Electronic Colloquium on Computational Complexity, Report No. 11 (2016)

Understanding Gentzen and Frege Systems for QBF

Olaf Beyersdorff Ján Pich
School of Computing, University of Leeds, United Kingdom
{o.beyersdorff, j.pich}@leeds.ac.uk

January 27, 2016

Abstract

Recently Beyersdorff, Bonacina, and Chew [7] introduced a natural class of Frege systems for quantified Boolean formulas (QBF) and showed strong lower bounds for restricted versions of these systems. Here we provide a comprehensive analysis of the new extended Frege system from [7], denoted $\mathsf{EF} + \forall\mathsf{red}$, which is a natural extension of classical extended Frege EF.

Our main results are the following: Firstly, we prove that the standard Gentzen-style system G_1^* p-simulates $\mathsf{EF} + \forall\mathsf{red}$ and that G_1^* is strictly stronger under standard complexity-theoretic hardness assumptions.

Secondly, we show a correspondence of $\mathsf{EF} + \forall\mathsf{red}$ to bounded arithmetic: $\mathsf{EF} + \forall\mathsf{red}$ can be seen as the non-uniform propositional version of intuitionistic S^1_2. Specifically, intuitionistic S^1_2 proofs of arbitrary statements in prenex form translate to polynomial-size $\mathsf{EF} + \forall\mathsf{red}$ proofs, and $\mathsf{EF} + \forall\mathsf{red}$ is in a sense the weakest system with this property.

Finally, we show that unconditional lower bounds for $\mathsf{EF} + \forall\mathsf{red}$ would imply either a major breakthrough in circuit complexity or in classical proof complexity, and in fact the converse implications hold as well. Therefore, the system $\mathsf{EF} + \forall\mathsf{red}$ naturally unites the central problems from circuit and proof complexity.

Technically, our results rest on a formalised strategy extraction theorem for $\mathsf{EF} + \forall\mathsf{red}$ akin to witnessing in intuitionistic S^1_2 and a normal form for $\mathsf{EF} + \forall\mathsf{red}$ proofs.

1 Introduction

Proof complexity addresses the main question of how hard it is to prove theorems in a given calculus, in particular: what is the length of the shortest proof of a given theorem in a fixed formal system, typically comprised of axioms and rules. This research bears tight and fruitful connections to computational complexity (separating complexity classes in an approach known as Cook's programme [20]), to first-order logic (theories of bounded arithmetic [19, 31]), as well as to practical SAT- and QBF-solving [15].

ISSN 1433-8092

While the bulk of activity in proof complexity concerns propositional proofs, there has been intense research during the last decade employing proof-complexity methods to further logics, most notably non-classical logics (cf. [11]) and proof complexity of quantified Boolean formulas (QBF).

Recent research in *QBF proof complexity* has been largely triggered by exciting advances in QBF solving—powerful algorithms that solve large classes of formulas from industrial applications. Compared to SAT solving, due to the PSPACE completeness of QBF the success of QBF solvers even extends to further fields such as planning [36, 24] and formal verification [5]. To model the strengths of modern QBF solvers, a number of resolution-based proof systems have been recently suggested and analysed from a proof complexity perspective (cf. [3, 8, 9, 10]).

While we have a relatively good understanding of these weak resolution-type systems, much less is known for strong proof systems, and this judgement applies to both propositional and QBF proof complexity. There are two main approaches for designing strong calculi: via sequent-style systems (Gentzen's LK [25]) and axiom-rule based systems known as Frege or Hilbert-type calculi [20]. In propositional logic, both Gentzen and Frege systems are equivalent from a proof complexity point of view [20, 31].

The situation is more intricate for QBF; and indeed the main aim of the present paper is to shed light on this topic.

Gentzen systems for QBF were already introduced in the late 80's by Krajíček and Pudlák [32], of which we use slightly modified versions G_i and G_i^* due to Cook and Morioka [18]. These systems are known to be strictly more powerful than QBF resolution [23], but lower bounds are out of reach with current techniques.

As for strong propositional systems, the main source of information on QBF Gentzen systems stems from their correspondence to Buss' theories of bounded arithmetic [13, 32, 18]. This correspondence allows to translate first-order formulas into sequences of QBFs, and indeed first-order proofs in S_2^i or T_2^i to polynomial-size G_i^* or G_i proofs, respectively [32, 18], thus providing the main tool to construct short propositional proofs.

On the other hand, *QBF Frege systems* were only developed very recently [7]. Their definition is very elegant, adding to classical Frege just one single $\forall$red rule for managing quantifiers, leading to the QBF system Frege + $\forall$red. Alternatively, they can be seen as substitution Frege systems with substitutions allowed just for universally quantified variables.

As for classical Frege, the strength of Frege + $\forall$red can be calibrated by allowing different classes of formulas (or more directly Boolean circuits [28]) as their underlying objects. With a technique [8, 7] uncovering a direct relation between circuit complexity and proof complexity, very strong lower bounds have been obtained for QBF Frege, the strongest of which yields an exponential lower bound for $\mathsf{AC}^0[p]$-Frege + $\forall$red. In sharp contrast, the strongest lower bound in the propositional world holds for AC^0-Frege [1, 35, 33], while lower bounds for the stronger $\mathsf{AC}^0[p]$-Frege constitute a major problem, open for more than twenty years.

This striking development prompts us to target at a better understanding of the new QBF Frege systems. What is their relation to the well-studied QBF Gentzen calculi? Does

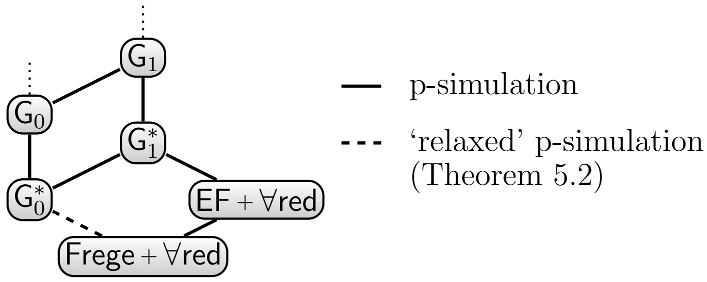

Figure 1: The simulation order of QBF Gentzen and Frege systems

QBF Frege also admit a correspondence to bounded arithmetic? Can we push lower bounds even beyond the current state-of-the-art bound for $\mathsf{AC}^0[\mathsf{p}]$-$\mathsf{Frege}+\forall\mathsf{red}$ from [7]?

In this paper we give answers to all of these three questions.

1.1 Our contributions

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

A. 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 [20]. In contrast, our findings show a more complex picture for QBF. We concentrate on the most important standard Gentzen-style systems G_0^* and G_1^* as well as the QBF Frege systems $\mathsf{Frege}+\forall\mathsf{red}$ and $\mathsf{EF}+\forall\mathsf{red}$, forming QBF analogues of the classical Frege and extended Frege system EF from [20].

