# Lower Bounds: From Circuits to QBF Proof Systems 

Olaf Beyersdorff<br>School of Computing University of Leeds, UK<br>o.beyersdorff@leeds.ac.uk

Ilario Bonacina<br>School of Computer Science and Communication KTH Royal Institute of Technology, Sweden<br>ilario@kth.se

Leroy Chew<br>School of Computing<br>University of Leeds, UK<br>mm12Inc@leeds.ac.uk


#### 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 $P+\forall$ red, which is inspired by the transition from resolution to Qresolution. For us the most important case is a new and natural hierarchy of QBF Frege systems $\mathcal{C}$-Frege $+\forall$ red that parallels the well-studied propositional hierarchy of $\mathcal{C}$-Frege systems, where lines in proofs are restricted to belong 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 $\mathcal{C}$-Frege $+\forall$ 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 the QBF proof system $\mathrm{AC}^{0}[p]$-Frege $+\forall$ red for all primes $p$;
(ii) an exponential separation of $\mathrm{AC}^{0}[p]$-Frege $+\forall$ red from $\mathrm{TC}^{0}$-Frege $+\forall$ red;
(iii) an exponential separation of the hierarchy of constantdepth systems $\mathrm{AC}_{d}^{0}$ - - rege $+\forall$ red by formulas of depth independent of $d$.

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

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.
ITCS'16, January 14-16, 2016, Cambridge, MA, USA
(C) 2016 ACM. ISBN 978-1-4503-4057-1/16/01 ... $\$ 15.00$

DOI: http://dx.doi.org/10.1145/2840728.2840740.

## Categories and Subject Descriptors

F.2.2 [Analysis of algorithms and problem complexity]: Nonnumerical Algorithms and Problems-Complexity of proof procedures

## Keywords

QBF proof complexity; Frege systems; proof complexity; circuit complexity

## 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 [Krajíček, 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 $\mathrm{AC}^{0} \subset \mathrm{AC}^{0}[p] \subset \mathrm{TC}^{0} \subseteq \mathrm{NC}^{1} \subseteq \mathrm{P} /$ 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 $\mathrm{AC}^{0}[p]$ [Razborov, 1987; Smolensky, 1987], 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 AC $^{0}[p]$ circuit lower to a proof size lower bound in $\mathrm{AC}^{0}[p]$-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 ( $=\mathrm{NC}^{1}$-Frege) or even extended Frege ( $=\mathrm{P} /$ 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 $\mathrm{AC}^{0}[p]$-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 $P+\forall$ red for closed prenex QBFs (Definition 3.1). Throughout the proof, the quantifier prefix is fixed, and lines in the system $P+\forall$ red are conceptually the same as lines in $P$, i.e. clauses in resolution, circuits from $\mathcal{C}$ in $\mathcal{C}$-Frege, or inequalities in cutting planes. Our new system $P+\forall$ 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 $\forall$ 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 $\forall$ red rule, resulting in a natural and robust system $P+\forall$ red.Our new systems $P+\forall$ 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 $P+\forall$ 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 $\mathcal{C}$-Frege $+\forall$ red of new QBF 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 $\mathrm{AC}^{0}$-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 $\mathcal{C}$ can be directly lifted to a proof size lower bound in $\mathcal{C}$-Frege $+\forall$ 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 $\mathcal{C}$-Frege $+\forall$ red we can efficiently extract a winning strategy for the universal player in a simple computational model we call $\mathcal{C}$-decision lists. We observe that $\mathcal{C}$-decision lists are easy to transform into $\mathcal{C}$ 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 $\mathcal{C}$. From $f$ we construct a family $\mathcal{Q}$ - $f_{n}$ of false QBFs such that each winning strategy of the universal player on $\mathcal{Q}-f_{n}$ has to compute $f$. By strategy extraction, refutations of $\mathcal{Q}$ - $f_{n}$ in $\mathcal{C}$-Frege $+\forall$ red yield $\mathcal{C}$-circuits for $f$; hence all such refutations must be long. In fact, we even show the converse implication to hold, i.e. from small $\mathcal{C}$-circuits for $f$ we construct short proofs of $\mathcal{Q}-f_{n}$ in $\mathcal{C}$-Frege $+\forall$ red.
Our lower bound technique widely generalises ideas recently used by Beyersdorff et al. [2015a] to show lower bounds for Q-Res and QU-Res for formulas originating from the 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 $\mathcal{C}$-Frege $+\forall$ red systems that are yet unparalleled in propositional proof complexity. The following results are contained in Section 5.
C.(a) Lower bounds and separations for the QBF proof system AC $^{0}[p]$-Frege $+\forall$ red. The seminal results of [Razborov, 1987; Smolensky, 1987] showed that Parity and more generally $M O D_{q}$ are the classic examples for functions that require exponential-size bounded-depth circuits with $M O D_{p}$ gates, where $p$ and $q$ are different primes. Using these functions, we define families of QBFs that require exponential-size proofs in $A C^{0}[p]$-Frege $+\forall$ red by strategy extraction.
To obtain separations of these proof systems, the exact formulation of the QBFs matters. When defining the PaRITY or $M O D_{q}$ formulas directly from (arbitrary) $\mathrm{NC}^{1}$ circuits computing these functions, we obtain polynomialsize upper bounds in Frege $+\forall$ red. However, when carefully choosing specific and indeed very natural encodings, we can prove upper bounds for the $M O D_{q}$ formulas even in $\mathrm{AC}^{0}[q]$-Frege $+\forall$ red, thus obtaining exponential separations of all the $\mathrm{AC}^{0}[p]$-Frege $+\forall$ red systems for distinct primes $p$.
As mentioned before, lower bounds for $\mathrm{AC}^{0}[p]$-Frege (as well as their separations) are major open problems in propositional proof complexity.
C.(b) $\mathrm{AC}^{0}[p]$-Frege $+\forall$ red and $\mathrm{TC}^{0}$-Frege $+\forall$ red are separated. MAJORITY is another classic function in circuit complexity, for which exponential lower bounds are known for constant-depth circuits with $M O D_{p}$ gates for each prime $p$ [Razborov, 1987; Smolensky, 1987]. Using our technique, we transfer these to lower bounds in $\mathrm{AC}^{0}[p]$-Frege $+\forall$ red for all primes $p$. Carefully choosing the QBF encoding of Majority, we obtain polynomial upper bounds for the Majority formulas in $\mathrm{TC}^{0}$-Frege $+\forall$ red, thus proving an exponential separation between the two QBF proof systems $\mathrm{AC}^{0}[p]$-Frege $+\forall$ red and $\mathrm{TC}^{0}-$ Frege $+\forall$ red. Again, such a separation is wide open in propositional proof complexity.
C.(c) CNFs separating the $\mathrm{AC}_{d}^{0}$-Frege $+\forall$ red hierarchy. As a third example for our approach we investigate the fine structure of $\mathrm{AC}^{0}$-Frege $+\forall$ red, comprising all $\mathrm{AC}_{d}^{0}$-Frege $+\forall$ 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 $\operatorname{SiPSER}_{d}$ 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 $\mathrm{AC}_{d-3}^{0}$-Frege $+\forall$ red from $\mathrm{AC}_{d}^{0}$-Frege $+\forall$ red, where the increased gap of size 3 comes from our transformation of $\mathcal{C}$-decision lists into $\mathcal{C}$ circuits.
The $\operatorname{Sipser}_{d}$ formulas achieving these separations are prenexed CNFs, i.e. the formulas have depth 2 . While in propositional proof complexity the hierarchy of $\mathrm{AC}_{d}^{0}$-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 Q-Res and 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 $A C^{0}$ lower bound for Parity is used to obtain exponential lower bounds for Q-Res and 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., 2000, 2004; Krajíček and Pudlák, 1998] feasible interpolation is not applicable to strong systems such as $\mathrm{AC}^{0}$-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.

