

# Frege Systems for Quantified Boolean Logic

OLAF BEYERSDORFF, University of Jena

ILARIO BONACINA, UPC Barcelona

LEROY CHEW, University of Leeds

JAN PICH, University of Oxford

We define and investigate Frege systems for quantified Boolean formulas (QBF). For these new proof systems, we develop a lower bound technique that directly lifts circuit lower bounds for a circuit class  $\mathcal{C}$  to the QBF Frege system operating with lines from  $\mathcal{C}$ . Such a direct transfer from circuit to proof complexity lower bounds has often been postulated for propositional systems but had not been formally established in such generality for any proof systems prior to this work.

This leads to strong lower bounds for restricted versions of QBF Frege, in particular an exponential lower bound for QBF Frege systems operating with  $AC^0[p]$  circuits. In contrast, any non-trivial lower bound for propositional  $AC^0[p]$ -Frege constitutes a major open problem.

Improving these lower bounds to unrestricted QBF Frege tightly corresponds to *the* major problems in circuit complexity and propositional proof complexity. In particular, proving a lower bound for QBF Frege systems operating with arbitrary  $P/poly$  circuits is equivalent to either showing a lower bound for  $P/poly$  or for propositional extended Frege (which operates with  $P/poly$  circuits).

We also compare our new QBF Frege systems to standard sequent calculi for QBF and establish a correspondence to intuitionistic bounded arithmetic.

CCS Concepts: • **Theory of computation** → **Proof complexity**; *Circuit complexity*; Complexity theory and logic;

Additional Key Words and Phrases: QBF proof complexity, Frege systems, sequent calculus, intuitionistic logic, strategy extraction, lower bounds, simulations

Preliminary versions of this article appeared in the proceedings of ITCS'16 [Beyersdorff et al. 2016a] and LICS'16 [Beyersdorff and Pich 2016].

This research was supported by grant nos. 48138 and 60842 from the John Templeton Foundation, EPSRC grant EP/L024233/1, and a Doctoral Prize Fellowship from EPSRC (third author). The second author was funded by the European Research Council under the European Union's Seventh Framework Programme (FP7/2007–2013)/ERC grant agreement no. 279611 and under the European Union's Horizon 2020 Research and Innovation Programme/ERC grant agreement no. 648276 AUTAR. The fourth author was supported by the Austrian Science Fund (FWF) under project number P28699 and by the European Research Council under the European Union's Seventh Framework Programme (FP7/2007–2014)/ERC Grant Agreement no. 61507.

Part of this work was done when Beyersdorff and Pich were at the University of Leeds and Bonacina at Sapienza University Rome.

Authors' addresses: O. Beyersdorff, University of Jena, Institute of Computer Science, Ernst-Abbe-Platz 2, 07743 Jena, Germany; I. Bonacina, UPC Barcelona, Computer Science Department, Jordi Girona Salgado 31, 08034 Barcelona, Spain; L. Chew, University of Leeds, School of Computing, Leeds, LS2 9JT, UK; J. Pich, University of Oxford, Department of Computer Science, Wolfson Building, Parks Road, Oxford, OX1 3QD, UK.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

© 2020 Copyright held by the owner/author(s).

0004-5411/2020/03-ART9

<https://doi.org/10.1145/3381881>

**ACM Reference format:**

Olaf Beyersdorff, Ilario Bonacina, Leroy Chew, and Jan Pich. 2020. Frege Systems for Quantified Boolean Logic. *J. ACM* 67, 2, Article 9 (March 2020), 36 pages.  
<https://doi.org/10.1145/3381881>

**1 INTRODUCTION**

*Proof complexity* investigates how difficult it is to prove theorems in different formal systems. The main question asks, given a formula  $\varphi$  and a proof system  $P$ , typically composed of axioms and rules, what is the size of the smallest proof of  $\varphi$  in  $P$ ? This question bears tight and fruitful relations to a number of further areas, in particular to computational complexity, where lower bounds to the size of proofs offer an approach towards the separation of complexity classes (Cook's Programme) and to first-order logic (bounded arithmetic theories and their separations). More recently, the tremendous success of SAT solving has been a main driver for proof complexity, as the analysis of proof systems underlying SAT solvers provides the main theoretical framework towards understanding the power and limitations of solving, cf. the survey by 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 by Ben-Sasson and Wigderson [2001], the feasible interpolation technique of Krajíček [1997], or game-theoretic techniques (cf. the 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 composed 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 compose the standard non-uniform classes:  $AC^0$ , which is the class of Boolean functions computed by families of polynomial-size constant-depth circuits with unbounded fan-in;  $AC^0[p]$ , which is similar to  $AC^0$  but allows mod- $p$  gates; and  $TC^0$ , which additionally allows threshold gates. Even stronger,  $NC^1$  is composed of the class of Boolean functions computed by families of polynomial-size logarithmic-depth circuits with bounded fan-in and P/poly of functions with polynomial-size circuits in general. For *uniform* families of circuits, one further imposes the condition that the circuit family can be generated efficiently. Here, we typically consider *non-uniform* families, where we just require existence of the family of small circuits as above. This is analogous to the non-uniform model in proof complexity, where again only the existence of small proofs for a sequence of formulas is required. The circuit classes are ordered as  $AC^0 \subset AC^0[p] \subset TC^0 \subseteq NC^1 \subseteq P/poly$ , giving rise to a similar hierarchy of Frege systems.

While the strongest non-uniform lower bounds known in circuit complexity hold for the class  $AC^0[p]$  [Razborov 1987; Smolensky 1987],  $AC^0$ -Frege is the strongest of the above Frege systems with non-trivial lower bounds [Ajtai 1994; Krajíček et al. 1995; Pitassi et al. 1993]. Despite enormous efforts, all attempts to transfer Razborov's and Smolensky's  $AC^0[p]$  circuit lower to a proof size lower bound in  $AC^0[p]$ -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 (=  $NC^1$ -Frege) or even extended Frege (EF = 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 article, 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  $AC^0[p]$ -Frege for QBFs via Razborov [1987] and 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. 2017; 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 (that are sound and complete) 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: utilizing CDCL (Conflict-Driven Clause Learning) 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 by Janota and Marques-Silva [2015] and Beyersdorff et al. [2014]. 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. 2015; Janota and Marques-Silva 2015].

From a proof complexity perspective, resolution is considered 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, not only due to their reliance on the weak propositional resolution system, but also because of weak instantiations when dealing with quantifiers.

In addition to these weak QBF systems, there exists 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. 2017].

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 had been considered in QBF prior to the conference paper [Beyersdorff et al. 2016a] underlying this article; and even a QBF version of the propositional Frege hierarchy mentioned above has not been considered before. Building on our work here, the recent paper [Beyersdorff et al. 2018] investigates an analogue of the cutting planes proof system for QBF and Beyersdorff et al. [2019] contains further work in this direction.

## 1.1 Summary of Results

Below, we summarize our main contributions of this article, 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  $P$  composed of axioms and rules, we design a system  $P + \forall\text{red}$  for closed prenex QBFs (Definition 3.1). Throughout the proof, the quantifier prefix is fixed, and lines in the system  $P + \forall\text{red}$  are conceptually the same as lines in  $P$ , i.e., clauses in resolution, circuits from  $\mathcal{C}$  in  $\mathcal{C}$ -Frege (where  $\mathcal{C}$  is  $\text{AC}^0$ ,  $\text{AC}^0[p]$ ,  $\text{TC}^0$ ,  $\text{NC}^1$ , or  $\text{P/poly}$ ), or inequalities in cutting planes. Our new system  $P + \forall\text{red}$  uses all the rules from  $P$  and can apply those on arbitrary lines, irrespective of whether the variables are existentially or universally quantified. To make the system complete, we introduce a  $\forall\text{red}$  rule that allows to replace universal variables by simple Herbrand functions, which can be represented as lines in  $P$ . The link to Herbrand functions provides a clear semantic meaning for the  $\forall\text{red}$  rule, resulting in a natural and robust system  $P + \forall\text{red}$ .

Our new systems  $P + \forall\text{red}$  are inspired by the approach taken in the definition of Q-Res [Kleine Büning et al. 1995]; and, indeed, when choosing resolution as the base system  $P$ , our system  $P + \forall\text{red}$  coincides with the previously studied QU-Res [Van Gelder 2012]. While our definitions are quite general and yield for example previously missing QBF versions of polynomial calculus or cutting planes, we concentrate here on exploring the hierarchy  $\mathcal{C}$ -Frege +  $\forall\text{red}$  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  $\text{AC}^0$ -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 +  $\forall\text{red}$ .

Conceptually, our lower bound method uses the idea of *strategy extraction*, an important paradigm in QBF (Theorem 4.3). Semantically, a QBF can be understood as a game between a universal and an existential player, where the universal player wins if and only if the QBF is false. Winning strategies for the universal player can be very complex. However, we show that from each refutation of a false QBF in a system  $\mathcal{C}$ -Frege +  $\forall\text{red}$ , 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  $Q-f_n$  of false QBFs such that each winning strategy of the universal player on  $Q-f_n$  has to compute  $f$ . By strategy extraction, refutations of  $Q-f_n$  in  $\mathcal{C}$ -Frege +  $\forall\text{red}$  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  $Q-f_n$  in  $\mathcal{C}$ -Frege +  $\forall\text{red}$ .

Our lower bound technique widely generalizes ideas recently used by Beyersdorff et al. [2015] to show lower bounds for Q-Res and QU-Res for formulas originating from the PARTY 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 +  $\forall\text{red}$  systems that are yet unparalleled in propositional proof complexity. The following results are contained in Section 5.

*C.(i) Lower bounds and separations for the QBF proof system Frege  $AC^0[p] + \forall\text{red}$ .* The seminal results of Razborov [1987] and Smolensky [1987] showed that 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 Frege  $AC^0[p] + \forall\text{red}$  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  $+ \forall\text{red}$ . However, when carefully choosing specific and indeed very natural encodings, we can prove upper bounds for the  $MOD_q$  formulas even in Frege  $AC^0[q] + \forall\text{red}$ , thus obtaining exponential separations of all the Frege  $AC^0[p] + \forall\text{red}$  systems for distinct primes  $p$ .

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

*C.(ii) Separating Frege  $AC^0[p] + \forall\text{red}$  and Frege  $TC^0 + \forall\text{red}$ .* 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 Frege  $AC^0[p] + \forall\text{red}$  for all primes  $p$ . Carefully choosing the QBF encoding of MAJORITY, we obtain polynomial upper bounds for the MAJORITY formulas in Frege  $TC^0 + \forall\text{red}$ , thus proving an exponential separation between the two QBF proof systems Frege  $AC^0[p] + \forall\text{red}$  and Frege  $TC^0 + \forall\text{red}$ . Again, such a separation is wide open in propositional proof complexity.

*C.(iii) CNFs separating the Frege  $AC^0_d + \forall\text{red}$  hierarchy.* As a third example for our approach, we investigate the fine structure of Frege  $AC^0 + \forall\text{red}$ , composing all Frege  $AC^0_d + \forall\text{red}$  systems, where all formulas in proofs are required to have at most depth  $d$  for a fixed constant  $d$ . Resolution is an important example of such a system for depth  $d = 1$ .<sup>1</sup> 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 Frege  $AC^0_{d-3} + \forall\text{red}$  from Frege  $AC^0_d + \forall\text{red}$ , 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 each have a matrix of 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.

*C.(iv) Characterizing lower bounds for QBF Frege.* The main question left open by the results described above is whether *unconditional* lower bounds can be obtained for Frege  $+ \forall\text{red}$  or even EF  $+ \forall\text{red}$ . We show that such a result would imply either a major breakthrough in circuit complexity (a lower bound for non-uniform  $NC^1$  or even P/poly) or a major breakthrough in propositional proof complexity (lower bounds for classical Frege or even EF); and in fact the opposite implications hold as well (Theorem 5.13).

This means that the problem of lower bounds for QBF Frege very naturally unites the central problem in circuit complexity with the central problem in proof complexity. Conceptually this is very interesting: The direct connection between progress in circuit complexity and proof complexity, which has often been postulated (cf. Beame and Pitassi [2001]), directly manifests in Frege  $+ \forall\text{red}$ , thus highlighting that Frege  $+ \forall\text{red}$  is indeed a natural and important system.

<sup>1</sup>Although CNF formulas have depth 2, it is customary to consider Resolution being of depth  $d = 1$ , as it handles CNF formulas as sets of clauses, i.e., sets of objects of depth  $d = 1$ .

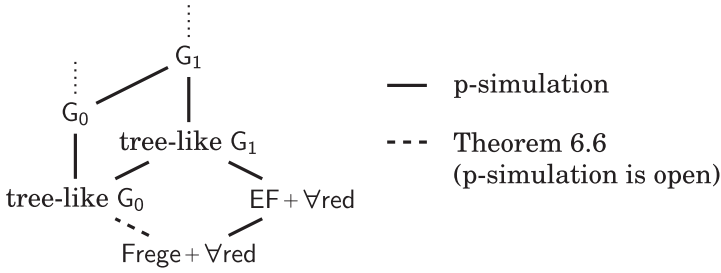


Fig. 1. The simulation order of QBF Gentzen and Frege systems.

Technically, this result uses a normal form that we achieve for  $Frege + \forall red$  proofs: these can be decomposed into a classical Frege proof followed by a number of  $\forall red$  steps (Theorem 4.5). We further show that even  $\forall red$  steps suffice that only substitute constants (Theorem 4.7).

*D. Gentzen vs. Frege in QBF: simulations and separations.* In classical proof complexity, Frege and Gentzen’s sequent system LK are p-equivalent, i.e., proofs can be efficiently translated between the systems [Cook and Reckhow 1979]. In contrast, our findings show a more complex picture for QBF, induced by the weak methods for handling (universal) quantifiers. We concentrate on the most important standard Gentzen-style systems  $G_0$  and  $G_1$  of Cook and Morioka [2005] as well as the QBF Frege systems  $Frege + \forall red$  and  $EF + \forall red$ . The indices in  $G_0$  and  $G_1$  refer to the quantifiers complexity of formulas allowed in cuts, cf. Section 6.1.1.

For these four systems, the following picture emerges (cf. Figure 1): We prove that tree-like  $G_1$  p-simulates  $EF + \forall red$  (Theorem 6.4) and tree-like  $G_0$  simulates  $Frege + \forall red$  under a relaxed notion of p-simulation (Theorem 6.6). However, the converse simulations are unlikely to hold. Under standard complexity-theoretic assumptions, we show that  $EF + \forall red$  is strictly weaker than tree-like  $G_1$  (Theorems 6.8, 6.10). Moreover,  $EF + \forall red$  is incomparable to both tree-like  $G_0$  and  $G_0$  (Theorems 6.11, 6.7). Hence, unlike in the propositional framework, Gentzen appears to be stronger than Frege in QBF.

While all these separations make use of complexity-theoretic assumptions, it will be hard to improve these results to unconditional lower bounds (see C.(iv) above). However, since we use a number of different and indeed partly incomparable assumptions, our separations seem very plausible.

*E. QBF Frege corresponds to intuitionistic logic.* The strongest tool for an understanding of classical Frege as well as propositional and QBF Gentzen systems comes from their correspondence to bounded arithmetic [Cook and Nguyen 2010; Krajíček 1995]. Here, we show such a correspondence between  $EF + \forall red$  and first-order intuitionistic logic  $IS_2^1$ , introduced in Buss [1986b] and Cook and Urquhart [1993]. For this, first-order arithmetic formulas are translated into sequences of QBFs [Krajíček and Pudlák 1990].