For these four systems the following picture emerges (cf. Figure 1): We prove that G_1^* p-simulates $\mathsf{EF}+\forall\mathsf{red}$ (Theorem 5.1) and likewise G_0^* p-simulates $\mathsf{Frege}+\forall\mathsf{red}$ (although the latter under a slightly more relaxed notion of p-simulation, Theorem 5.2). On the other hand, the converse simulations are unlikely to hold. Under standard complexity-theoretic assumptions we show that $\mathsf{EF}+\forall\mathsf{red}$ is strictly weaker than G_1^* (Theorems 3.1, 3.3). Moreover, $\mathsf{EF}+\forall\mathsf{red}$ is incomparable to both G_0^* and G_0 (Theorems 3.4, 3.5). 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 very hard to improve these results to unconditional lower bounds (see C. below). However, since we use a number of different and indeed partly incomparable assumptions, our separations seem very plausible.

B. 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 [31, 19]. Here we show such a correspondence between $\mathsf{EF}+\forall\mathsf{red}$ and first-order intuitionistic logic IS_2^1, introduced in [14, 22]. For this first-order arithmetic formulas are translated into sequences of QBFs [32].

Our main result on the correspondence states that translations of arbitrarily complex prenex theorems in IS^1_2 admit polynomial-size $\mathsf{EF}+\forall\mathsf{red}$ proofs (Theorem 7.1). Informally, this says that all IS^1_2 consequences can be efficiently derived in $\mathsf{EF}+\forall\mathsf{red}$, and moreover, $\mathsf{EF}+\forall\mathsf{red}$ is the weakest system with this property.

The second facet of the correspondence is that IS^1_2 can prove the correctness of $\mathsf{EF}+\forall\mathsf{red}$ in a suitable encoding (Theorem 7.2), and in a certain sense $\mathsf{EF}+\forall\mathsf{red}$ is the strongest proof system that is provably sound in the theory IS^1_2.

Technically, the correspondence as well as the simulation results mentioned under A. above rest on a formalisation of the Strategy Extraction Theorem for QBF Frege systems from [7]. This strategy extraction result states that for formulas provable in $\mathsf{EF}+\forall\mathsf{red}$ one can compute witnesses for all existential quantifiers with Boolean circuits that can be efficiently extracted from the $\mathsf{EF}+\forall\mathsf{red}$ proof.

We provide two formalisations for this result: one in first-order logic, where we formalise strategy extraction in S^1_2 (Theorem 4.1), and a second more direct one, where we construct Frege proofs for the witnessing properties (Theorem 4.3). While the second formalisation applies to more systems and gives the simulation structure detailed in A., the first formalisation is stronger and enables the correspondence to IS^1_2.

Although intuitionistic bounded arithmetic was already developed by Buss in the mid 80's [14], no QBF counterpart of this theory was found so far—in sharp contrast to most other arithmetic theories [19]. As we show here, the missing piece in the puzzle is the recent QBF Frege system $\mathsf{EF}+\forall\mathsf{red}$.

Indeed, the appealing link between IS^1_2 and $\mathsf{EF}+\forall\mathsf{red}$ comes via their witnessing properties: similarly as $\mathsf{EF}+\forall\mathsf{red}$ has strategy extraction for arbitrarily complex QBFs [7], the theory IS^1_2 admits a witnessing theorem for arbitrary first-order formulas [22].

C. Characterising lower bounds for QBF Frege. The main question left open by the recent advances in strong QBF lower bounds [7] is whether *unconditional* lower bounds can be obtained for $\mathsf{Frege}+\forall\mathsf{red}$ or even $\mathsf{EF}+\forall\mathsf{red}$. We show here that such a result would imply either a major breakthrough in circuit complexity (a lower bound for non-uniform NC^1 or even $\mathsf{P/poly}$) 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 8.1).

This means that the problem of lower bounds for QBF Frege very naturally unites the centeral problem in circuit complexity with the central problem in proof complexity. Indeed, by our simulations shown in A. this also means that a lower bound for any of the QBF Gentzen systems G_i or G^*_i for $i \geq 1$ would imply either a circuit lower bound or a lower bound for propositional Frege.

This is conceptually very interesting as a direct connection between progress in circuit complexity and proof complexity has been often postulated (cf. [4]). Our results show that this connection directly manifests in $\mathsf{Frege}+\forall\mathsf{red}$, thus highlighting that $\mathsf{Frege}+\forall\mathsf{red}$ is indeed a natural and important system.

Technically, this result uses a normal form that we achieve for $\mathsf{Frege}+\forall\mathsf{red}$ proofs: these can be decomposed into a classical Frege proof followed by a number of $\forall\mathsf{red}$ steps

(Theorem 6.1). We further show that even $\forall\mathsf{red}$ steps suffice that only substitute constants (Theorem 6.3).

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 enforces us also to include rather extensive preliminaries).

1.2 Organization

In Section 2 we provide background on proof complexity, bounded arithmetic, and QBF Gentzen and Frege systems. We prove the conditional separations and the simulations in Sections 3 and 5, respectively. Section 4 formalizes strategy extraction in QBF Frege in S^1_2 and Frege, and Section 6 derives from this a normalisation of $\mathsf{EF}+\forall\mathsf{red}$ proofs. This enables us to show the correspondence between the theory IS^1_2 and $\mathsf{EF}+\forall\mathsf{red}$ in Section 7. Finally, in Section 8 we give the characterization of $\mathsf{Frege}+\forall\mathsf{red}$ and $\mathsf{EF}+\forall\mathsf{red}$ lower bounds in terms of lower bounds for Boolean circuits or propositional Frege.

2 Preliminaries

2.1 Notions from computational complexity

We use standard notation and concepts from computational complexity (cf. [2]). In particular, we use the circuit class $\mathsf{P/poly}$ of functions computed by polynomial-size Boolean circuits and the class NC^1 of functions computed by polynomial-size circuits of logarithmic depth (cf. [37]). We say that a function is hard for $\mathsf{P/poly}$ if it is not computable by a sequence of polynomial-size circuits.

By $\mathsf{FP}^{\Sigma^p_i}[O(\log n)]$ we denote the set of functions computed by a polynomial-time Turing machine making at most $O(\log n)$ queries to a Σ^p_i-oracle. $\mathsf{FP}^{\Sigma^p_i}$ is defined analogously but without the restriction on the number of queries.

2.2 Notions from proof complexity

Proof systems. According to [20] a *proof system* for a language $\mathcal{L}$ is a polynomial-time onto function $P : \{0,1\}^* \to \mathcal{L}$. Each string $\phi \in \mathcal{L}$ is a *theorem* and if $P(\pi) = \phi$, π is a *proof* of ϕ in P. Given a polynomial-time function $P : \{0,1\}^* \to \{0,1\}^*$ the fact that $P(\{0,1\}^*) \subseteq \mathcal{L}$ is the *soundness property* for $\mathcal{L}$ and the fact that $P(\{0,1\}^*) \supseteq \mathcal{L}$ is the *completeness property* for $\mathcal{L}$.