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 $\mathcal{C}$-Frege $+\forall$ 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.

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 $\mathcal{C}$ and proof systems using lines from $\mathcal{C}$. 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 $\mathcal{Q}-f$ 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 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 $\mathcal{C}$-Frege systems and QBF. In Section 3 we define the QBF proof systems $\mathcal{C}$-Frege $+\forall$ 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 $\mathcal{C}$-Frege $+\forall$ red for several circuit classes $\mathcal{C}$. 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 $\mathcal{Q}-C$ (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 concludes with some open problems.

## 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 $\varphi\left[x_{1} / \theta_{1}, \ldots, x_{k} / \theta_{k}\right]$ 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 ${A C^{0}}^{0}$ contains all languages recognisable by polynomial-size circuits over the Boolean basis $\neg, \vee, \wedge$ with bounded depth and unbounded fan-in. When fixing the depth to a constant $d$, we denote the circuit class by $\mathrm{AC}_{d}^{0}$. The class $\mathrm{AC}^{0}[p]$ uses boundeddepth circuits with $M O D_{p}$ gates determining whether the sum of the inputs is 0 modulo $p$, and in $\mathrm{TC}^{0}$ bounded-depth circuits with threshold gates are permitted. Stronger classes
are obtained by using $\mathrm{NC}^{1}$ circuits of polynomial size and logarithmic depth, and by $\mathrm{P} /$ poly circuits of polynomial size.

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

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 $Q B F$ 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 $\mathcal{L}, P$ 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 $\mathcal{L}$ is called polynomially bounded if there exists a polynomial $p$ such that every $x \in \mathcal{L}$ 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 $\neg, \wedge$, and $\vee$. A Frege system comprises a finite set of axiom schemes and rules, e.g., $\varphi \vee \neg \varphi$ 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 setting of refutation Frege systems where we start with the negation of the formula that we want to prove and derive the contradiction $\perp$.

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

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

Resolution (Res) is a particular kind of $\mathrm{AC}_{1}^{0}$-Frege system ${ }^{1}$ 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

$$
\frac{C \vee x \quad D \vee \neg x}{C \vee D} \text { (Res rule), }
$$

where $C, D$ denote clauses and $x$ is a variable. A Res refutation derives the empty clause $\perp$.

Given a prime $p$, the $\mathrm{AC}^{0}[p]$-Frege systems are defined to be bounded-depth Frege systems in the language with Boolean connectives $\neg, \vee, \wedge$ and modular gates $M O D_{p}\left(x_{1}, \ldots, x_{n}\right)$. The $M O D_{p}$ predicate is true when $\sum_{i} x_{i} \equiv 0(\bmod p)$.

The TC ${ }^{0}$-Frege systems are defined to be bounded-depth Frege systems in the language with Boolean connectives $\neg$, $\vee, \wedge$ and threshold gates $T_{k}\left(x_{1}, \ldots, x_{n}\right)$. The $T_{k}$ predicate is true when at least $k$ of its inputs are true. Two different, but equivalent, formalizations of $\mathrm{TC}^{0}$-Frege proof systems are given by Buss and Clote [1996] and Bonet et al. [2000].
(Unrestricted) Frege systems correspond to the complexity class $N C^{1}$ in the same sense as bounded-depth Frege corresponds to the class $\mathrm{AC}^{0}$. We will refer sometimes to Frege as $N^{1}$-Frege.

Extended Frege systems EF allow the introduction of new extension variables that abbreviate formulas. EF can be understood as a Frege system that directly operates with Boolean circuits rather than formulas, where extension variables can be used to define the circuit gates (see [Jerábek, 2005] for the precise formulation). Therefore we will refer to EF also as P/poly-Frege. An alternative characterisation of EF is through substitution Frege systems SF that allow arbitrary substitution instances of derived formulas [Cook and Reckhow, 1979; Krajíček and Pudlák, 1989].
The Frege systems defined above form a hierarchy of proof systems
Res $\leq_{p} \mathrm{AC}^{0}$-Frege $\leq_{p} \mathrm{AC}^{0}[p]$-Frege $\leq_{p} \mathrm{TC}^{0}$-Frege $\leq_{p}$ Frege $\leq_{p} \mathrm{EF}$.
Currently lower bounds are only known for Res [Haken, 1985] and AC $^{0}$-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.

Quantified Boolean Formulas. A (closed prenix) Quantified Boolean Formula (QBF) is a formula in quantified propositional logic where each variable is quantified at the beginning of the formula, using either an existential or universal quantifier. We denote such formulas as $\mathcal{Q} . \varphi$, where $\varphi$ is a propositional Boolean formula in Conjunctive Normal Form (CNF), called matrix, and $\mathcal{Q}$ is its 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 $\mathcal{Q} . \varphi$, the quantification level of $y$ in $\mathcal{Q} . \varphi$, $q \operatorname{lv}(y)$, is the number of alternations of quantifiers $y$ has on $i$ its left in the quantifier prefix of $\mathcal{Q} . \varphi$. Given a variable $y$, we will sometimes refer to the variables with quantification level lower than $\operatorname{qlv}(y)$ as variables left of $y$; analogously the variables with quantification lever higher than $\operatorname{qlv}(y)$ will be right of $y$.

[^0]A $\operatorname{QBF} \mathcal{Q}_{1} x_{1} \cdots \mathcal{Q}_{k} x_{k} . \varphi$ can be seen as a game between two players: universal $(\forall)$ and existential ( $\exists$ ). In the $i$-th step of the game, the player $\mathcal{Q}_{i}$ 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 Büning 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 $\frac{C \vee x \quad D \vee \neg x}{C \vee D}$ 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

$$
\frac{C \vee u}{C},
$$

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 $\mathcal{C}$-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 $\mathcal{C}$ with some natural properties, e.g., closure under restrictions. In particular, $\mathcal{C}$ can be any of the circuit classes mentioned in Section 2.

Definition $3.1 \quad(\mathcal{C}$-Frege $+\forall$ red $)$. A refutation of a false $Q B F \mathcal{Q} . \varphi$ in the system $\mathcal{C}$-Frege $+\forall$ red is sequence of lines $L_{1}, \ldots, L_{\ell}$ where each line is a circuit from the class $\mathcal{C}$, $L_{1}=\varphi,{ }^{2} L_{\ell}=\perp$ and each $L_{i}$ is inferred from previous lines $L_{j}$ using the inference rules of $\mathcal{C}$-Frege or using the following rule

$$
\frac{L_{j}}{L_{j}[u / B]}(\forall \mathrm{red}),
$$

where $L_{j}[u / B]$ belongs to the class $\mathcal{C}, u$ is the innermost variable among the variables of $L_{j}$ and $B$ is a circuit from the class $\mathcal{C}$ containing only variables left of $u$.

[^1]The formal justification why $\mathcal{C}$-Frege $+\forall$ 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 $\forall$ red rule results in a natural proof system $\mathcal{C}$-Frege $+\forall$ red. Recall that we consider $\mathcal{C}$-Frege $+\forall$ red as a refutation system; hence we aim to refute false quantified $\mathcal{C}$ 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 $\mathcal{C}$ we should also restrict $B$ to that class, and substituting the Herbrand function into the formula should again preserve $\mathcal{C}$.
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 ). 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 Res as our propositional proof system, which is an $\mathrm{AC}_{1}^{0}$-Frege system, we obtain Res $+\forall$ red. In Res $+\forall$ red the $\forall$ 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 $\forall$ red rule in Q-Res, whereas substituting $u$ by 1 results in the useless tautology $T .{ }^{3}$ As Res $+\forall$ red can resolve on existential and universal variables, our system Res $+\forall$ 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 $\mathcal{C}$, the system $\mathcal{C}$-Frege $+\forall$ red is a refutational QBF proof system.

