
Proceedings Paper:
Beyersdorff, O, Bonacina, I and Chew, L (2016) Lower bounds: from circuits to QBF proof systems. In: Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science. ITCS '16, 14-16 Jan 2016, Cambridge, Massachusetts, USA. ACM , pp. 249-260. ISBN 978-1-4503-4057-1

https://doi.org/10.1145/2840728.2840740

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

October 17, 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 $P + \forall\mathsf{red}$, 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 $\mathcal{C}$-Frege $+ \forall\mathsf{red}$ that parallels the well-studied propositional hierarchy of $\mathcal{C}$-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 $\mathcal{C}$-Frege $+ \forall\mathsf{red}$.

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 $\mathsf{AC}^0[p]$-Frege $+ \forall\mathsf{red}$ for all primes p;

(ii) an exponential separation of $\mathsf{AC}^0[p]$-Frege $+ \forall\mathsf{red}$ from TC^0-Frege $+ \forall\mathsf{red}$;

(iii) an exponential separation of the hierarchy of constant-depth systems AC^0_d-Frege $+ \forall\mathsf{red}$ 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 φ and a proof system P, typically comprised of axioms and rules, what is the size of the smallest proof of φ 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 $\mathsf{AC}^0 \subset \mathsf{AC}^0[p] \subset \mathsf{TC}^0 \subseteq \mathsf{NC}^1 \subseteq \mathsf{P/poly}$, giving rise to a similar hierarchy of Frege systems.

While the strongest non-uniform lower bounds known in circuit complexity hold for the class $\mathsf{AC}^0[p]$ (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 $\mathsf{AC}^0[p]$ circuit lower to a proof size lower bound in $\mathsf{AC}^0[p]$-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 ($= \mathsf{NC}^1$-Frege) or even extended Frege ($= \mathsf{P/poly}$-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 $\mathsf{AC}^0[p]$-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 $P + \forall\mathsf{red}$ for closed prenex QBFs (Definition 3.1). Throughout the proof, the quantifier prefix is fixed, and lines in the system $P + \forall\mathsf{red}$ 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 $P + \forall\mathsf{red}$ 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 $\forall\mathsf{red}$ 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 $\forall\mathsf{red}$ rule, resulting in a natural and robust system $P + \forall\mathsf{red}$.

Our new systems $P + \forall\mathsf{red}$ 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 $P + \forall\mathsf{red}$ 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 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.

(a) Lower bounds and separations for $\mathsf{AC}^0[p]$-Frege + $\forall$red. By the seminal results of (Razborov, 1987; Smolensky, 1987), Parity and more generally MOD_q are the classic examples for functions that require exponential-size bounded-depth circuits with MOD_p gates, where p and q are different primes. Using these functions, we define families of QBFs that require exponential-size proofs in $\mathsf{AC}^0[p]$-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 MOD_q formulas directly from (arbitrary) NC^1-circuits computing these functions, we obtain polynomial-size upper bounds in Frege + $\forall$red. However, when carefully choosing specific and indeed very natural encodings, we can prove upper bounds for the MOD_q formulas even in $\mathsf{AC}^0[q]$-Frege + $\forall$red, thus obtaining exponential separations of all the $\mathsf{AC}^0[p]$-Frege + $\forall$red systems for distinct primes p.

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

(b) Separating $\mathsf{AC}^0[p]$-Frege + $\forall$red from TC^0-Frege + $\forall$red. Majority is another classic function in circuit complexity, for which exponential lower bounds are known for constant-depth circuits with MOD_p gates for each prime p (Razborov, 1987; Smolensky, 1987). Using our technique, we transfer these to lower bounds in $\mathsf{AC}^0[p]$-Frege + $\forall$red for all primes p. Carefully

choosing the QBF encoding of MAJORITY, we obtain polynomial upper bounds for the MAJORITY formulas in TC^0-$\mathsf{Frege}+\forall\mathsf{red}$, thus proving an exponential separation between $\mathsf{AC}^0[p]$-$\mathsf{Frege}+\forall\mathsf{red}$ and TC^0-$\mathsf{Frege}+\forall\mathsf{red}$. Again, such a separation is wide open in propositional proof complexity.

(c) Separating the AC^0_d-$\mathsf{Frege}+\forall\mathsf{red}$ hierarchy by CNFs. As a third example for our approach we investigate the fine structure of AC^0-$\mathsf{Frege}+\forall\mathsf{red}$, comprising all AC^0_d-$\mathsf{Frege}+\forall\mathsf{red}$ 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 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 AC^0_{d-3}-$\mathsf{Frege}+\forall\mathsf{red}$ from AC^0_d-$\mathsf{Frege}+\forall\mathsf{red}$, where the increased gap of size 3 comes from our transformation of $\mathcal{C}$-decision lists into $\mathcal{C}$-circuits.

The SIPSER$_d$ formulas achieving these separations are prenexed CNFs, i.e. the formulas have depth 2. While in propositional proof complexity the hierarchy of AC^0_d-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 AC^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., 2000a, 2004; Krajíček and Pudlák, 1998) feasible interpolation is not applicable to strong systems such as 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.