Our main result on the correspondence states that translations of arbitrarily complex prenex theorems in  $IS_2^1$  admit polynomial-size  $EF + \forall red$  proofs (Theorem 6.1). Informally, this says that all  $IS_2^1$  consequences can be efficiently derived in  $EF + \forall red$ , and moreover,  $EF + \forall red$  is the weakest system with this property.

The second facet of the correspondence is that  $IS_2^1$  can prove the correctness of  $EF + \forall red$  in a suitable encoding (Corollary 6.3), and in a certain sense  $EF + \forall red$  is the strongest proof system that is provably sound in the theory  $IS_2^1$ .

Technically, the correspondence as well as the simulation results mentioned under D. (above) rest on a formalization of the Strategy Extraction Theorem for QBF Frege systems. We provide two

formalizations for this result: in the first, we directly construct Frege proofs for the correctness of the witnessing properties (Theorem 4.4). In the second, we use first-order logic, where we formalize strategy extraction in the theory  $IS_2^1$  (Theorem 6.2). While the first formalization applies to more systems and gives the simulation structure detailed in D., the second formalization is stronger and enables the correspondence to  $IS_2^1$ .

Although intuitionistic bounded arithmetic was already developed by Buss [1986b] in the mid’80s, no QBF counterpart of this theory was found so far—in sharp contrast to most other arithmetic theories [Cook and Nguyen 2010]. As we show here, the missing piece in the puzzle is our new QBF Frege system  $EF + \forall red$ .

Indeed, the appealing link between  $IS_2^1$  and  $EF + \forall red$  comes via their witnessing properties: similarly as  $EF + \forall red$  has strategy extraction for arbitrarily complex QBFs, the theory  $IS_2^1$  admits a witnessing theorem for arbitrary first-order formulas [Cook and Urquhart 1993].

Conceptually, our work draws on the close interplay of ideas and techniques from proof complexity, computational complexity, and bounded arithmetic; and it is really the interaction of these areas and techniques that form the technical basis of our results (which forces us also to include rather extensive preliminaries).

## 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 et al. [2015]. Strategy extraction for Q-Res and QU-Res was shown by Goultiaeva et al. [2011] and Balabanov and Jiang [2012], but the idea to turn this into a lower bound argument for the proof size originates from Beyersdorff et al. [2015], 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. [2015] is solely confined to the resolution case. Here, we widely generalize 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. [2015], cf. Corollary 5.11 in the present article; and from Beyersdorff et al. [2015], 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 et al. [2017a] 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 Krajíček and Pudlák [1998], Bonet et al. [2000], and Bonet et al. [2004], 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. 2017a].

## 1.3 Organization of the Article

### Contents

<b>1 Introduction</b>	2
1.1 Summary of Results	4
1.2 Relations to previous work	7
1.3 Organization of the paper	7

<b>2 Preliminaries</b>	8
2.1 Circuit classes	8
2.2 Proof systems	8
2.3 Frege systems	9
2.4 Quantified Boolean Formulas	10
<b>3 Defining QBF Frege systems</b>	10
<b>4 Strategy extraction</b>	12
4.1 Formalized Strategy Extraction	14
4.2 Normal forms for C-Frege+ 8red proofs	16
<b>5 Separations and lower bounds via circuit complexity</b>	17
5.1 Lower bounds for bounded-depth QBF Frege systems	19
5.2 Lower bounds for constant depth QBF Frege systems	22
5.3 Characterizing QBF Frege and extended Frege lower bounds	24
<b>6 Relation of QBF Frege to sequent systems and bounded arithmetic</b>	25
6.1 Background on sequent systems and bounded arithmetic	25
6.1.1 Sequent Calculi	25
6.1.2 Bounded arithmetic	26
6.2 Intuitionistic logic corresponds to extended Frege for QBFs	27
6.3 Gentzen and Frege for QBFs	29
6.3.1 Formulas hard in Gentzen, but easy in Frege	31
6.3.2 Formulas easy in Gentzen, but hard in Frege	32
<b>7 Conclusion</b>	34

## 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 article. For a formula  $\varphi$ , we denote by  $\varphi[x_1/\theta_1, \dots, x_k/\theta_k]$  the formula  $\varphi$  where variables  $x_i$  have been substituted by formulas  $\theta_i$ .

### 2.1 Circuit Classes

We recall the definitions of standard circuit classes used in this article. The class  $AC^0$  contains all languages recognizable 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  $AC^0[p]$  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 P/poly circuits of polynomial size.

When defining circuit families  $C_n$  from a circuit class  $C$ , we distinguish between uniform and non-uniform families. For a uniform family, we require that there exists a Turing machine, which from input  $1^n$  efficiently constructs the circuit  $C_n$ . In the non-uniform setting, we merely require that the circuit  $C_n \in C$  exists and is of the required size.

For an in-depth account on circuit complexity, we refer to Vollmer [1999].

### 2.2 Proof Systems

According to Cook and Reckhow [1979] a *proof system* for a language  $\mathcal{L}$  is a polynomial-time onto function  $P : \{0, 1\}^* \rightarrow \mathcal{L}$ . Each string  $\varphi \in \mathcal{L}$  is a *theorem* and if  $P(\pi) = \varphi$ ,  $\pi$  is a *proof* of  $\varphi$  in  $P$ .



Given a polynomial-time function  $P : \{0, 1\}^* \rightarrow \{0, 1\}^*$  the fact that  $P(\{0, 1\}^*) \subseteq \mathcal{L}$  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 at most  $p(|x|)$ , where  $|x|$  is the size of string  $x$ .

### 2.3 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 composed of 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; 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 0.

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  $AC_d^0$ -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  $AC_1^0$ -Frege system<sup>2</sup> introduced by Blake [1937] and Robinson [1965]. It is a refutational proof system manipulating unsatisfiable CNFs as sets of clauses, where clauses are sets of literals. As we treat clauses as sets, factoring (to contract multiple occurrences of the same literal) is done automatically. The only inference rule of Resolution is

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

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

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

<sup>2</sup>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  $AC_1^0$ -Frege system even though it refutes CNFs, which are depth 2.

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

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

*Extended Frege systems* EF allow the introduction of new extension variables that abbreviate formulas. Consistent with the above treatment of  $\mathcal{C}$ -Frege, we define EF here 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 characterization 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

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

Currently lower bounds are only known for Res [Haken 1985] and  $\text{AC}^0$ -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.

## 2.4 Quantified Boolean Formulas

A (closed prenex) *Quantified Boolean Formula* (QBF) is a formula where quantifiers are introduced to propositional logic, which has constants 0,1, the usual operators  $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ , and propositional variables. Each variable is quantified at the beginning of the formula using either an existential or universal quantifier. We denote such formulas as  $Q\varphi$ , where  $\varphi$  is a propositional Boolean formula called *matrix*, and  $Q$  is its *quantifier prefix*. We typically use  $x_i$  for existentially quantified variables and  $u_i$  for universally quantified variables. Sometimes, we require the matrix to be a Conjunctive Normal Form (CNF); in particular, when we implement Resolution-style systems.

In a fully quantified prenex QBF, the quantifier prefix determines a total order of the variables. Given a variable  $y$ , we will sometimes refer to the variables preceding  $y$  in the prefix as variables *left of  $y$* ; analogously, we speak of the variables *right of  $y$* .

The quantifier complexity of QBFs is captured by sets  $\Sigma_i^q$  and  $\Pi_i^q$ , which are defined inductively.  $\Sigma_0^q = \Pi_0^q$  is the set of quantifier-free propositional formulas,  $\Sigma_{i+1}^q$  is the closure of  $\Pi_i^q$  under existential quantification, and  $\Pi_{i+1}^q$  is the closure of  $\Sigma_i^q$  under universal quantifiers.

A QBF  $Q_1x_1 \cdots Q_kx_k \varphi$  can be seen as a game between two players: *universal* ( $\forall$ ) and *existential* ( $\exists$ ). In the  $i$ th step of the game, the player  $Q_i$  assigns a value to the variable  $x_i$ . The existential player wins if  $\varphi$  evaluates to 1 under the assignment constructed in the game. The universal player wins if  $\varphi$  evaluates to 0. Given a universal variable  $u$  with index  $i$ , a *strategy for  $u$*  is a function from all variables of index  $< i$  to  $\{0, 1\}$ . A QBF is false if and only if there exists a *winning strategy* for the universal player; that is, if the universal player has a strategy for all universal variables that wins any possible game [Arora and Barak 2009; Goultiaeva et al. 2011].

## 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 [Beyersdorff et al. 2018; Cook et al. 1987].

For the following, we fix a circuit class  $\mathcal{C}$  with some natural properties, e.g., closure under restrictions.<sup>3</sup> In particular,  $\mathcal{C}$  can be any of the circuit classes mentioned in Section 2.

*Definition 3.1 (Frege  $\mathcal{C} + \forall\text{red}$ ).* A refutation of a false QBF  $Q \varphi$  in the system  $\mathcal{C}$ -Frege +  $\forall\text{red}$  is a sequence of lines  $L_1, \dots, L_\ell$  where each line is a circuit from the class  $\mathcal{C}$ ,  $L_1 = \varphi$ ,<sup>4</sup>  $L_\ell = 0$ , and each  $L_i$  is inferred from previous lines  $L_j$  using the inference rules of  $\mathcal{C}$ -Frege or using the following rule:

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

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

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

It is illustrative to see how our construction compares to previously studied QBF resolution systems. Choosing Res as our propositional proof system, which is an  $\text{AC}_1^0$ -Frege system, we obtain Res +  $\forall\text{red}$ . In Res +  $\forall\text{red}$  the  $\forall\text{red}$  rule can substitute a universal  $u$  by either a disjunction of literals or by a constant 0/1. In the former case, we simply obtain a weakening step. In the latter case, if  $u$  appears positively in the clause, then substituting  $u$  by 0 precisely corresponds to an application of the  $\forall\text{red}$  rule in Q-Res, whereas substituting  $u$  by 1 results in a useless tautology.<sup>5</sup> As Res +  $\forall\text{red}$  can resolve on existential and universal variables, our system Res +  $\forall\text{red}$  is exactly the well-known QU-Res (with weakening).

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

**THEOREM 3.2.** *For every circuit complexity class  $\mathcal{C}$ , the system  $\mathcal{C}$ -Frege +  $\forall\text{red}$  is a refutational QBF proof system.*

**PROOF.** Res +  $\forall\text{red}$  is complete as it p-simulates Q-Res, which is complete for QBF [Kleine Büning et al. 1995]. To obtain the completeness for  $\mathcal{C}$ -Frege +  $\forall\text{red}$ , 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 +  $\forall\text{red}$ .  $\mathcal{C}$ -Frege +  $\forall\text{red}$  p-simulates Res +  $\forall\text{red}$  and hence  $\mathcal{C}$ -Frege +  $\forall\text{red}$  is complete.

<sup>3</sup>In the context of a circuit class, “closure under restriction” means that for any circuit in the class, if we pick a partial assignment to some of the input variables and substitute in those constants, we still are guaranteed to be in the same circuit class.

<sup>4</sup>In the case where  $\mathcal{C}$  is  $\text{AC}_1^0$ , we require that  $\varphi = L_1 \wedge \dots \wedge L_m$  where  $L_j$  are lines in  $\text{AC}_1^0$ -Frege.

<sup>5</sup>Note that, contrasting the usual setting of Q-Res [Kleine Büning et al. 1995], our definition of Res +  $\forall\text{red}$  does not need to disallow tautologous resolvents, as these will always be reduced to 1.

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

$$\varphi_i = \begin{cases} \varphi & \text{if } i = 0, \\ \varphi \wedge L_1 \wedge \dots \wedge L_i & \text{otherwise.} \end{cases}$$

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  $L_\ell = 0$  and  $\mathcal{Q} \varphi_\ell \equiv 0$ .

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  $\forall\text{red}$  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  $\mathcal{Q} \varphi \models \mathcal{Q} \varphi_i \models \mathcal{Q} \varphi_{i+1}$ .

Suppose now that  $L_{i+1}$  was introduced by the  $\forall\text{red}$  rule, say  $L_{i+1} = L_j[u/B]$  with  $j \leq i$ ,  $u$  the innermost variable among the ones in  $L_j$  and  $B$  relying only on the variables left of  $u$ . Moreover, suppose that  $\mathcal{Q} \varphi_i = \mathcal{Q}_1 \vec{x} \forall u \mathcal{Q}_2 \vec{y} \varphi_i$ ; then, we have the following chain of equivalences

$$\mathcal{Q} \varphi_i = \mathcal{Q}_1 \vec{x} \forall u \mathcal{Q}_2 \vec{y} \varphi_i \tag{1}$$

$$\equiv \mathcal{Q}_1 \vec{x} \forall u \mathcal{Q}_2 \vec{y} \varphi_i \wedge L_j \tag{2}$$

$$\equiv \mathcal{Q}_1 \vec{x} \left( (\mathcal{Q}_2 \vec{y} \varphi_i[u/0] \wedge L_j[u/0]) \wedge (\mathcal{Q}_2 \vec{y} \varphi_i[u/1] \wedge L_j[u/1]) \right) \tag{3}$$

$$\equiv \mathcal{Q}_1 \vec{x} \left( L_j[u/0] \wedge L_j[u/1] \wedge (\mathcal{Q}_2 \vec{y} \varphi_i[u/0]) \wedge (\mathcal{Q}_2 \vec{y} \varphi_i[u/1]) \right) \tag{4}$$

$$\equiv \mathcal{Q}_1 \vec{x} \left( L_j[u/0] \wedge L_j[u/1] \wedge \forall u \mathcal{Q}_2 \vec{y} \varphi_i \right) \tag{5}$$

$$\equiv \mathcal{Q}_1 \vec{x} \left( L_j[u/0] \wedge L_j[u/1] \wedge L_j[u/B] \wedge \forall u \mathcal{Q}_2 \vec{y} \varphi_i \right) \tag{6}$$

$$\equiv \mathcal{Q}_1 \vec{x} \forall u \mathcal{Q}_2 \vec{y} \varphi_i \wedge L_j[u/0] \wedge L_j[u/1] \wedge L_j[u/B]. \tag{7}$$

In Equations (3) and (5), we used the definition of semantic expansion of a universal variable in a QBF; in Equations (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 Equation (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 +  $\forall\text{red}$  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  $\forall\text{red}$  rule in refutations (cf. also Beyersdorff et al. [2017b] for a formal definition of what qualifies as a “genuine” QBF lower bound).

#### 4 STRATEGY EXTRACTION

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 program of the following form:

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

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

This definition generalizes 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  $C_1, \dots, C_{\ell-1}$  and  $B_1, \dots, B_\ell$ , 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*

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

PROOF. We have that

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

where  $C_\ell$  is a circuit computing the constant 1 and for  $j = 1$ , we have an empty conjunct in the formula that is true.  $\square$

Balabanov and Jiang [2012] proved a strategy extraction result for QU-Res. Here, we generalize that result to the full hierarchy of  $\mathcal{C}$ -Frege +  $\forall$ red QBF proof systems. This result is the main tool we use to prove size lower bounds in such systems.

THEOREM 4.3 (STRATEGY EXTRACTION). *Given a false QBF  $Q \varphi$  and a refutation  $\pi$  of  $Q \varphi$  in  $\mathcal{C}$ -Frege +  $\forall$ red, it is possible to extract in linear time (w.r.t.  $|\pi|$ ) a collection of  $\mathcal{C}$ -decision lists  $D$  computing a winning strategy on the universal variables of  $\varphi$ .*

PROOF. Let  $\pi = (L_1, \dots, L_s)$  be a refutation of the false QBF  $Q \varphi$  and let

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

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

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

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

The statement of the Strategy Extraction Theorem corresponds to the case when  $i = 0$ . For the base case, we can define all the  $D_u^s$  as  $u \leftarrow 0$ , as any strategy will refute this QBF, so  $\sigma_u^s = 0$  is just picked arbitrarily.