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

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

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

Frege systems. Frege proof systems are the common 'textbook' proof systems for propositional logic based on axioms and rules [20]. The lines in a Frege proof are propositional formulas built from propositional variables x_i and Boolean connectives $\neg$, $\wedge$, and $\vee$. A Frege system comprises a finite set of axiom schemes and rules, e.g., $\phi \vee \neg\phi$ 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 [20] and [31, 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. Equivalently, we can view them as refutation Frege systems where we start with the negation of the formula that we want to prove and derive a contradiction, and we switch between the two different formulations when convenient.

A number of subsystems and extensions of Frege have been considered in the literature (cf. [4]). An elegant framework for these systems was introduced by Jeřábek [28], where $\mathcal{C}$-Frege directly operates with circuits from the set $\mathcal{C}$ using a finite set of derivation Frege rules. For example, if there are no restrictions on $\mathcal{C}$ then $\mathcal{C}$-Frege is p-equivalent to the extended Frege system EF, cf. [28]. If $\mathcal{C}$ is restricted to formulas, i.e., $\mathcal{C} = \mathsf{NC}^1$, then $\mathcal{C}$-Frege is just Frege. Throughout the paper, whenever we speak of EF we indeed mean $\mathsf{P/poly}$-Frege and Frege stands for NC^1-Frege.

Sequent calculus. Gentzen's sequent calculus [25] is another classical proof system, both for first-order and propositional logic (cf. [31]). Propositional sequent calculus LK operates with sequents $\Gamma \longrightarrow \Delta$ with the semantic meaning $\bigwedge_{\phi\in\Gamma} \phi \models \bigvee_{\psi\in\Delta} \psi$. An important rule in LK is the cut rule

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

where A is called the cut formula.

LK is well known to be p-equivalent to Frege (cf. [31]).

2.3 Quantified Boolean formulas

Quantified Boolean formulas (QBF) extend propositional formulas by propositional quantifiers $\forall x.\, \phi(x)$ with the semantic meaning $\phi(0) \wedge \phi(1)$, and $\exists x.\, \phi(x)$ meaning $\phi(0) \vee \phi(1)$.

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

Often it is useful to think of a QBF $\mathcal{Q}_1 X_1 \ldots \mathcal{Q}_k X_k.\, \phi$ as a *game* between the *universal* and the *existential player*. In the i-th step of the game, the player $\mathcal{Q}_i$ assigns values to all the variables X_i. The existential player wins the game iff the matrix ϕ evaluates to 1 under the assignment constructed in the game. The universal player wins iff the matrix ϕ evaluates to 0. Given a universal variable u with index i, a *strategy for* u is a function from all variables of index $< i$ to $\{0, 1\}$. A QBF is false iff there exists a *winning strategy* for the universal player, i.e. if the universal player has a strategy for all universal variables that wins any possible game [27], [2, Sec. 4.2.2].

2.4 Sequent calculi for QBF

Quantified propositional calculus G, as defined by Cook and Morioka [18], extends Gentzen's classical propositional sequent calculus LK, cf. [31, Chapter 4.3], by allowing quantified propositional formulas in sequents and by adopting the following extra quantification rules for $\forall$-introduction

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

and $\exists$-introduction

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

For the rules $\forall$-l and $\exists$-r, $\phi(x/\psi)$ is the result of substituting ψ for all free occurrences of x in ϕ. The formula ψ may be any quantifier-free formula (i.e., without bounded variables) that is free for substitution for x in ϕ (i.e., no free occurrence of x in ϕ is within the scope of a quantifier Qy such that y occurs in ψ). The variable p in the rules $\forall$-r and $\exists$-l 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. G_i^* denotes the subsystem of G_i allowing only tree-like proofs.

The systems G and G_i were originally introduced slightly differently, cf. [31, 32, 30], not restricting the formulas ψ in $\forall$-l and $\exists$-r to be quantifier-free, and defining G_i as the system G allowing only Σ_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 [18].

Notably, (for Cook and Morioka's definition) Jeřábek and Nguyen [29] showed that the system G_i with cuts restricted to prenex Σ_i^q-formulas is p-equivalent to G_i with cuts restricted to prenex Π_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 [18] also proved that their definition of G_i is p-equivalent to G_i from [32] for $i \geq 0$ and prenex $\Sigma_i^q \cup \Pi_i^q$-formulas (so by [29] also for non-prenex ones).

On propositional formulas G_0 is p-equivalent to Frege and G_1 is p-equivalent to the Extended Frege system EF, cf. [31].

Finally, the systems G_i and G_i^* have quite constructive *witnessing properties*. Whenever there are polynomial-size 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. [18, Theorem 7]. In case of G_0 the circuits witnessing Σ_1^q-formulas are from NC^1, cf. [18, Theorem 9]. The witnessing theorems can be generalized to systems G_i^* and G_i for $i \geq 1$ w.r.t. Σ_i^q-formulas and witnessing functions corresponding to higher levels of the polynomial hierarchy.

2.5 Frege systems for QBF

An alternative way how to define reasoning with QBFs was given in [7] by using systems denoted as $\mathcal{C}$-Frege + $\forall$red. $\mathcal{C}$-Frege + $\forall$red is a refutational proof system augmenting the classical $\mathcal{C}$-Frege system by a $\forall$red rule. Formally, a $\mathcal{C}$-Frege + $\forall$red refutation of a QBF $Q.\, \phi$ is a sequence of circuits $L_1, \ldots, L_l \in \mathcal{C}$ where $L_1 = \phi$, $L_l = \emptyset$, and each L_i is derived from previous L_j's using the inference rules of $\mathcal{C}$-Frege or using the following $\forall$red rule

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

where u is a universal variable that is the innermost (wrt. the quantifier prefix Q) among the variables of L_j, and $B \in \mathcal{C}$ is a circuit that contains only variables left of u. In particular, $\mathcal{C}$-Frege + $\forall$red does not manipulate the prefix of the given QBF, so it proves only QBFs in prenex form.

In principle, variables not quantified in the prefix of a QBF might appear in its $\mathcal{C}$-Frege + $\forall$red refutation as consequences of $\mathcal{C}$-Frege rules. However, all such variables can be substituted by arbitrary constants without changing the proven QBF. Therefore, we assume that there are no such 'redundant' variables.

If there are no restrictions on $\mathcal{C}$, we denote $\mathcal{C}$-Frege + $\forall$red as EF + $\forall$red. If $\mathcal{C}$ is restricted to formulas, we speak of Frege + $\forall$red.

Note that $\mathcal{C}$-Frege + $\forall$red is essentially a refutational substitution Frege system SF, cf. [31], with substitutions allowed only for rightmost universally quantified variables.

In Section 6.1 we will show that in fact restricting the substituting circuit B to constants $0, 1$ results in a p-equivalent proof system denoted $\mathcal{C}$-Frege + $\forall\mathsf{red}_{0,1}$.