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 $\mathcal{C}$-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.

More widely, in Section 6, we complement the reduction systems $P + \forall$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 $P + \forall$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 $\mathcal{C}$ 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 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

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 φ we denote by $\varphi[x_1/\theta_1, \ldots, x_k/\theta_k]$ the formula φ where variables x_i have been substituted by formulas θ_i.

Circuit classes. We recall the definitions of standard circuit classes used in this paper. The class AC^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 AC^0_d. The class $\mathsf{AC}^0[p]$ uses bounded-depth circuits with MOD_p gates determining whether the sum of the inputs is 0 modulo p, and in TC^0 bounded-depth circuits with threshold gates are permitted. Stronger classes are obtained by using NC^1 circuits of polynomial size and logarithmic depth, and by $\mathsf{P/poly}$ 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 $\mathcal{L}$ is a polynomial-time onto function $P : \{0,1\}^* \to \mathcal{L}$. Each string $\varphi \in \mathcal{L}$ is a *theorem* and if $P(\pi) = \varphi$, π is a *proof* of φ in P. Given a polynomial-time function $P : \{0,1\}^* \to \{0,1\}^*$ the fact that $P(\{0,1\}^*) \subseteq \mathcal{L}$ is the *soundness property* for $\mathcal{L}$ and the fact that $P(\{0,1\}^*) \supseteq \mathcal{L}$ 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 *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 $\mathcal{L}$, 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 $\bot$.

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 AC^0-Frege) are Frege systems where lines are formulas with negations only on variables and with a bounded number of alternations between $\wedge$'s and $\vee$'s. If the number of alternations is at most d, then the proof system is called AC^0_d-Frege. Bounded-depth Frege is called AC^0-Frege since lines in an AC^0-Frege proof are representable as AC^0-circuits.

Resolution (Res) is a particular kind of AC^0_1-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

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

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

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

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 $T_k(x_1, \ldots, x_n)$. The T_k predicate is true when at least k of its inputs are true. Two different, but equivalent, formalizations of TC^0-Frege proof systems are given by Buss and Clote (1996) and Bonet et al. (2000b).

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

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

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 φ 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.

[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 AC^0_1-Frege system even though it refutes CNFs, which are depth 2.

Given a variable y, either existentially quantified or universally quantified in $\mathcal{Q}\,.\,\varphi$, the *quantification level* of y in $\mathcal{Q}\,.\,\varphi$, $\mathrm{qlv}(y)$, is the number of alternations of quantifiers y has on 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 $\mathrm{qlv}(y)$ as variables *left* of y; analogously the variables with quantification lever higher than $\mathrm{qlv}(y)$ will be *right* of y.

A 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 φ evaluates to 1 under the assignment constructed in the game. The universal player wins if φ evaluates to 0. Given a universal variable u with index i, a *strategy for* u is a function from all variables of index $< i$ to $\{0,1\}$. A QBF is false 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 $\dfrac{C \vee x \qquad D \vee \neg x}{C \vee D}$ 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 ($\mathcal{C}$-Frege + $\forall$red)**.** *A refutation of a false QBF $\mathcal{Q}\,.\,\varphi$ 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] $L_\ell = \bot$ and each L_i is inferred from previous lines L_j using the inference rules of $\mathcal{C}$-Frege or using the following rule*

$$\frac{L_j}{L_j[u/B]}\ (\forall\mathsf{red}),$$

[2] In the case where $\mathcal{C}$ is AC^0_1 we require that $\varphi = L_1 \wedge \cdots \wedge L_m$ where L_j are lines in AC^0_1-Frege.

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.

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, 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 Res as our propositional proof system, which is an AC^0_1-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 $\top$.[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 $\mathcal{C}$, $\mathcal{C}$-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 $(L_1, \ldots, L_\ell)$ 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 $L_\ell = \{\bot\}$ and $\mathcal{Q}\,.\,\varphi_\ell \equiv \bot$.

Since $\mathcal{Q}\,.\,\varphi = \mathcal{Q}\,.\,\varphi_0$ the base case of the induction holds.

We show now that $\mathcal{Q}\,.\,\varphi \models \mathcal{Q}\,.\,\varphi_i$ implies $\mathcal{Q}\,.\,\varphi \models \mathcal{Q}\,.\,\varphi_{i+1}$. By definition, $\varphi_{i+1} = (\varphi_i \wedge L_{i+1})$ 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 $\varphi_i \models \varphi_{i+1}$ and clearly $\mathcal{Q}\,.\,\varphi \models \mathcal{Q}\,.\,\varphi_i \models \mathcal{Q}\,.\,\varphi_{i+1}$.

[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 $\top$.