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

- If  $L_i$  is derived by some Frege rule, then for each universal variable  $u$ , we set  $\sigma_u^{i-1} = \sigma_u^i$  and  $D_u^{i-1} = D_u^i$ .
- If  $L_i$  is the result of an application of a  $\forall$ red rule, then that is  $\frac{L_j}{L_j[u/B]}$ , where  $u$  is rightmost among the variables 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 all variables on the left of  $u'$  in the quantifier prefix of  $Q \varphi$ . Then, we define

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

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

$$\begin{aligned} &\text{if } \neg L_j[u/B](\vec{x}_u) \text{ then } u \leftarrow B(\vec{x}_u); \\ &\text{else } D_u^i(\vec{x}_u). \end{aligned}$$

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

- ▶  $\sigma_{u'}^{i-1}$  and  $D_{u'}^{i-1}$  are well defined. By construction  $L_j[u/B]$  is a formula in the variables  $\vec{x}$  left of  $u$ . This immediately implies that, for each universal variable  $u'$ , the strategy  $\sigma_{u'}^{i-1}$  is well defined and  $D_{u'}^{i-1}$  is also well defined. By induction hypothesis  $D_u^i$  is a  $\mathcal{C}$ -decision list, so  $D_u^{i-1}$  is also a  $\mathcal{C}$ -decision list.
- ▶  $\sigma^{i-1}$  and  $D_u^{i-1}$  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  $|\pi_{i-1}|$  (the number of characters in this subproof).
- ▶  $D_{u'}^{i-1}$  computes  $\sigma_{u'}^{i-1}$ . For  $u' \neq u$ , by induction hypothesis,  $D_{u'}^{i-1}$  computes  $\sigma_{u'}^i$ . The same happens, by construction, for  $u' = u$ .
- ▶  $\sigma^{i-1}$  is a winning strategy for  $Q \varphi_{i-1}$ . Fix an assignment  $\rho$  to the existential variables of  $\varphi$ . Let  $\tau_i$  be the complete assignment to existential and universal variables, constructed in response to  $\rho$  under the strategy  $\sigma^i$ . By induction hypothesis  $\tau_i$  falsifies  $\varphi_i$ . We need to show that  $\tau_{i-1}$  falsifies  $\varphi_{i-1}$ . To show this, we distinguish again two cases.

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

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

From the proof of the Strategy Extraction Theorem it is clear that the size of the  $\mathcal{C}$ -decision list computing the winning strategy extracted from the refutation  $\pi$  has size that is actually linear in the number of applications of the  $\forall$ red rule in  $\pi$ . More precisely, the size of the  $\mathcal{C}$ -decision list computing the winning strategy for variable  $u$  corresponds exactly to the number of  $\forall$ red rules on  $u$  in  $\pi$ . The size of a  $\mathcal{C}$ -decision list is intended to be its string representation. Interestingly, the same observation above holds if we consider the number of entries of the  $\mathcal{C}$ -decision list; i.e., the  $\mathcal{C}$ -decision list computing the winning strategy extracted from the refutation  $\pi$  has a number of entries that is linear in the number of applications of the  $\forall$ red rule in  $\pi$ .

#### 4.1 Formalized Strategy Extraction

We now observe that the strategy extraction from Theorem 4.3 is in fact provably correct in the corresponding Frege system. In Theorem 6.2, we also give a formalization of strategy extraction in the theory of bounded arithmetic  $S_2^1$ .

For this subsection (and also later occasionally), we assume w.l.o.g. that QBFs are of the form  $\exists x_1 \forall y_2 \cdots \exists x_n \forall y_n \varphi(x_1, \dots, x_n, y_1, \dots, y_n)$  with only one variable per quantifier block. This is no restriction, as a QBF with larger quantifier blocks can be transformed into this form by adding dummy variables to the prefix, which do not appear in the matrix of the formula. This will simplify our analysis.

**THEOREM 4.4.** *Let  $\mathcal{C}$  be  $AC^0$ ,  $AC^0[p]$ ,  $TC^0$ ,  $NC^1$ , or  $P/poly$ . Given a  $\mathcal{C}$ -Frege +  $\forall$ red refutation  $\pi$  of a QBF*

$$\exists x_1 \forall y_1 \cdots \exists x_n \forall y_n \varphi(x_1, \dots, x_n, y_1, \dots, y_n)$$

where  $\varphi \in \Sigma_0^q$ , we can construct in time  $|\pi|^{O(1)}$  a  $\mathcal{C}$ -Frege proof of

$$\bigwedge_{i=1}^n (y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})) \rightarrow \neg \varphi(x_1, \dots, x_n, y_1, \dots, y_n)$$

for some circuits  $C_i \in \mathcal{C}$ . (The depth of the  $\mathcal{C}$ -Frege proof increases by a constant compared to the depth of the  $\mathcal{C}$ -Frege +  $\forall$ red proof.)

**PROOF.** We inspect the proof of the Strategy Extraction Theorem above. Again let  $\pi = (L_1, \dots, L_s)$  be a  $\mathcal{C}$ -Frege +  $\forall$ red refutation of a QBF  $Q \varphi$  given as

$$\exists x_1 \forall y_1 \cdots \exists x_n \forall y_n \varphi(x_1, \dots, x_n, y_1, \dots, y_n)$$

where  $\varphi \in \Sigma_0^q$  and define  $\pi_i$  and  $\varphi_i$  as in the proof of Theorem 4.3. We will show by downward induction on  $i$  that from  $\pi_i$  it is possible to construct in linear time a winning strategy

$$\sigma^i = \{C_1^i(x_1), \dots, C_n^i(x_1, \dots, x_n, y_1, \dots, y_{n-1})\} \subseteq \mathcal{C}$$

for the universal player for the QBF  $Q \varphi_i$ . Moreover, the formula

$$\bigwedge_{l=1}^n (y_l \leftrightarrow C_l^i(x_1, \dots, x_l, y_1, \dots, y_{l-1})) \rightarrow \neg \varphi_i(x_1, \dots, x_n, y_1, \dots, y_n)$$

denoted  $\sigma^i(\varphi_i)$ , which witnesses the negation of  $Q \varphi$  will have a  $\mathcal{C}$ -Frege proof of size  $K|\pi_i|^K$  for a constant  $K$  depending only on the choice of the  $\mathcal{C}$ -Frege system. The statement of the theorem corresponds to the case  $i = 0$ .

In the base case,  $\varphi_s$  contains a contradiction so the winning strategy can be defined as the set of trivial circuits  $\{0, \dots, 0\}$  and it is trivially provably correct.

Assume now that  $\sigma^i(\varphi_i)$  has a  $\mathcal{C}$ -Frege proof of size  $K(s + 1 - i)|\pi_i|^K$ .

If  $L_i$  is derived by a  $\mathcal{C}$ -Frege rule, then  $\sigma^{i-1} = \sigma^i$ .

Now let  $L_i = L_j[u/B]$  be the result of an application of a  $\forall$ red rule on  $L_j$  where  $u$  is innermost among the variables in  $L_j$ . Then define  $C_l^{i-1} = C_l^i$  if  $u \neq y_l$ , otherwise set

$$C_l^{i-1}(z) = \begin{cases} B(z) & \text{if } L_j[u/B](z) = 0, \\ C_l^i(z) & \text{if } L_j[u/B](z) = 1. \end{cases}$$

This constructs strategies  $\sigma^i$  from  $\pi$  by a  $D|\pi_i|$ -time algorithm for a constant  $D$ . W.l.o.g.  $D < K$ . In fact, circuits  $C_l^i$  are in  $\mathcal{C}$ . (For constant depth  $\mathcal{C}$ 's, we take for circuits  $C_l^i$  the equivalent constant-depth circuits from Proposition 4.2).

We want to show that  $\sigma^{i-1}(\varphi_{i-1})$  has a  $\mathcal{C}$ -Frege proof of size  $K(s + 1 - (i - 1))|\pi_{i-1}|^K$ .

If  $L_i$  is derived by a  $\mathcal{C}$ -Frege rule, then  $\sigma^i$  also witnesses  $\neg \varphi_{i-1}$  because

$$\neg L_i \rightarrow \neg(L'_1 \wedge \cdots \wedge L'_i)$$

for some conjuncts  $L'_1, \dots, L'_i$  in  $\varphi_{i-1}$ . Note that  $C_l^{i-1}$ 's are then  $C_l^i$ 's. The implications

$$\neg \varphi_i \rightarrow \neg \varphi_{i-1}, \tag{8}$$

$$\sigma^i(\varphi_i) \wedge (\neg \varphi_i \rightarrow \neg \varphi_{i-1}) \rightarrow \sigma^{i-1}(\varphi_{i-1}), \tag{9}$$

can be derived by a fixed sequence of  $\mathcal{C}$ -Frege rules depending only on the choice of  $\mathcal{C}$ -Frege. (Note that the left-hand sides of the implications  $\sigma^i(\varphi_i)$  and  $\sigma^{i-1}(\varphi_{i-1})$  are identical, because  $\sigma^{i-1} = \sigma^i$  in this case.) Thus, the common size of  $\mathcal{C}$ -Frege proofs of both these implications is  $\leq K_0|\pi_{i-1}|^{K_0}$  where w.l.o.g.  $K_0 < K$ . Therefore,  $\sigma^{i-1}(\varphi_{i-1})$  has a  $\mathcal{C}$ -Frege proof of size

$\leq K(s+1-i)|\pi_i|^K + K_1|\pi_{i-1}|^{K_1} \leq K(s+1-(i-1))|\pi_{i-1}|^K$  where  $K_1 > K_0$  depends again on a fixed sequence of  $\mathcal{C}$ -Frege rules needed to derive  $\sigma^{i-1}(\varphi_{i-1})$  from Equations (8), (9), and  $\sigma^i(\varphi_i)$ , so w.l.o.g.  $K_1 < K$ .

Assume now that  $L_i = L_j[u/B]$  is the result of an application of  $\forall\text{red}$  where  $u = y_l$ . Then there is a fixed sequence of  $\mathcal{C}$ -Frege rules deriving the implications

$$\sigma^i(\varphi_i) \wedge \neg L_j[u/B] \rightarrow \sigma^{i-1}(\varphi_{i-1}), \quad (10)$$

$$\sigma^i(\varphi_i) \wedge L_j[u/B] \rightarrow \sigma^{i-1}(\varphi_{i-1}). \quad (11)$$

Equation (10) follows from the provable equation  $L_j \wedge (u \leftrightarrow B) \rightarrow L_j[u/B]$ , because  $L_j$  is a conjunct in  $\varphi_{i-1}$ ,  $u = y_l$  and  $C_l^{i-1}$  is  $B$ , because  $\neg L_j[u/B]$  holds in this case. Equation (11) follows from the provable formula  $\varphi^{i-1} \wedge L_j[u/B] \rightarrow \varphi_i$  and  $\bigwedge_{l=1}^n y_l \leftrightarrow C_l^{i-1} \rightarrow \bigwedge_{l=1}^n y_l \leftrightarrow C_l^i$  under the condition that  $C_l^{i-1} = C_l^i$ , which is the case if  $L_j[u/B]$  holds.

The total size of both  $\mathcal{C}$ -Frege derivations of Equations (10) and (11) is  $K_0|\pi_{i-1}|^{K_0}$  where  $K_0$  depends on the choice of  $\mathcal{C}$ -Frege and the size of  $C_l^{i-1}$ 's. The size of all  $C_l^{i-1}$ 's is bounded by  $K|\pi_{i-1}|^K$ . Hence, we can assume  $K_0 < K$ . It follows that  $\sigma^{i-1}(\varphi_{i-1})$  has a  $\mathcal{C}$ -Frege proof of size  $\leq K(s+1-i)|\pi_i|^K + K_1|\pi_{i-1}|^{K_1} \leq K(s+1-(i-1))|\pi_{i-1}|^K$  where as before  $K_1$  depends on a fixed sequence of  $\mathcal{C}$ -Frege rules needed to simulate a fixed set of ‘‘cut’’ rules, i.e., w.l.o.g.  $K_1 < K$ .  $\square$

## 4.2 Normal forms for $\mathcal{C}$ -Frege + $\forall\text{red}$ Proofs

We conclude this section with an application of the Strategy Extraction Theorem to obtain normal forms for  $\mathcal{C}$ -Frege +  $\forall\text{red}$  proofs. First, we show that any  $\mathcal{C}$ -Frege +  $\forall\text{red}$  refutation can be efficiently rewritten as a  $\mathcal{C}$ -Frege derivation followed essentially just by  $\forall\text{red}$  rules. Second, we show that in the  $\forall\text{red}$  rule it is sufficient to only substitute constants.

**THEOREM 4.5.** *Let  $\mathcal{C}$  be  $\text{AC}^0$ ,  $\text{AC}^0[p]$ ,  $\text{TC}^0$ ,  $\text{NC}^1$ , or  $\text{P/poly}$ . For any  $\mathcal{C}$ -Frege +  $\forall\text{red}$  refutation  $\pi$  of a QBF  $\psi$  of the form*

$$\exists x_1 \forall y_1 \cdots \exists x_n \forall y_n \varphi(x_1, \dots, x_n, y_1, \dots, y_n),$$

where  $\varphi \in \Sigma_0^q$ , there is a  $|\pi|^{O(1)}$ -size  $\mathcal{C}$ -Frege +  $\forall\text{red}$  refutation of  $\psi$  starting with a  $\mathcal{C}$ -Frege derivation of

$$\bigvee_{i=1}^n (y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})), \quad (12)$$

from  $\varphi$  for some circuits  $C_i \in \mathcal{C}$ , followed by  $n$  applications of the  $\forall\text{red}$  rule, gradually replacing the rightmost variable  $y_i$  by circuit  $C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})$  and cutting the inequality  $y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})$  out of the disjunction (12).

**PROOF.** Given a  $\mathcal{C}$ -Frege +  $\forall\text{red}$  refutation  $\pi$  of  $\psi$ , by Theorem 4.4, there is a  $|\pi|^{O(1)}$ -size  $\mathcal{C}$ -Frege proof of

$$\bigwedge_{i=1}^n (y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})) \rightarrow \neg \varphi(x_1, \dots, x_n, y_1, \dots, y_n).$$

Having  $\varphi$  freely available in the refutation,  $\mathcal{C}$ -Frege can derive (12) by applying the cut rule (derivable in  $\mathcal{C}$ -Frege).

The refutation then continues by  $n$  applications of the  $\forall\text{red}$  rule, which one-by-one replaces the rightmost variable  $y_i$  by  $C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})$  and eliminates

$$y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})$$

from the disjunction  $\bigvee_i y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})$ .  $\square$



Theorem 4.5 is an analogue of the midsequent theorem for sequent systems. An immediate consequence of Theorem 4.5 is the p-equivalence of  $\mathcal{C}$ -Frege +  $\forall\text{red}$  and its tree-like version. This is in contrast to the  $G_1, G_0$  systems where one has p-simulations of dag systems by tree systems only for prenex  $\Sigma_1^q$ -formulas (see Cook and Morioka 2005, Theorem 6 and the discussion after the proof).

