solving has been a main driver for proof complexity, as the analysis of proof systems underlying SAT solvers provides the main theoretical framework towards understanding the power and limitations of solving, cf. the survey of Buss (2012).

The bulk of research in proof complexity has concentrated on proof systems for classical propositional logic. Regarding the central question above, propositional proof complexity has made enormous progress over the past three decades in showing tight lower and upper bounds for many principles in various proof systems. Arguably even more important, a number of general lower bound techniques have been developed that can be employed to show lower bounds to the size of proofs. These include the seminal size-width relationship (Ben-Sasson and Wigderson, 2001), the feasible interpolation technique (Krajček, 1997), or game-theoretic techniques (cf. the recent overview in (Beyersdorff and Kullmann, 2014)).

Notwithstanding these advances, some of the most natural proof systems have resisted all attempts for lower bounds for decades. Frege systems (also known as Hilbert-type systems) are the typical textbook calculi comprised of axiom schemes and rules, and no non-trivial lower bounds are known for Frege. While the power of Frege does not depend on the choice of axioms or rules (Cook and Reckhow, 1979), their strength can be calibrated by restricting the class of allowed formulas. In particular, a hierarchy of Frege systems can be obtained by considering Boolean circuits of increasing strength as lines in Frege. These circuit classes comprise the standard classes $\text{AC}^0 \subset \text{AC}^0[p] \subset \text{TC}^0 \subseteq \text{NC}^1 \subseteq \text{P/poly}$, giving rise to a similar hierarchy of Frege systems.

While the strongest non-uniform lower bounds known in circuit complexity hold for the class $\text{AC}^0[p]$ (Razborov, 1987; Smolensky, 1987), $\text{AC}^0$-Frege is the strongest of the above Frege systems with non-trivial lower bounds (Ajtai, 1994; Krajíček et al., 1995; Pitassi et al., 1993). Despite enormous efforts, all attempts to transfer Razborov’s and Smolensky’s $\text{AC}^0[p]$ circuit lower to a proof size lower bound in $\text{AC}^0[p]$-Frege have failed so far. More widely, it seems the common belief in the proof complexity community that substantial progress in circuit complexity would also give rise to major new lower bounds in proof complexity, for Frege ($= \text{NC}^1$-Frege) or even extended Frege ($= \text{P/poly-Frege}$). Though this connection has been often postulated (cf. e.g. (Beame and Pitassi, 2001)), it could never have been made formal so far.

In this paper we establish a technique to transfer circuit lower bounds to proof size lower bounds for proof systems for quantified Boolean formulas (QBF). Our technique lifts arbitrary circuit lower bounds to proof size bounds for QBF Frege systems, yielding in particular exponential lower bounds for $\text{AC}^0[p]$-Frege for QBFs via (Razborov, 1987; Smolensky, 1987).

Before explaining our results in more detail, we discuss recent developments in QBF proof complexity.

QBF proof complexity is a relatively young field studying proof systems for quantified Boolean logic. Similarly as in the propositional case, one of the main motivations for the field comes via its intimate connection to solving. SAT and QBF solvers are powerful algorithms that efficiently solve the classically hard problems of SAT and QBF for large classes of practically relevant formulas, with modern solvers routinely solving industrial instances in millions of variables for various applications. Although QBF solving is at an earlier state, due to its PSPACE completeness, QBF even applies to further fields such as formal verification or planning (Benedetti and Mangassarian, 2008; Egly et al., 2014; Rintanen, 2007).

The connection to proof complexity comes from the fact that each successful run of a solver on an unsatisfiable instance can be interpreted as a proof of unsatisfiability; and modern SAT
and QBF solvers are known to correspond to the resolution proof system and its variants. In comparison to SAT, the picture is more complex in QBF as there exist two main solving approaches utilising CDCL and expansion-based solving. To model the strength of these QBF solvers, a number of resolution-based QBF proof systems have been developed. Q-resolution (Q-Res) by Kleine Büning et al. (1995) forms the core of the CDCL-based systems. To capture further ideas from CDCL solving, Q-Res has been augmented to long-distance resolution by Balabanov and Jiang (2012), universal resolution QU-Res by Van Gelder (2012), and their combinations (Balabanov et al., 2014). QBF resolution systems for expansion-based solving were developed in (Beyersdorff et al., 2014; Janota and Marques-Silva, 2015). Recent progress led to a complete understanding of the relative power of all these resolution-type QBF systems (Balabanov et al., 2014; Beyersdorff et al., 2015a; Janota and Marques-Silva, 2015).

From a proof complexity perspective, resolution is considered as a weak system, witnessed by the wealth of resolution lower bounds (cf. (Segerlind, 2007) for a survey); and the same classification applies to all of the QBF resolution calculi mentioned above. In addition to these weak QBF systems, there exist a number of very strong sequent calculi (Cook and Morioka, 2005; Egly, 2012; Krajíček and Pudlák, 1990) as well as the general proof checking format QRAT (Heule et al., 2014).

However, compared to propositional proof complexity, a number of other approaches is yet missing in QBF. In particular, algebraic systems such as polynomial calculus (Clegg et al., 1996) or systems based on integer programming as cutting planes (Cook et al., 1987) have received great attention in recent years in propositional proof complexity. These systems are interesting as they are of intermediate strength: stronger than resolution, but weaker than Frege. No analogues of these systems have been considered in QBF so far; and even a QBF version of the propositional Frege hierarchy mentioned above has not been considered in QBF prior to this paper.

1.1 Our contributions

Below we summarise our main contributions of this paper, sketching the main results and techniques.

A. From propositional to QBF: new QBF proof systems. We exhibit a general method how to transform a propositional proof system to a QBF proof system. Our method is both conceptually simple and elegant. Starting from a propositional proof system $P$ comprised of axioms and rules, we design a system $P + \forall\text{red}$ for closed prenex QBFs (Definition 3.1). Throughout the proof, the quantifier prefix is fixed, and lines in the system $P + \forall\text{red}$ are conceptually the same as lines in $P$, i.e. clauses in resolution, circuits from $C$ in $C$-Frege, or inequalities in cutting planes. Our new system $P + \forall\text{red}$ uses all the rules from $P$, and can apply those on arbitrary lines, irrespective of whether the variables are existentially or universally quantified. To make the system complete, we introduce a $\forall\text{red}$ rule that allows to replace universal variables by simple Herbrand functions, which can be represented as lines in $P$. The link to Herbrand functions provides a clear semantic meaning for the $\forall\text{red}$ rule, resulting in a natural and robust system $P + \forall\text{red}$.

Our new systems $P + \forall\text{red}$ are inspired by the approach taken in the definition of Q-Res (Kleine Büning et al., 1995); and indeed when choosing resolution as the base system $P$, our system $P + \forall\text{red}$ coincides with the previously studied QU-Res (Van Gelder, 2012). While our definitions are quite general and yield for example previously missing QBF versions of polynomial
calculus or cutting planes, we concentrate here on exploring the hierarchy $C$-$\text{Frege} + \forall\text{red}$ of new QBF $\text{Frege}$ systems.

**B. From circuit to QBF lower bounds: a general technique.** As mentioned above, it is a long-standing belief that circuit lower bounds correspond to proof size lower bounds, and clearly some of the strongest lower bounds in proof complexity as those for $AC^0$-$\text{Frege}$ are inspired by proof techniques in circuit complexity, cf. the survey of Beame and Pitassi (2001). Here we give a precise and formal account on how any circuit lower bound for $C$ can be directly lifted to a proof size lower bound in $C$-$\text{Frege} + \forall\text{red}$.

Conceptually, our lower bound method uses the idea of strategy extraction, an important paradigm in QBF (Theorem 4.3). Semantically, a QBF can be understood as a game between a universal and an existential player, where the universal player wins if and only if the QBF is false. Winning strategies for the universal player can be very complex. However, we show that from each refutation of a false QBF in a system $C$-$\text{Frege} + \forall\text{red}$ we can efficiently extract a winning strategy for the universal player in a simple computational model we call $C$-decision lists. We observe that $C$-decision lists are easy to transform into $C$ circuits itself, with only a slight increase in complexity.

To obtain a proof-size lower bound we need a function $f$ that is hard for $C$. From $f$ we construct a family $Q$-$f_n$ of false QBFs such that each winning strategy of the universal player on $Q$-$f_n$ has to compute $f$. By strategy extraction, refutations of $Q$-$f_n$ in $C$-$\text{Frege} + \forall\text{red}$ yield $C$-circuits for $f$; hence all such refutations must be long. In fact, we even show the converse implication to hold, i.e. from small $C$-circuits for $f$ we construct short proofs of $Q$-$f_n$ in $C$-$\text{Frege} + \forall\text{red}$.

Our lower bound technique widely generalises ideas recently used by Beyersdorff et al. (2015a) to show lower bounds for $Q$-$\text{Res}$ and $\text{QU-Res}$ for formulas originating from the $\text{PARITY}$ function.

**C. Lower bounds and separations: applying our framework.** We apply our proof technique to a number of famous circuit lower bounds, thus obtaining lower bounds and separations for $C$-$\text{Frege} + \forall\text{red}$ systems that are yet unparalleled in propositional proof complexity. The following results are contained in Section 5.

(a) **Lower bounds and separations for $AC^0[p]$-$\text{Frege} + \forall\text{red}$.** By the seminal results of (Razborov, 1987; Smolensky, 1987), $\text{PARITY}$ and more generally $\text{MOD}_q$ are the classic examples for functions that require exponential-size bounded-depth circuits with $\text{MOD}_p$ gates, where $p$ and $q$ are different primes. Using these functions, we define families of QBFs that require exponential-size proofs in $AC^0[p]$-$\text{Frege} + \forall\text{red}$ by strategy extraction.

To obtain separations of these proof systems, the exact formulation of the QBFs matters. When defining the $\text{PARITY}$ or $\text{MOD}_q$ formulas directly from (arbitrary) $NC^1$-circuits computing these functions, we obtain polynomial-size upper bounds in $\text{Frege} + \forall\text{red}$. However, when carefully choosing specific and indeed very natural encodings, we can prove upper bounds for the $\text{MOD}_p$ formulas even in $AC^0[q]$-$\text{Frege} + \forall\text{red}$, thus obtaining exponential separations of all the $AC^0[p]$-$\text{Frege} + \forall\text{red}$ systems for distinct primes $p$.

As mentioned before, lower bounds for $AC^0[p]$-$\text{Frege}$ (as well as their separations) are major open problems in propositional proof complexity.

(b) **Separating $AC^0[p]$-$\text{Frege} + \forall\text{red}$ from $TC^0$-$\text{Frege} + \forall\text{red}$.** $\text{MAJORITY}$ is another classic function in circuit complexity, for which exponential lower bounds are known for constant-depth circuits with $\text{MOD}_p$ gates for each prime $p$ (Razborov, 1987; Smolensky, 1987). Using our technique, we transfer these to lower bounds in $AC^0[p]$-$\text{Frege} + \forall\text{red}$ for all primes $p$. Carefully
choosing the QBF encoding of \textsc{Majority}, we obtain polynomial upper bounds for the \textsc{Majority} formulas in $\text{TC}^0$-$\text{Frege} + \forall\text{red}$, thus proving an exponential separation between $\text{AC}^0[p]$-$\text{Frege} + \forall\text{red}$ and $\text{TC}^0$-$\text{Frege} + \forall\text{red}$. Again, such a separation is wide open in propositional proof complexity.