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

Regarding the soundness of $\mathcal{C}$-Frege $+\forall$ red, let $\left(L_{1}, \ldots, L_{\ell}\right)$ be a refutation of $\mathcal{Q} . \varphi$ in the system $\mathcal{C}$-Frege $+\forall$ red and let

$$
\varphi_{i}= \begin{cases}\varphi & \text { if } i=0 \\ \varphi \wedge L_{1} \wedge \cdots \wedge L_{i} & \text { otherwise }\end{cases}
$$

By induction on $i$ we prove that $\mathcal{Q} . \varphi$ semantically entails $\mathcal{Q} . \varphi_{i}$, i.e. $\mathcal{Q} . \varphi \models \mathcal{Q} . \varphi_{i}$. Hence, at step $i=\ell$ we will immediately obtain that $\mathcal{Q} . \varphi$ is false, since $L_{\ell}=\{\perp\}$ and $\mathcal{Q} . \varphi_{\ell} \equiv \perp$.
Since $\mathcal{Q} \cdot \varphi=\mathcal{Q} . \varphi_{0}$ the base case of the induction holds.
We show now that $\mathcal{Q} . \varphi \models \mathcal{Q} . \varphi_{i}$ implies $\mathcal{Q} . \varphi \vDash \mathcal{Q} . \varphi_{i+1}$. By definition, $\varphi_{i+1}=\left(\varphi_{i} \wedge L_{i+1}\right)$ and $L_{i+1}$ was either introduced by a $\mathcal{C}$-Frege rule or by the $\forall$ red rule. If $L_{i+1}$ was introduced by a $\mathcal{C}$-Frege rule then $\varphi_{i} \models L_{i+1}$, so $\varphi_{i}=\varphi_{i+1}$ and clearly $\mathcal{Q} . \varphi \vDash \mathcal{Q} . \varphi_{i}=\mathcal{Q} . \varphi_{i+1}$.

[^2]Suppose now that $L_{i+1}$ was introduced by the $\forall$ 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 $\mathcal{Q} \cdot \varphi_{i}=\mathcal{Q}_{1} \vec{x} \forall u \mathcal{Q}_{2} \vec{y} \cdot \varphi_{i}$, then we have the following chain of equivalences

$$
\begin{align*}
& \mathcal{Q} \cdot \varphi_{i}=\mathcal{Q}_{1} \vec{x} \forall u \mathcal{Q}_{2} \vec{y} \cdot \varphi_{i}  \tag{1}\\
& \equiv \mathcal{Q}_{1} \vec{x} \forall u \mathcal{Q}_{2} \vec{y} \cdot \varphi_{i} \wedge L_{j}  \tag{2}\\
& \equiv \mathcal{Q}_{1} \vec{x}\left(\left(\mathcal{Q}_{2} \vec{y} \cdot \varphi_{i}[u / 0] \wedge L_{j}[u / 0]\right) \wedge\left(\mathcal{Q}_{2} \vec{y} \cdot \varphi_{i}[u / 1] \wedge L_{j}[u / 1]\right)\right)  \tag{3}\\
& \equiv \mathcal{Q}_{1} \vec{x}\left(L_{j}[u / 0] \wedge L_{j}[u / 1] \wedge\left(\mathcal{Q}_{2} \vec{y} \cdot \varphi_{i}[u / 0]\right) \wedge\left(\mathcal{Q}_{2} \vec{y} \cdot \varphi_{i}[u / 1]\right)\right)  \tag{4}\\
& \equiv \mathcal{Q}_{1} \vec{x}\left(L_{j}[u / 0] \wedge L_{j}[u / 1] \wedge \forall u \mathcal{Q}_{2} \vec{y} \cdot \varphi_{i}\right)  \tag{5}\\
& \equiv \mathcal{Q}_{1} \vec{x}\left(L_{j}[u / 0] \wedge L_{j}[u / 1] \wedge L_{j}[u / B] \wedge \forall u \mathcal{Q}_{2} \vec{y} \cdot \varphi_{i}\right)  \tag{6}\\
& \equiv \mathcal{Q}_{1} \vec{x} \forall u \mathcal{Q}_{2} \vec{y} \cdot \varphi_{i} \wedge L_{j}[u / 0] \wedge L_{j}[u / 1] \wedge L_{j}[u / B] . \tag{7}
\end{align*}
$$

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 $\vec{y}$ variables. From (7) follows, by weakening, that

$$
\mathcal{Q} \cdot \varphi_{i}=\mathcal{Q}_{1} \vec{x} \forall u \mathcal{Q}_{2} \vec{y} \cdot \varphi_{i} \wedge L_{j}[u / B],
$$

hence $\mathcal{Q} . \varphi \models \mathcal{Q} . \varphi_{i+1}$.
Clearly lower bounds on the complexity of $\mathcal{C}$-Frege $+\forall$ red follow from lower bounds on $\mathcal{C}$-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 $\forall$ red rule in refutations.

## 4. STRATEGY EXTRACTION

We introduce now the simple computational model of $\mathcal{C}$-decision lists.

Definition $4.1 \quad(\mathcal{C}$-decision list). $A \mathcal{C}$-decision list is a programme of the following form

```
if C}\mp@subsup{C}{1}{}(\vec{x})\mathrm{ then }u\leftarrow\mp@subsup{B}{1}{}(\vec{x})\mathrm{ ;
    else if C2 (\vec{x})\mathrm{ then }u\leftarrow\mp@subsup{B}{2}{(\vec{x});}
        else if C C-1 (\vec{x})\mathrm{ then }u\leftarrow\mp@subsup{B}{\ell-1}{}(\vec{x})\mathrm{ ;}
        else }u\leftarrow\mp@subsup{B}{\ell}{}(\vec{x})
```

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

This definition generalises decision lists from [Rivest, 1987], where the conditions $C_{i}(\vec{x})$ are expressible as terms. We note that for many cases $\mathcal{C}$-decision lists can be easily transformed into $\mathcal{C}$-circuits.

Proposition 4.2. Let $D$ be a $\mathcal{C}$-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 $D^{\prime} \in \mathcal{C}$ computing the same function $g$, such that the size of $D^{\prime}$ is linear in the size of $D$ and
$\operatorname{depth}\left(D^{\prime}\right) \leq \max \left\{\max _{1 \leq i \leq \ell-1}\left\{\operatorname{depth}\left(C_{i}\right)\right\}, \max _{1 \leq i \leq \ell}\left\{\operatorname{depth}\left(B_{i}\right)\right\}\right\}+2$.

Proof. We have that

$$
u \equiv \bigvee_{j=1}^{\ell}\left(C_{j}(\vec{x}) \wedge B_{j}(\vec{x}) \wedge \bigwedge_{k<j} \neg C_{k}(\vec{x})\right)
$$

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 $\mathcal{C}$-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). Given a false $Q B F \mathcal{Q} . \varphi$ and a refutation $\pi$ of $Q . \varphi$ in $\mathcal{C}$-Frege $+\forall$ red, it is possible to extract in linear time (w.r.t. $|\pi|$ ) a collection of $\mathcal{C}$-decision lists $D$ computing a winning strategy on the universal variables of $\varphi$.