**COROLLARY 4.6.** *Let  $\mathcal{C}$  be  $AC^0, AC^0[p], TC^0, NC^1$ , or P/poly. Then,  $\mathcal{C}$ -Frege +  $\forall\text{red}$  is p-equivalent to tree-like  $\mathcal{C}$ -Frege +  $\forall\text{red}$ .*

**PROOF.** By Theorem 4.5, any  $\mathcal{C}$ -Frege +  $\forall\text{red}$  derivation can be efficiently replaced by a proof in the normal form. The  $\mathcal{C}$ -Frege part of such derivation can be efficiently replaced by a tree-like  $\mathcal{C}$ -Frege proof, cf. Krajíček [1995], and the rest of the  $\mathcal{C}$ -Frege +  $\forall\text{red}$  refutation given in the normal form is tree-like.  $\square$

Finally, we further simplify  $\mathcal{C}$ -Frege +  $\forall\text{red}$  so every application of the  $\forall\text{red}$  rule only substitutes constants 0/1 instead of general circuits. We denote the resulting system as  $\mathcal{C}$ -Frege +  $\forall\text{red}_{0,1}$ . This shows that  $\mathcal{C}$ -Frege +  $\forall\text{red}$  systems are indeed very robustly defined.

**THEOREM 4.7.** *Let  $\mathcal{C}$  be  $AC^0, AC^0[p], TC^0, NC^1$ , or P/poly. Then,  $\mathcal{C}$ -Frege +  $\forall\text{red}$  and  $\mathcal{C}$ -Frege +  $\forall\text{red}_{0,1}$  are p-equivalent.*

**PROOF.** It is enough to show that any  $\mathcal{C}$ -Frege +  $\forall\text{red}$  refutation can be transformed efficiently into a refutation where the  $\forall\text{red}$  rule substitutes only constants. By Theorem 4.5, for any  $\mathcal{C}$ -Frege +  $\forall\text{red}$  refutation  $\pi$  of  $Q \varphi$  there is a  $|\pi|^{O(1)}$ -size  $\mathcal{C}$ -Frege derivation of

$$\bigvee_{i=1}^n (y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1}))$$

from  $\varphi(x_1, \dots, x_n, y_1, \dots, y_n)$ . Applying  $\forall\text{red}_{0,1}$  on  $y_n$ , we can then derive

$$(C_n(x_1, \dots, x_n, y_1, \dots, y_{n-1}) \leftrightarrow c) \vee \bigvee_{i=1}^{n-1} (y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1}))$$

for both constants  $c = 0, 1$ .

However, there is a polynomial-size  $\mathcal{C}$ -Frege proof of

$$(C_n(x_1, \dots, x_n, y_1, \dots, y_{n-1}) \leftrightarrow 1) \vee (C_n(x_1, \dots, x_n, y_1, \dots, y_{n-1}) \leftrightarrow 0),$$

so we can derive  $\bigvee_{i < n} (y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1}))$ . In this way, we can efficiently cut all disjuncts and derive a contradiction in  $\mathcal{C}$ -Frege +  $\forall\text{red}_{0,1}$ .  $\square$

## 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 (Q- $C_n$ ).** Let  $n$  be an integer and  $C_n$  be a circuit with inputs  $x_1, \dots, x_n$ . Let  $t_1, \dots, t_{m-1}$  be a topological ordering of the internal gates of  $C_n$ , and let the output gate of  $C_n$  be  $t_m$ . We define

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

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  $Q-C_n$  expresses that there exists an input  $\vec{x}$  such that  $C_n(\vec{x})$  neither evaluates to 0 nor 1, an obvious contradiction, as  $C_n$  computes a total function on  $\{0, 1\}^n$ . The formulas  $G_i$  can be considered as the result of a Tseitin translation used widely in SAT and QBF solving. We intentionally place the universal variable  $u$  to the left of the Tseitin variables  $t_i$ , thus making the Tseitin variables inaccessible when constructing the strategy of  $u$ . We note that the hardness of the formulas crucially depends on this choice of the order of quantification (compare also Beyersdorff et al. [2016b]).

Using these formulas together with the Strategy Extraction Theorem, we now establish a tight 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  $AC^0$ ,  $AC^0[p]$ ,  $TC^0$ ,  $NC^1$ ,  $P/poly$  and let  $(C_n)_{n \in \mathbb{N}}$  be a non-uniform family of circuits where  $C_n$  is a circuit with  $n$  inputs. Then the following implications hold:*

- (i) *if the QBFs  $Q-C_n$  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  $Q-C_n$  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  $Q-C_n$  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  $Q-C_n$  the quantifier prefix looks like  $\exists x_1 \cdots \exists x_n \forall u \exists \vec{t}$ . Now, by construction,  $u \leftrightarrow C_n(x_1, \dots, x_n)$ , hence a winning strategy for the universal player must consist of playing  $u = C_n(x_1, \dots, x_n)$ . 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.

Note that the circuits  $C'_n$  and  $C_n$  are equivalent but not identical. The first one  $C'_n$  is the strategy extracted from a decision list and depends on the proof in question, whereas  $C_n$  is the original circuit encoded into  $Q-C_n$  with Tseitin variables.

Regarding (ii), we define the  $t_i$  variables ( $1 \leq i \leq m$ ) for  $Q-C_n$  as in Definition 5.1. 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  $|D_i|$ .

In the base case, we have that  $\mathcal{C}$ -Frege is able to prove  $x \leftrightarrow x$  for every input variable  $x$ .

For the inductive step, suppose that  $t_i$  corresponds to a gate  $\odot(t_{j_1}, \dots, t_{j_\ell})$  with fan-in  $\ell$ , where  $\odot$  could be an  $\wedge, \vee, \neg, \oplus, MOD_p, T_k, \dots$  from the gates allowed in the class  $\mathcal{C}$  and  $j_1 \dots j_\ell$  is a sequence of indices less than  $i$ . By the inductive property, we know that  $t_k \leftrightarrow D_k$  is provable in  $\mathcal{C}$ -Frege with proofs of size polynomial in  $|D_k|$ , for every  $k < i$  (as well as any input variables). Hence,  $t_{j_k} \leftrightarrow D_{j_k}$  is provable in  $\mathcal{C}$ -Frege with proofs of size polynomial in  $|D_{j_k}|$  for every input gate variable  $t_{j_k}$ . Moreover,  $\mathcal{C}$ -Frege is able to make the following inference in a polynomial number of steps:

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

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

$$\frac{t_m \leftrightarrow D_m \quad u \leftrightarrow \neg t_m}{u \leftrightarrow \neg D_m} .$$

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

In particular, a Boolean function  $f$  is computable by polynomial-size  $\mathcal{C}$  circuits if and only if  $Q\text{-}C_n$  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 in 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 QBF 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 Frege  $AC^0[p] + \forall$ red, regardless of the encoding for PARITY.

**COROLLARY 5.3 (Q-PARITY LOWER BOUNDS).** *Let  $C_n$  be a family of polynomial-size circuits computing PARITY. For each odd prime  $p$ , the QBFs  $Q\text{-}C_n$  require refutations of exponential size in Frege  $AC^0[p] + \forall$ red.*

**PROOF.** The exponential lower bound for the refutation size in Frege  $AC^0[p] + \forall$ 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].  $\square$

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

**COROLLARY 5.4 (Q-PARITY UPPER BOUNDS).** *Let  $C_n$  be a family of  $NC^1$  circuits computing PARITY. Then, the QBFs  $Q\text{-}C_n$  have polynomial-size refutations in Frege +  $\forall$ 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 Frege +  $\forall$ red follows immediately from Theorem 5.2.  $\square$

In fact, this upper bound can be improved to the QBF proof system Frege  $AC^0[2] + \forall$ 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  $PARITY(x_1, \dots, x_n) = PARITY(x_1, \dots, x_{n-1}) \oplus x_n$ . 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  $Q\text{-}PARITY$  was considered by Beyersdorff et al. [2015], where the formulas  $\Phi_n$  are shown to be hard for Q-Res and QU-Res. Here, we obtain:

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

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

Then it is easy to see, by induction on  $i$ , that Frege proves  $t_i \leftrightarrow \oplus(x_1, x_2, \dots, x_i)$  with a proof of size linear in  $i$  for each  $i = 2, \dots, n$ . Hence, similarly to what was done in Theorem 5.2, we get

$$u \leftrightarrow \neg \oplus(x_1, x_2, \dots, x_n). \quad (13)$$

Then,  $u$  is the rightmost variable in Equation (13); hence, by the  $\forall$ 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.  $\square$

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

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

For  $r \leq p-1$  let

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

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

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

and for  $r = 0$  by

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

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

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

**COROLLARY 5.6.** *For each pair  $p, q$  of distinct primes the  $\text{MOD}_p$ -formulas  $\Theta_n^p$  require refutations of exponential size in Frege  $\text{AC}^0[q] + \forall$ red, but have polynomial-size refutations in Frege  $\text{AC}^0[p] + \forall$ red.*

**PROOF.** The exponential lower bound for the QBF proof system Frege  $\text{AC}^0[q] + \forall$ red follows from Theorem 5.2 together with the result from Razborov [1987] and Smolensky [1987] that for distinct primes  $p, q$  any family of bounded-depth circuits with  $\text{MOD}_q$  gates computing  $\text{MOD}_p$  must be of exponential size.

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

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

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

$$u \leftrightarrow \neg \text{MOD}_p(x_1, \dots, x_n, \underbrace{1, 1, \dots, 1}_p). \quad (14)$$

Then  $u$  is the rightmost variable in (14); hence, by the  $\forall$ red rule, we have

$$1 \leftrightarrow \neg \text{MOD}_p(x_1, \dots, x_n, \underbrace{1, 1, \dots, 1}_p) \quad \text{and} \quad 0 \leftrightarrow \neg \text{MOD}_p(x_1, \dots, x_n, \underbrace{1, 1, \dots, 1}_p),$$

which gives an immediate contradiction.  $\square$

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  $Q$ -MAJORITY).** *Let  $C_n$  be a family of polynomial-size circuits computing MAJORITY( $x_1, \dots, x_n$ ). Then, for every prime  $p$ , the QBFs  $Q$ - $C_n$  require refutations of exponential size in Frege  $\text{AC}^0[p] + \forall$ red.*

**PROOF.** The lower bound follows again applying Theorem 5.2 and the fact that MAJORITY requires exponential-size bounded-depth circuits with  $\text{MOD}_p$  gates [Razborov 1987; Smolensky 1987].  $\square$

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

**COROLLARY 5.8 ( $Q$ -MAJORITY UPPER BOUNDS).** *Let  $C_n$  be a family of  $\text{NC}^1$  circuits computing MAJORITY( $x_1, \dots, x_n$ ). Then, the QBFs  $Q$ - $C_n$  have polynomial-size refutations in the QBF proof system Frege +  $\forall$ red.*

**PROOF.** By a result of Muller and Preparata [1975], the function MAJORITY is computable in  $\text{NC}^1$  and hence  $Q$ - $C_n$  are well defined. The upper bound then follows from Theorem 5.2.  $\square$

As for the  $\text{MOD}_p$  functions, we can improve on this upper bound by considering explicit QBF encodings of MAJORITY, thereby even obtaining a separation of Frege  $\text{AC}^0[p] + \forall$ red systems from Frege  $\text{TC}^0 + \forall$ red.<sup>6</sup> Explicit QBFs for MAJORITY can be defined using the following property of the  $k$ -threshold function:

$$T_k(x_1, \dots, x_i) \equiv T_k(x_1, \dots, x_{i-1}) \vee (T_{k-1}(x_1, \dots, x_{i-1}) \wedge x_i). \quad (15)$$

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

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

**COROLLARY 5.9.** *For each prime  $p$ , the MAJORITY-based formulas  $\Psi_n$  require refutations of exponential-size in the QBF proof system Frege  $\text{AC}^0[p] + \forall$ red, but have polynomial-size refutations in Frege  $\text{TC}^0 + \forall$ red.*

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

<sup>6</sup>Clearly, such a separation already follows from Corollary 5.6 together with the simulation of Frege  $\text{AC}^0[p] + \forall$ red by Frege  $\text{TC}^0 + \forall$ red. Here, we will prove the stronger result that all these systems are separated by *one* natural principle—namely, MAJORITY.

Regarding the polynomial-size refutations of the QBF formula  $\Psi_n$  in Frege  $\text{TC}^0 + \forall\text{red}$ , we can proceed similarly as for  $\text{PARITY}$  in Frege. The crucial feature here is that  $T_k$  are, by definition of  $\text{TC}^0$ , in the language of  $\text{TC}^0$ -Frege. Hence (15) can be used to prove  $t_k^j \leftrightarrow T_k(x_1, \dots, x_j)$  and we can easily refute  $\Psi_n$  in Frege  $\text{TC}^0 + \forall\text{red}$ .  $\square$

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

## 5.2 Lower Bounds for Constant Depth QBF Frege Systems

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

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

- (i) *if the QBFs  $Q-C_n$  have Frege  $\text{AC}_d^0 + \forall\text{red}$  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  $Q-C_n$  have polynomial-size refutations in Frege  $\text{AC}_d^0 + \forall\text{red}$ .*

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

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

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

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

$$\frac{u \leftrightarrow \neg t_m \quad t_m \leftrightarrow \bigwedge_{j \leq \ell} t_{i_j}}{u \leftrightarrow \bigvee_{j \leq \ell} \neg t_{i_j}},$$

from which we obtain both

$$u \vee \bigwedge_{j \leq \ell} t_{i_j}, \tag{16}$$

$$\neg u \vee \bigvee_{j \leq \ell} \neg t_{i_j}. \tag{17}$$

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

$$t_{i_j} \vee \neg D_{i_j}, \tag{18}$$

$$\neg t_{i_j} \vee D_{i_j}. \tag{19}$$

Hence from (17) and (18) follows that  $\neg u \vee \bigvee_{j \leq \ell} \neg D_{i_j}$ , which is an  $AC_d^0$ -formula only over the variables  $u, x_1, \dots, x_n$ . Hence, by the  $\forall$ red rule, we get

$$\bigvee_{j \leq \ell} \neg D_{i_j}. \tag{20}$$

Similarly, from (16), we get first that  $\bigwedge_{j \leq \ell} (u \vee t_{i_j})$  and then using (19), we get  $\bigwedge_{j \leq \ell} (u \vee D_{i_j})$ , which, again, is an  $AC_d^0$ -formula over the variables  $u, x_1, \dots, x_n$ . By the  $\forall$ red rule, we get

$$\bigwedge_{j \leq \ell} D_{i_j}. \tag{21}$$

From (20) and (21) follows immediately a contradiction.  $\square$

From Theorem 5.10, we obtain a wealth of lower bounds for Res +  $\forall$ red.

**COROLLARY 5.11.** *Let  $f(x_1, \dots, x_n)$  be a Boolean function requiring exponential-size depth-3 circuits and let  $(C_n)_{n \in \mathbb{N}}$  be polynomial-size circuits (of unbounded depth) computing  $f$ . Then the QBFs  $Q-C_n$  require exponential-size refutations in Frege  $AC_1^0 + \forall$ red and hence, in particular, in Res +  $\forall$ red.*

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

$$SIPSER_d = \bigwedge_{i_1 \leq m_1} \bigvee_{i_2 \leq m_2} \bigwedge_{i_3 \leq m_3} \cdots \bigodot_{i_d \leq m_d} x_{i_1 i_2 i_3 \dots i_d},$$

where  $\bigodot = \bigvee$  or  $\bigwedge$  depending on the parity of  $d$ . The variables  $x_1, \dots, x_n$  appear as  $x_{i_1 i_2 i_3 \dots i_d}$  for  $i_j \leq m_j$ , where  $m_1 = \sqrt{m/\log m}$ ,  $m_2 = m_3 = \dots = m_{d-1} = m$ ,  $m_d = \sqrt{dm \log m/2}$  and  $m = (n\sqrt{2/d})^{1/(d-1)}$ .