(c) **Separating the $\text{AC}^0_d$-$\text{Frege} + \forall\text{red}$ hierarchy by CNFs.** As a third example for our approach we investigate the fine structure of $\text{AC}^0_d$-$\text{Frege} + \forall\text{red}$, comprising all $\text{AC}^0_d$-$\text{Frege} + \forall\text{red}$ systems, where all formulas in proofs are required to have at most depth $d$ for a fixed constant $d$. Resolution is an important example of such a system for depth $d = 1$. In circuit complexity the $\text{SIPSER}_d$ functions from (Boppana and Sipser, 1990) provide an exponential separation of depth-$(d-1)$ from depth-$d$ circuits (Håstad, 1986). With our technique, this separation translates into a separation of $\text{AC}^0_{d-3}$-$\text{Frege} + \forall\text{red}$ from $\text{AC}^0_d$-$\text{Frege} + \forall\text{red}$, where the increased gap of size 3 comes from our transformation of $\mathcal{C}$-decision lists into $\mathcal{C}$-circuits.

The $\text{SIPSER}_d$ formulas achieving these separations are prenexed CNFs, i.e. the formulas have depth 2. While in propositional proof complexity the hierarchy of $\text{AC}^0_d$-$\text{Frege}$ systems is exponentially separated (Ajtai, 1994; Krajíček et al., 1995; Pitassi et al., 1993), such a separation by formulas of depth independent of $d$ is a major open problem.

1.2 **Relations to previous work**

In addition to the developments in propositional and QBF proof complexity sketched in the beginning, the main precursor of our work is the paper (Beyersdorff, Chew, and Janota, 2015a). Strategy extraction for $\text{Q-Res}$ and $\text{QU-Res}$ was shown by Balabanov and Jiang (2012), but the idea to turn this into a lower bound argument for the proof size originates from (Beyersdorff et al., 2015a), where the $\text{AC}^0$ lower bound for \textsc{Parity} is used to obtain exponential lower bounds for $\text{Q-Res}$ and $\text{QU-Res}$. However, the treatment in (Beyersdorff et al., 2015a) is solely confined to the resolution case. Here we widely generalise these concepts and uncover the full potential of that approach. In fact, quite weak circuit lower bounds would suffice for the proof-size lower bounds of (Beyersdorff et al., 2015a), cf. Corollary 5.11 in the present paper; and from (Beyersdorff et al., 2015a) it is not clear how the full spectrum of the state-of-the-art circuit lower bounds could be used to get proof size lower bounds.

Feasible interpolation is another technique relating circuit lower bounds to proof size bounds. Feasible interpolation has been successfully applied to show lower bounds for a number of propositional proof systems, including resolution (Krajíček, 1997) and cutting planes (Pudlák, 1997). Indeed, Beyersdorff, Chew, Mahajan, and Shukla (2015b) have recently shown that feasible interpolation is also effective for QBF resolution calculi. Interpolation transfers monotone circuit lower bounds to proof size lower bounds. Hence, different from strategy extraction, there is no connection between the circuit model and the lines in the proof system. Also, by results of (Bonet et al., 2000a, 2004; Krajíček and Pudlák, 1998) feasible interpolation is not applicable to strong systems such as $\text{AC}^0$-$\text{Frege}$ and beyond. Another restriction of interpolation is that it only applies to special formulas, and for these — at least in the case of QBF resolution systems — it can be understood as a special case of strategy extraction (Beyersdorff et al., 2015b).

1.3 **Innovations**

Our work opens up two lines of research that we believe will have a great influence on QBF proof complexity and beyond.
A. Exploring new QBF proof systems. The first of these is the study of natural and powerful QBF proof systems that correspond to ideas developed in propositional proof complexity for many years. While we concentrate here on the hierarchy $C$-$\text{Frege} + \forall \text{red}$ of new QBF Frege systems, our definitions introduce meaningful versions of algebraic and geometric proof systems for QBF. These systems will be very interesting to study from a theoretical perspective and also might provide an important stimulus on QBF solving — analogous to the impact of integer linear programming and polynomial calculus on SAT solving.

More widely, in Section 6, we complement the reduction systems $P + \forall \text{red}$ by two further general methods to lift propositional systems to QBF systems. The first method uses the idea of expanding universal variables, thus generalising the resolution system for expansion-based solving of Janota and Marques-Silva (2015). Comparing the $P + \forall \text{red}$ systems with the expansion systems we prove that they are incomparable in strength (using the lower bounds from C. above). This motivates our last general approach via instantiations, which unifies both reduction and expansion systems in a natural way. These general instantiation systems are inspired by a QBF resolution calculus recently introduced by Beyersdorff, Chew, and Janota (2014). Again the theoretical study of these new expansion and instantiation systems might exert a fruitful influence on QBF solving as modern solvers utilise these approaches.

B. Understanding the transfer from circuit to proof complexity. As far as we know, for the first time in the literature, our lower bound technique via strategy extraction gives a formal and rigorous account on the relation between a circuit class $C$ and proof systems using lines from $C$. Building on the previous work (Beyersdorff et al., 2015a) we establish this relation for a full hierarchy of QBF systems. This yields very strong results in QBF proof complexity. In the recent survey of Buss (2012), the propositional versions of our results C.(a) and (c) in Section 1.1 are referenced as ‘the main open problems at the “frontier” of Cook’s program’.

We believe that this transfer has the potential to generate lots of further research, both in QBF and indeed for further logics, possibly even including the most important classical propositional case. As for QBFs, the hard formulas $Q-f$ that we generate from a Boolean function $f$ have a special syntactic form, i.e. for all functions we use here they are prefixed by $\exists\forall\exists$. Can we also apply our technique to conceptually different types of QBFs? It is also possible that similar ideas are effective for further logics, possibly modal or intuitionistic logics as they share the same $\text{PSPACE}$ complexity, and strong lower bounds are known for Frege systems in these logics as well (Hrubeš, 2009; Jeřábek, 2009).

1.4 Organisation of the paper

Section 2 contains definitions and notations on $C$-$\text{Frege}$ systems and QBF. In Section 3 we define the QBF proof systems $C$-$\text{Frege} + \forall \text{red}$ (Definition 3.1) and prove their soundness and completeness (Theorem 3.2). Section 4 contains the proof of the Strategy Extraction Theorem (Theorem 4.3), which is our main technical tool to relate circuit complexity and proof size.

In Section 5 we prove our exponential lower bounds for $C$-$\text{Frege} + \forall \text{red}$ for several circuit classes $C$. All the results in this section ultimately rely on the Strategy Extraction Theorem from Section 4 and on a general way to encode a circuit $C$ in a (false) QBF $Q-C$ (Definition 5.1). The structure of Section 5 largely follows the order of the results already sketched in item C of Section 1.1.

Section 6 explains and compares the three general ways of extending propositional proof systems to QBF proof systems mentioned in Section 1.3 above. Section 7 concludes with some
2 Preliminaries

We assume familiarity with basic notions from computational complexity, cf. (Arora and Barak, 2009), as well as from logic, cf. (Krajíček, 1995), but define all specific concepts needed in this paper. For a formula $\varphi$ we denote by $\varphi[x_1/\theta_1, \ldots, x_k/\theta_k]$ the formula $\varphi$ where variables $x_i$ have been substituted by formulas $\theta_i$.

Circuit classes. We recall the definitions of standard circuit classes used in this paper. The class $\text{AC}^0$ contains all languages recognisable by polynomial-size circuits over the Boolean basis $\neg$, $\lor$, $\land$ with bounded depth and unbounded fan-in. When fixing the depth to a constant $d$, we denote the circuit class by $\text{AC}^0_d$. The class $\text{AC}^0[p]$ uses bounded-depth circuits with $\text{MOD}_p$ gates determining whether the sum of the inputs is 0 modulo $p$, and in $\text{TC}^0$ bounded-depth circuits with threshold gates are permitted. Stronger classes are obtained by using $\text{NC}^1$ circuits of polynomial size and logarithmic depth, and by $\text{P/poly}$ circuits of polynomial size. For further information we refer to the monograph (Vollmer, 1999).

Proof systems. According to Cook and Reckhow (1979) a proof system for a language $L$ is a polynomial-time onto function $P : \{0,1\}^* \to L$. Each string $\varphi \in L$ is a theorem and if $P(\pi) = \varphi$, $\pi$ is a proof of $\varphi$ in $P$. Given a polynomial-time function $P : \{0,1\}^* \to \{0,1\}^*$ the fact that $P(\{0,1\}^*) \subseteq L$ is the soundness property for $L$ and the fact that $P(\{0,1\}^*) \supseteq L$ is the completeness property for $L$.

Proof systems for the language TAUT of propositional tautologies are called propositional proof systems and proof systems for the language TQBF of true QBF formulas are called QBF proof systems. Equivalently, propositional proof systems and QBF proof systems can be defined respectively for the languages UNSAT of unsatisfiable propositional formulas and FQBF of false QBF formulas, in this second case we call them refutational.

Given two proof systems $P$ and $Q$ for the same language $L$, $P$ p-simulates $Q$ (denoted $Q \leq_p P$) if there exists a polynomial-time function $t$ such that for each $\pi \in \{0,1\}^*$, $P(t(\pi)) = Q(\pi)$. Two systems are called p-equivalent if they p-simulate each other.

A proof system $P$ for $L$ is called polynomially bounded if there exists a polynomial $p$ such that every $x \in L$ has a $P$-proof of size $\leq p(|x|)$.

Frege systems. Frege proof systems are the common ‘textbook’ proof systems for propositional logic based on axioms and rules (Cook and Reckhow, 1979). The lines in a Frege proof are propositional formulas built from propositional variables $x_i$ and Boolean connectives $\neg$, $\land$, and $\lor$. A Frege system comprises a finite set of axiom schemes and rules, e.g., $\varphi \lor \neg \varphi$ is a possible axiom scheme. A Frege proof is a sequence of formulas where each formula is either a substitution instance of an axiom, or can be inferred from previous formulas by a valid inference rule. Frege systems are required to be sound and implicationally complete. The exact choice of the axiom schemes and rules does not matter as any two Frege systems are p-equivalent, even when changing the basis of Boolean connectives (Cook and Reckhow, 1979) and (Krajíček, 1995, Theorem 4.4.13). Therefore we can assume w.l.o.g. that modus ponens is the only rule of inference.

Usually Frege systems are defined as proof systems where the last formula is the proven formula. To include also weak systems as resolution in this picture we use here the equivalent open problems.
setting of refutation \textit{Frege} systems where we start with the negation of the formula that we want to prove and derive the contradiction \(\bot\).

Given a circuit class \(C\), a general definition of \(C\)-\textit{Frege} is contained in (Jeřábek, 2005). Below we explicitly present the definitions of \(C\)-\textit{Frege} for the circuit classes we will need later.

There are several common restrictions that can be imposed on \textit{Frege}; for example \textit{bounded-depth Frege} systems (or \(AC^0\)-\textit{Frege}) are \textit{Frege} systems where lines are formulas with negations only on variables and with a bounded number of alternations between \&‘s and \lor’s. If the number of alternations is at most \(d\), then the proof system is called \(AC^d\)-\textit{Frege}. Bounded-depth \textit{Frege} is called \(AC^0\)-\textit{Frege} since lines in an \(AC^0\)-\textit{Frege} proof are representable as \(AC^0\)-circuits.