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 $\mathcal{Q} \,.\, \varphi_i = \mathcal{Q}_1\vec{x}\,\forall u\,\mathcal{Q}_2\vec{y} \,.\, \varphi_i$, then we have the following chain of equivalences

$$\begin{aligned}
\mathcal{Q} \,.\, \varphi_i &= \mathcal{Q}_1\vec{x}\,\forall u\,\mathcal{Q}_2\vec{y} \,.\, \varphi_i && (1)\\
&\equiv \mathcal{Q}_1\vec{x}\,\forall u\,\mathcal{Q}_2\vec{y} \,.\, \varphi_i \wedge L_j && (2)\\
&\equiv \mathcal{Q}_1\vec{x}\Big(\big(\mathcal{Q}_2\vec{y} \,.\, \varphi_i[u/0] \wedge L_j[u/0]\big) \wedge \big(\mathcal{Q}_2\vec{y} \,.\, \varphi_i[u/1] \wedge L_j[u/1]\big)\Big) && (3)\\
&\equiv \mathcal{Q}_1\vec{x}\Big(L_j[u/0] \wedge L_j[u/1] \wedge \big(\mathcal{Q}_2\vec{y} \,.\, \varphi_i[u/0]\big) \wedge \big(\mathcal{Q}_2\vec{y} \,.\, \varphi_i[u/1]\big)\Big) && (4)\\
&\equiv \mathcal{Q}_1\vec{x}\Big(L_j[u/0] \wedge L_j[u/1] \wedge \forall u\mathcal{Q}_2\vec{y} \,.\, \varphi_i\Big) && (5)\\
&\equiv \mathcal{Q}_1\vec{x}\Big(L_j[u/0] \wedge L_j[u/1] \wedge L_j[u/B] \wedge \forall u\mathcal{Q}_2\vec{y} \,.\, \varphi_i\Big) && (6)\\
&\equiv \mathcal{Q}_1\vec{x}\forall u\mathcal{Q}_2\vec{y} \,.\, \varphi_i \wedge L_j[u/0] \wedge L_j[u/1] \wedge L_j[u/B]. && (7)
\end{aligned}$$

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

$$\mathcal{Q} \,.\, \varphi_i \models \mathcal{Q}_1\vec{x}\forall u\mathcal{Q}_2\vec{y} \,.\, \varphi_i \wedge L_j[u/B],$$

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 for QBF Frege systems

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

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

$$\begin{array}{l}
\texttt{if } C_1(\vec{x}) \texttt{ then } u \leftarrow B_1(\vec{x})\texttt{;}\\
\quad \texttt{else if } C_2(\vec{x}) \texttt{ then } u \leftarrow B_2(\vec{x})\texttt{;}\\
\qquad\qquad \vdots\\
\qquad \texttt{else if } C_{\ell-1}(\vec{x}) \texttt{ then } u \leftarrow B_{\ell-1}(\vec{x})\texttt{;}\\
\qquad\quad \texttt{else } u \leftarrow B_\ell(\vec{x})\texttt{,}
\end{array}$$

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 $D' \in \mathcal{C}$ computing the same function g, such that the size of D' is linear in the size of D and*

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

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_ℓ 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 + ∀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 $\mathcal{Q}\,.\,\varphi$ and a refutation π of $\mathcal{Q}\,.\,\varphi$ in $\mathcal{C}$-Frege + ∀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 φ.*

Proof. Let $\pi = (L_1, \ldots, L_\ell)$ be a refutation of the false QBF $\mathcal{Q}\,.\,\varphi$ 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 π_i it is possible to construct in linear time (w.r.t. $|\pi_i|$) a winning strategy σ^i for the universal player for the QBF formula $\mathcal{Q}\,.\,\varphi_i$, 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^i_u computing σ^i_u as a function of the variables in $\mathcal{Q}$ left of u, having size $O(|\pi_i|)$.

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

We show now how to construct σ^{i-1}_u and D^{i-1}_u from σ^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 $D^{i-1}_u = D^i_u$.
- Assume that L_i is the result of an application of a ∀red rule, that is $\dfrac{L_j}{L_j[u/B]}$, 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 $\vec{x}_{u'}$ denote the variables on the left of u' in the quantifier prefix of $\mathcal{Q}\,.\,\varphi$. 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:

$$\texttt{if } \neg L_j[u/B](\vec{x}_u) \texttt{ then } u \leftarrow B(\vec{x}_u); \\ \texttt{else } D^u_i(\vec{x}_u).$$

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.

▶ *σ^{i-1} and $D^{i-1}_{u'}$ are constructed in linear time w.r.t. $|\pi_{i-1}|$.* This holds by inductive hypothesis and the fact that computing $\neg L_j(u/B)$ 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 $u' = u$.

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

If L_i is derived by some Frege rule, then $\sigma^{i-1} = \sigma^i$ and $\tau_{i-1} = \tau_i$. Hence by induction hypothesis, τ_i falsifies a conjunct from φ_i. To argue that τ_{i-1} also falsifies a conjunct from φ_{i-1} we only need to look at the case when the falsified conjunct is L_i. As L_i is false under τ_i and L_i is derived by 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 τ_{i-1} falsifies φ_{i-1}.

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

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 π has size that is actually linear in the number of applications of the $\forall$red rule in π. 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 π.