**COROLLARY 5.12.** *Fix an integer  $d \geq 2$ . Let  $(C_d^n)_{n \in \mathbb{N}}$  be a family of polynomial-size depth- $(d+3)$  circuits computing the function  $SIPSER_{d+3}(x_1, \dots, x_n)$ . Then the QBFs  $Q-C_d^n$  need exponential-size refutations in Frege  $AC_d^0 + \forall$ red, but have polynomial-size refutations in Frege  $AC_{d+3}^0 + \forall$ red.*

**PROOF.** The lower bound follows from Theorem 5.10 and from the result that for every  $d$ ,  $SIPSER_{d+3}$  needs exponential-size depth- $(d+2)$  circuits [Håstad 1986]. Regarding the upper bound, by construction  $C_d^n$  has depth  $d+3$  and polynomial-size. Hence, by Theorem 5.10, the family  $Q-C_d^n$  has polynomial-size refutations in Frege  $AC_{d+3}^0 + \forall$ red.  $\square$

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 Characterizing QBF Frege and Extended Frege Lower Bounds

We finally address the question of lower bounds for Frege +  $\forall$ red or even EF +  $\forall$ red. Our next result states that achieving such lower bounds unconditionally will either imply a major breakthrough in circuit complexity or a major breakthrough in classical proof complexity. (Notice that it might be much easier to obtain the disjunction than any of the disjuncts.)

**THEOREM 5.13.** *Let  $\mathcal{C}$  be either P/poly or  $\text{NC}^1$ .  $\mathcal{C}$ -Frege +  $\forall\text{red}$  is not polynomially bounded if and only if  $\text{PSPACE} \not\subseteq \mathcal{C}$  or  $\mathcal{C}$ -Frege is not polynomially bounded.<sup>7</sup>*

**PROOF.** Clearly if  $\mathcal{C}$ -Frege is not polynomially bounded then  $\mathcal{C}$ -Frege +  $\forall\text{red}$  is not polynomially bounded. If  $\text{PSPACE} \not\subseteq \mathcal{C}$ , then let  $f$  be a Boolean function in  $\text{PSPACE}$  but not in  $\mathcal{C}$ . Since QBF is  $\text{PSPACE}$ -complete there exists a QBF  $Q\vec{w}\varphi(\vec{w}, x_1, \dots, x_n)$  with a CNF  $\varphi$  such that

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

We define

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

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

In the opposite direction, assume that  $\mathcal{C}$ -Frege +  $\forall\text{red}$  is not polynomially bounded. Then there is a sequence of true QBFs  $Q\psi_n$  such that  $\neg Q\psi_n$  do not have polynomial-size refutations in  $\mathcal{C}$ -Frege +  $\forall\text{red}$ . Let  $Q\psi_n$  have the form

$$\forall x_1 \exists y_1 \cdots \forall x_n \exists y_n \psi_n(x_1, \dots, x_n, y_1, \dots, y_n).$$

If  $\text{PSPACE} \not\subseteq \mathcal{C}$ , then we are done. Otherwise, there are polynomial-size circuits  $C_i$  witnessing the existential quantifiers in  $Q\psi_n$ . That is, for any  $x_1, \dots, x_n, y_1, \dots, y_n$

$$\bigwedge_{i=1}^n (y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})) \rightarrow \psi_n(x_1, \dots, x_n, y_1, \dots, y_n). \quad (22)$$

We claim that (22) is a sequence of tautologies without polynomial-size EF proofs. Otherwise, having  $\neg\psi_n$ ,  $\mathcal{C}$ -Frege can derive  $\bigvee_i y_i \neq C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})$  by a polynomial-size proof, and so as in Theorem 4.5,  $\mathcal{C}$ -Frege +  $\forall\text{red}$  can efficiently refute  $\neg Q\psi_n$ .  $\square$

Recall that a problem is in *uniform*  $\text{NC}^1$  if it is in  $\text{NC}^1$  and, in addition, there is a polynomial-time algorithm that for each input length generates an  $\text{NC}^1$  circuit solving the problem. We remark that we do have a separation between *uniform*  $\text{NC}^1$  and  $\text{PSPACE}$ , because  $\text{uniform NC}^1 \subseteq \text{L}$  and  $\text{L} \neq \text{PSPACE}$  by the space hierarchy theorem. Therefore, choosing  $f \in \text{PSPACE} \setminus \text{uniform NC}^1$  and considering the prenex formulas  $\Theta_n$  arising from  $Q\text{-}f_n$ , we can infer the weaker result that Frege +  $\forall\text{red}$  has no *uniform* short proofs of  $\Theta_n$ .

## 6 RELATION OF QBF FREGE TO SEQUENT SYSTEMS AND BOUNDED ARITHMETIC

Having defined and analyzed the new QBF Frege systems, it is natural to ask how they compare to classic sequent calculi—which have a long history for QBF [Cook and Morioka 2005; Dowd 1985; Egly 2012; Krajíček and Pudlák 1990]—and first-order theories of bounded arithmetic. After reviewing the necessary prerequisites, we approach both of these questions in this section.

### 6.1 Background on Sequent Systems and Bounded Arithmetic

**6.1.1 Sequent Calculi.** Gentzen's sequent calculus [Gentzen 1935] is a classical proof system, both for first-order and propositional logic, cf. Krajíček [1995]. The propositional sequent calculus LK operates with sequents  $\Gamma \longrightarrow \Delta$  with the semantic meaning  $\bigwedge_{\varphi \in \Gamma} \varphi \models \bigvee_{\psi \in \Delta} \psi$ .

<sup>7</sup>By  $\text{NC}^1$ , we mean *non-uniform*  $\text{NC}^1$ . Note that by the space hierarchy theorem it is known that  $\text{PSPACE} \not\subseteq \text{uniform NC}^1$ , but this does not suffice for Frege +  $\forall\text{red}$  lower bounds.



An important rule in LK is the cut rule

$$\frac{\Gamma \longrightarrow \Delta, A \quad A, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta} \text{(cut rule),}$$

where  $A$  is called the cut formula. Standard axioms such as  $0 \longrightarrow$  and  $\longrightarrow 1$  are included in the system LK as well. LK is well known to be p-equivalent to Frege, cf. Krajíček [1995].

The *quantified propositional calculus*  $G$ , as defined by Cook and Morioka [2005], extends Gentzen's classical propositional sequent calculus LK by allowing quantified propositional formulas in sequents and by adopting the following extra quantification rules for  $\forall$ -introduction:

$$\frac{\phi(x/\psi), \Gamma \longrightarrow \Delta}{\forall x \phi, \Gamma \longrightarrow \Delta} (\forall\text{-I}) \quad \frac{\Gamma \longrightarrow \Delta, \phi(x/p)}{\Gamma \longrightarrow \Delta, \forall x \phi} (\forall\text{-r})$$

and  $\exists$ -introduction

$$\frac{\phi(x/p), \Gamma \longrightarrow \Delta}{\exists x \phi, \Gamma \longrightarrow \Delta} (\exists\text{-I}) \quad \frac{\Gamma \longrightarrow \Delta, \phi(x/\psi)}{\Gamma \longrightarrow \Delta, \exists x \phi} (\exists\text{-r}).$$

For the rules  $\forall$ -I and  $\exists$ -r,  $\phi(x/\psi)$  is the result of substituting  $\psi$  for all free occurrences of  $x$  in  $\phi$ . The formula  $\psi$  may be any quantifier-free formula (i.e., without bounded variables) that is free for substitution for  $x$  in  $\phi$  (i.e., no free occurrence of  $x$  in  $\phi$  is within the scope of a quantifier  $Qy$  such that  $y$  occurs in  $\psi$ ). The variable  $p$  in the rules  $\forall$ -r and  $\exists$ -I must not occur free in the bottom sequent.

For  $i \geq 0$ ,  $G_i$  is a subsystem of  $G$  with cuts restricted to prenex  $\Sigma_i^q \cup \Pi_i^q$ -formulas. On propositional formulas  $G_0$  is p-equivalent to Frege and  $G_1$  is p-equivalent to EF, cf. Krajíček [1995]. The systems  $G$  and  $G_i$  were originally introduced slightly differently, cf. Krajíček and Takeuti [1992], Krajíček [1995], and Krajíček and Pudlák [1990], not restricting the formulas  $\psi$  in  $\forall$ -I and  $\exists$ -r to be quantifier-free, and defining  $G_i$  as the system  $G$  allowing only  $\Sigma_i^q$ -formulas in sequents. Hence,  $G_i$ 's could not prove all true QBFs. We will, however, use the redefinition of these systems by Cook and Morioka [2005]. Notably, (for Cook and Morioka's definition) Jerábek and Nguyen [2011] showed that the system  $G_i$  with cuts restricted to prenex  $\Sigma_i^q$ -formulas is p-equivalent to  $G_i$  with cuts restricted to prenex  $\Pi_i^q$ -formulas and p-equivalent to  $G_i$  with cuts restricted to (not necessarily prenex)  $\Sigma_i^q \cup \Pi_i^q$ -formulas. Moreover, these equivalences hold as well for the tree-like versions of these systems. Cook and Morioka [2005] also proved that their definition of  $G_i$  is p-equivalent to  $G_i$  from Krajíček and Pudlák [1990] for  $i \geq 0$  and prenex  $\Sigma_i^q \cup \Pi_i^q$ -formulas (so, by Jerábek and Nguyen [2011], also for non-prenex ones). Finally, the systems  $G_i$  and tree-like  $G_i$  have quite constructive *witnessing properties*. Whenever there are polynomial-size tree-like  $G_1$  proofs of formulas  $\exists y A_n(x, y)$  for  $A_n(x, y) \in \Sigma_1^q$ , there exist polynomial-size circuits  $C_n$  witnessing the existential quantifiers, i.e., the formula  $A_n(x, C_n(x))$  holds, cf. Cook and Morioka [2005], Theorem 7. In case of  $G_0$ , the circuits witnessing  $\Sigma_1^q$ -formulas are from  $\text{NC}^1$ , cf. Cook and Morioka [2005], Theorem 9. The witnessing theorems can be generalized to systems tree-like  $G_i$  and  $G_i$  for  $i \geq 1$  w.r.t.  $\Sigma_i^q$ -formulas and witnessing functions corresponding to higher levels of the polynomial hierarchy.

**6.1.2 Bounded Arithmetic.** In first-order logic, it is customary to consider the language  $L = \{0, S, +, \cdot, \leq, \lfloor \frac{x}{2} \rfloor, |x|, \#\}$ , where the function  $|x|$  is intended to mean "the length of the binary representation of  $x$ " and  $x\#y = 2^{|x| \cdot |y|}$ .

A quantifier is *bounded* if it has the form  $\exists x, x \leq t$  or  $\forall x, x \leq t$  for  $x$  not occurring in the term  $t$ . A bounded quantifier is *sharply bounded* if  $t$  has the form  $|s|$  for some term  $s$ . By  $\Sigma_0^b (= \Pi_0^b = \Delta_0^b)$ , we denote the set of all formulas in the language  $L$  with all quantifiers sharply bounded. For  $i \geq 0$ , the sets  $\Sigma_{i+1}^b$  and  $\Pi_{i+1}^b$  are defined inductively.  $\Sigma_{i+1}^b$  is the closure of  $\Pi_i^b$  under bounded existential and sharply bounded quantifiers, and  $\Pi_{i+1}^b$  is the closure of  $\Sigma_i^b$  under bounded universal and sharply bounded quantifiers; that is, the complexity of bounded formulas in the language  $L$  (formulas with

all quantifiers bounded) is defined by counting the number of alternations of bounded quantifiers, ignoring the sharply bounded ones. For  $i > 0$ ,  $\Delta_i^b$  denotes  $\Sigma_i^b \cap \Pi_i^b$ .

Bounded formulas capture the polynomial hierarchy: for any  $i > 0$  the  $i$ th level  $\Sigma_i^p$  of the polynomial hierarchy coincides with the sets of natural numbers definable by  $\Sigma_i^b$ -formulas. Dually for  $\Pi_i^p$  and  $\Pi_i^b$ .

Buss [1986a] introduced theories of bounded arithmetic  $S_2^i, T_2^i$  for  $i \geq 1$  in the language  $L$ . The axioms of  $S_2^i$  consist of a set of basic axioms defining properties of symbols from  $L$ , cf. Krajíček [1995], and length induction  $\Sigma_i^b$ -LIND, which is the following scheme for  $\Sigma_i^b$ -formulas  $A$  (or equivalently, for  $A \in \Pi_i^b$ , in which case, we speak of  $\Pi_i^b$ -LIND):

$$A(0) \wedge \forall x (A(x) \rightarrow A(x+1)) \rightarrow \forall x A(|x|).$$

Theories  $T_2^i$  are defined similarly, but here the induction scheme is

$$A(0) \wedge \forall x (A(x) \rightarrow A(x+1)) \rightarrow \forall x A(x)$$

for  $A \in \Sigma_i^b$ .

By  $\text{FP}_i^{\Sigma_i^b}[O(\log n)]$ , we denote the set of functions computed by a polynomial-time Turing machine making at most  $O(\log n)$  queries to a  $\Sigma_i^p$ -oracle.  $\text{FP}_i^{\Sigma_i^b}$  is defined analogously but without the restriction on the number of queries.  $T_2^i$  proves the totality of functions  $\text{FP}_i^{\Sigma_i^b}$  computable in polynomial time under a  $\Sigma_i^p$  oracle, cf. Krajíček [1995], Theorem 6.1.2. More precisely, for any  $f \in \text{FP}_i^{\Sigma_i^b}$  there is a  $\Sigma_{i+1}^b$ -formula  $f(x) = y$  such that  $T_2^i \vdash \forall x \exists y f(x) = y$ . In the same way,  $S_2^i$  proves the totality of functions in  $\text{FP}_i^{\Sigma_i^b}[O(\log n)]$ , which are computed in polynomial time with at most  $O(\log n)$  queries to a  $\Sigma_i^p$ -oracle, cf. Krajíček [1995], Theorem 6.2.2. By Parikh's theorem,  $T_2^i \vdash \exists y f(x) = y$  implies  $T_2^i \vdash \exists y (|y| \leq p(|x|) \wedge f(x) = y)$  for some polynomial  $p$ , and the same is true for  $S_2^i$ , cf. Buss [1986a] and Parikh [1971].

$S_2^i$  can be seen as a first-order non-uniform version of tree-like  $G_i$ ,  $i \geq 1$ . First, for  $j \geq 1$  any  $\Sigma_j^b$ -formula  $\varphi(x)$  can be translated into a sequence  $\|\varphi(x)\|^n$  of  $\Sigma_j^q$ -formulas, where  $n$  denotes the size of the input  $x$  in binary (cf. Krajíček [1995], Definition 9.2.1). Then, for  $i, j \geq 1$ , whenever  $S_2^i \vdash A$  for  $A \in \Sigma_j^b$ , there is a polynomial  $p$  such that formulas  $\|A\|^n$  have tree-like  $G_i$ -proofs of size  $p(n)$ . This also holds for  $T_2^i$  in place of  $S_2^i$  if tree-like  $G_i$  is replaced by  $G_i$ . The ability to use arbitrary  $j$  is due to Cook and Morioka [2005] (Theorem 3), who generalized a standard result, cf. Krajíček [1995] (Theorem 9.2.6), which worked for  $j = i$ .

If  $A \in \Pi_1^b$ , then we abuse notation and also denote by  $\|A\|^n$  the propositional formulas obtained as in  $\|A\|^n$ , but leaving the universally quantified variables free.  $S_2^i \vdash A$  for  $A \in \Pi_1^b$  implies that  $S_2^i$  proves the existence of polynomial-size tree-like  $G_1$ -proofs of propositional formulas  $\|A\|^n$ , cf. Krajíček [1995] (Theorems 9.2.6 and 9.2.7).