\textit{Resolution} (\textit{Res}) is a particular kind of \(AC^0\)-\textit{Frege} system\footnote{We will consistently treat \(C\)-\textit{Frege} systems as operating with lines from \(C\). As \textit{Res} operates with clauses we will call it a \(AC^1\)-\textit{Frege} system even though it refutes CNFs, which are depth 2.} introduced by Blake (1937) and Robinson (1965). It is a refutational proof system manipulating unsatisfiable CNFs as sets of clauses. The only inference rule is

\[
\frac{C \lor x}{C \lor \neg x} \quad \text{(Res rule)}
\]

where \(C, D\) denote clauses and \(x\) is a variable. A \textit{Res} refutation derives the empty clause \(\bot\).

Given a prime \(p\), the \(AC^0[p]\)-\textit{Frege} systems are defined to be bounded-depth \textit{Frege} systems in the language with Boolean connectives \(\neg, \lor, \land\) and modular gates \(MOD_p(x_1, \ldots, x_n)\). The \(MOD_p\) predicate is true when \(\sum_i x_i \equiv 0 \mod p\).

The \(TC^0\)-\textit{Frege} systems are defined to be bounded-depth \textit{Frege} systems in the language with Boolean connectives \(\neg, \lor, \land\) and threshold gates \(T_k(x_1, \ldots, x_n)\). The \(T_k\) predicate is true when at least \(k\) of its inputs are true. Two different, but equivalent, formalizations of \(TC^0\)-\textit{Frege} proof systems are given by Buss and Clote (1996) and Bonet et al. (2000b).

(Unrestricted) \textit{Frege} systems correspond to the complexity class \(NC^1\) in the same sense as bounded-depth \textit{Frege} corresponds to the class \(AC^0\). We will refer sometimes to \textit{Frege} as \(NC^1\)-\textit{Frege}.

\textit{Extended Frege} systems \(\textit{EF}\) allow the introduction of new extension variables that abbreviate formulas. \(\textit{EF}\) can be understood as a \textit{Frege} system that directly operates with Boolean circuits rather than formulas, where extension variables can be used to define the circuit gates (see (Jeřábek, 2005) for the precise formulation). Therefore we will refer to \(\textit{EF}\) also as \(P/poly\)-\textit{Frege}.

An alternative characterisation of \(\textit{EF}\) is through substitution \textit{Frege} systems \(\textit{SF}\) that allow arbitrary substitution instances of derived formulas (Cook and Reckhow, 1979; Krajíček and Pudlák, 1989).

The \textit{Frege} systems defined above form a hierarchy of proof systems

\[
\text{Res} \leq_p \text{AC}^0\text{-Frege} \leq_p \text{AC}^0[p]\text{-Frege} \leq_p \text{TC}^0\text{-Frege} \leq_p \text{Frege} \leq_p \text{EF}.
\]

Currently lower bounds are only known for \textit{Res} (Haken, 1985) and \(AC^0\)-\textit{Frege} (Ajtai, 1994; Krajíček et al., 1995; Pitassi et al., 1993), whereas super-polynomial lower bounds for any of the stronger systems constitute major problems in proof complexity.

\textbf{Quantified Boolean Formulas.} A (closed prenex) \textit{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 \(Q \varphi\), where \(\varphi\) is a propositional Boolean formula in Conjunctive Normal Form (CNF), called \textit{matrix}, and \(Q\) is its \textit{quantifier prefix}. We typically use \(x_i\) for existentially quantified variables and \(u_i\) for universally quantified variables.
Given a variable \( y \), either existentially quantified or universally quantified in \( Q \cdot \varphi \), the quantification level of \( y \) in \( Q \cdot \varphi \), \( \text{qlv}(y) \), is the number of alternations of quantifiers \( y \) has on its left in the quantifier prefix of \( Q \cdot \varphi \). Given a variable \( y \), we will sometimes refer to the variables with quantification level lower than \( \text{qlv}(y) \) as variables left of \( y \); analogously the variables with quantification lever higher than \( \text{qlv}(y) \) will be right of \( y \).

A QBF \( Q_1x_1 \cdots Q_kx_k \cdot \varphi \) can be seen as a game between two players: universal (\( \forall \)) and existential (\( \exists \)). In the \( i \)-th step of the game, the player \( Q_i \) assigns a value to the variable \( x_i \). The existential player wins if \( \varphi \) evaluates to 1 under the assignment constructed in the game. The universal player wins if \( \varphi \) 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 if and only if there exists a winning strategy for the universal player, that is if the universal player has a strategy for all universal variables that wins any possible game (Arora and Barak, 2009; Goultiaeva et al., 2011).

### QBF resolution calculi

**Q-resolution** (Q-Res) by Kleine Buening et al. (1995) is a resolution-like calculus that operates on QBFs in prenex form where the matrix is a CNF. It uses the propositional resolution rule

\[
\frac{C \lor x \quad D \lor \neg x}{C \lor D}
\]

with the side conditions that variable \( x \) is existential and if \( z \in C \), then \( \neg z \notin D \). In addition Q-Res has a universal reduction rule

\[
\frac{C \lor u}{C}
\]

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

**Universal resolution**, QU-Res introduced by Van Gelder (2012), additionally allows to resolve on universal variables, under the same side condition as in Q-Res not to derive tautologous clauses.

For definitions of further resolution-based QBF proof system and their complexity we refer to (Beyersdorff et al., 2015a).

### 3 Defining QBF Frege systems

In this section we provide a general method of transforming a propositional proof system into a QBF proof system. While this method works for a wide range of proof systems operating with lines and rules, we will concentrate here on the hierarchy of C-Frege systems introduced in the previous section. However, our method also works for further propositional proof systems such as polynomial calculus (Clegg et al., 1996) or cutting planes (Cook et al., 1987).

For the following we fix a circuit class \( C \) with some natural properties, e.g., closure under restrictions. In particular, \( C \) can be any of the circuit classes mentioned in Section 2.

**Definition 3.1** (C-Frege + \( \forall \text{red} \)). A refutation of a false QBF \( Q \cdot \varphi \) in the system C-Frege + \( \forall \text{red} \) is sequence of lines \( L_1, \ldots, L_\ell \) where each line is a circuit from the class \( C \), \( L_1 = \varphi \),\(^2\) \( L_\ell = \bot \) and each \( L_i \) is inferred from previous lines \( L_j \) using the inference rules of C-Frege or using the following rule

\[
\frac{L_j}{L_j[u/B]} \quad (\forall \text{red}),
\]

\(^2\)In the case where \( C \) is \( \text{AC}^0 \) we require that \( \varphi = L_1 \land \cdots \land L_m \) where \( L_j \) are lines in \( \text{AC}^0 \)-Frege.
where \( L_j[u/B] \) belongs to the class \( C \), \( u \) is the innermost variable among the variables of \( L_j \) and \( B \) is a circuit from the class \( C \) containing only variables left of \( u \).

The formal justification why \( C\text{-Frege} + \forall \text{red} \) is a sound and complete QBF proof system is given in Theorem 3.2 below. However, let us pause a moment to see why adding the \( \forall \text{red} \) rule results in a natural proof system \( C\text{-Frege} + \forall \text{red} \). Recall that we consider \( C\text{-Frege} + \forall \text{red} \) as a refutation system; hence we aim to refute false quantified \( C \) formulas. A standard approach to witness the falsity of quantified formulas is through Herbrand functions, which replace a universal variable \( u \) by a function in the existential variables left of \( u \). These functions can be viewed as ‘counterexample functions’. In Definition 3.1, \( B \) plays the role of the Herbrand function. Clearly, when restricting formulas to a class \( C \) we should also restrict \( B \) to that class, and substituting the Herbrand function into the formula should again preserve \( C \).

Note that we are even allowed to choose different Herbrand functions \( B \) for the same variable \( u \) in different parts of the proof. In general, this will be unsound (unless variables right of \( u \) are renamed, cf. Section 6.3 for a stronger proof system implementing this). However, it is safe to do if the line \( L_j \) does not contain any variables right of \( u \).

It is illustrative to see how our construction compares to previously studied QBF resolution systems. Choosing \( \text{Res} \) as our propositional proof system, which is an \( \text{AC}^0 \text{-Frege} \) system, we obtain \( \text{Res} + \forall \text{red} \). In \( \text{Res} + \forall \text{red} \) the \( \forall \text{red} \) rule can substitute a universal \( u \) by either another variable or by a constant 0/1. In the former case, we simply obtain a weakening step. In the latter case, if \( u \) appears positively in the clause then substituting \( u \) by 0 precisely corresponds to an application of the \( \forall \text{red} \) rule in Q-Res, whereas substituting \( u \) by 1 results in the useless tautology \( \top \).\(^3\) As \( \text{Res} + \forall \text{red} \) can resolve on existential and universal variables, our system \( \text{Res} + \forall \text{red} \) is exactly the well-known QU-Res (with weakening).

We now proceed to show soundness and completeness of the new QBF systems.

**Theorem 3.2.** For every circuit complexity class \( C \), \( C\text{-Frege} + \forall \text{red} \) is a refutational QBF proof system.

**Proof.** \( \text{Res} + \forall \text{red} \) is complete as it \( p \)-simulates Q-Res, which is complete for QBF (Kleine Büning et al., 1995). To obtain the completeness for \( C\text{-Frege} + \forall \text{red} \) we first use de Morgan’s rules to expand the formula into a CNF. This is possible as, by definition, \( C\text{-Frege} \) is implicationally complete. Now we can refute the CNF by \( \text{Res} + \forall \text{red} \). \( C\text{-Frege} + \forall \text{red} \) p-simulates \( \text{Res} + \forall \text{red} \) and hence \( C\text{-Frege} + \forall \text{red} \) is complete.

Regarding the soundness of \( C\text{-Frege} + \forall \text{red} \), let \( (L_1, \ldots, L_\ell) \) be a refutation of \( Q \cdot \varphi \) in the system \( C\text{-Frege} + \forall \text{red} \) and let

\[
\varphi_i = \begin{cases} 
\varphi & \text{if } i = 0, \\
\varphi \land L_1 \land \cdots \land L_i & \text{otherwise.}
\end{cases}
\]

By induction on \( i \) we prove that \( Q \cdot \varphi \) semantically entails \( Q \cdot \varphi_i \), i.e. \( Q \cdot \varphi \models Q \cdot \varphi_i \). Hence, at step \( i = \ell \) we will immediately obtain that \( Q \cdot \varphi \) is false, since \( L_\ell = \{ \bot \} \) and \( Q \cdot \varphi_\ell \equiv \bot \).

Since \( Q \cdot \varphi = Q \cdot \varphi_0 \) the base case of the induction holds.

We show now that \( Q \cdot \varphi \models Q \cdot \varphi_i \) implies \( Q \cdot \varphi \models Q \cdot \varphi_{i+1} \). By definition, \( \varphi_{i+1} = (\varphi_i \land L_{i+1}) \) and \( L_{i+1} \) was either introduced by a \( C\text{-Frege} \) rule or by the \( \forall \text{red} \) rule. If \( L_{i+1} \) was introduced by a \( C\text{-Frege} \) rule then \( \varphi_i \models L_{i+1} \), so \( \varphi_i \models \varphi_{i+1} \) and clearly \( Q \cdot \varphi \models Q \cdot \varphi_i \models Q \cdot \varphi_{i+1} \).