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 ($\mathcal{Q}$-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*

$$\mathcal{Q}\text{-}C_n = \exists x_1 \cdots \exists x_n \forall u \exists t_1 \cdots \exists t_m \,.\, (u \leftrightarrow \neg t_m) \wedge \bigwedge_{i=1}^{m} G_i,$$

where $u \leftrightarrow \neg t_m \equiv (u \vee t_m) \wedge (\neg u \vee \neg t_m)$ 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 $\wedge$ of t_j and t_k then

$$G_i = t_i \leftrightarrow (t_j \wedge t_k) \equiv (\neg t_i \vee t_j) \wedge (\neg t_i \vee t_k) \wedge (t_i \vee \neg t_j \vee \neg t_k),$$

similarly if gate i computes $\neg$, $\vee$, $\oplus$, MOD_p, T_k or some other Boolean function.

Informally, the 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 AC^0, $\mathsf{AC}^0[p]$, TC^0, NC^1, $\mathsf{P/poly}$ 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 $\mathcal{Q}$-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 where C'_n is of size $O(q(n))$ and uses the gates and depth allowed in $\mathcal{C}$;

(ii) if $(C_n)_{n\in\mathbb{N}}$ is a polynomial-size circuit family from $\mathcal{C}$ then the QBFs $\mathcal{Q}$-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 $C'_n \in \mathcal{C}$ 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, $u \not\equiv C_n(x_1, \ldots, x_n)$, 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 $\mathcal{Q}$-$C_n = \exists x_1 \cdots \exists x_n \forall u \exists t_1 \cdots \exists t_m \,.\, (u \leftrightarrow \neg t_m) \wedge \varphi_n$, where φ_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 $|D_i|$. Suppose that t_i corresponds to a gate $\odot(t_{j_1}, \ldots, t_{j_\ell})$ with fan-in ℓ, where $\odot$ could be an $\wedge, \vee, \neg, \oplus, MOD_p, T_k, \ldots$ 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 $|D_{j_k}|$. Moreover, $\mathcal{C}$-Frege is able to prove

$$\frac{t_{j_1} \leftrightarrow D_{j_1} \qquad \cdots \qquad t_{j_\ell} \leftrightarrow D_{j_\ell} \qquad t_i \leftrightarrow \odot(t_{j_1}, \ldots, t_{j_\ell})}{t_i \leftrightarrow \odot(D_{j_1}, \ldots, D_{j_\ell})} \,.$$

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

$$\frac{t_m \leftrightarrow D_m \qquad u \leftrightarrow \neg t_m}{u \leftrightarrow \neg D_m} \,.$$

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

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

which leads to an immediate contradiction in $\mathcal{C}$-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 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 $\mathcal{C}$.

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 $\mathsf{AC}^0[p]$-$\mathsf{Frege}+\forall\mathsf{red}$, regardless of the encoding for PARITY.

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

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

We highlight that non-trivial lower bounds for $\mathsf{AC}^0[p]$-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 $\mathsf{Frege}+\forall\mathsf{red}$.

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

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

In fact, this upper bound can be improved to $\mathsf{AC}^0[2]$-$\mathsf{Frege}+\forall\mathsf{red}$, albeit not for arbitrary 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 $\textsc{Parity}(x_1,\dots,x_n)=\textsc{Parity}(x_1,\dots,x_{n-1})\oplus x_n$. This leads to the QBFs

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

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 Φ_n are shown to be hard for Q-Res and QU-Res. Here we obtain:

Corollary 5.5. *The* PARITY*-formulas Φ_n require exponential-size* $\mathsf{AC}^0[p]$-$\mathsf{Frege}+\forall\mathsf{red}$ *for each odd prime p, but have polynomial-size* $\mathsf{AC}^0[2]$-$\mathsf{Frege}+\forall\mathsf{red}$ *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 $\mathsf{AC}^0[2]$-$\mathsf{Frege}+\forall\mathsf{red}$ system uses the connectives $\{\wedge,\vee,\neg,\leftrightarrow,\oplus\}$.

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

$$u\leftrightarrow\neg\oplus(x_1,x_2,\dots,x_n). \tag{8}$$

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

$$1\leftrightarrow\neg\oplus(x_1,x_2,\dots,x_n)\quad\text{and}\quad 0\leftrightarrow\neg\oplus(x_1,x_2,\dots,x_n),$$

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* $\mathsf{AC}^0[p]$-$\mathsf{Frege}+\forall\mathsf{red}$ systems. For this we consider the function

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

For $r \leq p-1$ let

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

If we want to use MOD_p for a separation of $\mathsf{AC}^0[p]$-$\mathsf{Frege}+\forall\mathsf{red}$ and $\mathsf{AC}^0[q]$-$\mathsf{Frege}+\forall\mathsf{red}$ 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 Parity, an arbitrary NC^1 encoding as in Corollary 5.3 will also not work (this would just give upper bounds in $\mathsf{Frege}+\forall\mathsf{red}$), 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

$$MOD_{p,r}(x_1,\dots,x_i)=(MOD_{p,r}(x_1,\dots,x_{i-1})\wedge\neg x_i)\vee(MOD_{p,r-1}(x_1,\dots,x_{i-1})\wedge x_i),$$

and for $r=0$ by

$$MOD_{p,0}(x_1,\dots,x_i)=(MOD_{p,0}(x_1,\dots,x_{i-1})\wedge\neg x_i)\vee(MOD_{p,p-1}(x_1,\dots,x_{i-1})\wedge x_i).$$