A characteristic property of the $\mathcal{C}$-Frege + $\forall$red systems is the so called *Strategy Extraction Theorem.* The theorem obtained in [7] says that whenever there is a $\mathcal{C}$-Frege + $\forall$red refutation π of a QBF $\exists x_1 \forall y_1, \ldots, \exists x_k \forall y_k.\, \phi(x_1, \ldots, x_k, y_1, \ldots, y_k)$, then there are $O(|\pi|)$-size witnessing circuits $C_1, \ldots, C_k \in \mathcal{C}$ satisfying

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

2.6 Bounded arithmetic

In first-order logic we will work with 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 Σ^b_0 $(=\Pi^b_0 = \Delta^b_0)$ we denote the set of all formulas in the language L with all quantifiers sharply bounded. For $i \geq 0$, the sets Σ^b_{i+1} and Π^b_{i+1} are defined inductively. Σ^b_{i+1} is the closure of Π^b_i under bounded existential and sharply bounded quantifiers, and Π^b_{i+1} is the closure of Σ^b_i 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 $i > 0$, Δ^b_i denotes $\Sigma^b_i \cap \Pi^b_i$.

Bounded formulas capture the polynomial hierarchy: for any $i > 0$ the i-th level $\mathsf{\Sigma^p_i}$ of the polynomial hierarchy coincides with the sets of natural numbers definable by Σ^b_i-formulas. Dually for $\mathsf{\Pi^p_i}$ and Π^b_i.

Buss [13] introduced theories of bounded arithmetic S^i_2, T^i_2 for $i \geq 1$ in the language L. The axioms of S^i_2 consist of a set of basic axioms defining properties of symbols from L, cf. [31], and length induction Σ^b_i-LIND, which is the following scheme for Σ^b_i-formulas A (or equivalently, for $A \in \Pi^b_i$, in which case we speak of Π^b_i-LIND):

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

Theories T^i_2 are defined similarly, but here the induction scheme is

$$A(0) \wedge \forall x.\, (A(x) \to A(x+1)) \to \forall x.\, A(x)$$

for $A \in \Sigma^b_i$.

T^i_2 proves the totality of $\mathsf{FP}^{\mathsf{\Sigma^p_i}}$ functions, cf. [31, Theorem 6.1.2]. More precisely, for any $f \in \mathsf{FP}^{\mathsf{\Sigma^p_i}}$ there is a Σ^b_{i+1}-formula $f(x) = y$ such that $T^i_2 \vdash \forall x \exists y.\, f(x) = y$. In the same way, S^i_2 proves the totality of functions in $\mathsf{FP}^{\mathsf{\Sigma^p_i}}[O(\log n)]$, cf. [31, Theorem 6.2.2]. By Parikh's theorem, $T^i_2 \vdash \exists y.\, f(x) = y$ implies $T^i_2 \vdash \exists y.\, |y| \leq p(|x|) \wedge f(x) = y$ for some polynomial p, and the same is true for S^i_2 (cf. [34, 13]).

S^i_2 can be seen as a first-order non-uniform version of G^*_i, $i \geq 1$. Firstly, for $j \geq 1$ any Σ^b_j-formula $\phi(x)$ can be translated into a sequence $\|\phi(x)\|^n$ of Σ^q_j-formulas, where n denotes the size of the input x in binary (cf. [31, Definition 9.2.1]). Then, for $i, j \geq 1$ whenever $S^i_2 \vdash A$ for $A \in \Sigma^b_j$, there is a polynomial p such that formulas $\|A\|^n$ have G^*_i-proofs of size $p(n)$. This also holds for T^i_2 in place of S^i_2 if G^*_i is replaced by G_i. The ability to use arbitrary j is due to Cook and Morioka [18, Theorem 3] who generalized a standard result, cf. [31, Theorem 9.2.6], which worked for $j = i$.

If $A \in \Pi^b_1$, we abuse notation and also denote by $\|A\|^n$ the propositional formulas obtained as in $\|A\|^n$, but leaving the universally quantified variables free. $S^1_2 \vdash A$ for $A \in \Pi^b_1$ implies that S^1_2 proves the existence of polynomial-size G^*_1-proofs of propositional formulas $\|A\|^n$, cf. [31, Theorems 9.2.6 and 9.2.7].

3 Separating Gentzen and Frege for QBF

We start with proving a number of conditional separations between Gentzen and Frege systems for QBF. As we will show later in Section 8, improving these separations to unconditional results tightly corresponds to major open problems in circuit complexity and proof complexity.

3.1 Formulas easy in Gentzen, but hard in Frege

We first provide three different properties that are easy for QBF Gentzen systems, but hard for $\mathsf{EF}+\forall\mathsf{red}$. Our first conditional result shows that there are Σ_2^q-formulas with polynomial-size G_1^* proofs but no polynomial-size $\mathsf{EF}+\forall\mathsf{red}$ proofs, and this result generalises to stronger systems.

Theorem 3.1. *Let $i \geq 1$. Assume $f \in \mathsf{FP}^{\Sigma_i^p}$ is hard for $\mathsf{P/poly}$. Then 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 Σ_{i+1}^b-formula, have polynomial-size G_i proofs and require super-polynomial-size $\mathsf{EF}+\forall\mathsf{red}$ proofs. If $f \in \mathsf{FP}^{\Sigma_i^p}[O(\log n)]$ then G_i can be replaced by G_i^*.*

Proof. As T_2^i proves the totality of $\mathsf{FP}^{\Sigma_i^p}$ functions [13], it proves the totality of f and the proof can be transformed into a sequence of polynomial-size G_i proofs [32, 18]. If the totality of f can be shown by polynomial-size proofs in $\mathsf{EF}+\forall\mathsf{red}$, then, by the Strategy Extraction Theorem [7], f is in $\mathsf{P/poly}$.

Similarly, S_2^i proves the totality of $\mathsf{FP}^{\Sigma_i^p}[O(\log n)]$ functions and such proofs translate into sequences of polynomial-size G_i^* proofs [13, 32, 18]. $\square$

It seems that the separation above of G_1^* and $\mathsf{EF}+\forall\mathsf{red}$ by Σ_2^q-formulas cannot be improved to Σ_1^q-formulas as it is tight in the following sense. If we had Σ_1^q-formulas $\exists y.\, A_n(x, y)$ with polynomial-size G_1^* proofs but without polynomial-size $\mathsf{EF}+\forall\mathsf{red}$ proofs, this would imply that EF is not polynomially bounded: by the witnessing theorem for G_1^*, cf. [18, 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 EF.

G_1^* and $\mathsf{EF}+\forall\mathsf{red}$ can be conditionally separated also on the bounded collection scheme.

Definition 3.2. *The* bounded collection scheme *$BB(\phi)$ is the formula*

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

where $\phi(i, u)$ is a formula which 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, $BB(\phi)$ says that u's witnessing $\phi(i, u)$ can be collected in a sequence w:

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

Theorem 3.3. G_1^* *has polynomial-size proofs of* $\|BB(\phi)\|^n$ *for all* $\phi \in \Sigma_1^b$*. In contrast, there exists* $\phi \in \Sigma_1^b$ *such that formulas* $\|BB(\phi)\|^n$ *are hard for* $\mathsf{EF} + \forall\mathsf{red}$ *unless each polynomial-time permutation with* n *inputs can be inverted by polynomial-size circuits with probability* $\geq 1 - 1/n$*.*

Proof. The upper bound follows from the S_2^1-provability of $BB(\phi)$ for $\phi \in \Sigma_1^b$, cf.[13, Theorem 14], and its transformation to G_1^* proofs [32, 18].