Proof. Let $\pi=\left(L_{1}, \ldots, L_{\ell}\right)$ be a refutation of the false $\operatorname{QBF} \mathcal{Q} . \varphi$ and let

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

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

$$
\varphi_{i}= \begin{cases}\varphi & \text { if } i=0 \\ \varphi \wedge L_{1} \wedge \cdots \wedge L_{i} & \text { otherwise }\end{cases}
$$

such that for each universal variable $u$ in $\mathcal{Q} . \varphi$, there exists a $\mathcal{C}$-decision list $D_{u}^{i}$ computing $\sigma_{u}^{i}$ as a function of the variables in $\mathcal{Q}$ left of $u$, having size $O\left(\left|\pi_{i}\right|\right)$.

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 $L_{\ell}=\perp$, and we can define all the $D_{u}^{\ell}$ as $u \leftarrow 0$.
We show now how to construct $\sigma_{u}^{i-1}$ and $D_{u}^{i-1}$ from $\sigma_{u}^{i}$ and $D_{u}^{i}$ :

- If $L_{i}$ is derived by some Frege rule, then for each universal variable $u$ we set $\sigma_{u}^{i-1}=\sigma_{u}^{i}$ and $D_{u}^{i-1}=D_{u}^{i}$.
- If $L_{i}$ is the result of an application of a $\forall$ red rule, that is $\frac{L_{j}}{L_{j}[u / B]}$, where $u$ is the rightmost variable in $L_{j}, L_{j}[u / B]$ is a circuit in $\mathcal{C}$ using only variables on the left of $u$, and $L_{j}(u / B)=L_{i}$. Let $\vec{x}_{u^{\prime}}$ denote the variables on the left of $u^{\prime}$ in the quantifier prefix of $\mathcal{Q} \cdot \varphi$. Then we define

$$
\sigma_{u^{\prime}}^{i-1}\left(\vec{x}_{u^{\prime}}\right)= \begin{cases}\sigma_{u^{\prime}}^{i}\left(\vec{x}_{u^{\prime}}\right) & \text { if } u^{\prime} \neq u, \\ B\left(\vec{x}_{u}\right) & \text { if } u^{\prime}=u \text { and } L_{j}[u / B]\left(\vec{x}_{u}\right)=0, \\ \sigma_{u}^{i}\left(\vec{x}_{u}\right) & \text { if } u^{\prime}=u \text { and } L_{j}[u / B]\left(\vec{x}_{u}\right)=1 .\end{cases}
$$

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

$$
\begin{aligned}
& \text { if } \neg L_{j}[u / B]\left(\vec{x}_{u}\right) \text { then } u \leftarrow B\left(\vec{x}_{u}\right) \text {; } \\
& \text { else } D_{i}^{u}\left(\vec{x}_{u}\right) .
\end{aligned}
$$

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

- $\sigma_{u^{\prime}}^{i-1}$ and $D_{u^{\prime}}^{i-1}$ 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 $u^{\prime}$, the strategy $\sigma_{u^{\prime}}^{i-1}$ is well defined and $D_{u}^{i-1}$ is also well defined. By induction hypothesis $D_{u}^{i}$ is a $\mathcal{C}$-decision list, so $D_{u}^{i-1}$ is also a $\mathcal{C}$-decision list.
$\checkmark \sigma^{i-1}$ and $D_{u^{\prime}}^{i-1}$ are constructed in linear time w.r.t. $\left|\pi_{i-1}\right|$. This holds by inductive hypothesis and the fact that computing $\neg L_{j}(u / B)$ is linear in $\left|\pi_{i-1}\right|$.
- $D_{u^{\prime}}^{i-1}$ computes $\sigma_{u^{\prime}}^{i-1}$. For $u^{\prime} \neq u$, by induction hypothesis, $D_{u^{\prime}}^{i-{ }^{u^{\prime}}}$ computes $\sigma_{u^{\prime}}^{i}$. The same happens, by construction, for $u^{\prime}=u$.
$\downarrow \sigma^{i-1}$ is a winning strategy for $\mathcal{Q} . \varphi_{i-1}$. 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 $B\left(\tau_{i}(\vec{x})\right)$, 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 $\forall$ 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 $\forall$ 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 $5.1 \quad\left(\mathcal{Q}-C_{n}\right)$. 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

$$
\mathcal{Q}-C_{n}=\exists x_{1} \cdots \exists x_{n} \forall u \exists t_{1} \cdots \exists t_{m} \cdot\left(u \leftrightarrow \neg t_{m}\right) \wedge \bigwedge_{i=1}^{m} G_{i}
$$

where $u \leftrightarrow \neg t_{m} \equiv\left(u \vee t_{m}\right) \wedge\left(\neg u \vee \neg t_{m}\right)$ 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 $\wedge$ of $t_{j}$ and $t_{k}$ then
$G_{i}=t_{i} \leftrightarrow\left(t_{j} \wedge t_{k}\right) \equiv\left(\neg t_{i} \vee t_{j}\right) \wedge\left(\neg t_{i} \vee t_{k}\right) \wedge\left(t_{i} \vee \neg t_{j} \vee \neg t_{k}\right)$,
similarly if gate $i$ computes $\neg, \vee, \oplus, M O D_{p}, T_{k}$ or some other Boolean function.

Informally, the $\mathrm{QBF} \mathcal{Q}-C_{n}$ 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 $\mathcal{C}$ and $\mathcal{C}$-Frege $+\forall$ red.

Theorem 5.2. Let $\mathcal{C}$ be one of the circuit classes $\mathrm{AC}^{0}$, $\mathrm{AC}^{0}[p], \mathrm{TC}^{0}, \mathrm{NC}^{1}, \mathrm{P} /$ poly and let $\left(C_{n}\right)_{n \in \mathbb{N}}$ be a non-uniform family of circuits where $C_{n}$ is a circuit with $n$ inputs. Then the following implications hold:
(i) if the $\operatorname{QBFs} \mathcal{Q}-C_{n}$ have $\mathcal{C}$-Frege $+\forall$ red refutations of size bounded by a function $q(n)$, then for each $n, C_{n}$ is equivalent to a circuit $C_{n}^{\prime}$ where $C_{n}^{\prime}$ is of size $O(q(n))$ and uses the gates and depth allowed in $\mathcal{C}$;
(ii) if $\left(C_{n}\right)_{n \in \mathbb{N}}$ is a polynomial-size circuit family from $\mathcal{C}$ then the $Q B F s \mathcal{Q}-C_{n}$ have polynomial-size refutations in $\mathcal{C}$-Frege $+\forall$ red.

Proof. Regarding ( $i$ ), by the Strategy Extraction Theorem and Proposition 4.2, if the QBF $\mathcal{Q}-C_{n}$ has a refutation in $\mathcal{C}$-Frege $+\forall$ red of size $S$ then a winning strategy for the universal player can be computed by a circuit $C_{n}^{\prime} \in \mathcal{C}$ of size $O(S)$. We have that in $\mathcal{Q}-C_{n}$ the quantifier prefix looks like $\exists x_{1} \cdots \exists x_{n} \forall u \exists \vec{t}$. Now, by construction, $u \not \equiv C_{n}\left(x_{1}, \ldots, x_{n}\right)$, hence a winning strategy for the universal player must consist of playing $u=C_{n}\left(x_{1}, \ldots, x_{n}\right)$. This means that the circuit $C_{n}^{\prime}$ computing the winning strategy for the universal player is equivalent to the circuit $C_{n}$ and the size bound follows.