\(^3\)Note that, contrasting the usual setting of Q-Res (Kleine Büning et al., 1995), our definition of \( \text{Res} + \forall \text{red} \) does not need to disallow tautologous resolvents as these will always be reduced to \( \top \).
Suppose now that \( L_{i+1} \) was introduced by the \( \forall \text{red} \) rule, say \( L_{i+1} = L_j[u/B] \) with \( j \leq i \), \( u \) the innermost variable among the ones in \( L_j \) and \( B \) relying only on the variables left of \( u \). Moreover suppose that \( Q \cdot \varphi_i = Q_1 \bar{x} \forall u Q_2 \bar{y} \cdot \varphi_i \), then we have the following chain of equivalences

\[
Q \cdot \varphi_i = Q_1 \bar{x} \forall u Q_2 \bar{y} \cdot \varphi_i = Q_1 \bar{x} \forall u Q_2 \bar{y} \cdot \varphi_i \land L_j
\]

(1)

\[
\equiv Q_1 \bar{x} (Q_2 \bar{y} \cdot \varphi_i[u/0] \land L_j[u/0]) \land (Q_2 \bar{y} \cdot \varphi_i[u/1] \land L_j[u/1])
\]

(2)

\[
\equiv Q_1 \bar{x} (L_j[u/0] \land L_j[u/1] \land (Q_2 \bar{y} \cdot \varphi_i[u/0]) \land (Q_2 \bar{y} \cdot \varphi_i[u/1]))
\]

(3)

\[
\equiv Q_1 \bar{x} (L_j[u/0] \land L_j[u/1] \land \forall u Q_2 \bar{y} \cdot \varphi_i)
\]

(4)

\[
\equiv Q_1 \bar{x} (L_j[u/0] \land L_j[u/1] \land \forall u Q_2 \bar{y} \cdot \varphi_i)
\]

(5)

\[
\equiv Q_1 \bar{x} (L_j[u/0] \land L_j[u/1] \land L_j[u/B] \land \forall u Q_2 \bar{y} \cdot \varphi_i)
\]

(6)

\[
\equiv Q_1 \bar{x} \forall u Q_2 \bar{y} \cdot \varphi_i \land L_j[u/0] \land L_j[u/1] \land L_j[u/B].
\]

(7)

In (3) and (5) we used the definition of semantic expansion of a universal variable in a QBF; in (4), (6) and (7) we used the fact that \( L_j[u/0] \), \( L_j[u/1] \) and \( L_j[u/B] \) do not contain \( \bar{y} \) variables. From (7) follows, by weakening, that

\[
Q \cdot \varphi_i \models Q_1 \bar{x} \forall u Q_2 \bar{y} \cdot \varphi_i \land L_j[u/B],
\]

hence \( Q \cdot \varphi \models Q \cdot \varphi_{i+1}. \)

Clearly lower bounds on the complexity of \( C \text{-Frege} + \forall \text{red} \) follow from lower bounds on \( C \text{-Frege} \). The lower bounds we show later will be of a different kind as they will be ‘purely for QBF proof systems’ in the sense that they will lower bound the number of occurrences of the \( \forall \text{red} \) rule in refutations.

### 4 Strategy extraction for QBF Frege systems

We introduce now the simple computational model of \( C \)-decision lists.

**Definition 4.1 (C-decision list).** A \( C \)-decision list is a programme of the following form

if \( C_1(\bar{x}) \) then \( u \leftarrow B_1(\bar{x}) \);

else if \( C_2(\bar{x}) \) then \( u \leftarrow B_2(\bar{x}) \);

\[ \vdots \]

else if \( C_{\ell-1}(\bar{x}) \) then \( u \leftarrow B_{\ell-1}(\bar{x}) \);

else \( u \leftarrow B_{\ell}(\bar{x}) \),

where \( C_1, \ldots, C_{\ell-1} \) and \( B_1, \ldots, B_{\ell} \) are circuits in the class \( C \). Hence a decision list as above computes a Boolean function \( u = g(\bar{x}) \).

This definition generalises decision lists from (Rivest, 1987), where the conditions \( C_i(\bar{x}) \) are expressible as terms. We note that for many cases \( C \)-decision lists can be easily transformed into \( C \)-circuits.
**Proposition 4.2.** Let $D$ be a $C$-decision list using circuits $C_1, \ldots, C_{\ell-1}$ and $B_1, \ldots, B_{\ell}$, such that $D$ computes the Boolean function $g$. Then there exists a circuit $D' \in C$ computing the same function $g$, such that the size of $D'$ is linear in the size of $D$ and

$$\text{depth}(D') \leq \max \left\{ \max_{1 \leq i < \ell-1} \{ \text{depth}(C_i) \}, \max_{1 \leq i \leq \ell} \{ \text{depth}(B_i) \} \right\} + 2.$$  

**Proof.** We have that

$$u \equiv \bigvee_{j=1}^{\ell} \left( C_j(\vec{x}) \land B_j(\vec{x}) \land \bigwedge_{k < j} \neg C_k(\vec{x}) \right),$$

where $C_\ell$ is a circuit computing the constant 1.

---

Balabanov and Jiang (2012) proved a strategy extraction result for QU-Res. Here we generalise that result to the full hierarchy of $C$-Frege + $\forall$Red QBF proof systems. This result is the main tool we use to prove size lower bounds in such systems.

**Theorem 4.3** (Strategy Extraction Theorem). Given a false QBF $Q \cdot \varphi$ and a refutation $\pi$ of $Q \cdot \varphi$ in $C$-Frege + $\forall$Red, it is possible to extract in linear time (w.r.t. $|\pi|$) a collection of $C$-decision lists $D$ computing a winning strategy on the universal variables of $\varphi$.

**Proof.** Let $\pi = (L_1, \ldots, L_\ell)$ be a refutation of the false QBF $Q \cdot \varphi$ and let

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

We show, by downward induction on $i$, that from $\pi_i$ it is possible to construct in linear time (w.r.t. $|\pi_i|$) a winning strategy $\sigma^i$ for the universal player for the QBF formula $Q \cdot \varphi_i$, where

$$\varphi_i = \begin{cases} \varphi & \text{if } i = 0, \\ \varphi \land L_1 \land \cdots \land L_i & \text{otherwise}, \end{cases}$$

such that for each universal variable $u$ in $Q \cdot \varphi$, there exists a $C$-decision list $D_u^i$ computing $\sigma^i_u$ as a function of the variables in $Q$ left of $u$, having size $O(|\pi_i|)$.

The statement of the Strategy Extraction Theorem correspond to the case when $i = 0$. The base case of the induction is for $i = \ell$. In this case $\sigma^\ell$ is trivial since $\varphi_\ell$ contains the line $L_\ell = \bot$, and we can define all the $D_u^i$ as $u \leftarrow 0$.

We show now how to construct $\sigma^{i-1}_u$ and $D^{i-1}_u$ from $\sigma^i_u$ and $D^i_u$:

- If $L_i$ is derived by some Frege rule, then for each universal variable $u$ we set $\sigma^{i-1}_u = \sigma^i_u$ and $D^{i-1}_u = D^i_u$.

- If $L_i$ is the result of an application of a $\forall$Red rule, that is $L_i = \frac{L_j}{L_j[u/B]}$, where $u$ is the rightmost variable in $L_j$, $L_j[u/B]$ is a circuit in $C$ using only variables on the left of $u$, and $L_j(u/B) = L_i$. Let $\vec{x}_{u'}$ denote the variables on the left of $u'$ in the quantifier prefix of $Q \cdot \varphi$. Then we define

$$\sigma^{i-1}_{u'}(\vec{x}_{u'}) = \begin{cases} \sigma^i_{u'}(\vec{x}_{u'}) & \text{if } u' \neq u, \\ B(\vec{x}_{u}) & \text{if } u' = u \text{ and } L_j[u/B](\vec{x}_{u}) = 0, \\ \sigma^i_{u}(\vec{x}_{u}) & \text{if } u' = u \text{ and } L_j[u/B](\vec{x}_{u}) = 1. \end{cases}$$

Moreover for each $u' \neq u$ we set $D^{i-1}_{u'} = D^i_{u'}$, and we set $D^{i-1}_u$ as follows:
We now check that for each \( u' \), \( \sigma^{i-1}_{u'} \) respects all the properties of the inductive claim.

\( \sigma^{i-1}_{u'} \) and \( D^{i-1}_{u'} \) are well defined. By construction \( L_j[u/B] \) is a formula in the variables \( \vec{x} \) left of \( u \). This immediately implies that, for each universal variable \( u' \), the strategy \( \sigma^{i-1}_{u'} \) is well defined and \( D^{i-1}_{u} \) is also well defined. By induction hypothesis \( D^{i}_{u} \) is a \( \mathcal{C} \)-decision list, so \( D^{i-1}_{u} \) is also a \( \mathcal{C} \)-decision list.

\( \sigma^{i-1} \) and \( D^{i-1}_{u} \) are constructed in linear time \( \text{w.r.t.} |\pi_{i-1}| \). This holds by inductive hypothesis and the fact that computing \( -L_j(u/B) \) is linear in \( |\pi_{i-1}| \).

\( D^{i-1}_{u} \) computes \( \sigma^{i-1}_{u} \). For \( u' \neq u \), by induction hypothesis, \( D^{i-1}_{u'} \) computes \( \sigma^{i}_{u'} \). The same happens, by construction, for \( u' = u \).

\( \sigma^{i-1} \) is a winning strategy for \( \mathcal{Q} \cdot \varphi_{i-1} \). Fix an assignment \( \rho \) to the existential variables of \( \varphi \). Let \( \tau_i \) be the complete assignment to existential and universal variables, constructed in response to \( \rho \) under the strategy \( \sigma^i \). By induction hypothesis \( \tau_i \) falsifies \( \varphi_i \). We need to show that \( \tau_{i-1} \) falsifies \( \varphi_{i-1} \). To show this we distinguish again two cases.

If \( L_i \) is derived by some Frege rule, then \( \sigma^{i-1} = \sigma^i \) and \( \tau_{i-1} = \tau_i \). Hence by induction hypothesis, \( \tau_i \) falsifies a conjunct from \( \varphi_i \). To argue that \( \tau_{i-1} \) also falsifies a conjunct from \( \varphi_{i-1} \) we only need to look at the case when the falsified conjunct is \( L_i \). As \( L_i \) is false under \( \tau_i \) and \( L_i \) is derived by a sound Frege rule, one of the parent formulas of \( L_i \) in the application of the Frege rule must be falsified as well. Hence \( \tau_{i-1} \) falsifies \( \varphi_{i-1} \).

Let now \( L_i = L_j[u/B] \) for some \( j < i \). In this case, our strategy \( \sigma^{i-1} \) changes the assignment \( \tau_i \) only when \( \tau_i \) made the universal player win by falsifying \( L_i \). As we set \( u \) to \( B(\tau_i(\vec{x})) \), the modified assignment \( \tau_{i-1} \) falsifies \( L_j \). Otherwise, if \( \tau_i \) does not falsify \( L_i \) we keep \( \tau_{i-1} = \tau_i \) and hence falsify one of the conjuncts of \( \varphi_{i-1} \) by induction hypothesis.

From the proof of the Strategy Extraction Theorem it is clear that the size of the \( \mathcal{C} \)-decision list computing the winning strategy extracted from the refutation \( \pi \) has size that is actually linear in the number of applications of the \texttt{\forall \exists \text{red}} rule in \( \pi \). More precisely, the size of the \( \mathcal{C} \)-decision list computing the winning strategy for variable \( u \) corresponds exactly to the number of \texttt{\forall \exists \text{red}} rules on \( u \) in \( \pi \).

## 5 Separations and lower bounds via circuit complexity

We now introduce a class of QBFs defined from some circuits \( C_n \) computing a function \( f \). Choosing different functions \( f \), these formulas will form the basis of our lower bounds.