For the lower bound we will use a result by Cook and Thapen [21] showing that Cook's theory PV does not prove $BB(\phi)$ for all $\phi \in \Sigma_0^b$ unless factoring is in probabilistic polynomial time.

Let $a = 2^n$ and $\phi(i, u)$ be the formula $f(u) = [y]_i$ for a polynomial-time permutation f (defined by a Σ_1^b formula), and y encoding a sequence of n strings of length n.

Assume that $\mathsf{EF} + \forall\mathsf{red}$ has polynomial-size proofs of $\|BB(\phi)\|^n$. By the Strategy Extraction Theorem [7] there are polynomial-size circuits B, C such that

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

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 such that $\Pr_{y \in \{0,1\}^d}[C(y) = i_0] \leq 1/n$ where d is the number of inputs in C. Define $y_{z,s}$ to be the sequence of elements $z, f(s_1), \ldots, f(s_{n-1})$ ordered so that $[y_{z,s}]_{i_0} = z$ and let $x_{z,s}$ be the sequence of $z, s_1, \ldots, s_{n-1}$ ordered so that $f([x_{z,s}]_i) = [y_{z,s}]_i$ for $i \neq i_0$. Then $\Pr_{z,s_1,\ldots,s_n \in \{0,1\}^d}[C(y_{z,s}) = i_0] \leq 1/n$. Therefore, with probability $\geq 1 - 1/n$, $f([x_{z,s}]_{C(y_{z,s})}) = [y_{z,s}]_{C(y_{z,s})}$ and $f([B(y_{z,s})]_{i_0}) = z$. □

While the previous two results exhibited formulas easy for G_1^* and hard for $\mathsf{EF} + \forall\mathsf{red}$, we now show that even G_0^* can prove Σ_2^q-formulas hard for $\mathsf{EF} + \forall\mathsf{red}$ (modulo hardness of factoring).

For this we use a result by Bonet, Pitassi, and Raz [12], 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.)

Theorem 3.4. *There are* Σ_2^q*-formulas with polynomial-size* G_0^* *proofs. However, assuming factoring of Blum integers is not computable by polynomial-size circuits, these formulas require* $\mathsf{EF} + \forall\mathsf{red}$ *proofs of super-polynomial size.*

Proof. In [12] it is shown 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 G_0^* on propositional formulas [31] and so it is possible to derive in G_0^* the sequents in Figure 2.

Therefore, the Σ_2^q-formulas

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

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

Figure 2: The G_0^* derivation in the proof of Theorem 3.4

have polynomial-size G_0^* proofs.

If these formulas had polynomial-size $\mathsf{EF}+\forall\mathsf{red}$ proofs, then, by the Strategy Extraction Theorem [7], there would be polynomial-size circuits computing b from x and thus recognizing which of $A_0(x,y)$, $A_1(x,u)$ holds. $\square$

We remark that the assumptions of Theorems 3.3 and 3.4 are stronger than the assumption of Theorem 3.1. 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.

3.2 Formulas hard in Gentzen, but easy in Frege

We now give the opposite separation, exhibiting formulas (conditionally) hard for G_0, but easy for $\mathsf{EF}+\forall\mathsf{red}$. Thus G_0^* and G_0 appear to be incomparable to $\mathsf{EF}+\forall\mathsf{red}$.

Theorem 3.5. *If* $\mathsf{P/poly} \neq \mathsf{NC}^1$ *then there are* Σ_1^q*-formulas with polynomial-size* $\mathsf{EF}+\forall\mathsf{red}$ *proofs but without polynomial-size* G_0 *proofs.*

Proof. Let f be a function in $\mathsf{P/poly}$. Then $\mathsf{EF}+\forall\mathsf{red}$ has simple polynomial-size proofs of Σ_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 $\mathsf{EF}+\forall\mathsf{red}$ 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 had polynomial-size G_0 proofs, by the Σ_1^q witnessing property, cf. [18, Theorem 9], f would be in NC^1. $\square$

Notably, in Section 6 we show that $\mathsf{Frege}+\forall\mathsf{red}$ and $\mathsf{EF}+\forall\mathsf{red}$ 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.

4 Formalized strategy extraction

In order to prove that G_1^* p-simulates $\mathsf{EF}+\forall\mathsf{red}$ we first formalize the Strategy Extraction Theorem from [7]. We provide two different formalizations, one in S_2^1 and another one directly in EF. Both are sufficient for the simulation result. These formalizations guarantee that the extracted strategy is not just correct, but EF (resp. $\mathcal{C}$-Frege) provably correct.

Theorem 4.1 (Formalized Strategy Extraction)**.** *There is a linear-time algorithm A such that S^1_2 proves the following. Assume that π is an $\mathsf{EF}+\forall\mathsf{red}$ refutation of a QBF ψ of the form*

$$\exists x_1 \forall y_2 \dots \exists x_n \forall y_n.\, \phi(x_1, \dots, x_n, y_1, \dots, y_n)$$

where $\phi \in \Sigma^q_0$. Then $A(\pi)$ outputs circuits $C_1(x_1, \pi)$, $\dots$, $C_n(x_1, \dots, x_n, y_1, \dots, y_{n-1}, \pi)$ defining a winning strategy for the universal player on formula ψ; that is,

$$\forall x_1, \dots, x_n, y_1, \dots, y_n. \Big[\bigwedge_{i=1}^{n} (y_i \leftrightarrow C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1}, \pi)) \to \neg\phi(x_1, \dots, x_n, y_1, \dots, y_n) \Big].$$

Proof. We will inspect the original proof of the Strategy Extraction Theorem from [7], and point out that it essentially uses a Π^b_1-induction on the number of steps in the proof π, i.e., Π^b_1-LIND available in S^1_2.

Let $\pi = (L_1, \dots, L_s)$ be an $\mathsf{EF}+\forall\mathsf{red}$ refutation of the QBF $Q.\,\phi$ given as in Theorem 4.1 and put

$$\pi_s := \emptyset,\ \pi_i := (L_{i+1}, \dots, L_s) \text{ for } i < s$$
$$\phi_0 := \phi,\ \phi_i := \phi \wedge L_1 \wedge \dots \wedge L_i \text{ for } i > 0.$$

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

$$\sigma^i = \{C^i_1(x_1, \pi_i), \dots, C^i_n(x_1, \dots, x_n, y_1, \dots, y_{n-1}, \pi_i)\}$$

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

In the base case, ϕ_s contains a contradiction and the winning strategy can be defined as the set of trivial circuits $\{0, \dots, 0\}$.

Assume now that σ^i is a winning strategy for $Q.\,\phi_i$.

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 $\forall\mathsf{red}$ rule on L_j where u is the rightmost variable in L_j. We define $C^{i-1}_l := C^i_l$ if $u \neq y_l$, otherwise we set

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

This constructs circuits C^i_l from π_i by a standard $O(|\pi_i|)$-time algorithm.