Regarding (ii), let

$$
\mathcal{Q}-C_{n}=\exists x_{1} \cdots \exists x_{n} \forall u \exists t_{1} \cdots \exists t_{m} .\left(u \leftrightarrow \neg t_{m}\right) \wedge \varphi_{n},
$$

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 $D_{i} \in \mathcal{C}$ such that $t_{i} \leftrightarrow D_{i}$ is derivable in $\mathcal{C}$-Frege with size polynomial in $\left|D_{i}\right|$. Suppose that $t_{i}$ corresponds to a gate $\odot\left(t_{j_{1}}, \ldots, t_{j_{\ell}}\right)$ with fan-in $\ell$, where $\odot$ could be an $\wedge, \vee, \neg, \oplus, M O D_{p}, T_{k}, \ldots$ from the gates allowed in the class $\mathcal{C}$. 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 $\left|D_{j_{k}}\right|$. Moreover, $\mathcal{C}$-Frege is able to prove

$$
\frac{t_{j_{1}} \leftrightarrow D_{j_{1}} \quad \cdots \quad t_{j_{\ell}} \leftrightarrow D_{j_{\ell}} \quad t_{i} \leftrightarrow \odot\left(t_{j_{1}}, \ldots, t_{j_{\ell}}\right)}{t_{i} \leftrightarrow \odot\left(D_{j_{1}}, \ldots, D_{j_{\ell}}\right)} .
$$

Let then $D_{i}=\odot\left(D_{j_{1}}, \ldots, D_{j_{\ell}}\right)$. At the $m$-th step $\mathcal{C}$-Frege proves that $t_{m} \leftrightarrow D_{m}$, from which follows that

$$
\frac{t_{m} \leftrightarrow D_{m} \quad u \leftrightarrow \neg t_{m}}{u \leftrightarrow \neg D_{m}} .
$$

Since now $u$ is universal and the innermost variable of $u \leftrightarrow$ $\neg D_{m}$, we can apply the $\forall$ red rule and get $0 \leftrightarrow \neg D_{m}, 1 \leftrightarrow$ $\neg D_{m}$, which leads to an immediate contradiction in the QBF proof system $\mathcal{C}$-Frege $+\forall$ red.

In particular, a Boolean function $f$ is computable by polynomial-size $\mathcal{C}$ circuits if and only if $\mathcal{Q}-C_{n}$ have polynomialsize $\mathcal{C}$-Frege refutations for each choice of Boolean circuits $\left(C_{n}\right)_{n \in \mathbb{N}}$ computing $f$. Note that the circuits $C_{n}$ are not necessarily circuits from the class $\mathcal{C}$.
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 $\mathrm{AC}^{0}[p]$-Frege $+\forall$ red, regardless of the encoding for Parity.

Corollary 5.3 ( $\mathcal{Q}$-Parity lower bounds). Let $C_{n}$ be a family of polynomial-size circuits computing Parity. For each odd prime $p$ the QBFs $\mathcal{Q}-C_{n}$ require proofs of exponential size in $\mathrm{AC}^{0}[p]$-Frege $+\forall$ red.

Proof. The exponential lower bound for the proof size in $\mathrm{AC}^{0}[p]$-Frege $+\forall$ red follows from Theorem 5.2 and the fact that for each odd prime $p$ any family of bounded-depth circuits with $M O D_{p}$ gates computing Parity must be of exponential size [Razborov, 1987; Smolensky, 1987].
We highlight that non-trivial lower bounds for $\mathrm{AC}^{0}[p]$-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 NC ${ }^{1}$ encodings of Parity in Frege $+\forall$ red.
Corollary 5.4 ( $\mathcal{Q}$-Parity upper bounds). Let $C_{n}$ be a family of $\mathrm{NC}^{1}$ circuits computing Parity. Then the QBFs $\mathcal{Q}-C_{n}$ have polynomial-size proofs in Frege $+\forall$ red.

Proof. By a result of Muller and Preparata [1975], Parity can be computed by circuits in $N C^{1}$. Hence if we consider a family $C_{n}$ of $\mathrm{NC}^{1}$ 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 the QBF proof system $\mathrm{AC}^{0}[2]$-Frege $+\forall$ red, albeit not for arbitrary $\mathrm{NC}^{1}$-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 $\operatorname{Parity}\left(x_{1}, \ldots, x_{n}\right)=\operatorname{Parity}\left(x_{1}, \ldots, x_{n-1}\right) \oplus x_{n}$. This leads to the QBFs

$$
\begin{aligned}
\Phi_{n}=\exists x_{1} \cdots \exists x_{n} \forall u \exists t_{2} \cdots \exists t_{n} .\left(t_{2} \leftrightarrow\left(x_{1} \oplus x_{2}\right)\right) \wedge \\
\bigwedge_{i=3}^{n}\left(t_{i} \leftrightarrow\left(t_{i-1} \oplus x_{i}\right)\right) \wedge\left(u \leftrightarrow \neg t_{n}\right),
\end{aligned}
$$

where $a \leftrightarrow(b \oplus c) \equiv(\neg a \vee \neg b \vee \neg c) \wedge(\neg a \vee b \vee c) \wedge(a \vee$ $\neg b \vee c) \wedge(a \vee b \vee \neg c)$. This formulation of $\mathcal{Q}$-Parity was considered by Beyersdorff et al. [2015a], where the formulas $\Phi_{n}$ are shown to be hard for Q-Res and QU-Res. Here we obtain:

Corollary 5.5. The Parity-formulas $\Phi_{n}$ require refutations of exponential size inAC ${ }^{0}[p]$-Frege $+\forall$ red for each odd prime $p$, but it have polynomial-size $\mathrm{AC}^{0}[2]-F r e g e+\forall$ 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 $\mathrm{AC}^{0}[2]$-Frege $+\forall$ red system uses the connectives $\{\wedge, \vee, \neg, \leftrightarrow, \oplus\}$.
Then it is easy to see, by induction on $i$, that Frege proves $t_{i} \leftrightarrow \oplus\left(x_{1}, x_{2}, \ldots, x_{i}\right)$ with a proof of size linear in $i$. Hence, similarly to what was done in Theorem 5.2, we get

$$
\begin{equation*}
u \leftrightarrow \neg \oplus\left(x_{1}, x_{2}, \ldots, x_{n}\right) . \tag{8}
\end{equation*}
$$

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

$$
1 \leftrightarrow \neg \oplus\left(x_{1}, x_{2}, \ldots, x_{n}\right) \quad \text { and } \quad 0 \leftrightarrow \neg \oplus\left(x_{1}, x_{2}, \ldots, x_{n}\right)
$$

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

$$
\operatorname{MOD}_{p}\left(x_{1}, \ldots, x_{n}\right)= \begin{cases}1 & \text { if } \sum_{i=1}^{n} x_{i} \equiv 0 \quad(\bmod p) \\ 0 & \text { otherwise }\end{cases}
$$

For $r \leq p-1$ let

$$
M O D_{p, r}\left(x_{1}, \ldots, x_{n}\right)= \begin{cases}1 & \text { if } \sum_{i=1}^{n} x_{i} \equiv r \quad(\bmod p) \\ 0 & \text { otherwise }\end{cases}
$$

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

$$
\begin{aligned}
M O D_{p, r}\left(x_{1}, \ldots, x_{i}\right)= & \left(M O D_{p, r}\left(x_{1}, \ldots, x_{i-1}\right) \wedge \neg x_{i}\right) \vee \\
& \left(M O D_{p, r-1}\left(x_{1}, \ldots, x_{i-1}\right) \wedge x_{i}\right)
\end{aligned}
$$

and for $r=0$ by

$$
\begin{aligned}
M O D_{p, 0}\left(x_{1}, \ldots, x_{i}\right)= & \left(M O D_{p, 0}\left(x_{1}, \ldots, x_{i-1}\right) \wedge \neg x_{i}\right) \vee \\
& \left(M O D_{p, p-1}\left(x_{1}, \ldots, x_{i-1}\right) \wedge x_{i}\right)
\end{aligned}
$$