**Definition 5.1** (\( \mathcal{Q} \cdot \mathcal{C}_n \)). Let \( n \) be an integer and \( C_n \) be a circuit with inputs \( x_1, \ldots, x_n \). Let \( t_1, \ldots, t_{m-1} \) be a topological ordering of the internal gates of \( C_n \), and let the output gate of \( C_n \) be \( t_m \). We define

\[
\mathcal{Q} \cdot \mathcal{C}_n = \exists x_1 \cdots \exists x_n \forall u \exists t_1 \cdots \exists t_m \cdot (u \leftrightarrow -t_m) \land \bigwedge_{i=1}^{m} G_i,
\]

where \( u \leftrightarrow -t_m \equiv (u \lor t_m) \land (-u \lor -t_m) \) and \( G_i \) expresses as a CNF the function computed in the circuit \( C_n \) at gate \( i \), e.g. if node \( t_i \) computes the \( \land \) of \( t_j \) and \( t_k \) then

\[
G_i = t_i \leftrightarrow (t_j \land t_k) \equiv (-t_i \lor t_j) \land (-t_i \lor t_k) \land (t_i \lor -t_j \lor -t_k),
\]
similarly if gate $i$ computes $\neg, \lor, \oplus, \text{MOD}_p, T_k$ or some other Boolean function.

Informally, the QBF $Q\cdot C_n$ expresses that there exists an input $\vec{x}$ such that $C_n(\vec{x})$ evaluates to both 0 and 1, an obvious contradiction. Using these formulas together with the Strategy Extraction Theorem, we now establish a deep connection between the circuit class $C$ and $\mathcal{C}$-Frege + $\forall\text{red}$.

**Theorem 5.2.** Let $C$ be one of the circuit classes $\text{AC}^0$, $\text{AC}^0[p]$, $\text{TC}^0$, $\text{NC}^1$, $\text{P/poly}$ and let $(C_n)_{n \in \mathbb{N}}$ be a non-uniform family of circuits where $C_n$ is a circuit with $n$ inputs. Then the following implications hold:

(i) if the QBFs $Q\cdot C_n$ have $\mathcal{C}$-Frege + $\forall\text{red}$ refutations of size bounded by a function $q(n)$, then for each $n$, $C_n$ is equivalent to a circuit $C'_n$ where $C'_n$ is of size $O(q(n))$ and uses the gates and depth allowed in $C$;

(ii) if $(C_n)_{n \in \mathbb{N}}$ is a polynomial-size circuit family from $C$ then the QBFs $Q\cdot C_n$ have polynomial-size refutations in $\mathcal{C}$-Frege + $\forall\text{red}$.

**Proof.** Regarding (i), by the Strategy Extraction Theorem and Proposition 4.2, if the QBF $Q\cdot C_n$ has a refutation in $\mathcal{C}$-Frege + $\forall\text{red}$ of size $S$ then a winning strategy for the universal player can be computed by a circuit $C'_n \in C$ of size $O(S)$. We have that in $Q\cdot C_n$ the quantifier prefix looks like $\exists x_1 \cdots \exists x_n \forall u \exists \vec{t}$. Now, by construction, $u \not\equiv C_n(x_1, \ldots, x_n)$, hence a winning strategy for the universal player must consist of playing $u = C_n(x_1, \ldots, x_n)$. This means that the circuit $C'_n$ computing the winning strategy for the universal player is equivalent to the circuit $C_n$ and the size bound follows.

Regarding (ii), let $Q\cdot C_n = \exists x_1 \cdots \exists x_n \forall u \exists \vec{t}_1 \cdots \exists \vec{t}_m \cdot (u \leftrightarrow \neg \vec{t}_m) \land \varphi_n$, where $\varphi_n$ is a formula depending on the circuit $C_n$. By definition, the $t_i$ are indexed w.r.t. a topological ordering of the nodes of $C_n$.

We prove, by induction on $i$, that there exists a circuit $D_i \in C$ such that $t_i \leftrightarrow D_i$ is derivable in $\mathcal{C}$-Frege with size polynomial in $|D_i|$. Suppose that $t_i$ corresponds to a gate $\odot(t_{j_1}, \ldots, t_{j_k})$ with fan-in $\ell$, where $\odot$ could be an $\land, \lor, \neg, \oplus, \text{MOD}_p, T_k, \ldots$ from the gates allowed in the class $C$. By the inductive property we know that $t_{j_k} \leftrightarrow D_{j_k}$ is provable in $\mathcal{C}$-Frege with proofs of size polynomial in $|D_{j_k}|$. Moreover, $\mathcal{C}$-Frege is able to prove

$$t_{j_1} \leftrightarrow D_{j_1} \quad \cdots \quad t_{j_k} \leftrightarrow D_{j_k} \quad t_i \leftrightarrow \odot(t_{j_1}, \ldots, t_{j_k})$$

Let then $D_i = \odot(D_{j_1}, \ldots, D_{j_k})$. At the $m$-th step $\mathcal{C}$-Frege proves that $t_m \leftrightarrow D_m$, from which follows that

$$t_m \leftrightarrow D_m \quad u \leftrightarrow \neg t_m \quad u \equiv D_m$$

Since now $u$ is universal and the innermost variable of $u \leftrightarrow \neg D_m$, we can apply the $\forall\text{red}$ rule and get

$$0 \leftrightarrow \neg D_m, \quad 1 \leftrightarrow \neg D_m,$$

which leads to an immediate contradiction in $\mathcal{C}$-Frege + $\forall\text{red}$. \qed

In particular, a Boolean function $f$ is computable by polynomial-size $C$ circuits if and only if $Q\cdot C_n$ have polynomial-size $\mathcal{C}$-Frege refutations for each choice of Boolean circuits $(C_n)_{n \in \mathbb{N}}$ computing $f$. Note that the circuits $C_n$ are not necessarily circuits from the class $C$.

In the remainder of this section we apply Theorem 5.2 to a number of circuit classes and transfer circuit lower bounds to proof size lower bounds.
5.1 Lower bounds for bounded-depth Frege systems

PARITY is one of the best-studied functions in terms of its circuit complexity. With Theorem 5.2 we can immediately transfer circuit lower bounds for PARITY to $AC^0[p]$-Frege + $\forall$red, regardless of the encoding for PARITY.

Corollary 5.3 (lower bounds for Q-PARITY). Let $C_n$ be a family of polynomial-size circuits computing $\text{PARITY}(x_1, \ldots, x_n)$. For each odd prime $p$ the QBFs $Q-C_n$ require proofs of exponential size in $AC^0[p]$-Frege + $\forall$red.

Proof. The exponential lower bound for the proof size in $AC^0[p]$-Frege + $\forall$red follows from Theorem 5.2 and the fact that for each odd prime $p$ any family of bounded-depth circuits with $\text{MOD}_p$ gates computing PARITY must be of exponential size (Razborov, 1987; Smolensky, 1987).

We highlight that non-trivial lower bounds for $AC^0[p]$-Frege are one of the major open problems in propositional proof complexity. We complement the lower bound in Corollary 5.3 with an upper bound for arbitrary $\text{NC}^1$ encodings of PARITY in Frege + $\forall$red.

Corollary 5.4 (upper bounds for Q-PARITY). Let $C_n$ be a family of $\text{NC}^1$ circuits computing $\text{PARITY}(x_1, \ldots, x_n)$. Then the QBFs $Q-C_n$ have polynomial-size proofs in Frege + $\forall$red.

Proof. By a result of Muller and Preparata (1975), PARITY can be computed by circuits in $\text{NC}^1$. Hence if we consider a family $C_n$ of $\text{NC}^1$ circuits computing PARITY then the polynomial upper bound in Frege + $\forall$red follows immediately from Theorem 5.2.

In fact, this upper bound can be improved to $AC^0[2]$-Frege + $\forall$red, albeit not for arbitrary $\text{NC}^1$-encodings of PARITY, as it is not clear how these could be handled in bounded depth. For this purpose, we consider explicit QBFs for PARITY, which can be built from its inductive definition $\text{PARITY}(x_1, \ldots, x_n) = \text{PARITY}(x_1, \ldots, x_{n-1}) \oplus x_n$. This leads to the QBFs

$$\Phi_n = \exists x_1 \cdots \exists x_n \forall u \exists t_2 \cdots \exists t_n \cdot (t_2 \leftrightarrow (x_1 \oplus x_2)) \land \bigwedge_{i=3}^{n} (t_i \leftrightarrow (t_{i-1} \oplus x_i)) \land (u \leftrightarrow -t_n),$$

where $a \leftrightarrow (b \oplus c) \equiv (-a \lor -b \land -c) \land (a \lor b \lor -c) \land (a \lor b \lor c) \land (a \lor -b \lor c) \land (a \lor -b \lor -c)$. This formulation of Q-PARITY was considered by Beyersdorff et al. (2015a), where the formulas $\Phi_n$ are shown to be hard for $\text{Q-Res}$ and QU-Res. Here we obtain:

Corollary 5.5. The PARITY-formulas $\Phi_n$ require exponential-size $AC^0[2]$-Frege + $\forall$red for each odd prime $p$, but have polynomial-size $AC^0[2]$-Frege + $\forall$red refutations.

Proof. The lower bound follows as in Corollary 5.3. For the upper bound we cannot use Theorem 5.2, but need to give a more direct proof. Without loss of generality we can assume that our $AC^0[2]$-Frege + $\forall$red system uses the connectives $\{\land, \lor, \neg, \leftrightarrow, \oplus\}$.

Then it is easy to see, by induction on $i$, that Frege proves $t_i \leftrightarrow \oplus(x_1, x_2, \ldots, x_i)$ with a proof of size linear in $i$. Hence, similarly to what was done in Theorem 5.2, we get

$$u \leftrightarrow -\oplus(x_1, x_2, \ldots, x_n).$$

Then $u$ is the rightmost variable in (9); hence by the $\forall$red rule we have

$$1 \leftrightarrow -\oplus(x_1, x_2, \ldots, x_n) \text{ and } 0 \leftrightarrow -\oplus(x_1, x_2, \ldots, x_n),$$

which gives an immediate contradiction. 

\[\Box\]
In fact, we can further strengthen Corollary 5.5 and use Smolensky’s circuit lower bounds for an even more ambitious separation of all $\text{AC}^0[p]$-$\text{Frege} + \forall \text{red}$ systems. For this we consider the function

$$MOD_p(x_1, \ldots, x_n) = \begin{cases} 1 & \text{if } \sum_{i=1}^n x_i \equiv 0 \pmod{p} \\ 0 & \text{otherwise.} \end{cases}$$

For $r \leq p - 1$ let

$$MOD_{p,r}(x_1, \ldots, x_n) = \begin{cases} 1 & \text{if } \sum_{i=1}^n x_i \equiv r \pmod{p} \\ 0 & \text{otherwise.} \end{cases}$$

If we want to use $MOD_p$ for a separation of $\text{AC}^0[p]$-$\text{Frege} + \forall \text{red}$ and $\text{AC}^0[q]$-$\text{Frege} + \forall \text{red}$ for different primes $p$, $q$, then $MOD_p$ has to be encoded as a QBF in the language common to both proof systems, which means that we cannot use $MOD_p$ or $MOD_q$ gates. As for $\text{PARITY}$, an arbitrary $\text{NC}^1$ encoding as in Corollary 5.3 will also not work (this would just give upper bounds in $\text{Frege} + \forall \text{red}$), so we need to devise again explicit QBF encodings for $MOD_p$. Such QBFs can be built using the fact that $MOD_p$, that is $MOD_{p,0}$, can be defined for $r \neq 0$ by

$$MOD_{p,r}(x_1, \ldots, x_i) = (MOD_{p,r}(x_1, \ldots, x_{i-1}) \land \neg x_i) \lor (MOD_{p,r-1}(x_1, \ldots, x_{i-1}) \land x_i),$$

and for $r = 0$ by

$$MOD_{p,0}(x_1, \ldots, x_i) = (MOD_{p,0}(x_1, \ldots, x_{i-1}) \land \neg x_i) \lor (MOD_{p,0}(x_1, \ldots, x_{i-1}) \land x_i).$$