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

$$\begin{aligned}\Theta_n^p =&\exists x_1\cdots\exists x_n\forall u\exists s_1^0\exists s_1^1\exists s_2^0\exists s_2^1\exists s_2^2\cdots\exists s_n^0\cdots\exists s_n^{p-1}\,.\,(u\leftrightarrow\neg s_n^0)\wedge(s_1^1\leftrightarrow x_1)\wedge(s_1^0\leftrightarrow\neg x_1)\wedge\\ &\bigwedge_{\substack{1<i\leq n\\ 0<r\leq p-1}}\Big(s_i^r\leftrightarrow(s_{i-1}^r\wedge\neg x_i)\vee(s_{i-1}^{r-1}\wedge x_i)\Big)\wedge\bigwedge_{1<i\leq n}\Big(s_i^0\leftrightarrow(s_{i-1}^0\wedge\neg x_i)\vee(s_{i-1}^{p-1}\wedge x_i)\Big).\end{aligned}$$

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

Proof. The exponential lower bound for $\mathsf{AC}^0[q]$-$\mathsf{Frege}+\forall\mathsf{red}$ 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 $\mathsf{AC}^0[p]$-Frege system uses the connectives $\{\wedge,\vee,\neg,\leftrightarrow,MOD_p\}$. Then it is easy to see, by induction on i, that $\mathsf{AC}^0[p]$-Frege proves

$$s_i^r\leftrightarrow MOD_p(x_1,\dots,x_i,\underbrace{1,1,\dots,1}_{p-r}),$$

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

$$u\leftrightarrow\neg MOD_p(x_1,\dots,x_n,\underbrace{1,1,\dots,1}_{p}). \tag{9}$$

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

$$1\leftrightarrow\neg MOD_p(x_1,\dots,x_n,\underbrace{1,1,\dots,1}_{p})\quad\text{and}\quad 0\leftrightarrow\neg MOD_p(x_1,\dots,x_n,\underbrace{1,1,\dots,1}_{p}),$$

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* $\textsc{Majority}(x_1, \ldots, x_n)$*. Then for every prime p, the QBFs $\mathcal{Q}$-C_n require proofs of exponential size in* $\mathsf{AC}^0[p]$-$\mathsf{Frege} + \forall\mathsf{red}$*.*

Proof. The lower bound follows again applying Theorem 5.2 and the fact that MAJORITY requires exponential-size bounded-depth circuits with MOD_p gates (Razborov, 1987; Smolensky, 1987). □

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

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

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

As for the MOD_p functions, we can improve on this upper bound by considering explicit QBF encodings of MAJORITY, thereby even obtaining a separation of $\mathsf{AC}^0[p]$-$\mathsf{Frege} + \forall\mathsf{red}$ systems from TC^0-$\mathsf{Frege} + \forall\mathsf{red}$.[4] Explicit QBFs for MAJORITY can be defined using the following property of the k-threshold function

$$T_k(x_1, \ldots, x_i) \equiv T_k(x_1, \ldots, x_{i-1}) \vee (T_{k-1}(x_1, \ldots, x_{i-1}) \wedge x_i). \tag{10}$$

Using variables t_k^i for $T_k(x_1, \ldots, x_i)$ this gives rise to the QBFs

$$\Psi_n = \exists x_1 \cdots \exists x_n \forall u \exists t_1^1 \cdots \exists t_{n/2}^n \,.\, (u \leftrightarrow \neg t_{n/2}^n) \wedge \bigwedge_{i \le n} t_0^i \wedge (t_1^1 \leftrightarrow x_1) \wedge \bigwedge_{\substack{k \le n/2 \\ i \le n}} \left(t_k^i \leftrightarrow t_k^{i-1} \vee (t_{k-1}^{i-1} \wedge x_i)\right).$$

Corollary 5.9. *For each prime p the* MAJORITY*-formulas Ψ_n require proofs of exponential-size in* $\mathsf{AC}^0[p]$-$\mathsf{Frege} + \forall\mathsf{red}$*, but have polynomial-size proofs in* TC^0-$\mathsf{Frege} + \forall\mathsf{red}$*.*