Using variables $s_{i}^{r}$ for $M O D_{p, r}\left(x_{1}, \ldots, x_{i}\right)$ this leads to the QBFs

$$
\begin{aligned}
\Theta_{n}^{p}= & \exists x_{1} \cdots \exists x_{n} \forall u \exists s_{1}^{0} \exists s_{1}^{1} \exists s_{2}^{0} \exists s_{2}^{1} \exists s_{2}^{2} \cdots \exists s_{n}^{0} \cdots \exists s_{n}^{p-1} . \\
& \left(u \leftrightarrow \neg s_{n}^{0}\right) \wedge\left(s_{1}^{1} \leftrightarrow x_{1}\right) \wedge\left(s_{1}^{0} \leftrightarrow \neg x_{1}\right) \wedge \\
& \bigwedge_{\substack{1<i \leq n \\
0<r \leq p-1}}\left(s_{i}^{r} \leftrightarrow\left(s_{i-1}^{r} \wedge \neg x_{i}\right) \vee\left(s_{i-1}^{r-1} \wedge x_{i}\right)\right) \wedge \\
& \bigwedge_{1<i \leq n}\left(s_{i}^{0} \leftrightarrow\left(s_{i-1}^{0} \wedge \neg x_{i}\right) \vee\left(s_{i-1}^{p-1} \wedge x_{i}\right)\right) .
\end{aligned}
$$

Corollary 5.6. For each pair p, q of distinct primes the $M O D_{p}$-formulas $\Theta_{n}^{p}$ require proofs of exponential size in $\mathrm{AC}^{0}[q]$-Frege $+\forall$ red, but have polynomial-size proofs in $\mathrm{AC}^{0}[p]$-Frege $+\forall$ red .

Proof. The exponential lower bound for the QBF proof systemAC ${ }^{0}[q]$-Frege $+\forall$ 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 $M O D_{q}$ gates computing $M O D_{p}$ must be of exponential size.

Regarding the upper bound, without loss of generality we can assume that our $\mathrm{AC}^{0}[p]$-Frege system uses the connectives $\left\{\wedge, \vee, \neg, \leftrightarrow, M O D_{p}\right\}$. Then it is easy to see, by induction on
$i$, that $\mathrm{AC}^{0}[p]$-Frege proves

$$
s_{i}^{r} \leftrightarrow M O D_{p}(x_{1}, \ldots, x_{i}, \underbrace{1,1, \ldots, 1}_{p-r}),
$$

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

$$
\begin{equation*}
u \leftrightarrow \neg M O D_{p}(x_{1}, \ldots, x_{n}, \underbrace{1,1, \ldots, 1}_{p}) . \tag{9}
\end{equation*}
$$

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

$$
\begin{aligned}
& 1 \leftrightarrow \neg \operatorname{MOD}_{p}(x_{1}, \ldots, x_{n}, \underbrace{1,1, \ldots, 1}_{p}) \text { and } \\
& 0 \leftrightarrow \neg M O D_{p}(x_{1}, \ldots, x_{n}, \underbrace{1,1, \ldots, 1}_{p}),
\end{aligned}
$$

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

Corollary 5.7 (LOWER BOUNDS FOR $\mathcal{Q}$-Majority). Let $C_{n}$ be a family of polynomial-size circuits computing $\operatorname{MajORITY}\left(x_{1}, \ldots, x_{n}\right)$. Then for every prime $p$, the QBFs $\mathcal{Q}-C_{n}$ require proofs of exponential size in $\mathrm{AC}^{0}[p]$-Frege $+\forall$ red.

Proof. The lower bound follows again applying Theorem 5.2 and the fact that MAJORITY requires exponential-size bounded-depth circuits with $M O D_{p}$ gates [Razborov, 1987; Smolensky, 1987].

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

Corollary 5.8 ( $\mathcal{Q}$-Majority upper bounds). Let $C_{n}$ be a family of $\mathrm{NC}^{1}$ circuits computing $\operatorname{MAJORITY}\left(x_{1}, \ldots, x_{n}\right)$. Then the QBFs $\mathcal{Q}-C_{n}$ have polynomial-size proofs in the $Q B F$ proof system Frege $+\forall$ red.

Proof. By a result of Muller and Preparata [1975], the function MAJORITY is computable in $\mathrm{NC}^{1}$ and hence $\mathcal{Q}-C_{n}$ are well defined. The upper bound then follows from Theorem 5.2.

As for the $M O D_{p}$ functions, we can improve on this upper bound by considering explicit QBF encodings of MAJORITY, thereby even obtaining a separation of $\mathrm{AC}^{0}[p]$-Frege $+\forall$ red systems from TC ${ }^{0}$-Frege $+\forall$ red. ${ }^{4}$ Explicit QBFs for Majority can be defined using the following property of the $k$-threshold function
$T_{k}\left(x_{1}, \ldots, x_{i}\right) \equiv T_{k}\left(x_{1}, \ldots, x_{i-1}\right) \vee\left(T_{k-1}\left(x_{1}, \ldots, x_{i-1}\right) \wedge x_{i}\right)$.
Using variables $t_{k}^{i}$ for $T_{k}\left(x_{1}, \ldots, x_{i}\right)$ this gives rise to the QBFs

$$
\begin{aligned}
\Psi_{n} & =\exists x_{1} \cdots \exists x_{n} \forall u \exists t_{1}^{1} \cdots \exists t_{n / 2}^{n} \cdot\left(u \leftrightarrow \neg t_{n / 2}^{n}\right) \wedge \\
& \bigwedge_{i \leq n} t_{0}^{i} \wedge\left(t_{1}^{1} \leftrightarrow x_{1}\right) \wedge \bigwedge_{\substack{k \leq n / 2 \\
i \leq n}}\left(t_{k}^{i} \leftrightarrow t_{k}^{i-1} \vee\left(t_{k-1}^{i-1} \wedge x_{i}\right)\right)
\end{aligned}
$$

[^3]Corollary 5.9. For each prime $p$ the Majority-based formulas $\Psi_{n}$ require proofs of exponential-size in the $Q B F$ proof system $\mathrm{AC}^{0}[p]$-Frege $+\forall$ red, but have polynomial-size proofs in $\mathrm{TC}^{0}$-Frege $+\forall$ red .

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

Regarding the polynomial-size proof of the QBF formula $\Psi_{n}$ in $\mathrm{TC}^{0}$-Frege $+\forall$ red we can proceed similarly as for PARITY in Frege. The crucial feature here is that $T_{k}$ are, by definition of $\mathrm{TC}^{0}$, in the language of $\mathrm{TC}^{0}$-Frege. Hence (10) can be used to prove $t_{k}^{j} \leftrightarrow T_{k}\left(x_{1}, \ldots, x_{j}\right)$ and we can easily refute $\Psi_{n}$ in TC $^{0}$-Frege $+\forall$ red.