Using variables $s^r_i$ for $MOD_{p,r}(x_1, \ldots, x_i)$ this leads to the QBFs

$$\bigwedge_{0 < r \leq p-1} \bigwedge_{1 < i \leq n} \left( s^r_i \leftrightarrow (s^{r-1}_{i-1} \land \neg x_i) \lor (s^{r-1}_{i-1} \land x_i) \right) \land \bigwedge_{1 < i \leq n} \left( s^0_i \leftrightarrow (s^0_{i-1} \land \neg x_i) \lor (s^0_{i-1} \land x_i) \right).$$

**Corollary 5.6.** For each pair $p$, $q$ of distinct primes the $MOD_p$-formulas $\Theta^p_n$ require proofs of exponential size in $\text{AC}^0[q]$-$\text{Frege} + \forall \text{red}$, but have polynomial-size proofs in $\text{AC}^0[p]$-$\text{Frege} + \forall \text{red}.$

**Proof.** The exponential lower bound for $\text{AC}^0[q]$-$\text{Frege} + \forall \text{red}$ follows from Theorem 5.2 together with the result from (Razborov, 1987; Smolensky, 1987) that for distinct primes $p$, $q$ any family of bounded-depth circuits with $MOD_q$ gates computing $MOD_p$ must be of exponential size.

Regarding the upper bound, without loss of generality we can assume that our $\text{AC}^0[p]$-$\text{Frege}$ system uses the connectives $\{\land, \lor, \neg, \leftrightarrow, MOD_p\}$. Then it is easy to see, by induction on $i$, that $\text{AC}^0[p]$-$\text{Frege}$ proves

$$s^r_i \leftrightarrow MOD_p(x_1, \ldots, x_i, 1, 1, \ldots, 1),$$

with a proof of size linear in $i$. Hence, similarly to what was done in Theorem 5.2 and Corollary 5.5, we get

$$u \leftrightarrow \neg MOD_p(x_1, \ldots, x_n, 1, 1, \ldots, 1). \quad (9)$$

Then $u$ is the rightmost variable in (9); hence by the $\forall \text{red}$ rule we have

$$1 \leftrightarrow \neg MOD_p(x_1, \ldots, x_n, 1, 1, \ldots, 1) \quad \text{and} \quad 0 \leftrightarrow \neg MOD_p(x_1, \ldots, x_n, 1, 1, \ldots, 1),$$

which gives an immediate contradiction. \qed
Another notorious function in circuit complexity is \textsc{Majority}. Again we can transform circuit lower bounds to proof size lower bounds for arbitrary encodings of \textsc{Majority}.

\textbf{Corollary 5.7} (lower bounds for \textsc{Q-Majority}). Let $C_n$ be a family of polynomial-size circuits computing \textsc{Majority}($x_1, \ldots, x_n$). Then for every prime $p$, the QBFs $Q.C_n$ require proofs of exponential size in $\text{AC}^0[p]$.\textsc{-Frege} + $\forall$\textsc{red}.

\textit{Proof.} The lower bound follows again applying Theorem 5.2 and the fact that \textsc{Majority} requires exponential-size bounded-depth circuits with $\text{MOD}_p$ gates (Razborov, 1987; Smolensky, 1987).

For general encodings, we can again show $\text{Frege} + \forall$\textsc{red} upper bounds.

\textbf{Corollary 5.8} (upper bounds for \textsc{Q-Majority}). Let $C_n$ be a family of $\text{NC}^1$ circuits computing \textsc{Majority}($x_1, \ldots, x_n$). Then the QBFs $Q.C_n$ have polynomial-size proofs in $\text{Frege} + \forall$\textsc{red}.

\textit{Proof.} By a result of Muller and Preparata (1975), \textsc{Majority} is computable in $\text{NC}^1$ and hence $Q.C_n$ are well defined. The upper bound then follows from Theorem 5.2.

As for the $\text{MOD}_p$ functions, we can improve on this upper bound by considering explicit QBF encodings of \textsc{Majority}, thereby even obtaining a separation of $\text{AC}^0[p]$.\textsc{-Frege} + $\forall$\textsc{red} systems from $\text{TC}^0$.\textsc{-Frege} + $\forall$\textsc{red}.

\textbf{Corollary 5.9.} For each prime $p$ the Majority-formulas $\Psi_n$ require proofs of exponential-size in $\text{AC}^0[p]$.\textsc{-Frege} + $\forall$\textsc{red}, but have polynomial-size proofs in $\text{TC}^0$.\textsc{-Frege} + $\forall$\textsc{red}.

\textit{Proof.} The exponential lower bound on $\textsc{Parity}$ from (Razborov, 1987; Smolensky, 1987) will give us the exponential lower bound w.r.t. the size of $\Psi_n$ in $\text{AC}^0[p]$.\textsc{-Frege} + $\forall$\textsc{red}, since the size of $\Psi_n$ is $O(n^2)$.

Regarding the polynomial-size proof of $\Psi_n$ in $\text{TC}^0$.\textsc{-Frege} + $\forall$\textsc{red} we can proceed similarly as for \textsc{Parity} in $\text{Frege}$. The crucial feature here is that $T_k$ are, by definition of $\text{TC}^0$, in the language of $\text{TC}^0$.\textsc{-Frege}. Hence (10) can be used to prove $t_k^j \leftrightarrow T_k(x_1, \ldots, x_j)$ and we can easily refute $\Psi_n$ in $\text{TC}^0$.\textsc{-Frege} + $\forall$\textsc{red}.

We note that a separation of $\text{AC}^0[p]$.\textsc{-Frege}$ from $\text{TC}^0$.\textsc{-Frege}$ constitutes a major open problem in propositional proof complexity as we are currently lacking lower bounds for $\text{AC}^0[p]$.\textsc{-Frege}.

---

\textsuperscript{4}Clearly, such a separation already follows from Corollary 5.6 together with the simulation of $\text{AC}^0[p]$.\textsc{-Frege} + $\forall$\textsc{red}$ by $\text{TC}^0$.\textsc{-Frege} + $\forall$\textsc{red}$. Here we will prove the stronger result that all these systems are separated by one natural principle, namely $\textsc{Majority}$. 

17
5.2 Lower bounds for depth- \( d \) Frege systems

We now aim at a fine-grained analysis of \( AC^0 \)-Frege by studying its subsystems \( AC^0_d \)-Frege. Our next result is a version of Theorem 5.2, however, we need to be a bit more careful for circuits of fixed depth \( d \).

**Theorem 5.10.** Let \((C_n)_{n \in \mathbb{N}}\) be a non-uniform family of circuits where \( C_n \) is a circuit with \( n \) inputs. Then the following implications hold:

(i) if the QBFs \( Q \cdot C_n \) have \( AC^0_d \)-Frege + \( \forall \) refutations of size bounded by a function \( q(n) \), then for each \( n \), \( C_n \) is equivalent to a depth- \((d + 2)\) circuit \( C'_n \) of size \( O(q(n)) \);

(ii) if \((C_n)_{n \in \mathbb{N}}\) is a family of polynomial-size depth- \( d \) circuits, then the QBFs \( Q \cdot C_n \) have polynomial-size refutations in \( AC^0_d \)-Frege + \( \forall \) red.

**Proof.** The proof of (i) follows the proof of the analogous statement of Theorem 5.2. The Strategy Extraction Theorem in this case tell us that from refutations of \( Q \cdot C_n \) in \( AC^0_d \)-Frege + \( \forall \) red of size \( S \) we can extract a winning strategy for the universal player that can be computed by \( AC^0_{d+2} \)-decision lists of size \( O(S) \). By Proposition 4.2, this means that the winning strategy can be also computed by \( AC^0_{d+2} \) circuits and the size upper bound follows.

The proof of point (ii) follows the proof of the analogous statement of Theorem 5.2. That proof will give us that \( Q \cdot C_n \) has polynomial-size refutations in \( AC^0_{d+2} \)-Frege + \( \forall \) red. Here we want to prove that \( Q \cdot C_n \) has actually polynomial-size proofs in \( AC^0_d \)-Frege + \( \forall \) red. Without loss of generality suppose that the last gate \( t_m \) of \( C_n \) is an \( \forall \), that is

\[
Q \cdot C_n = \exists x_1 \cdots \exists x_n \forall u \exists t_1 \cdots \exists t_m . (u \leftrightarrow -t_m) \land (t_m \leftrightarrow \bigwedge_{j \leq \ell} t_{ij}) \land \varphi_n,
\]

where each \( t_{ij} \) is a \( \lor \) gate and \( \varphi_n \) is the encoding of the rest of the circuit \( C_n \). We clearly have that

\[
\begin{align*}
  u & \leftrightarrow -t_m & t_m & \leftrightarrow \bigwedge_{j \leq \ell} t_{ij} \\
  u & \leftrightarrow \bigvee_{j \leq \ell} -t_{ij}
\end{align*}
\]

From which we obtain both

\[
\begin{align*}
  u & \vee \bigwedge_{j \leq \ell} t_{ij}, & (11) \\
  -u & \vee \bigvee_{j \leq \ell} -t_{ij}, & (12)
\end{align*}
\]

Now we can proceed, similarly as in Theorem 5.2. By induction (on the depth of \( C_n \)) \( AC^0_d \)-Frege is able to substitute \( t_{ij} \) with \( D_{ij} \) where \( D_{ij} \) is an \( AC^0_{d-1} \)-formula over the \( x_1, \ldots, x_n \) variables starting with an \( \lor \). More precisely by induction we can prove that \( AC^0_d \)-Frege proves both

\[
\begin{align*}
  t_{ij} & \vee -D_{ij}, & (13) \\
  -t_{ij} & \vee D_{ij}. & (14)
\end{align*}
\]

Hence from (12) and (13) follows that

\[
-u \vee \bigvee_{j \leq \ell} -D_{ij},
\]
which is an $\text{AC}^0_d$-formula only over the variables $u, x_1, \ldots, x_n$. Hence by the $\forall \text{red}$ rule we get
\[
\bigvee_{j \leq \ell} \neg D_{ij}.
\]  \hfill (15)

Similarly from (11) we get first that
\[
\bigwedge_{j \leq \ell} (u \vee t_{ij})
\]
and then using (14) we get
\[
\bigwedge_{j \leq \ell} (u \vee D_{ij}),
\]
which, again, is an $\text{AC}^0_d$-formula over the variables $u, x_1, \ldots, x_n$. By the $\forall \text{red}$ rule we get
\[
\bigwedge_{j \leq \ell} D_{ij}.
\]  \hfill (16)

From (15) and (16) follows immediately a contradiction.

From Theorem 5.2 we immediately obtain a wealth of lower bounds for $\text{Res} + \forall \text{red}$.

**Corollary 5.11.** Let $f(x_1, \ldots, x_n)$ be a Boolean function requiring exponential-size depth-3 circuits and let $(C_n)_{n \in \mathbb{N}}$ be polynomial-size circuits (of unbounded depth) computing $f$. Then the QBFs $Q\cdot C_n$ require exponential-size refutations in $\text{AC}^0_1\cdot \text{Frege} + \forall \text{red}$ and hence, in particular, in $\text{Res} + \forall \text{red}$.