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

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

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

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

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 $\mathcal{Q}$-C_n have AC^0_d-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 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 $\mathcal{Q}$-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 $\mathcal{Q}$-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-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 $\mathcal{Q}$-C_n has polynomial-size refutations in AC^0_{d+2}-Frege $+\,\forall$red. Here we want to prove that $\mathcal{Q}$-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 $\bigwedge$, that is

$$\mathcal{Q}\text{-}C_n = \exists x_1 \cdots \exists x_n \forall u \exists t_1 \cdots \exists t_m \,.\, (u \leftrightarrow \neg t_m) \wedge (t_m \leftrightarrow \bigwedge_{j\le\ell} t_{i_j}) \wedge \varphi_n,$$

where each t_{i_j} is an $\bigvee$ gate and φ_n is the encoding of the rest of the circuit C_n. We clearly have that

$$\frac{u \leftrightarrow \neg t_m \qquad t_m \leftrightarrow \bigwedge_{j\le\ell} t_{i_j}}{u \leftrightarrow \bigvee_{j\le\ell} \neg t_{i_j}}$$

From which we obtain both

$$u \vee \bigwedge_{j\le\ell} t_{i_j}, \tag{11}$$

$$\neg u \vee \bigvee_{j\le\ell} \neg t_{i_j}. \tag{12}$$

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_{i_j} with D_{i_j} where D_{i_j} is an AC^0_{d-1}-formula over the $x_1, \ldots, x_n$ variables starting with an $\bigvee$. More precisely by induction we can prove that AC^0_d-Frege proves both

$$t_{i_j} \vee \neg D_{i_j}, \tag{13}$$

$$\neg t_{i_j} \vee D_{i_j}. \tag{14}$$

Hence from (12) and (13) follows that

$$\neg u \vee \bigvee_{j\le\ell} \neg D_{i_j},$$

which is an AC^0_d-formula only over the variables $u, x_1, \ldots, x_n$. Hence by the $\forall$red rule we get

$$\bigvee_{j \le \ell} \neg D_{i_j}. \tag{15}$$

Similarly from (11) we get first that

$$\bigwedge_{j \le \ell} (u \vee t_{i_j})$$

and then using (14) we get

$$\bigwedge_{j \le \ell} (u \vee D_{i_j}),$$

which, again, is an AC^0_d-formula over the variables $u, x_1, \ldots, x_n$. By the $\forall$red rule we get

$$\bigwedge_{j \le \ell} D_{i_j}. \tag{16}$$

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 $f(x_1, \ldots, x_n)$ 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 $\mathcal{Q}$-C_n require exponential-size refutations in AC^0_1-Frege + $\forall$red and hence, in particular, in* Res + $\forall$red.

We now approach the 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 $\textsc{Sipser}_d$ function from Boppana and Sipser (1990):

$$\textsc{Sipser}_d = \bigwedge_{i_1 \le m_1} \bigvee_{i_2 \le m_2} \bigwedge_{i_3 \le m_3} \cdots \bigodot_{i_d \le m_d} x_{i_1 i_2 i_3 \ldots i_d},$$

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 $i_j \le m_j$, 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 $d \ge 2$. Let $(C^n_d)_{n \in \mathbb{N}}$ be a family of polynomial-size depth-$(d+3)$ circuits computing the function $\textsc{Sipser}_{d+3}(x_1, \ldots, x_n)$. Then the QBFs $\mathcal{Q}$-C^n_d need exponential-size proofs in AC^0_d-Frege + $\forall$red, but have polynomial-size proofs in AC^0_{d+3}-Frege + $\forall$red.*

Proof. The lower bound follows from Theorem 5.10 and from the result that for every d, $\textsc{Sipser}_{d+3}$ 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 $\mathcal{Q}$-C^n_d has polynomial-size proofs in AC^0_{d+3}-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 $\mathsf{Frege} + \forall\mathsf{red}$ and $\mathsf{EF} + \forall\mathsf{red}$. 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* non-uniform NC^1 *or* $\mathsf{P/poly}$. *If* $\mathsf{PSPACE} \not\subset \mathcal{C}$ *then* $\mathcal{C}$-$\mathsf{Frege} + \forall\mathsf{red}$ *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 $\mathcal{Q}\vec{w} \,.\, \varphi(\vec{w}, x_1, \ldots, x_n)$ with a CNF φ such that

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

We define

$$\mathcal{Q}\text{-}f_n = \exists x_1 \cdots \exists x_n \forall u \,.\, (u \leftrightarrow \mathcal{Q}\vec{w} \,.\, \varphi(\vec{w}, x_1, \ldots, x_n)),$$

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

We remark that we do have a separation between *uniform* NC^1 and PSPACE, because $\mathsf{NC}^1 \subseteq \mathsf{L}$ and $\mathsf{L} \neq \mathsf{PSPACE}$ by the space hierarchy theorem. Therefore, choosing $f \in \mathsf{PSPACE} \setminus \mathsf{NC}^1$ and considering the prenex formulas Θ_n arising from $\mathcal{Q}\text{-}f_n$ we can infer the weaker result that $\mathsf{Frege} + \forall\mathsf{red}$ has no uniform short proofs of Θ_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 $\forall\mathsf{red}$ 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 $\mathcal{Q}\vec{y}\forall u\exists x_1 \cdots \exists x_k \,.\, \varphi$, we have the following semantical equivalences

$$\begin{aligned}\mathcal{Q}\vec{y}\forall u\exists x_1 \cdots \exists x_k \,.\, \varphi \equiv & \mathcal{Q}\vec{y} \,(\exists x_1 \cdots \exists x_k \,.\, \varphi[u/0, x_1, \ldots, x_k] \wedge \exists x_1 \cdots \exists x_k \,.\, \varphi[u/1, x_1, \ldots, x_k]) \\ \equiv & \mathcal{Q}\vec{y} \,\exists x_1^{u/0} \cdots \exists x_k^{u/0} \exists x_1^{u/1} \cdots \exists x_k^{u/1} \,. \\ & \varphi[u/0, x_1/x_1^{u/0}, \ldots, x_k/x_k^{u/0}] \wedge \varphi[u/1, x_1/x_1^{u/1}, \ldots, x_k/x_k^{u/1}],\end{aligned}$$