## 6.2 Intuitionistic Logic Corresponds to Extended Frege for QBFs

The main information on strong propositional and QBF systems stems from their correspondence to first-order theories of bounded arithmetic, cf. Beyersdorff [2009], Cook and Nguyen [2010], and Krajíček [1995]. In this sense, tree-like  $G_1$  corresponds to  $S_2^1$  and  $G_1$  to  $T_2^1$  as explained above. Here, we will establish such a correspondence between first-order intuitionistic logic and  $\text{EF} + \forall\text{red}$ .

Buss [1986b] developed an intuitionistic version of  $S_2^1$ , denoted  $\text{IS}_2^1$ , and showed that for *any* formula  $A$ ,  $\text{IS}_2^1 \vdash \exists y A(x, y)$  implies the existence of a polynomial-time function  $f$  such that  $A(x, f(x))$  holds. This witnessing property resembles the Strategy Extraction Theorem for  $\text{EF} + \forall\text{red}$ . Using

the formalized Strategy Extraction Theorem, we can make the correspondence between these systems formal.<sup>8</sup>

First, we recall the definition of  $IS_2^1$  by Cook and Urquhart [1993]. It is equivalent to Buss' original definition, cf. Buss [1986b].  $IS_2^1$  is a theory in the language  $L$  (like  $S_2^1$ ), with underlying intuitionistic predicate logic, a set of basic axioms defining properties of symbols from  $L$ , and a polynomial induction scheme for  $\Sigma_1^{b+}$ -formulas  $A$ :

$$A(0) \wedge \forall x \left( A \left( \left\lfloor \frac{x}{2} \right\rfloor \right) \rightarrow A(x) \right) \rightarrow \forall x A(x),$$

where  $\Sigma_1^{b+}$ -formulas are  $\Sigma_1^b$ -formulas without negation and implication connectives.  $S_2^1$  is  $\Sigma_0^b$ -conservative over  $IS_2^1$ , cf. Cook and Urquhart [1993] (Corollary 1.7); that is, any  $\Sigma_0^b$  formula provable in  $S_2^1$  is provable already in  $IS_2^1$ .

We will also use Cook and Urquhart's conservative extension of  $IS_2^1$  denoted IPV, cf. Cook and Urquhart [1993] (Chapter 4 and Theorem 4.12). IPV is defined by adding intuitionistic predicate logic to Cook's theory PV, cf. Cook [1975]. The language of IPV consists of symbols for all polynomial-time functions. The hierarchy of formulas  $\Pi_i^b$ (IPV) is defined analogously as  $\Pi_i^b$  but in the language of IPV. Also, propositional translations  $\|A\|^n$  for  $\Pi_1^b$ (IPV)-formulas  $A$  are defined analogously as in the case of  $A \in \Pi_1^b$ . Consequently,  $IPV \vdash A$  for  $A \in \Pi_1^b$ (IPV) implies that propositional formulas  $\|A\|^n$  have polynomial-size EF proofs, cf. Krajíček [1995] (Theorem 9.2.7).

Cook and Urquhart [1993] (Corollary 8.18) generalized Buss' witnessing theorem: Whenever  $IPV \vdash \forall x \exists y A(x, y)$  for an arbitrarily complex formula  $A$ , then there is a polynomial-time function  $f$  (with an IPV function symbol  $f$ ) such that  $IPV \vdash \forall x A(x, f(x))$ .

We are now ready to derive the correspondence between  $IS_2^1$  and  $EF + \forall red$ . The correspondence consists of two parts (cf. Beyersdorff [2009]). For the first part, we translate first-order formulas  $\varphi$  into sequences of QBFs [Krajíček and Pudlák 1990] and show that translations of provable  $IS_2^1$  formulas have short  $EF + \forall red$  proofs.

**THEOREM 6.1.** *If  $IS_2^1$  proves a statement  $T$  in prenex form, then there exist polynomial-size  $EF + \forall red$  refutations of  $\|\neg T\|^n$  where  $n$  denotes the size of the input variables in binary.*

**PROOF.** By Cook and Urquhart's improvements of Buss' witnessing theorem, if  $IS_2^1$  proves  $T$  of the form

$$\forall x_1 \exists y_1 \cdots \forall x_n \exists y_n T'(x_1, \dots, x_n, y_1, \dots, y_n)$$

for  $T' \in \Sigma_0^b$ , then there is an IPV-function  $f_1(x_1)$  such that

$$IPV \vdash \forall x_1 \forall x_2 \exists y_2 \cdots \forall x_n \exists y_n T'(x_1, \dots, x_n, f_1(x_1), y_2, \dots, y_n).$$

Iterating this argument all existential quantifiers of  $T$  can be witnessed provably in IPV by polynomial-time functions  $f_1, \dots, f_n$ . Therefore, IPV proves the  $\Pi_1^b$ (IPV) formula

$$\varphi = \bigwedge_{i=1}^n (y_i \leftrightarrow f_i(x_1, \dots, x_i)) \rightarrow T'(x_1, \dots, x_n, y_1, \dots, y_n) \quad (23)$$

and the formulas  $\|\varphi\|^n$  have polynomial-size EF proofs.  $EF + \forall red$  can now refute  $\|\neg T\|^n$  in polynomial size by deriving  $\bigvee_i (y_i \neq f_i(x_1, \dots, x_i))$  and cutting all the disjuncts as in the proof of Theorem 4.5.  $\square$

<sup>8</sup>It could be tempting to expect that an adequate counterpart to  $IS_2^1$  would be intuitionistic propositional logic. However, intuitionistic propositional logic admits the feasible interpolation property, cf. Buss and Mints [1999], while  $IS_2^1$  can (constructively) prove  $\forall x, z [A(x, y) \vee B(x, z)]$ , in principle, without the existence of an efficient interpolant. It is also known, cf. Ghasemloo and Pich [2013], that  $IS_2^1 \vdash \forall y A(x, y) \vee \forall z B(x, z)$  implies the existence of an efficient interpolating circuit, but moving the universal quantifiers inside the disjunction is *a priori* not allowed in intuitionistic logic.

The second part of the correspondence consists in proving the soundness of the proof systems in the first-order theory. For this, we need to express the correctness of  $\text{EF} + \forall\text{red}$  by QBFs. This is typically done by the *reflection principle* of a proof system  $P$ , stating that whenever  $\varphi$  has a  $P$ -proof (respectively, a  $P$ -refutation), then  $\varphi$  is true (respectively, false).

Here, the Formalized Strategy Extraction Theorem allows us to express the reflection principle of  $\text{EF} + \forall\text{red}$  by a  $\Pi_1^b$ -formula  $\text{REF}(\text{EF} + \forall\text{red})$ . More precisely, we define  $\text{REF}(\text{EF} + \forall\text{red})$  as the  $\Pi_1^b$ -formula expressing that if  $\pi$  is a proof of a QBF, then circuits  $C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})$  obtained as in the Strategy Extraction Theorem witness the existential quantifiers in the QBF as in the statement of Theorem 6.2 below.

To show this reflection principle in  $\text{IS}_2^1$ , we return again to the Strategy Extraction Theorem and provide a different formalization than in Theorem 4.4, this time in the theory  $\text{S}_2^1$ .

**THEOREM 6.2 (FORMALIZED STRATEGY EXTRACTION).** *There is a linear-time algorithm  $A$  such that  $\text{S}_2^1$  proves the following: Assume that  $\pi$  is an  $\text{EF} + \forall\text{red}$  refutation of a QBF  $\psi$  of the form*

$$\exists x_1 \forall y_1 \cdots \exists x_n \forall y_n \varphi(x_1, \dots, x_n, y_1, \dots, y_n),$$

where  $\varphi \in \Sigma_0^q$ . Then  $A(\pi)$  outputs  $n$  circuits  $C_1(x_1), \dots, C_n(x_1, \dots, x_n, y_1, \dots, y_{n-1})$  defining a winning strategy for the universal player on formula  $\psi$ ; that is,

$$\forall x_1 \cdots \forall x_n \forall y_1 \cdots \forall y_n \left[ \bigwedge_{i=1}^n (y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})) \rightarrow \neg \varphi(x_1, \dots, x_n, y_1, \dots, y_n) \right].$$

**PROOF.** It is just sufficient to inspect the proof of the Strategy Extraction Theorem from Section 4 and point out that it essentially uses a  $\Pi_1^b$ -induction on the number of steps in the proof  $\pi$ ; that is,  $\Pi_1^b$ -LIND available in  $\text{S}_2^1$ . For convenience of the reader, we recap here what was the approach. Let  $\pi = (L_1, \dots, L_s)$  be an  $\text{EF} + \forall\text{red}$  refutation of the QBF  $Q \varphi$  given as in Theorem 6.2 and put

$$\begin{aligned} \pi_s &= \emptyset, & \pi_i &= (L_{i+1}, \dots, L_s) \text{ for } i < s, \\ \varphi_0 &= \varphi, & \varphi_i &= \varphi \wedge L_1 \wedge \cdots \wedge L_i \text{ for } i > 0. \end{aligned}$$

We show by downward induction on  $i$ , that from  $\pi_i$  it is possible to construct in linear time a winning strategy

$$\sigma^i = \{C_1^i(x_1), \dots, C_n^i(x_1, \dots, x_n, y_1, \dots, y_{n-1})\}$$

for the universal player for the QBF  $Q \varphi_i$ . The statement of the Formalized Strategy Extraction Theorem corresponds to the case  $i = 0$ .

In the base case,  $\varphi_s$  contains a contradiction, and the winning strategy can be defined as the set of trivial circuits  $\{0, \dots, 0\}$ . Assume now that  $\sigma^i$  is a winning strategy for  $Q \varphi_i$ . If  $L_i$  is derived by an EF rule, then we set  $\sigma^{i-1} = \sigma^i$ . Assume now that  $L_i = L_j[u/B]$  is the result of an application of a  $\forall\text{red}$  rule on  $L_j$  where  $u$  is the rightmost variable in  $L_j$ . We define  $C_l^{i-1} = C_l^i$  if  $u \neq y_l$ ; otherwise, we set

$$C_l^{i-1}(z) = \begin{cases} B(z) & \text{if } L_j[u/B](z) = 0, \\ C_l^i(z) & \text{if } L_j[u/B](z) = 1. \end{cases}$$

This constructs circuits  $C_l^i$  from  $\pi_i$  by a standard  $O(|\pi_i|)$ -time algorithm. To show that the strategies  $\sigma^i$  are winning for any  $0 \leq i \leq |\pi|$ , we need to analyze the inductive step.

Assume that  $\sigma^i$  is the winning strategy for the universal player on  $Q \varphi_i$ . If  $L_i$  is derived by an EF rule, then the winning strategy for  $Q \varphi_i$  works also for  $Q \varphi_{i-1}$ , because a falsification of  $L_i$  by a given assignment implies a falsification of one of its predecessors. If  $L_i$  is the result of an application of  $\forall\text{red}$ , then  $C_l^{i-1}(z)$  is redefined only if  $L_j[u/B](z) = 0$ . For  $z$  such that  $L_j[u/B](z) = 1$ , the strategy  $\sigma^i$  has to work also for  $Q \varphi_{i-1}$ . Therefore,  $\sigma^{i-1}$  is a winning strategy for the universal player on  $Q \varphi_{i-1}$ .

An NP predicate is a set of binary strings accepted by a non-deterministic polynomial-time machine, and similarly for coNP predicates. The statement that a strategy  $\sigma$  is winning for the universal player on  $Q\psi$  is a coNP predicate (given  $\pi$ ) expressible as a well-behaved  $\Pi_1^b$ -formula. The induction we used is on the number of steps in  $\pi$ . Hence, the presented proof is an  $S_2^1$ -proof.  $\square$

This implies the second part of the correspondence of  $IS_2^1$  to  $EF + \forall\text{red}$ .

**COROLLARY 6.3.**  $IS_2^1$  proves  $\text{REF}(EF + \forall\text{red})$ .

**PROOF.** The claim follows from Theorem 6.2 together with the  $\Sigma_0^b$ -conservativity of  $S_2^1$  over  $IS_2^1$  [Cook and Urquhart 1993].  $\square$

Corollary 6.3 implies that  $EF + \forall\text{red}$  is the weakest proof system that allows short proofs of all  $IS_2^1$  theorems, i.e., whenever Theorem 6.1 holds for a “decent” proof system  $P$  in place of  $EF + \forall\text{red}$ , then  $P$   $p$ -simulates  $EF + \forall\text{red}$  on QBFs: If Theorem 6.1 holds for a proof system  $P$ , then by Corollary 6.3, there are polynomial-size  $P$ -proofs of  $\|\text{REF}(EF + \forall\text{red})\|^n$ . Hence, if  $\pi$  is an  $EF + \forall\text{red}$  proof of a QBF  $\psi$ , then  $P$  has  $|\pi|^{O(1)}$ -size proofs of  $\psi$  with the existential quantifiers witnessed by some circuits. By  $P$  being decent, we mean that  $P$  can introduce efficiently the existential quantifiers in place of the witnessing circuits and this way prove  $\psi$  efficiently in the size of  $\pi$ ; that is,  $P$  is decent if it can derive  $\psi$  efficiently in the length of the shortest derivation of  $\psi$  witnessed by some circuits.

However,  $EF + \forall\text{red}$  is intuitively the strongest proof system for which  $IS_2^1$  proves the reflection principle. Technically, this only holds for proof systems that admit the Strategy Extraction Theorem, as for other systems, we would need to define the reflection principle as a more complex statement. (Nevertheless,  $IS_2^1$  provability of the reflection principle for  $\Sigma_k^q$ -formulas for any fixed  $k$  implies strategy extraction for the given proof system.)

### 6.3 Gentzen and Frege for QBFs

We now compare the classic Gentzen systems with our new Frege systems. The two formalisms are well known to be equivalent in the classical propositional case [Krajíček 1995]. By applying the formalized Strategy Extraction Theorem, we show that Gentzen systems simulate Frege systems in the QBF context (cf. Figure 1 in Section 1.1). However, the opposite simulations (Gentzen by Frege) are very likely false as we show by a number of conditional separations.

**THEOREM 6.4.** *Tree-like  $G_1$   $p$ -simulates  $EF + \forall\text{red}$ .*

**PROOF.** By Theorem 4.5, any  $EF + \forall\text{red}$  refutation  $\pi$  of a QBF  $\psi$  of the form

$$\exists x_1 \forall y_1 \cdots \exists x_n \forall y_n \varphi(x_1, \dots, x_n, y_1, \dots, y_n)$$

where  $\varphi \in \Sigma_0^q$  can be transformed in time  $|\pi|^{O(1)}$  into an  $EF$  proof of

$$\bigwedge_{i=1}^n (y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})) \rightarrow \neg\varphi(x_1, \dots, x_n, y_1, \dots, y_n)$$

for certain circuits  $C_i$ . We want to derive  $\neg\psi$  in tree-like  $G_1$ . Since we do not distinguish between a refutation of  $\psi$  and provability of  $\neg\psi$ , this will prove the theorem.

**CLAIM 6.5.** *There is a  $|\pi|^{O(1)}$ -size tree-like  $G_1$  proof of the following sequent*

$$\{y_i = C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})\}_{i=1}^n \longrightarrow \neg\varphi(x_1, \dots, x_n, y_1, \dots, y_n)$$

where the encoding of circuits  $C_i$  might use some auxiliary variables.