To show that the strategies σ^i are winning for any $0 \leq i \leq |\pi|$, we need to analyze the inductive step.

Assume that σ^i is the winning strategy for the universal player on $Q.\,\phi_i$. If L_i is derived by an EF rule, the winning strategy for $Q.\,\phi_i$ works also for $Q.\,\phi_{i-1}$ 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 $\forall$red, $C_l^{i-1}(z)$ is redefined only if $L_j[u/B](z) = 0$. For z such that $L_j[u/B](z) = 1$, the strategy σ^i has to work also for $Q.\,\phi_{i-1}$. Therefore, σ^{i-1} is a winning strategy for the universal player on $Q.\,\phi_{i-1}$.

The statement that a strategy σ is winning for the universal player on $Q.\,\psi$ is a coNP predicate (given π) expressible as a well-behaved Π_1^b-formula. The induction we used is on the number of steps in π. Hence, the presented proof is an S_2^1-proof. □

The statement provable in S_2^1 in Theorem 4.1 is a coNP predicate expressible by a Π_1^b-formula. Consequently, translating the S_2^1 proof to EF, the extracted strategy is even EF-provably correct:

Corollary 4.2. *Given an* EF + $\forall$red *refutation* π *of a QBF*

$$\exists x_1 \forall y_2 \dots \exists x_n \forall y_n.\, \phi(x_1, \dots, x_n, y_1, \dots, y_n)$$

where $\phi \in \Sigma_0^q$, *we can construct in time* $|\pi|^{O(1)}$ *an* EF *proof of*

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

for some circuits C_i.

We will now show the same result as in the last corollary for Frege + $\forall$red (and in fact provide an alternative direct proof without making use of bounded arithmetic for EF + $\forall$red as well).

Theorem 4.3. *Let* $\mathcal{C}$ *be the circuit class* NC^1 *or* P/poly.[1] *Given a* $\mathcal{C}$-Frege + $\forall$red *refutation* π *of a QBF*

$$\exists x_1 \forall y_2 \dots \exists x_n \forall y_n.\, \phi(x_1, \dots, x_n, y_1, \dots, y_n)$$

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

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

for some circuits $C_i \in \mathcal{C}$.

Proof. Again, we will inspect the original proof of the Strategy Extraction Theorem.

Let $\pi = (L_1, \dots, L_s)$ be a $\mathcal{C}$-Frege + $\forall$red refutation of a QBF $Q.\,\phi$ given as in Theorem 4.3 and put

$$\pi_s := \emptyset,\ \pi_i := (L_{i+1}, \dots, L_s) \text{ for } i < s$$
$$\phi_0 := \phi,\ \phi_i := \phi \wedge L_1 \wedge \dots \wedge L_i \text{ for } i > 0.$$

[1] Indeed, the result should be easily generalisable to further 'natural' circuit classes $\mathcal{C}$ such as AC^0 or TC^0, but we will focus here on the two most interesting cases NC^1 and P/poly leading to Frege and EF systems, respectively.

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

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

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

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

denoted $\sigma^i(\phi_i)$ 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, ϕ_s contains a contradiction so the winning strategy can be defined as the set of trivial circuits $\{0, \ldots, 0\}$ and it is trivially provably correct.

Assume now that $\sigma^i(\phi_i)$ 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 $\sigma^{i-1} := \sigma^i$.

Let now $L_i = L_j[u/B]$ be the result of an application of a $\forall$red rule on L_j where u is the rightmost variable 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 σ^i from π 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 $\mathcal{C}$.

We want to show that $\sigma^{i-1}(\phi_{i-1})$ 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 σ^i also witnesses $\neg\phi_{i-1}$ because

$$\neg L_i \rightarrow \neg(L_1' \wedge \cdots \wedge L_t')$$

for some conjuncts $L_1', \ldots, L_t'$ in ϕ_{i-1}. Note that C_l^{i-1}'s are then C_l^i's. The implications

$$\begin{gathered} \neg\phi_i \rightarrow \neg\phi_{i-1} \\ \sigma^i(\phi_i) \wedge (\neg\phi_i \rightarrow \neg\phi_{i-1}) \rightarrow \sigma^{i-1}(\phi_{i-1}) \end{gathered} \tag{1}$$

can be derived by a fixed sequence of $\mathcal{C}$-Frege rules depending only on the choice of $\mathcal{C}$-Frege. 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 $\sigma^{i-1}(\phi_{i-1})$ 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 $\sigma^{i-1}(\phi_{i-1})$ from (1) and $\sigma^i(\phi_i)$, so w.l.o.g. $K_1 < K$.

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

$$\begin{aligned} \sigma^i(\phi_i) \wedge \neg L_j[u/B] &\rightarrow C_l^{i-1} = B \wedge \sigma^{i-1}(\phi_{i-1}) \\ \sigma^i(\phi_i) \wedge L_j[u/B] &\rightarrow C_l^{i-1} = C_l^i \wedge \sigma^{i-1}(\phi_{i-1}). \end{aligned}$$

The total size of both $\mathcal{C}$-Frege derivations 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 $\sigma^{i-1}(\phi_{i-1})$ 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. $K_1 < K$. □

5 Gentzen simulates Frege for QBF

We now apply the formalised Strategy Extraction Theorem from the last section to show that Gentzen systems simulate Frege systems in the QBF context. Frege and Gentzen are well known to be equivalent in the classical propositional case [31]. However, in QBF the opposite simulations (Gentzen by Frege) are very likely false as shown by the conditional separations in Section 3.

Theorem 5.1. G_1^* *p-simulates* $\mathsf{EF}+\forall\mathsf{red}$.

Proof. By Corollary 4.2, any $\mathsf{EF}+\forall\mathsf{red}$ refutation π of a QBF ψ (given as in Corollary 4.2) can be transformed in time $|\pi|^{O(1)}$ into an EF proof of

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

for certain circuits C_i.

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

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

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 p-equivalence of EF and G_1^* (cf. [31]), the EF proof obtained above can be turned into a $|\pi|^{O(1)}$-size G_1^*-proof of the formula

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

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

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

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

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

Finally, G_1^* derives the sequent we want by 'not introducing' $\wedge$ in the antecedent. This proves the claim. $\square$

Applying $\exists$-r and $\exists$-l introductions, G_1^* then derives

$$\Gamma, \exists y_n.\, y_n = C_n(x_1, \dots, x_n, y_1, \dots, y_{n-1}) \longrightarrow \exists y_n.\, \neg\phi(x_1, \dots, x_n, y_1, \dots, y_n)$$

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

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

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

Now, we use $\forall$-r introduction to obtain

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

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

To introduce the quantifyer prefix of ψ in the previous proof we needed to cut Σ_1^q-formulas. We would like to use a similar proof to simulate $\mathsf{Frege} + \forall\mathsf{red}$ by G_0^*. However, G_0^* is allowed to cut only Σ_0^q-formulas. Therefore we obtain just a simulation of $\mathsf{Frege} + \forall\mathsf{red}$ by G_0^* where the proven sequent in G_0^* contains a nonempty (easily derivable) antecedent.