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 $\mathcal{Q} \,.\, \varphi$: it is a QBF $\mathcal{Q}' \,.\, \varphi'$ where $\mathcal{Q}'$ consists exclusively of existential quantifiers. Moreover,

each existential variable x_i in $\mathcal{Q}\,.\,\varphi$ becomes an $x_i^{[\tau]_i}$ in $\mathcal{Q}'\,.\,\varphi'$, for each mapping τ from the universal variables into $\{0,1\}$ and where $[\tau]_i$ is the restriction of τ to the variables left of x_i. It is immediate to observe that $\mathcal{Q}\,.\,\varphi$ and its full universal expansion $\mathcal{Q}'\,.\,\varphi'$ are semantically equivalent, but $\mathcal{Q}'\,.\,\varphi'$ may have exponentially many more variables than $\mathcal{Q}\,.\,\varphi$.

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

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

We indicate by the index 0,1 in $\forall\mathsf{exp}_{0,1}$ 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 $P + \forall\mathsf{exp}$ where we substitute universal variables by more complex Boolean functions.

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

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

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

Choosing Res as the propositional base system, $\mathsf{Res} + \forall\mathsf{exp}_{0,1}$ coincides with the system $\forall\mathsf{Exp}{+}\mathsf{Res}$ 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 $P + \forall\mathsf{exp}_{0,1}$ p-simulates $Q + \forall\mathsf{exp}_{0,1}$.*

Proof. If P p-simulates Q then clearly $P + \forall\mathsf{exp}_{0,1}$ p-simulates $Q + \forall\mathsf{exp}_{0,1}$. The other direction follows since P and Q are just particular cases of $P + \forall\mathsf{exp}_{0,1}$ and $Q + \forall\mathsf{exp}$ 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 $\mathcal{C}\text{-}\mathsf{Frege} + \forall\mathsf{red}_{0,1}$ of $\mathcal{C}\text{-}\mathsf{Frege} + \forall\mathsf{red}$, where universal variables can only be replaced by constants. Formally, $\mathcal{C}\text{-}\mathsf{Frege} + \forall\mathsf{red}_{0,1}$ uses the inference rules of $\mathcal{C}\text{-}\mathsf{Frege}$ and the following restricted version of the $\forall\mathsf{red}$ rule:

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

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 $\mathcal{C}$, $\mathcal{C}$-Frege $+ \forall\mathsf{red}_{0,1}$ is a refutational QBF proof system.*

Proof. The soundness follows from the fact that $\mathcal{C}$-Frege $+ \forall\mathsf{red}$ p-simulates $\mathcal{C}$-Frege $+ \forall\mathsf{red}_{0,1}$ and the completeness by the fact that $\mathcal{C}$-Frege $+ \forall\mathsf{red}_{0,1}$ 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 $P + \forall\mathsf{exp}_{0,1}$ and $P + \forall\mathsf{red}_{0,1}$. We call this system $P + \forall\mathsf{inst}_{0,1}$. 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 $\mathcal{C}$-Frege $+ \forall\mathsf{inst}_{0,1}$, but it will be clear that this definition can be adapted to other proof systems.

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

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

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

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

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

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

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

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

Since $\mathcal{Q}\,.\,\varphi$ 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 $\mathrm{qlv}(x) > \mathrm{qlv}(u)$ such that the collection of all f_x is a winning strategy for the existential player.

Let ψ_i be the result of substituting in $\varphi \wedge L_1 \wedge \cdots \wedge L_i$ 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 $f_x(u_1/c_1, \ldots, u_k/c_k)$:

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

Let $\forall\vec{u}$ be the quantifier prefix of $\mathcal{Q}\,.\,\varphi$ when pruned of all the existential variables. By induction on i, we prove that $\forall\vec{u}\,.\,\psi_i$ is true for every $i = 1, \ldots, \ell$. For $i = \ell$ this gives a contradiction, since $L_\ell = \bot$ is appearing in ψ_ℓ and hence it is false.

The base case of the induction holds since the Skolem functions f_x must satisfy φ 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 $\psi_{i+1} = \psi_i \wedge L_{i+1}[x^\tau/f_x(\tau),\ldots]$ and L_{i+1} was either introduced by a $\mathcal{C}$-Frege rule or by the $\forall\mathsf{inst}_{0,1}$ rule.