We now approach the separation of constant-depth $\text{Frege} + \forall \text{red}$ systems. For this we employ the Sipser functions separating the hierarchy of constant-depth circuits. We quote the definition of the $\text{SIPSER}_d$ function from Boppana and Sipser (1990):
\[
\text{SIPSER}_d = \bigwedge_{i_1 \leq m_1} \bigvee_{i_2 \leq m_2} \bigwedge_{i_3 \leq m_3} \cdots \bigcirc_{i_d \leq m_d} x_{i_1i_2i_3\ldots i_d},
\]
where $\bigcirc = \lor$ or $\land$ depending on the parity of $d$. The variables $x_1, \ldots, x_n$ appear as $x_{i_1i_2i_3\ldots i_d}$ for $i_j \leq m_j$, where $m_1 = \sqrt{m/\log m}$, $m_2 = m_3 = \cdots = m_{d-1} = m$, $m_d = \sqrt{dm \log m/2}$ and $m = (n\sqrt{2/d})^{1/(d-1)}$.

**Corollary 5.12.** Fix an integer $d \geq 2$. Let $(C^n_d)_{n \in \mathbb{N}}$ be a family of polynomial-size depth-$(d + 3)$ circuits computing the function $\text{SIPSER}_{d+3}(x_1, \ldots, x_n)$. Then the QBFs $Q\cdot C^n_d$ need exponential-size proofs in $\text{AC}^0_{d}\cdot \text{Frege} + \forall \text{red}$, but have polynomial-size proofs in $\text{AC}^0_{d+3}\cdot \text{Frege} + \forall \text{red}$.

**Proof.** The lower bound follows from Theorem 5.10 and from the result that for every $d$, $\text{SIPSER}_{d+3}$ needs exponential-size depth-$(d + 2)$ circuits (Håstad, 1986). Regarding the upper bound, by construction $C^n_d$ has depth $d + 3$ and polynomial-size. Hence, by Theorem 5.10, the family $Q\cdot C^n_d$ has polynomial-size proofs in $\text{AC}^0_{d+3}\cdot \text{Frege} + \forall \text{red}$. \hfill \Box

Note that the gap of size 1 in the circuit separation of (Håstad, 1986) increases to a gap of size 3 in our proof system separation, due to the transformation in Proposition 4.2. We highlight that in contrast to Corollary 5.12 where our separating formulas are CNFs, a separation of the depth-$d$ $\text{Frege}$ hierarchy with formulas of depth independent of $d$ is a major open problem in propositional proof complexity.
5.3 Conditional lower bounds for Frege and extended Frege

We end this section with conditional lower bounds for Frege + ∀red and EF + ∀red. Turning these conditional lower bounds into unconditional ones — at least with our technique — will depend on major breakthroughs in circuit complexity.

**Theorem 5.13.** Let $C$ be either non-uniform NC$^1$ or P/poly. If PSPACE $\notin C$ then $C$-Frege + ∀red is not polynomially bounded.

**Proof.** Let $f$ be a Boolean function in PSPACE but not in $C$. Since QBF is PSPACE-complete there exists a QBF $Q\bar{w}.\varphi(\bar{w}, x_1, \ldots, x_n)$ with a CNF $\varphi$ such that

$$f(x_1, \ldots, x_n) \equiv Q\bar{w}.\varphi(\bar{w}, x_1, \ldots, x_n).$$

We define

$$Q\cdot f_n = \exists x_1 \cdots \exists x_n \forall u. (u \leftrightarrow Q\bar{w}.\varphi(\bar{w}, x_1, \ldots, x_n)),$$

which can be rewritten into formulas $\Theta_n$ in prenex form. Notice that the only winning strategy for the universal player on both $Q\cdot f_n$ and $\Theta_n$ is to compute $u = f(x_1, \ldots, x_n)$. Therefore, the Strategy Extraction Theorem together with $f \notin C$ immediately implies super-polynomial lower bounds for $\Theta_n$ in $C$-Frege + ∀red. 

We remark that we do have a separation between uniform NC$^1$ and PSPACE, because NC$^1 \subseteq L$ and $L \neq$ PSPACE by the space hierarchy theorem. Therefore, choosing $f \in$ PSPACE \ NC$^1$ and considering the prenex formulas $\Theta_n$ arising from $Q\cdot f_n$ we can infer the weaker result that Frege + ∀red has no uniform short proofs of $\Theta_n$.

6 From propositional to QBF proof systems — the global view

In this section we lift proof systems from propositional logic to QBF proof systems in a uniform way. In addition to the ∀red systems considered so far, we define two more general paradigms to transform a propositional system $P$ into a QBF system: via expansions and via instantiations.

We consider all three paradigms in the same, slightly simplified setting, where we only substitute by constants, to allow for a comparison of the different approaches. We remark that although our constructions are quite general, some natural conditions on $P$ are needed to lift them to sound and complete QBF systems. These conditions hold for the systems $P$ commonly studied in proof complexity.

6.1 Expansion QBF proof systems

Given a QBF $Q\bar{y}\forall u\exists x_1 \cdots \exists x_k. \varphi$, we have the following semantical equivalences

$$Q\bar{y}\forall u\exists x_1 \cdots \exists x_k. \varphi \equiv Q\bar{y}(\exists x_1 \cdots \exists x_k. \varphi[u/0, x_1, \ldots, x_k] \land \exists x_1 \cdots \exists x_k. \varphi[u/1, x_1, \ldots, x_k])$$

$$\equiv Q\bar{y}\exists x_1^{u/0} \cdots \exists x_k^{u/0} \exists x_1^{0/1} \cdots \exists x_k^{0/1} \cdot \varphi[u/0, x_1^{u/0}, \ldots, x_k^{u/0}] \land \varphi[u/1, x_1^{0/1}, \ldots, x_k^{0/1}],$$

where $x_i^{u/b}$ are new fresh variables. The latter QBF is the expansion on $u$ of the original QBF. By repeated expansion on the innermost universal variable we define the full universal expansion of a QBF $Q. \varphi$: it is a QBF $Q'. \varphi'$ where $Q'$ consists exclusively of existential quantifiers. Moreover,
each existential variable $x_i$ in $Q \cdot \varphi$ becomes an $x_i^{[\tau]}$ in $Q' \cdot \varphi'$, for each mapping $\tau$ from the universal variables into $\{0, 1\}$ and where $[\tau]_i$ is the restriction of $\tau$ to the variables left of $x_i$.

It is immediate to observe that $Q \cdot \varphi$ and its full universal expansion $Q' \cdot \varphi'$ are semantically equivalent, but $Q' \cdot \varphi'$ may have exponentially many more variables than $Q \cdot \varphi$.

**Proposition 6.1.** Given a QBF $Q \cdot \varphi$ and a clause $C$ it is possible to determine in polynomial time (w.r.t. the size of $Q \cdot \varphi$) whether $C$ belongs to the full universal expansion of $Q \cdot \varphi$. □

**Definition 6.2** ($P + \forall \exp_{0,1}$). Let $P$ be a refutational propositional proof system and $Q \cdot \varphi$ a false QBF. Let $Q' \cdot \varphi'$ be the full universal expansion of $Q \cdot \varphi$ and let $\dot{\varphi} \subseteq \varphi'$. If $\pi$ is a $P$-proof of $\varphi$ then we define $(\pi, Q \cdot \varphi)$ to be a proof of the QBF $Q \cdot \varphi$ in the system $P + \forall \exp_{0,1}$.

We indicate by the index 0,1 in $\forall \exp_{0,1}$ that the universal variables are only replaced by constants. Similarly as for the reduction systems in Section 3 we can also define a more general version $P + \forall \exp$ where we substitute universal variables by more complex Boolean functions.

**Theorem 6.3.** If $P$ is a refutational propositional proof system then $P + \forall \exp_{0,1}$ is a refutational QBF proof system.

**Proof.** A QBF $Q \cdot \varphi$ is false if and only if its full universal expansion $Q' \cdot \varphi'$ is false. Moreover, since $Q'$ consists purely of existential quantifiers, then $Q' \cdot \varphi'$ is false if and only if $\varphi'$ is unsatisfiable. From this, and the fact that $P$ is well-defined and its range is UNSAT, it follows that $P + \forall \exp_{0,1}$ is well-defined and that the range of $P + \forall \exp_{0,1}$ is FQBF.

By Proposition 6.1 and since $P$ is polynomial-time computable, it follows that $P + \forall \exp_{0,1}$ is polynomial-time computable. □

Choosing $\text{Res}$ as the propositional base system, $\text{Res} + \forall \exp_{0,1}$ coincides with the system $\forall \exp + \text{Res}$ defined by Janota and Marques-Silva (2015).

There is a direct correspondence between the simulation order of propositional proof systems and expansion QBF systems.

**Proposition 6.4.** Let $P$ and $Q$ be propositional proof systems. Then $P$ p-simulates $Q$ if and only if $P + \forall \exp_{0,1}$ p-simulates $Q + \forall \exp_{0,1}$.

**Proof.** If $P$ p-simulates $Q$ then clearly $P + \forall \exp_{0,1}$ p-simulates $Q + \forall \exp_{0,1}$. The other direction follows since $P$ and $Q$ are just particular cases of $P + \forall \exp_{0,1}$ and $Q + \forall \exp$ when they act on existentially quantified QBFs. □

### 6.2 Reduction QBF proof systems revisited

To compare the expansion systems to the reduction systems investigated earlier, we consider a restricted version $\mathcal{C}^{\text{Frege}} + \forall \text{red}_{0,1}$ of $\mathcal{C}^{\text{Frege}} + \forall \text{red}$, where universal variables can only be replaced by constants. Formally, $\mathcal{C}^{\text{Frege}} + \forall \text{red}_{0,1}$ uses the inference rules of $\mathcal{C}^{\text{Frege}}$ and the following restricted version of the $\forall \text{red}$ rule:

$$\frac{L_j}{L_j [u/b]} \ (\forall \text{red}_{0,1})$$

where $b \in \{0, 1\}$ and $u$ is the innermost variable in $L_j$ w.r.t. the quantifier prefix of the QBF being refuted.
Theorem 6.5. For a circuit class $C$, $C$-Frege + $\forall$red$_{0,1}$ is a refutational QBF proof system.

Proof. The soundness follows from the fact that $C$-Frege + $\forall$red p-simulates $C$-Frege + $\forall$red$_{0,1}$ and the completeness by the fact that $C$-Frege + $\forall$red$_{0,1}$ can transform arbitrary Boolean formulas into CNF and then p-simulate Q-Res.

6.3 Instantiation QBF proof systems

We now define a QBF proof system that naturally generalises both $P + \forall$exp$_{0,1}$ and $P + \forall$red$_{0,1}$. We call this system $P + \forall$inst$_{0,1}$. A version of an instantiation system for Res, called IR-calc, was considered by Beyersdorff et al. (2014). As for the reduction systems we just define $C$-Frege + $\forall$inst$_{0,1}$, but it will be clear that this definition can be adapted to other proof systems.

Given a QBF $Q . \varphi$, an existentially quantified variable $x$ in $Q . \varphi$, and an assignment $\tau$ to all variables $u$ with $\qbf v (u) < \qbf v (x)$, we defined the annotated variable $x^\tau$ to have the same quantification level as $x$, $\qbf v (x^\tau) = \qbf v (x)$. An annotation on $u$ is expressed by a circuit in the (possibly annotated) variables $z$ where $\qbf v (z) < \qbf v (u)$.