Theorem 5.2. *There is a polynomial-time function t such that given any $\mathsf{Frege} + \forall\mathsf{red}$ refutation of a QBF ψ of the form*

$$\exists x_1 \forall y_2 \dots \exists x_n \forall y_n.\, \phi(x_1, \dots, x_n, y_1, \dots, y_n)$$

where $\phi \in \Sigma_0^q$, $t(\pi)$ is a G_0^* proof of the sequent

$$\forall x_1 \exists y_2 \dots \forall x_n \exists y_n.\, \bigwedge_{i=1}^{n} y_i = C_i(x_1, \dots, x_i, y_1, \dots, y_{i-1}) \longrightarrow \neg\psi$$

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

Proof. By Theorem 4.3, any $\mathsf{Frege} + \forall\mathsf{red}$ refutation π of a QBF ψ can be transformed in time $|\pi|^{O(1)}$ into a Frege proof of

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

for certain formulas C_i.

Analogously as in the proof of Theorem 5.1, we efficiently obtain a $|\pi|^{O(1)}$-size G_0^* proof of

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

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

$$\forall x_n \exists y_n. \bigwedge_{i=1}^{n} y_i = C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1}) \longrightarrow \forall x_n \exists y_n. \neg\phi.$$

In this way we efficiently introduce all quantifiers and derive the required sequent in G_0^*. □

6 Normal forms for QBF Frege proofs

In this section we apply results from Section 4 to obtain two normal forms for $\mathsf{Frege}+\forall\mathsf{red}$ and $\mathsf{EF}+\forall\mathsf{red}$ proofs. Firstly, we show that any $\mathsf{EF}+\forall\mathsf{red}$ refutation can be efficiently rewritten as an EF derivation followed essentially just by $\forall\mathsf{red}$ rules, and the same normalisation applies to $\mathsf{Frege}+\forall\mathsf{red}$. Secondly, we show that in the $\forall\mathsf{red}$ rule it is sufficient to only substitute constants.

Theorem 6.1. *Let $\mathcal{C}$ be the circuit class NC^1 or $\mathsf{P/poly}$. For any $\mathcal{C}$-$\mathsf{Frege}+\forall\mathsf{red}$ refutation π of a QBF ψ of the form*

$$\exists x_1 \forall y_2 \ldots \exists x_n \forall y_n. \, \phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$$

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

$$\bigvee_{i=1}^{n} (y_i \neq C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})) \tag{2}$$

for some circuits C_i, followed by n applications of the $\forall\mathsf{red}$ rule, gradually replacing the rightmost y_i by $C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})$ and cutting $y_i \neq C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})$ out of the disjunction (2).

Proof. Given a $\mathcal{C}$-$\mathsf{Frege}+\forall\mathsf{red}$ refutation π of ψ, by Theorem 4.3, there is a $|\pi|^{O(1)}$-size $\mathcal{C}$-Frege proof of

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

Having ψ freely available in the refutation, $\mathcal{C}$-Frege can derive (2) by applying the cut rule (derivable in $\mathcal{C}$-Frege).

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

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

from the disjunction $\bigvee_i y_i \neq C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})$. □

As the Frege (resp. EF) derivation can be efficiently replaced by a tree-like Frege (resp. EF) proof, cf. [31], and the rest of the $\mathcal{C}$-Frege + ∀red refutation given above is tree-like we obtain the following.

Corollary 6.2. Frege + ∀red *is p-equivalent to tree-like* Frege + ∀red*. Likewise,* EF + ∀red *is p-equivalent to tree-like* EF + ∀red*.*

6.1 Substituting constants in ∀red is sufficient

Frege + ∀red and EF + ∀red proofs can be further simplified so that every ∀red rule substitutes only constants instead of general circuits. This shows that the systems are indeed very robustly defined.

Theorem 6.3. Frege + ∀red *is p-equivalent to* Frege + $\forall\mathsf{red}_{0,1}$*. Likewise,* EF + ∀red *is p-equivalent to* EF + $\forall\mathsf{red}_{0,1}$*.*

Proof. Let $\mathcal{C}$ be either NC^1 or P/poly. It is enough to show that any $\mathcal{C}$-Frege + ∀red refutation can be transformed efficiently into a refutation where the ∀red rule substitutes only constants. By Theorem 6.1, for any $\mathcal{C}$-Frege + ∀red refutation π of $Q.\,\phi$ there is a $|\pi|^{O(1)}$-size $\mathcal{C}$-Frege derivation of

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

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

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

for both constants $c = 0, 1$. However, there is a polynomial-size $\mathcal{C}$-Frege proof of

$$C_n(x_1, \ldots, x_n, y_1, \ldots, y_{n-1}) = 1 \;\vee\; C_n(x_1, \ldots, x_n, y_1, \ldots, y_{n-1}) = 0,$$

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

7 Intuitionistic logic corresponds to EF + ∀red

The main information on strong propositional and QBF systems stems from their correspondence to first-order theories of bounded arithmetic (cf. [31, 19, 6]). In this sense, G_1^* corresponds to S_2^1 and G_1 to T_2^1 (cf. Section 2.6). Here we will establish such a correspondence between first-order intuitionistic logic and EF + ∀red.

In [14] Buss developed an intuitionistic version of S_2^1, denoted IS_2^1, and showed that for *any* formula A, $IS_2^1 \vdash \exists y.\, A(x, y)$ 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 $\mathsf{EF}+\forall\mathsf{red}$. Using the formalized Strategy Extraction Theorem we can make the correspondence between these systems formal.[2]

First, we recall the definition of IS^1_2 by Cook and Urquhart [22]. It is equivalent to Buss' original definition, cf. [14]. IS^1_2 is a theory in the language L (like S^1_2), with underlying intuitionistic predicate logic, cf. [22], a set of basic axioms defining properties of symbols from L, cf. [22], and a polynomial induction scheme for Σ^{b+}_1-formulas A:

$$A(0) \wedge \forall x. \Big(A(\Big\lfloor \frac{x}{2} \Big\rfloor) \to A(x)\Big) \to \forall x. A(x).$$

Here, Σ^{b+}_1-formulas are Σ^b_1-formulas without negation and implication signs.

S^1_2 is Σ^b_0-conservative over IS^1_2, cf. [22, Corollary 1.7].

We will also use Cook and Urquhart's conservative extension of IS^1_2 denoted IPV, cf. [22, Chapter 4 and Theorem 4.12]. IPV is defined by adding intuitionistic predicate logic to Cook's theory PV, cf. [17]. The language of IPV consist of symbols for all polynomial-time functions. The hierarchy of formulas $\Pi^b_i(PV)$ is defined analogously as Π^b_i but in the language of IPV. Also, propositional translations $\|A\|^n$ for $\Pi^b_1(PV)$-formulas A are defined analogously as in the case of $A \in \Pi^b_1$. Consequently, $IPV \vdash A$ for $A \in \Pi^b_1(PV)$ implies that propositional formulas $\|A\|^n$ have polynomial-size EF proofs, cf. [31, Theorem 9.2.7].