If L_{i+1} was introduced by a $\mathcal{C}$-Frege rule then $\psi_i \models L_{i+1}[x^\tau/f_x(\tau),\ldots]$. 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 $\forall\mathsf{inst}_{0,1}$ rule, say $L_{i+1} = L_j[v/b, x^\tau/x^{\tau\cup\{v/b\}},\ldots]$ with $j \leq i$. For shortness let $L'_j = L_j[x^\tau/f_x(\tau),\ldots]$ and suppose that $\forall\vec{u}\,.\,\psi_i = \forall\vec{u}_1\forall v\forall\vec{u}_2\,.\,\psi_i$. Then we have the following transformations:

$$\begin{aligned}
\forall\vec{u}_1\forall v\forall\vec{u}_2\,.\,\psi_i &\equiv \forall\vec{u}_1\forall v\forall\vec{u}_2\,.\,\psi_i \wedge L'_j && (17)\\
&\equiv \forall\vec{u}_1\forall\vec{u}_2\forall v\,.\,\psi_i \wedge L'_j && (18)\\
&\equiv \forall\vec{u}_1\forall\vec{u}_2\,.\,\psi_i[v/0] \wedge L'_j[v/0] \wedge \psi_i[v/1] \wedge L'_j[v/1] && (19)\\
&\equiv \forall\vec{u}_1\forall\vec{u}_2\,.\,(L'_j[v/0] \wedge L'_j[v/1] \wedge \forall v\,.\,\psi_i) && (20)\\
&\equiv \forall\vec{u}_1\forall\vec{u}_2\forall v\,.\,L'_j[v/0] \wedge L'_j[v/1] \wedge \psi_i && (21)\\
&\models \forall\vec{u}_1\forall v\forall\vec{u}_2\,.\,\psi_i \wedge L'_j[v/b]. && (22)
\end{aligned}$$

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

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

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 $\forall\mathsf{red}_{0,1}$ and the $\forall\mathsf{red}$ rules we can define a more general version $\forall\mathsf{inst}$ of the $\forall\mathsf{inst}_{0,1}$ rule. In the system $\mathcal{C}$-Frege + $\forall\mathsf{inst}$ 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):

$$\begin{aligned}
F_n = \exists e_1\forall u_1\exists c_1^1\exists c_1^2\cdots\exists e_i\forall u_i\exists c_i^1\exists c_i^2\cdots\exists e_n\forall u_n\exists c_n^1 c_n^2\,.\,\bigvee_{i=1}^{n}(\neg c_i^1 \vee \neg c_i^2)\wedge\\
\bigwedge_{i=1}^{n}(e_i \to c_i^1) \wedge (u_i \to c_i^1) \wedge (\neg e_i \to c_i^2) \wedge (\neg u_i \to c_i^2).
\end{aligned} \tag{23}$$

Janota and Marques-Silva (2015) use these formulas to show that $\forall$Exp+Res does not simulate Q-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 $P + \forall\mathsf{exp}_{0,1}$.

(ii) The QBFs F_n have polynomial-size proofs in $\mathsf{Res} + \forall\mathsf{red}_{0,1}$.

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 $P + \forall\mathsf{exp}_{0,1}$ refutation, every $P + \forall\mathsf{exp}_{0,1}$ 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 $\mathsf{Res} + \forall\mathsf{red}_{0,1}$, 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 $P + \forall\mathsf{exp}_{0,1}$ does not simulate $\mathsf{Res} + \forall\mathsf{red}_{0,1}$.*

For the full separation between expansion and reduction systems we consider again the QBFs $\mathcal{Q}$-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 $\mathcal{Q}$-C_n have polynomial-size refutations in $\mathsf{Res} + \forall\mathsf{exp}_{0,1}$.*

Proof. Let C_n be a circuit family computing Parity. The formulas $\mathcal{Q}$-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, $\mathsf{AC}^0[p]$-Frege $+ \forall\mathsf{red}$ does not simulate $\mathsf{Res} + \forall\mathsf{exp}_{0,1}$.*

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.

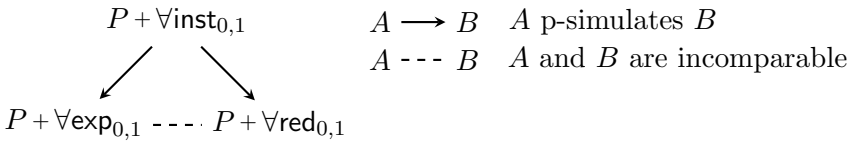

Figure 1: A slice of the simulation order of QBF proof systems

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 + ∀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 $P + \forall\mathsf{red}$ 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

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, 2000a.

Maria Luisa Bonet, Toniann Pitassi, and Ran Raz. On interpolation and automatization for frege systems. *SIAM J. Comput.*, 29(6):1939–1967, 2000b.

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 EF. *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 *CP*, pages 647–663, 2012.

Heribert Vollmer. *Introduction to Circuit Complexity – A Uniform Approach*. Texts in Theoretical Computer Science. Springer Verlag, Berlin Heidelberg, 1999.