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

### 5.2 Lower bounds for depth-d Frege systems

We now aim at a fine-grained analysis of $A C^{0}$-Frege by studying its subsystems $\mathrm{AC}_{d}^{0}$-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 $\left(C_{n}\right)_{n \in \mathbb{N}}$ 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 $\mathcal{Q}-C_{n}$ have $\mathrm{AC}_{d}^{0}$-Frege $+\forall$ red refutations of size bounded by a function $q(n)$, then for each $n, C_{n}$ is equivalent to a depth- $(d+2)$ circuit $C_{n}^{\prime}$ of size $O(q(n))$;
(ii) if $\left(C_{n}\right)_{n \in \mathbb{N}}$ is a family of polynomial-size depth-d circuits, then the $Q B F s \mathcal{Q}-C_{n}$ have polynomial-size refutations in $\mathrm{AC}_{d}^{0}$-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 $\mathcal{Q}-C_{n}$ in $\mathrm{AC}_{d}^{0}$-Frege $+\forall$ red of size $S$ we can extract a winning strategy for the universal player that can be computed by $\mathrm{AC}_{d}^{0}$-decision lists of size $O(S)$. By Proposition 4.2, this means that the winning strategy can be also computed by $\mathrm{AC}_{d+2}^{0}$ 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 $\mathcal{Q}-C_{n}$ has polynomial-size refutations in $\mathrm{AC}_{d+2}^{0}$-Frege $+\forall$ red. Here we want to prove that $\mathcal{Q}-C_{n}$ has actually polynomialsize proofs in $\mathrm{AC}_{d}^{0}$-Frege $+\forall$ red. Without loss of generality suppose that the last gate $t_{m}$ of $C_{n}$ is an $\Lambda$, that is

$$
\begin{aligned}
\mathcal{Q}-C_{n}=\exists x_{1} \cdots \exists x_{n} \forall u \exists t_{1} \cdots \exists t_{m} \cdot & \left(u \leftrightarrow \neg t_{m}\right) \wedge \\
& \wedge\left(t_{m} \leftrightarrow \bigwedge_{j \leq \ell} t_{i_{j}}\right) \wedge \varphi_{n},
\end{aligned}
$$

where each $t_{i_{j}}$ is an $\bigvee$ gate and $\varphi_{n}$ is the encoding of the rest of the circuit $C_{n}$. We clearly have that

$$
\frac{u \leftrightarrow \neg t_{m} \quad t_{m} \leftrightarrow \bigwedge_{j \leq \ell} t_{i_{j}}}{u \leftrightarrow \bigvee_{j \leq \ell} \neg t_{i_{j}}}
$$

From which we obtain both

$$
\begin{align*}
& u \vee \bigwedge_{j \leq \ell} t_{i_{j}}  \tag{11}\\
& \neg u \vee \bigvee_{j \leq \ell} \neg t_{i_{j}} \tag{12}
\end{align*}
$$

Now we can proceed, similarly as in Theorem 5.2. By induction (on the depth of $C_{n}$ ) $\mathrm{AC}_{d}^{0}$-Frege is able to substitute $t_{i_{j}}$ with $D_{i_{j}}$ where $D_{i_{j}}$ is an $\mathrm{AC}_{d-1}^{0}$-formula over the $x_{1}, \ldots, x_{n}$ variables starting with an $\bigvee$. More precisely by induction we can prove that $\mathrm{AC}_{d}^{0}$-Frege proves both

$$
\begin{align*}
& t_{i_{j}} \vee \neg D_{i_{j}}  \tag{13}\\
& \neg t_{i_{j}} \vee D_{i_{j}} \tag{14}
\end{align*}
$$

Hence from (12) and (13) follows that $\neg u \vee \bigvee_{j \leq \ell} \neg D_{i_{j}}$, which is an $\mathrm{AC}_{d}^{0}$-formula only over the variables $u, x_{1}, \ldots, x_{n}$. Hence by the $\forall$ red rule we get

$$
\begin{equation*}
\bigvee_{j \leq \ell} \neg D_{i_{j}} \tag{15}
\end{equation*}
$$

Similarly from (11) we get first that $\bigwedge_{j \leq \ell}\left(u \vee t_{i_{j}}\right)$ and then using (14) we get $\bigwedge_{j \leq \ell}\left(u \vee D_{i_{j}}\right)$, which, again, is an $\mathrm{AC}_{d^{-}}^{0}$ formula over the variab̄les $u, x_{1}, \ldots, x_{n}$. By the $\forall$ red rule we get

$$
\begin{equation*}
\bigwedge_{j \leq \ell} D_{i_{j}} . \tag{16}
\end{equation*}
$$

From (15) and (16) follows immediately a contradiction.
From Theorem 5.2 we immediately obtain a wealth of lower bounds for Res $+\forall$ red.

Corollary 5.11. Let $f\left(x_{1}, \ldots, x_{n}\right)$ be a Boolean function requiring exponential-size depth-3 circuits and let $\left(C_{n}\right)_{n \in \mathbb{N}}$ be polynomial-size circuits (of unbounded depth) computing $f$. Then the $Q B F s$ Q $-C_{n}$ require exponential-size refutations in $\mathrm{AC}_{1}^{0}$-Frege $+\forall$ red and hence, in particular, in Res $+\forall$ red.

We now prove a separation of constant-depth Frege $+\forall$ red systems. For this we employ the Sipser functions separating the hierarchy of constant-depth circuits. We quote the definition of the $\mathrm{SIPSER}_{d}$ function from Boppana and Sipser [1990]:

$$
\operatorname{SIPSER}_{d}=\bigwedge_{i_{1} \leq m_{1}} \bigvee_{i_{2} \leq m_{2}} \bigwedge_{i_{3} \leq m_{3}} \cdots \bigodot_{i_{d} \leq m_{d}} x_{i_{1} i_{2} i_{3} \ldots i_{d}}
$$

where $\bigodot=\bigvee$ or $\bigwedge$ depending on the parity of $d$. The variables $x_{1}, \ldots, x_{n}$ appear as $x_{i_{1} i_{2} i_{3} \ldots i_{d}}$ for $i_{j} \leq m_{j}$, where $m_{1}=\sqrt{m / \log m}, m_{2}=m_{3}=\cdots=m_{d-1}=m, m_{d}=$ $\sqrt{d m \log m / 2}$ and $m=(n \sqrt{2 / d})^{1 /(d-1)}$.

Corollary 5.12. Fix an integer $d \geq 2$. Let $\left(C_{d}^{n}\right)_{n \in \mathbb{N}}$ be a family of polynomial-size depth- $(d+3)$ circuits computing the function $\operatorname{SiPSER}_{d+3}\left(x_{1}, \ldots, x_{n}\right)$. Then the QBFs $\mathcal{Q}-C_{d}^{n}$ need exponential-size proofs in $\mathrm{AC}_{d}^{0}$-Frege $+\forall$ red, but have polynomial-size proofs in $\mathrm{AC}_{d+3}^{0}$-Frege $+\forall$ red.

Proof. The lower bound follows from Theorem 5.10 and from the result that for every $d$, $\operatorname{SIPSER}_{d+3}$ needs exponentialsize depth- $(d+2)$ circuits [Håstad, 1986]. Regarding the upper bound, by construction $C_{d}^{n}$ has depth $d+3$ and polynomial-size. Hence, by Theorem 5.10, the family $\mathcal{Q}-C_{d}^{n}$ has polynomial-size proofs in $\mathrm{AC}_{d+3}^{0}$-Frege $+\forall$ red.

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- $d$ 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 $+\forall$ red and EF $+\forall$ 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 $\mathcal{C}$ be either $\mathrm{P} /$ poly or non-uniform $\mathrm{NC}^{1}$. If PSPACE $\not \subset \mathcal{C}$ then the $\mathcal{C}$-Frege $+\forall$ red is not polynomially bounded.

Proof. Let $f$ be a Boolean function in PSPACE but not in $\mathcal{C}$. Since QBF is PSPACE-complete there exists a QBF $\mathcal{Q} \vec{w} \cdot \varphi\left(\vec{w}, x_{1}, \ldots, x_{n}\right)$ with a CNF $\varphi$ such that

$$
f\left(x_{1}, \ldots, x_{n}\right) \equiv \mathcal{Q} \vec{w} \cdot \varphi\left(\vec{w}, x_{1}, \ldots, x_{n}\right) .
$$

We define

$$
\mathcal{Q}-f_{n}=\exists x_{1} \cdots \exists x_{n} \forall u \cdot\left(u \leftrightarrow \mathcal{Q} \vec{w} \cdot \varphi\left(\vec{w}, x_{1}, \ldots, x_{n}\right)\right),
$$

which can be rewritten into formulas $\Theta_{n}$ in prenex form. Notice that the only winning strategy for the universal player on both $\mathcal{Q}-f_{n}$ and $\Theta_{n}$ is to compute $u=f\left(x_{1}, \ldots, x_{n}\right)$. Therefore, the Strategy Extraction Theorem together with $f \notin \mathcal{C}$ immediately implies super-polynomial lower bounds for $\Theta_{n}$ in $\mathcal{C}$-Frege $+\forall$ red.