Definition 6.6 ($C$-Frege + $\forall$inst$_{0,1}$). Let $C$ be a circuit class. A refutation of a false QBF $Q . \varphi$ in the system $C$-Frege + $\forall$inst$_{0,1}$ is a sequence of lines $L_1, \ldots, L_t$, where each line is a circuit from $C$, $L_1 = \varphi$, $L_t = \bot$ and each $L_i$ is inferred from previous lines $L_j$ using the inference rules of $C$-Frege or using the following rule

$$
\frac{L_j}{L_j[u/b, x^\tau/x^{\tau \cup \{u/b\}}, \ldots]} (\forall\text{inst}_{0,1}),
$$

where $b \in \{0, 1\}$ and and the replacement of $x^\tau$ with $x^{\tau \cup \{u/b\}}$ occurs for every $x^\tau$ such that $\qbf v (x^\tau) > \qbf v (u)$ and $u \notin \text{dom}(\tau)$.

In the next theorem we show that $C$-Frege + $\forall$inst$_{0,1}$ is a well-defined QBF proof system. Before doing that we observe that the $\forall$inst$_{0,1}$ rule generalises both the $\forall$exp$_{0,1}$ rule and the $\forall$red$_{0,1}$ rule. Hence $C$-Frege + $\forall$inst$_{0,1}$ p-simulates both $C$-Frege + $\forall$exp$_{0,1}$ and $C$-Frege + $\forall$red$_{0,1}$.

Theorem 6.7. $C$-Frege + $\forall$inst$_{0,1}$ is a refutational QBF proof system.

Proof. The completeness of $C$-Frege + $\forall$inst$_{0,1}$ follows from the fact that it p-simulates the complete QBF proof system $C$-Frege + $\forall$red$_{0,1}$.

Regarding the soundness of $C$-Frege + $\forall$inst$_{0,1}$, by contradiction, suppose that $(L_1, \ldots, L_t)$ is a refutation of a true QBF $Q . \varphi$ in the system $C$-Frege + $\forall$inst$_{0,1}$.

Since $Q . \varphi$ is true, then by the two-player game semantics, for each existentially quantified variable $x$ there exists a Skolem function $f_x$ depending only on the universal variables $u$ with $\qbf v (x) > \qbf v (u)$ such that the collection of all $f_x$ is a winning strategy for the existential player.

Let $\psi_i$ be the result of substituting in $\varphi \land L_1 \land \cdots \land L_i$ each occurrence of $x^{[u_1/c_1, \ldots, u_k/c_k]}$ by its Skolem function $f_x$ with argument $u_1/c_1, \ldots, u_k/c_k$, that is $f_x(u_1/c_1, \ldots, u_k/c_k)$:

$$
\psi_i = \begin{cases} 
\varphi[x^\tau/f_x(\tau), \ldots] & \text{if } i = 0, \\
\varphi \land L_1 \land \cdots \land L_i[x^\tau/f_x(\tau), \ldots] & \text{otherwise.}
\end{cases}
$$

Let $\forall \bar{u}$ be the quantifier prefix of $Q . \varphi$ when pruned of all the existential variables. By induction on $i$, we prove that $\forall \bar{u} . \psi_i$ is true for every $i = 1, \ldots, \ell$. For $i = \ell$ this gives a contradiction, since $L_\ell = \bot$ is appearing in $\psi_\ell$ and hence it is false.
The base case of the induction holds since the Skolem functions $f_x$ must satisfy $\varphi$ when substituted for $x$ under every assignment to $\vec{u}$. This gives exactly that $\forall \vec{u}. \psi_0$ is true.

Suppose now that, by induction hypothesis, that $\forall \vec{u}. \psi_i$ is true. We show that $\forall \vec{u}. \psi_{i+1}$ is true. By definition $\psi_{i+1} = \psi_i \land L_{i+1}[x^7/f_x(\tau), \ldots]$ and $L_{i+1}$ was either introduced by a $\mathcal{C}$-Frege rule or by the $\forall \text{inst}_0,1$ rule.

If $L_{i+1}$ was introduced by a $\mathcal{C}$-Frege rule then $\psi_i \models L_{i+1}[x^7/f_x(\tau), \ldots]$. Moreover, by inductive hypothesis, $\mathcal{Q}. \psi_i$ is true; therefore $\mathcal{Q}. \psi_{i+1}$ is true as well.

Let $L_{i+1}$ now be introduced by the $\forall \text{inst}_0,1$ rule, say $L_{i+1} = L_j[v/b, x^7/x^7 \cup \{v/b\}, \ldots]$ with $j \leq i$. For shortness let $L_j' = L_j[v^7/f_x(\tau), \ldots]$ and suppose that $\forall \vec{u}. \psi_i = \forall \vec{u}_1 \forall \vec{u}_2 . \psi_i$. Then we have the following transformations:

\[
\begin{align*}
\forall \vec{u}_1 \forall \vec{u}_2 . \psi_i & \equiv \forall \vec{u}_1 \forall \vec{u}_2 \forall \psi_i \land L_j' \\
& \equiv \forall \vec{u}_1 \forall \vec{u}_2 . \psi_i[0/v] \land L_j'[0/v] \land \psi_i[1/v] \land L_j'[1/v] \\
& \equiv \forall \vec{u}_1 \forall \vec{u}_2 . (L_j'[0/v] \land L_j'[1/v] \land \forall \psi_i) \\
& \equiv \forall \vec{u}_1 \forall \vec{u}_2 . L_j'[0/v] \land L_j'[1/v] \land \psi_i \\
& = \forall \vec{u}_1 \forall \vec{u}_2 . \psi_i \land L_j'[v/b].
\end{align*}
\]

Notice that the replacement $v/b$ in $L_j'$ also replaces $v$ as an argument in the Skolem functions, hence

\[
L_j'[v/b] = L_j'[v/b][x^7/x^7 \cup \{v/b\}, \ldots] = L_j[v/b][x^7 \cup \{v/b\}/f_x(\tau \cup \{v/b\}), \ldots].
\]

From the previous chain of equalities follows that formula (22) is semantically equivalent to $\forall \vec{u}. \psi_{i+1}$. Hence $\forall \vec{u}. \psi_{i+1}$ is true.

Similarly to the relation between the $\forall \text{red}_0,1$ and the $\forall \text{red}$ rules we can define a more general version $\forall \text{inst}$ of the $\forall \text{inst}_0,1$ rule. In the system $\mathcal{C}$-Frege + $\forall \text{inst}$ variables can be annotated as $u/g$ where $g$ is a function.

### 6.4 Towards understanding the simulation order of QBF systems

To compare the different families of QBF systems defined above we consider the following family of QBFs from Janota and Marques-Silva (2015):

\[
F_n = \exists e_1 \forall u_1 \exists c^1_1 \exists c^2_1 \cdots \exists e_i \forall u_i \exists c^1_i \exists c^2_i \cdots \exists e_n \forall u_n \exists c^1_n c^2_n, \quad \bigwedge_{i=1}^n \left( \neg c^1_i \lor \neg c^2_i \right) \land \\
\bigwedge_{i=1}^n (e_i \rightarrow c^1_i) \land (u_i \rightarrow c^1_i) \land (\neg e_i \rightarrow c^2_i) \land (\neg u_i \rightarrow c^2_i).
\]

Janota and Marques-Silva (2015) use these formulas to show that $\forall \text{Exp} + \text{Res}$ does not simulate $Q\text{-Res}$. Their argument easily generalises to the stronger systems we consider here:

**Proposition 6.8.**

(i) Let $P$ be a propositional proof system. Then the QBFs $F_n$ require exponential-size proofs in $P + \forall \text{exp}_0,1$.

(ii) The QBFs $F_n$ have polynomial-size proofs in $\text{Res} + \forall \text{red}_0,1$.  

23
Proof. Regarding the first claim, Janota and Marques-Silva (2015) showed that for semantic reasons every clause is needed in the full universal expansion of $F_n$ to make the expanded formula false. Since there are exponentially many such clauses and all must be lines in a $P + \forall\text{exp}_{0,1}$ refutation, every $P + \forall\text{exp}_{0,1}$ refutation is of exponential size.

For the second claim, Janota and Marques-Silva (2015) showed that $F_n$ has proofs in Q-Res of polynomial size, hence short proofs also exist in Res + $\forall\text{red}_{0,1}$, since the latter is p-equivalent to the stronger QBF proof system QU-Res.

This immediately implies that none of the expansion systems is able to simulate even the weakest of the reduction systems that we consider here.

**Corollary 6.9.** Let $P$ be a propositional proof system. Then $P + \forall\text{exp}_{0,1}$ does not simulate Res + $\forall\text{red}_{0,1}$.

For the full separation between expansion and reduction systems we consider again the QBFs $Q-C_n$ from Section 5. In an argument similar to (Beyersdorff et al., 2015a, Lemma 15) we obtain:

**Proposition 6.10.** Let $C_n$ be a polynomial-size circuit computing PARITY$(x_1, \ldots, x_n)$. Then the QBFs $Q-C_n$ have polynomial-size refutations in Res + $\forall\text{exp}_{0,1}$.

**Proof.** Let $C_n$ be a circuit family computing PARITY. The formulas $Q-C_n$ in Definition 5.1 have exactly one universal variable $u$, which we expand in both polarities 0 and 1. This does not affect the $x_i$ variables, but creates different copies $t_i^{u/0}$ and $t_i^{u/1}$ of the existential variables right of $u$. Using the clauses from $G_i$ expressing the circuit gates, we can inductively derive clauses representing $t_i^{u/0} = t_i^{u/1}$. This lets us derive a contradiction using the clauses $t_m^{u/0}$ and $\neg t_m^{u/1}$.

Clearly, this argument generalises to QBFs originating from further functions considered in Section 5. The previous proposition together with Corollary 5.3 immediately implies the following.

**Corollary 6.11.** For every prime $p$, AC$^0[p]$-Frege + $\forall\text{red}$ does not simulate Res + $\forall\text{exp}_{0,1}$.

As observed earlier, instantiation systems by definition simulate both expansion and reduction systems. However, they are strictly stronger by the incomparability of expansion and reduction systems shown above. Figure 1 shows a slice of the simulation order of the QBF proof systems studied here.

$$
\begin{array}{ccc}
P + \forall\text{inst}_{0,1} & A \rightarrow B & A \ p\text{-simulates} \ B \\
\downarrow & & \\
P + \forall\text{exp}_{0,1} & A \longrightarrow B & A \text{ and } B \text{ are incomparable} \\
\end{array}
$$

Figure 1: A slice of the simulation order of QBF proof systems

7 Conclusion and open problems

We already outlined the main directions of this paper’s potential for impact in Section 1.3. The most immediate specific open problem arising from this work is to show lower bounds for
Frege $+ \forall \text{red}$. While such a lower bound via our technique would need a major breakthrough in circuit complexity (cf. Theorem 5.13), we ask the (possibly very challenging) question whether a lower bound can be shown via a different method.

While we consider the reduction systems $P + \forall \text{red}$ the most natural ones — as they have a very clear semantic meaning via Herbrand functions — it also remains open to show lower bounds for the stronger instantiation systems defined in Section 6.3.

Acknowledgements. The authors are grateful to Nicola Galesi and Albert Atserias for interesting discussions about this work and circuit complexity in general.

This research was supported by grant no. 48138 from the John Templeton Foundation, EPSRC grant EP/L024233/1, and a Doctoral Training Grant from EPSRC (3rd author).

References