PROOF OF CLAIM. To see that the claim holds, note first that by the p-equivalence of EF and tree-like  $G_1$  (cf. Krajíček [1995]), the EF proof obtained above can be turned into a  $|\pi|^{O(1)}$ -size tree-like  $G_1$ -proof of the formula

$$\neg \left( \bigwedge_{i=1}^n y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1}) \right) \vee \neg \varphi.$$

This proof can be easily modified so the  $\vee$  connective is not introduced, leading to a  $|\pi|^{O(1)}$ -size tree-like  $G_1$ -proof of the sequent

$$\longrightarrow \neg \left( \bigwedge_{i=1}^n y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1}) \right), \neg \varphi.$$

Moving  $\neg(\bigwedge_{i=1}^n y_i = C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1}))$  from the succedent to the antecedent, we obtain

$$\bigwedge_{i=1}^n (y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})) \longrightarrow \neg \varphi.$$

Finally, tree-like  $G_1$  derives the sequent we want by “not introducing”  $\wedge$  in the antecedent. This proves the claim.  $\square$

Moving  $\neg \varphi$  to the succedent, applying  $\forall$ -I and  $\exists$ -I introductions, tree-like  $G_1$  then derives

$$\forall y_n \varphi(x_1, \dots, x_n, y_1, \dots, y_n), \Gamma, \exists y_n (y_n \leftrightarrow C_n(x_1, \dots, x_n, y_1, \dots, y_{n-1})) \longrightarrow$$

where  $\Gamma = \{y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})\}_{i=1}^{n-1}$ .

As tree-like  $G_1$  proves efficiently  $\longrightarrow \exists y (y \leftrightarrow C(x))$  for any circuit  $C$ , we can cut the formula  $\exists y_n (y_n \leftrightarrow C_n(x_1, \dots, x_n, y_1, \dots, y_{n-1}))$  out of the antecedent and derive

$$\forall y_n \varphi, \{y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})\}_{i=1}^{n-1} \longrightarrow .$$

Now, we use  $\exists$ -I introduction to obtain

$$\exists x_n \forall y_n \varphi, \{y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})\}_{i=1}^{n-1} \longrightarrow .$$

In this way, we can gradually cut out all remaining formulas from the antecedent, quantify all variables, move  $\psi$  to the succedent, and derive  $\neg \psi$  in tree-like  $G_1$  by a proof of size  $|\pi|^{O(1)}$ .  $\square$

To introduce the quantifier prefix of  $\psi$  in the previous proof, we needed to cut  $\Sigma_1^q$ -formulas. We would like to use a similar proof to simulate Frege +  $\forall$ red by tree-like  $G_0$ . However, tree-like  $G_0$  is allowed to cut only  $\Sigma_0^q$ -formulas. Therefore, we obtain just a simulation of Frege +  $\forall$ red by tree-like  $G_0$  where the proven sequent in tree-like  $G_0$  contains a non-empty (easily derivable) antecedent.

THEOREM 6.6. *There is a polynomial-time function  $t$  such that given any Frege +  $\forall$ red refutation of a QBF  $\psi$  of the form*

$$\exists x_1 \forall y_2 \cdots \exists x_n \forall y_n \varphi(x_1, \dots, x_n, y_1, \dots, y_n)$$

where  $\varphi \in \Sigma_0^q$ ,  $t(\pi)$  is a tree-like  $G_0$  proof of the sequent

$$\forall x_1 \exists y_1 \cdots \forall x_n \exists y_n \bigwedge_{i=1}^n y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1}) \longrightarrow \neg \psi$$

for some formulas  $C_i$ . Note that the antecedent has a tree-like  $G_0$  proof of size  $|\pi|^{O(1)}$ .

PROOF. By Theorem 4.5, any Frege +  $\forall$ red refutation  $\pi$  of a QBF  $\psi$  can be transformed in time  $|\pi|^{O(1)}$  into a -Frege proof of

$$\bigwedge_{i=1}^n (y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1})) \rightarrow \neg\varphi(x_1, \dots, x_n, y_1, \dots, y_n)$$

for certain formulas  $C_i$ . Analogously as in the proof of Theorem 6.4, we efficiently obtain a  $|\pi|^{O(1)}$ -size tree-like  $G_0$  proof of

$$\bigwedge_{i=1}^n y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1}) \rightarrow \neg\varphi.$$

Applying rules  $\forall$ -I,  $\exists$ -I,  $\forall$ -I,  $\exists$ -I (in this order), we derive

$$\exists x_n \forall y_n \varphi, \forall x_n \exists y_n \bigwedge_{i=1}^n y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1}) \rightarrow .$$

In this way, we efficiently introduce all quantifiers, then move  $\psi$  to the succedent, and derive the required sequent in tree-like  $G_0$ .  $\square$

We now prove some conditional separations between Gentzen and Frege systems for QBF. As we saw in Section 5.3, improving these separations to unconditional results tightly corresponds to major open problems in circuit complexity and proof complexity.

**6.3.1 Formulas Hard in Gentzen, but Easy in Frege.** We first give formulas (conditionally) hard for  $G_0$ , but easy for  $EF + \forall$ red.

**THEOREM 6.7.** *If  $P/poly \neq NC^1$ , then there are  $\Sigma_1^q$ -formulas with polynomial-size  $EF + \forall$ red proofs but without polynomial-size  $G_0$  proofs.*

PROOF. Let  $f$  be a function in  $P/poly$ . Then  $EF + \forall$ red has simple polynomial-size proofs of  $\Sigma_1^q$  formulas  $\exists y \exists z f(x) = y$  expressing the totality of  $f$  with auxiliary variables  $z$  representing nodes of a polynomial-size circuit computing  $f$ . The  $EF + \forall$ red proof refutes the propositional formula  $f(x) \neq y$  by gradually replacing each variable from  $z, y$  by the circuit it represents. If the totality of  $f$  has polynomial-size  $G_0$  proofs, then by the  $\Sigma_1^q$  witnessing property, cf. Cook and Morioka [2005] (Theorem 9),  $f$  is in  $NC^1$ .  $\square$

Notably, in Section 4.2, we showed that  $Frege + \forall$ red and  $EF + \forall$ red are p-equivalent to their tree-like versions. This is open for  $G_0$  and  $G_1$ , thus providing some further evidence for the incomparability of Gentzen and Frege in QBF.

**6.3.2 Formulas Easy in Gentzen, but Hard in Frege.** We now provide three different properties that are easy for QBF Gentzen systems, but hard for  $EF + \forall$ red. Our first conditional result shows that there are  $\Sigma_2^q$ -formulas with polynomial-size tree-like  $G_1$  proofs but no polynomial-size  $EF + \forall$ red proofs, and this result generalizes to stronger systems.

**THEOREM 6.8.** *Let  $i \geq 1$ . Assume  $f \in FP^{\Sigma_i^p}$  is hard for  $P/poly$ . Then the formulas  $\|\exists y (|y| \leq p(|x|) \wedge f(x) = y)\|^n$ , where  $p$  is a polynomial and  $f(x) = y$  is expressed by a  $\Sigma_{i+1}^b$ -formula, have polynomial-size  $G_i$  proofs and require super-polynomial-size  $EF + \forall$ red proofs. If  $f \in FP^{\Sigma_i^p}[O(\log n)]$ , then  $G_i$  can be replaced by tree-like  $G_i$ .*

PROOF. Since  $T_2^i$  proves the totality of  $FP^{\Sigma_i^p}$  functions [Buss 1986a], it proves the totality of  $f$  and the proof can be transformed into a sequence of polynomial-size  $G_i$  proofs [Cook and Morioka

2005; Krajíček and Pudlák 1990]. If the totality of  $f$  can be shown by polynomial-size proofs in  $\text{EF} + \forall\text{red}$ , then, by the Strategy Extraction Theorem,  $f$  is in  $\text{P/poly}$ .

Similarly,  $S_2^i$  proves the totality of  $\text{FP}^{\Sigma_1^p}[O(\log n)]$  functions and such proofs translate into sequences of polynomial-size tree-like  $G_i$  proofs [Buss 1986a; Cook and Morioka 2005; Krajíček and Pudlák 1990].  $\square$

It seems that the separation above of tree-like  $G_1$  and  $\text{EF} + \forall\text{red}$  by  $\Sigma_2^q$ -formulas cannot be improved to  $\Sigma_1^q$ -formulas, as it is tight in the following sense. If we had  $\Sigma_1^q$ -formulas  $\exists y A_n(x, y)$  with polynomial-size tree-like  $G_1$  proofs but without polynomial-size  $\text{EF} + \forall\text{red}$  proofs, then this would imply that  $\text{EF}$  is not polynomially bounded: By the witnessing theorem for tree-like  $G_1$ , cf. Cook and Morioka [2005] (Theorem 7), there would be polynomial-size circuits  $C_n$  such that formulas  $A_n(x, C_n(x))$  are true, and so  $\neg A_n(x, C_n(x))$  would be hard to refute in  $\text{EF}$ .

The QBF proof systems tree-like  $G_1$  and  $\text{EF} + \forall\text{red}$  can be conditionally separated also on the bounded collection scheme.

*Definition 6.9.* The *bounded collection scheme*  $\text{BB}(\varphi)$  is the formula

$$\exists i < |a| \exists w < t(a) \forall u < a \forall j < |a| (\varphi(i, u) \rightarrow \varphi(j, [w]_j)),$$

where  $\varphi(i, u)$  is a formula that can have other free variables,  $[w]_j$  is the  $j$ th element of the sequence coded by  $w$ , and  $t(a)$  is a concrete  $L$ -term depending on the choice of the encoding of sequences.

Roughly,  $\text{BB}(\varphi)$  says that  $u$ 's witnessing  $\varphi(i, u)$  can be collected in a sequence  $w$ :

$$\forall i < |a| \exists u < a, \varphi(i, u) \rightarrow \exists w < t(a) \forall j < |a|, \varphi(j, [w]_j).$$

**THEOREM 6.10.** *The QBF proof system tree-like  $G_1$  has polynomial-size proofs of  $\|\text{BB}(\varphi)\|^n$  for all  $\varphi \in \Sigma_1^b$ . In contrast, there exists  $\varphi \in \Sigma_1^b$  such that formulas  $\|\text{BB}(\varphi)\|^n$  are hard for  $\text{EF} + \forall\text{red}$  unless each polynomial-time permutation with  $n$  inputs can be inverted by polynomial-size circuits with probability at least  $1 - 1/n$ .*

**PROOF.** The upper bound follows from the  $S_2^1$ -provability of  $\text{BB}(\varphi)$  for  $\varphi \in \Sigma_1^b$ , cf. Buss [1986a] (Theorem 14), and its transformation to tree-like  $G_1$  proofs [Cook and Morioka 2005; Krajíček and Pudlák 1990]. For the lower bound, we will use a result by Cook and Thapen [2006] showing that Cook's theory  $\text{PV}$  does not prove  $\text{BB}(\varphi)$  for all  $\varphi \in \Sigma_0^b$  unless factoring is in probabilistic polynomial time.

Let  $a = 2^n$  and  $\varphi(i, u)$  be the formula  $f(u) = [y]_i$  for a polynomial-time permutation  $f$  (defined by a  $\Sigma_1^b$  formula), and  $y$  encoding a sequence of  $n$  strings of length  $n$ .

Assume that  $\text{EF} + \forall\text{red}$  has polynomial-size proofs of  $\|\text{BB}(\varphi)\|^n$ . By the Strategy Extraction Theorem, there are polynomial-size circuits  $B, C$  such that

$$\exists u < 2^n, f(u) = [y]_{C(y)} \rightarrow \forall j < n, f([B(y)]_j) = [y]_j. \quad (24)$$

To invert  $f$ , we proceed as follows: Given  $z \in \{0, 1\}^n$ , pick randomly  $n$  strings  $s_i \in \{0, 1\}^n$  and let  $i_0$  be a position (a non-uniform advice) such that  $\Pr_y[C(y) = i_0] \leq 1/n$  where  $y$ 's are sequences of  $n$  strings of length  $n$ . Define  $y_{z,s}$  to be the sequence of elements  $z, f(s_1), \dots, f(s_{n-1})$  ordered so  $[y_{z,s}]_{i_0} = z$  and let  $x_{z,s}$  be the sequence of  $z, s_1, \dots, s_{n-1}$  ordered so  $f([x_{z,s}]_i) = [y_{z,s}]_i$  for  $i \neq i_0$ . For random strings  $z, s_1, \dots, s_{n-1}$ , we have that  $y_{z,s}$  is a random sequence of  $n$  strings of length  $n$  and  $\Pr_{z, s_1, \dots, s_n}[C(y_{z,s}) = i_0] \leq 1/n$ . Consequently, with probability at least  $1 - 1/n$ ,  $f([x_{z,s}]_{C(y_{z,s})}) = [y_{z,s}]_{C(y_{z,s})}$  holds and by Equation (24) the inverse of  $f$  on  $z$  is  $[B(y_{z,s})]_{i_0}$ .  $\square$

While the previous two results exhibited formulas easy for tree-like  $G_1$  and hard for  $\text{EF} + \forall\text{red}$ , we now show that even tree-like  $G_0$  can prove  $\Sigma_2^q$ -formulas hard for  $\text{EF} + \forall\text{red}$  (modulo a hardness assumption).



$$\begin{array}{c}
 \longrightarrow A_0(x, y), A_1(x, z) \\
 \hline
 \longrightarrow (A_0(x, y) \wedge \neg 0) \vee (A_1(x, u) \wedge 0), (A_0(x, v) \wedge \neg 1) \vee (A_1(x, z) \wedge 1) \\
 \hline
 \longrightarrow \forall y, u ((A_0(x, y) \wedge \neg 0) \vee (A_1(x, u) \wedge 0)), (A_0(x, v) \wedge \neg 1) \vee (A_1(x, z) \wedge 1) \\
 \hline
 \longrightarrow \forall y, u ((A_0(x, y) \wedge \neg 0) \vee (A_1(x, u) \wedge 0)), \forall y, u ((A_0(x, y) \wedge \neg 1) \vee (A_1(x, u) \wedge 1)) \\
 \hline
 \longrightarrow \exists b \forall y, u ((A_0(x, y) \wedge \neg b) \vee (A_1(x, u) \wedge b)), \exists b \forall y, u ((A_0(x, v) \wedge \neg b) \vee (A_1(x, z) \wedge b)) \\
 \hline
 \longrightarrow \exists b \forall y, u ((A_0(x, y) \wedge \neg b) \vee (A_1(x, u) \wedge b))
 \end{array}$$

Fig. 2. The tree-like  $G_0$  derivation in the proof of Theorem 6.11.

For this, we use a result by Bonet et al. [2000], who showed that Frege systems do not admit the so-called feasible interpolation property unless factoring of Blum integers is solvable by polynomial-size circuits. (A Blum integer is the product of two distinct primes, which are both congruent 3 modulo 4.)

It is possible to separate tree-like  $G_0$  and  $EF + \forall\text{red}$  even under the assumption  $NP \not\subseteq P/\text{poly}$ . The separating  $\Sigma_2^q$ -formulas are of the form

$$\forall x \exists y \forall z (\text{SAT}(x, y) \vee \neg \text{SAT}(x, z))$$

and state that each propositional formula is either satisfiable or unsatisfiable. These formulas have polynomial-size tree-like  $G_0$  proofs, because their two-sorted formulation is easily provable in the theory known as  $VNC^1$ , the two-sorted version of tree-like  $G_0$ , cf. Cook and Morioka [2005]. (In fact, this is already provable in the two-sorted logic without the extra axioms of  $VNC^1$ .) However, if these formulas were easy for  $EF + \forall\text{red}$ , by strategy extraction, we would get polynomial-size circuits for SAT. As presenting this argument formally would require to introduce two-sorted theories of bounded arithmetic and the corresponding machinery, we prove here only the separation based on the stronger assumption of the hardness of factoring.