We remark that we do have a separation between uniform $N C^{1}$ and PSPACE, because $N C^{1} \subseteq L$ and $L \neq$ PSPACE by the space hierarchy theorem. Therefore, choosing $f \in$ PSPACE $\backslash$ $\mathrm{NC}^{1}$ and considering the prenex formulas $\Theta_{n}$ arising from $\mathcal{Q}-f_{n}$ we can infer the weaker result that Frege $+\forall$ red has no uniform short proofs of $\Theta_{n}$.

## 6. 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 $+\forall$ 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.

## 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).
This work was completed while the 2nd author was affiliated to the Computer Science Department of Sapienza University of Rome (Italy). The 2nd author was funded by the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement no. 279611.

## References

Miklós Ajtai. The complexity of the pigeonhole-principle. Combinatorica, 14(4):417-433, 1994.

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

Valeriy Balabanov and Jie-Hong R. Jiang. Unified QBF certification and its applications. Form. Methods Syst. Des., 41(1):45-65, August 2012.

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

Paul Beame and Toniann Pitassi. Propositional proof complexity: Past, present, and future. In G. Paun, G. Rozenberg, and A. Salomaa, editors, Current Trends in Theoretical Computer Science: Entering the 21st Century, pages 42-70. World Scientific Publishing, 2001.

Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow - resolution made simple. Journal of the ACM, 48(2): 149-169, 2001.

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

Olaf Beyersdorff and Oliver Kullmann. Unified characterisations of resolution hardness measures. In SAT, pages 170-187, 2014.

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

Olaf Beyersdorff, Leroy Chew, and Mikolás Janota. Proof complexity of resolution-based QBF calculi. In 32nd International Symposium on Theoretical Aspects of Computer Science (STACS 2015), pages 76-89, 2015a.

Olaf Beyersdorff, Leroy Chew, Meena Mahajan, and Anil Shukla. Feasible interpolation for QBF resolution calculi. In ICALP. Springer, 2015b.

Archie Blake. Canonical Expressions in Boolean Algebra. PhD thesis, 1937. University of Chicago.

Maria Luisa Bonet, Toniann Pitassi, and Ran Raz. On interpolation and automatization for Frege systems. SIAM Journal on Computing, 29(6):1939-1967, 2000.

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

Ravi B. Boppana and Michael Sipser. Handbook of theoretical computer science (vol. A). chapter The Complexity of Finite Functions, pages 757-804. MIT Press, Cambridge, MA, USA, 1990.
Samuel R. Buss. Towards NP-P via proof complexity and search. Ann. Pure Appl. Logic, 163(7):906-917, 2012.

Samuel R. Buss and Peter Clote. Cutting planes, connectivity, and threshold logic. Archive for Mathematical Logic, 35 (1):33-62, 1996.

Matthew Clegg, Jeff Edmonds, and Russell Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In Proc. 28th ACM Symposium on Theory of Computing, pages 174-183, 1996.

Stephen A. Cook and Tsuyoshi Morioka. Quantified propositional calculus and a second-order theory for NC1. Arch. Math. Log., 44(6):711-749, 2005.

Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. Journal of Symbolic Logic, 6:169-184, 1979.

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

Uwe Egly. On sequent systems and resolution for qbfs. In Theory and Applications of Satisfiability Testing - SAT 2012, pages 100-113, 2012.

Uwe Egly, Martin Kronegger, Florian Lonsing, and Andreas Pfandler. Conformant planning as a case study of incremental QBF solving. In Artificial Intelligence and Symbolic Computation AISC 2014, pages 120-131, 2014.

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

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

Johan Håstad. Almost optimal lower bounds for small depth circuits. In Proc. 18th STOC, pages 6-20. ACM Press, 1986.

Marijn Heule, Martina Seidl, and Armin Biere. A unified proof system for QBF preprocessing. In IJCAR, pages 91-106, 2014.

Pavel Hrubeš. On lengths of proofs in non-classical logics. Annals of Pure and Applied Logic, 157(2-3):194-205, 2009.
Mikolás Janota and Joao Marques-Silva. Expansion-based QBF solving versus Q-resolution. Theor. Comput. Sci., 577:25-42, 2015.

Emil Jeřábek. Weak pigeonhole principle, and randomized computation. PhD thesis, Faculty of Mathematics and Physics, Charles University, Prague, 2005.

Emil Jeřábek. Substitution Frege and extended Frege proof systems in non-classical logics. Annals of Pure and Applied Logic, 159(1-2):1-48, 2009.

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

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

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

Jan Krajíček and Pavel Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. The Journal of Symbolic Logic, 54(3): 1063-1079, 1989.

Jan Krajíček and Pavel Pudlák. Quantified propositional calculi and fragments of bounded arithmetic. Zeitschrift für mathematische Logik und Grundlagen der Mathematik, 36:29-46, 1990.

Jan Krajíček and Pavel Pudlák. Some consequences of cryptographical conjectures for $S_{2}^{1}$ and $E F$. Information and Computation, 140(1):82-94, 1998.

Jan Krajíček, Pavel Pudlák, and Alan Woods. Exponential lower bounds to the size of bounded depth Frege proofs of the pigeonhole principle. Random Structures and Algorithms, 7(1):15-39, 1995.

David E. Muller and Franco P. Preparata. Bounds to complexities of networks for sorting and for switching. J. ACM, 22(2):195-201, 1975.

Toniann Pitassi, Paul Beame, and Russell Impagliazzo. Exponential lower bounds for the pigeonhole principle. Computational Complexity, 3:97-140, 1993.

Pavel Pudlák. Lower bounds for resolution and cutting planes proofs and monotone computations. The Journal of Symbolic Logic, 62(3):981-998, 1997.

Alexander A. Razborov. Lower bounds for the size of circuits of bounded depth with basis $\{\&, \oplus\}$. Math. Notes Acad. Sci. USSR, 41(4):333-338, 1987.

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

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

John Alan Robinson. A machine-oriented logic based on the resolution principle. J. ACM, 12(1):23-41, 1965.

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

Roman Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In Proc. of 19th ACM STOC, pages 77-82, 1987.

Allen Van Gelder. Contributions to the theory of practical quantified Boolean formula solving. In $C P$, pages 647-663, 2012.


[^0]:    ${ }^{1}$ We will consistently treat $\mathcal{C}$-Frege systems as operating with lines from $\mathcal{C}$. As Res operates with clauses we will call it a $\mathrm{AC}_{1}^{0}$-Frege system even though it refutes CNFs, which are depth 2.

[^1]:    ${ }^{2}$ In the case where $\mathcal{C}$ is $\mathrm{AC}_{1}^{0}$ we require that $\varphi=L_{1} \wedge \cdots \wedge L_{m}$ where $L_{j}$ are lines in $\mathrm{AC}_{1}^{0}$-Frege.

[^2]:    ${ }^{3}$ Note that, contrasting the usual setting of Q-Res [Kleine Büning et al., 1995], our definition of Res $+\forall$ red does not need to disallow tautologous resolvents as these will always be reduced to $T$.

[^3]:    ${ }^{4}$ Clearly, such a separation already follows from Corollary 5.6 together with the simulation of $\mathrm{AC}^{0}[p]$-Frege $+\forall$ red by $\mathrm{TC}^{0}-$ Frege $+\forall$ red. Here we will prove the stronger result that all these systems are separated by one natural principle, namely Majority.