**THEOREM 6.11.** *There are  $\Sigma_2^q$ -formulas with polynomial-size tree-like  $G_0$  proofs. However, assuming factoring of Blum integers is not computable by polynomial-size circuits, these formulas require  $EF + \forall\text{red}$  proofs of super-polynomial size.*

**PROOF.** Bonet et al. [2000] showed that there are propositional formulas  $A_0(x, y), A_1(x, z)$  with common variables  $x$  such that  $A_0(x, y) \vee A_1(x, z)$  have polynomial-size Frege proofs but, unless factoring of Blum integers is computable by polynomial-size circuits, there are no polynomial-size circuits  $C(x)$  recognizing which of  $A_0(x, y)$  or  $A_1(x, z)$  holds for a given  $x$ .

Frege is p-equivalent to tree-like  $G_0$  on propositional formulas [Krajíček 1995] and so it is possible to derive in tree-like  $G_0$  the sequents in Figure 2.

Therefore, the  $\Sigma_2^q$ -formulas

$$\exists b \forall y \forall u ((A_0(x, y) \wedge \neg b) \vee (A_1(x, u) \wedge b))$$

have polynomial-size tree-like  $G_0$  proofs.

If these formulas had polynomial-size  $EF + \forall\text{red}$  proofs, then, by the Strategy Extraction Theorem, there would be polynomial-size circuits computing  $b$  from  $x$  and thus recognizing which of  $A_0(x, y)$  and  $A_1(x, u)$  holds.  $\square$

We remark that the assumptions of Theorems 6.10 and 6.11 are stronger than the assumption of Theorem 6.8. However, while factoring forms a good candidate for a one-way function, it is not known if the existence of one-way functions implies the existence of one-way permutations.

## 7 CONCLUSION

Our work opens up two lines of research that we believe might have a significant influence on QBF proof complexity and beyond.

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

*Understanding the transfer from circuit to proof complexity.* As far as we know, for the first time in the literature, our lower bound technique via strategy extraction gives a formal and rigorous account on the relation between a circuit class  $\mathcal{C}$  and proof systems using lines from  $\mathcal{C}$ . Building on the previous work of Beyersdorff et al. [2015], 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.(i) and (iii) in Section 1.1 are referenced as “the main open problems at the ‘frontier’ of Cook’s program.”

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

## ACKNOWLEDGMENTS

The authors are grateful to Nicola Galesi and Albert Atserias for interesting discussions on this work and circuit complexity in general, and to Emil Jeřábek for pointing out the separation of tree-like  $G_0$  and EF +  $\forall$ red under the weaker assumption  $NP \not\subseteq P/poly$ .

We also thank the anonymous reviewers for their very careful reading of the manuscript and their detailed and useful comments.

## REFERENCES

- Miklós Ajtai. 1994. The complexity of the pigeonhole-principle. *Combinatorica* 14, 4 (1994), 417–433.
- Sanjeev Arora and Boaz Barak. 2009. *Computational Complexity—A Modern Approach*. Cambridge University Press.
- Valeriy Balabanov and Jie-Hong R. Jiang. 2012. Unified QBF certification and its applications. *Form. Methods Syst. Des.* 41, 1 (Aug. 2012), 45–65.
- Valeriy Balabanov, Magdalena Widl, and Jie-Hong R. Jiang. 2014. QBF resolution systems and their proof complexities. In *Proceedings of the International Conference on Theory and Applications of Satisfiability Testing (SAT’14)*. 154–169.
- Paul Beame and Toniann Pitassi. 2001. Propositional proof complexity: Past, present, and future. In *Current Trends in Theoretical Computer Science: Entering the 21st Century*, G. Paun, G. Rozenberg, and A. Salomaa (Eds.). World Scientific Publishing, 42–70.
- Eli Ben-Sasson and Avi Wigderson. 2001. Short proofs are narrow—Resolution made simple. *J. ACM* 48, 2 (2001), 149–169.
- Marco Benedetti and Hratch Mangassarian. 2008. QBF-based formal verification: Experience and perspectives. *J. Satis. Boolean Model. Comput.* 5, 1–4 (2008), 133–191.
- Olaf Beyersdorff. 2009. On the correspondence between arithmetic theories and propositional proof systems – A survey. *Math. Log. Quart.* 55, 2 (2009), 116–137.

- Olaf Beyersdorff, Joshua Blinkhorn, and Luke Hinde. 2019. Size, cost, and capacity: A semantic technique for hard random QBFs. *Log. Methods Comput. Sci.* 15, 1 (2019).
- Olaf Beyersdorff, Ilario Bonacina, and Leroy Chew. 2016a. Lower bounds: From circuits to QBF proof systems. In *Proceedings of the ACM Conference on Innovations in Theoretical Computer Science (ITCS'16)*. ACM, 249–260.
- Olaf Beyersdorff, Leroy Chew, and Mikoláš Janota. 2014. On unification of QBF resolution-based calculi. In *Proceedings of the Symposium on Mathematical Foundations of Computer Science (MFCS'14)*. Springer, 81–93.
- Olaf Beyersdorff, Leroy Chew, and Mikoláš Janota. 2015. Proof complexity of resolution-based QBF calculi. In *Proceedings of the 32nd International Symposium on Theoretical Aspects of Computer Science (STACS'15)*. 76–89.
- Olaf Beyersdorff, Leroy Chew, and Mikoláš Janota. 2016b. Extension variables in QBF resolution. In *Beyond NP, Papers from the 2016 AAAI Workshop*. AAAI Press.
- Olaf Beyersdorff, Leroy Chew, Meena Mahajan, and Anil Shukla. 2017a. Feasible interpolation for QBF resolution calculi. *Log. Methods Comput. Sci.* 13 (2017).
- Olaf Beyersdorff, Leroy Chew, Meena Mahajan, and Anil Shukla. 2018. Understanding cutting planes for QBFs. *Inf. Comput.* 262 (2018), 141–161.
- Olaf Beyersdorff, Luke Hinde, and Ján Pich. 2017b. Reasons for hardness in QBF proof systems. In *Proceedings of the 37th IARCS Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'17)*. 14:1–14:15.
- Olaf Beyersdorff and Oliver Kullmann. 2014. Unified characterisations of resolution hardness measures. In *Proceedings of the International Conference on Theory and Applications of Satisfiability Testing (SAT'14)*. Springer, 170–187.
- Olaf Beyersdorff and Ján Pich. 2016. Understanding Gentzen and Frege systems for QBF. In *Proceedings of the ACM/IEEE Symposium on Logic in Computer Science (LICS'16)*.
- Archie Blake. 1937. *Canonical Expressions in Boolean Algebra*. Ph.D. Dissertation. University of Chicago.
- Maria Luisa Bonet, Carlos Domingo, Ricard Gavaldà, Alexis Maciel, and Toniann Pitassi. 2004. Non-automatizability of bounded-depth Frege proofs. *Computat. Complex.* 13, 1–2 (2004), 47–68.
- Maria Luisa Bonet, Toniann Pitassi, and Ran Raz. 2000. On interpolation and automatization for Frege systems. *SIAM J. Comput.* 29, 6 (2000), 1939–1967.
- Ravi B. Boppana and Michael Sipser. 1990. *Handbook of Theoretical Computer Science (Vol. A)*. The MIT Press, Cambridge, MA, Chapter: The Complexity of Finite Functions, 757–804.
- Samuel R. Buss. 1986a. *Bounded Arithmetic*. Bibliopolis, Napoli.
- Samuel R. Buss. 1986b. The polynomial hierarchy and intuitionistic bounded arithmetic. In *Proceedings of the Structure in Complexity Theory Conference*. 77–103.
- Samuel R. Buss. 2012. Towards NP-P via proof complexity and search. *Ann. Pure Appl. Logic* 163, 7 (2012), 906–917.
- Samuel R. Buss and Peter Clote. 1996. Cutting planes, connectivity, and threshold logic. *Arch. Math. Log.* 35, 1 (1996), 33–62.
- Samuel R. Buss and Grigori Mints. 1999. The complexity of the disjunction and existential properties in intuitionistic logic. *Ann. Pure Appl. Log.* 99, 1–3 (1999), 93–104.
- Matthew Clegg, Jeff Edmonds, and Russell Impagliazzo. 1996. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the 28th ACM Symposium on Theory of Computing*. 174–183.
- Stephen Cook and Tsuyoshi Morioka. 2005. Quantified propositional calculus and a second-order theory for  $NC^1$ . *Arch. Math. Logic* 44, 6 (2005), 711–749. DOI : <https://doi.org/10.1007/s00153-005-0282-2>.
- Stephen A. Cook. 1975. Feasibly constructive proofs and the propositional calculus. In *Proceedings of the 7th ACM Symposium on Theory of Computing*. 83–97.
- Stephen A. Cook and Phuong Nguyen. 2010. *Logical Foundations of Proof Complexity*. Cambridge University Press.
- Stephen A. Cook and Robert A. Reckhow. 1979. The relative efficiency of propositional proof systems. *J. Symb. Log.* 6 (1979), 169–184.
- Stephen A. Cook and Neil Thapen. 2006. The strength of replacement in weak arithmetic. *ACM Trans. Comput. Log.* 7, 4 (2006), 749–764.
- Stephen A. Cook and Alasdair Urquhart. 1993. Functional interpretations of feasibly constructive arithmetic. *Ann. Pure Appl. Log.* 63, 2 (1993), 103–200.
- William Cook, Collette R. Coullard, and György Turán. 1987. On the complexity of cutting-plane proofs. *Disc. Appl. Math.* 18, 1 (1987), 25–38.
- Martin Dowd. 1985. Model-Theoretic Aspects of  $P \neq NP$ . (1985). Unpublished manuscript. [https://www.researchgate.net/publication/337090251\\_Model\\_Theoretic\\_Aspects\\_of\\_P\\_N\\_P](https://www.researchgate.net/publication/337090251_Model_Theoretic_Aspects_of_P_N_P).
- Uwe Egly. 2012. On sequent systems and resolution for QBFs. In *Proceedings of the Conference on Theory and Applications of Satisfiability Testing (SAT'12)*. 100–113.
- Uwe Egly, Martin Kronegger, Florian Lonsing, and Andreas Pfandler. 2017. Conformant planning as a case study of incremental QBF solving. *Ann. Math. Artif. Intell.* 80, 1 (2017), 21–45. DOI : <https://doi.org/10.1007/s10472-016-9501-2>.
- Gerhard Gentzen. 1935. Untersuchungen über das logische Schließen. *Math. Zeit.* 39 (1935), 68–131.

- Kaveh Ghasemloo and Ján Pich. 2013. A note on natural proofs and intuitionism. (2013). Retrieved from [karlin.mff.cuni.cz/~pich/natcons.pdf](http://karlin.mff.cuni.cz/~pich/natcons.pdf).
- Alexandra Goultiaeva, Allen Van Gelder, and Fahiem Bacchus. 2011. A uniform approach for generating proofs and strategies for both true and false QBF formulas. In *Proceedings of the International Joint Conference on Artificial Intelligence (IJCAI'11)*. 546–553.
- Amin Haken. 1985. The intractability of resolution. *Theoret. Comput. Sci.* 39 (1985), 297–308.
- Johan Håstad. 1986. Almost optimal lower bounds for small depth circuits. In *Proceedings of the 18th Symposium on the Theory of Computing (STOC'86)*. ACM Press, 6–20.
- Marijn J. H. Heule, Martina Seidl, and Armin Biere. 2017. Solution validation and extraction for QBF preprocessing. *J. Autom. Reason.* 58, 1 (2017), 97–125.
- Pavel Hrubeš. 2009. On lengths of proofs in non-classical logics. *Ann. Pure Appl. Log.* 157, 2–3 (2009), 194–205.
- Mikoláš Janota and Joao Marques-Silva. 2015. Expansion-based QBF solving versus Q-resolution. *Theor. Comput. Sci.* 577 (2015), 25–42.
- Emil Jeřábek. 2005. *Weak Pigeonhole Principle, and Randomized Computation*. Ph.D. Dissertation. Faculty of Mathematics and Physics, Charles University, Prague.
- Emil Jeřábek. 2009. Substitution Frege and extended Frege proof systems in non-classical logics. *Ann. Pure Appl. Log.* 159, 1–2 (2009), 1–48.
- Emil Jeřábek and Phuong Nguyen. 2011. Simulating non-prenex cuts in quantified propositional calculus. *Math. Log. Q.* 57, 5 (2011), 524–532.
- Hans Kleine Büning, Marek Karpinski, and Andreas Flögel. 1995. Resolution for quantified Boolean formulas. *Inf. Comput.* 117, 1 (1995), 12–18.
- Jan Krajíček and Gaisi Takeuti. 1992. On induction-free provability. *Ann. Math. Artif. Intell.* 6, 1–3 (1992), 107–125.
- Jan Krajíček. 1995. *Bounded Arithmetic, Propositional Logic, and Complexity Theory*. Encyclopedia of Mathematics and Its Applications, Vol. 60. Cambridge University Press, Cambridge, UK.
- Jan Krajíček. 1997. Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic. *J. Symb. Log.* 62, 2 (1997), 457–486.
- Jan Krajíček and Pavel Pudlák. 1989. Propositional proof systems, the consistency of first order theories and the complexity of computations. *J. Symb. Log.* 54, 3 (1989), 1063–1079.
- Jan Krajíček and Pavel Pudlák. 1990. Quantified propositional calculi and fragments of bounded arithmetic. *Zeit. Math. Log. Grund. Math.* 36 (1990), 29–46.
- Jan Krajíček and Pavel Pudlák. 1998. Some consequences of cryptographic conjectures for  $S_2^1$  and  $EF$ . *Inf. Computat.* 140, 1 (1998), 82–94.
- Jan Krajíček, Pavel Pudlák, and Alan Woods. 1995. Exponential lower bounds to the size of bounded depth Frege proofs of the pigeonhole principle. *Rand. Struct. Algor.* 7, 1 (1995), 15–39.
- David E. Muller and Franco P. Preparata. 1975. Bounds to complexities of networks for sorting and for switching. *J. ACM* 22, 2 (1975), 195–201.
- Rohit Parikh. 1971. Existence and feasibility in arithmetic. *J. Symb. Log.* 36, 3 (1971), 494–508.
- Toniann Pitassi, Paul Beame, and Russell Impagliazzo. 1993. Exponential lower bounds for the pigeonhole principle. *Computat. Complex.* 3 (1993), 97–140.
- Pavel Pudlák. 1997. Lower bounds for resolution and cutting planes proofs and monotone computations. *J. Symb. Log.* 62, 3 (1997), 981–998.
- Alexander A. Razborov. 1987. Lower bounds for the size of circuits of bounded depth with basis  $\{\&, \oplus\}$ . *Math. Notes Acad. Sci. USSR* 41, 4 (1987), 333–338.
- Jussi Rintanen. 2007. Asymptotically optimal encodings of conformant planning in QBF. In *Proceedings of the AAAI Conference on Artificial Intelligence (AAAI'07)*. AAAI Press, 1045–1050.
- Ronald L. Rivest. 1987. Learning decision lists. *Mach. Learn.* 2, 3 (1987), 229–246.
- John Alan Robinson. 1965. A machine-oriented logic based on the resolution principle. *J. ACM* 12, 1 (1965), 23–41.
- Nathan Segerlind. 2007. The complexity of propositional proofs. *Bull. Symb. Log.* 13, 4 (2007), 417–481.
- Roman Smolensky. 1987. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proceedings of the 19th ACM Symposium on the Theory of Computing (STOC'87)*. 77–82.
- Allen Van Gelder. 2012. Contributions to the theory of practical quantified Boolean formula solving. In *Proceedings of the International Conference on Principles and Practice of Constraint Programming (CP'12)*. 647–663.
- Heribert Vollmer. 1999. *Introduction to Circuit Complexity—A Uniform Approach*. Springer Verlag, Berlin.

Received September 2016; revised August 2019; accepted February 2020