Cook and Urquhart [22, 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^1_2 and $\mathsf{EF}+\forall\mathsf{red}$. The correspondence consists of two parts (cf. [6]). For the first part we translate first-order formulas ϕ into sequences of QBFs [32] and show that translations of provable IS^1_2 formulas have short $\mathsf{EF}+\forall\mathsf{red}$ proofs.

Theorem 7.1. *If IS^1_2 proves a statement T in prenex form, then there exist polynomial-size* $\mathsf{EF}+\forall\mathsf{red}$ *refutations of $\|\neg T\|^n$.*

Proof. By Cook and Urquhart's improvements of Buss' witnessing theorem, if IS^1_2 proves T of the form

$$\forall x_1 \exists y_1 \ldots \forall x_n \exists y_n. T'(x_1, \ldots, x_n, y_1, \ldots, y_n)$$

for $T' \in \Sigma^b_0$, there is an IPV-function $f_1(x_1)$ such that

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

[2] It could be tempting to expect that an adequate counterpart to IS^1_2 would be intuitionistic propositional logic. However, intuitionistic propositional logic admits the feasible interpolation property, cf. [16], while IS^1_2 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. [26], that $IS^1_2 \vdash \forall y. A(x,y) \vee \forall z. B(x,z)$ implies the existence of an efficient interpolating circuit, but moving the universal quantifiers inside the disjunction is a priori not allowed in intuitionistic logic.

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

$$\bigwedge_{i=1}^{n} (y_i \leftrightarrow f_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})) \to T'(x_1, \ldots, x_n, y_1, \ldots, y_n) \tag{3}$$

and the formulas $\|(3)\|^n$ have polynomial-size EF proofs. $\mathsf{EF} + \forall\mathsf{red}$ can now refute $\|\neg T\|^n$ in polynomial size by deriving $\bigvee_i (y_i \neq f_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1}))$ and cutting all the disjuncts as in the proof of Theorem 6.1. $\square$

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 $\mathsf{EF} + \forall\mathsf{red}$ by QBFs. This is typically done by the *reflection principle* of a proof system P, stating that whenever ϕ has a P-proof (resp. a P-refutation), then ϕ is true (resp. false).

Here, the Formalized Strategy Extraction Theorem allows us to express the reflection principle of $\mathsf{EF} + \forall\mathsf{red}$ by a Π_1^b-formula $\mathsf{Ref}(\mathsf{EF} + \forall\mathsf{red})$. More precisely, we define $\mathsf{Ref}(\mathsf{EF} + \forall\mathsf{red})$ as the Π_1^b-formula expressing that if π is a proof of a QBF, then circuits $C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1}, \pi)$ obtained as in the Strategy Extraction Theorem witness the existential quantifiers in the QBF as in the statement of Theorem 4.1.

Theorem 7.2. *IS_2^1 proves* $\mathsf{Ref}(\mathsf{EF} + \forall\mathsf{red})$.

Proof. The claim follows from Theorem 4.1 together with the Σ_0^b-conservativity of S_2^1 over IS_2^1 [22]. $\square$

Theorem 7.2 implies that $\mathsf{EF} + \forall\mathsf{red}$ is the weakest proof system that allows short proofs of all IS_2^1 theorems, i.e., whenever Theorem 7.1 holds for a 'decent' proof system P in place of $\mathsf{EF} + \forall\mathsf{red}$, then P p-simulates $\mathsf{EF} + \forall\mathsf{red}$ on QBFs: If Theorem 7.1 holds for a proof system P, then by Theorem 7.2, there are polynomial-size P-proofs of $\|\mathsf{Ref}(\mathsf{EF} + \forall\mathsf{red})\|^n$. Hence, if π is an $\mathsf{EF} + \forall\mathsf{red}$ proof of a QBF ψ, then P has $|\pi|^{O(1)}$-size proofs of ψ 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 ψ efficiently in the size of π.

On the other hand, $\mathsf{EF} + \forall\mathsf{red}$ 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.

8 Characterising QBF Frege lower bounds

We finally address the question of lower bounds for $\mathsf{Frege} + \forall\mathsf{red}$ or even $\mathsf{EF} + \forall\mathsf{red}$. 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.

Theorem 8.1.

1. $\mathsf{EF}+\forall\mathsf{red}$ *is not polynomially bounded if and only if* EF *is not polynomially bounded or* $\mathsf{PSPACE} \not\subseteq \mathsf{P/poly}$.

2. $\mathsf{Frege}+\forall\mathsf{red}$ *is not polynomially bounded if and only if* Frege *is not polynomially bounded or* $\mathsf{PSPACE} \not\subseteq \mathsf{NC}^1$.[3]

Proof. If $\mathsf{PSPACE} \not\subseteq \mathsf{P/poly}$ then $\mathsf{EF}+\forall\mathsf{red}$ is not polynomially bounded by [7, Theorem 5.13]. Clearly, also if EF is not polynomially bounded then $\mathsf{EF}+\forall\mathsf{red}$ is not polynomially bounded.

In the opposite direction, assume that $\mathsf{EF}+\forall\mathsf{red}$ 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 $\mathsf{EF}+\forall\mathsf{red}$. Let $Q.\,\psi_n$ have the form

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

If $\mathsf{PSPACE} \not\subseteq \mathsf{P/poly}$, we are done. Otherwise, there are polynomial-size circuits C_i witnessing the existential quantifiers in $Q.\,\psi_n$. That is, for any $x_1, \ldots, x_n, y_1, \ldots, y_n$

$$\bigwedge_{i=1}^{n} (y_i \leftrightarrow C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})) \to \psi_n(x_1, \ldots, x_n, y_1, \ldots, y_n). \tag{4}$$

We claim that (4) is a sequence of tautologies without polynomial-size EF proofs. Otherwise, having $\neg\psi_n$, EF can derive $\bigvee_i y_i \neq C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})$ by a polynomial-size proof, and so as in Theorem 6.1, $\mathsf{EF}+\forall\mathsf{red}$ can efficiently refute $\neg Q.\,\psi_n$.

The analogous argument works for item 2 of the theorem. $\square$

This result also essentially answers the main question left open in [7], whether a lower bound for $\mathsf{Frege}+\forall\mathsf{red}$ can be shown by a different technique than the strategy extraction technique established in that paper. By Theorem 8.1, any such technique for $\mathsf{Frege}+\forall\mathsf{red}$ would immediately transfer to classical Frege, thus solving *the* main problem in propositional proof complexity.

9 Conclusion

In this paper we have undertaken a comprehensive analysis of QBF Frege systems, clarifying their relationships to bounded arithmetic and to Gentzen systems. While the emerging picture clearly shows that Gentzen systems are strictly stronger than Frege in QBF, one question left open by our results is whether the simulation of $\mathsf{Frege}+\forall\mathsf{red}$ by G_0^* in Theorem 5.2 can be made to work in the standard way, i.e., whether G_0^* p-simulates $\mathsf{Frege}+\forall\mathsf{red}$.

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

Acknowledgements

This research was supported by grant no. 48138 from the John Templeton Foundation and EPSRC grant EP/L024233/1.

References

[1] M. Ajtai. The complexity of the pigeonhole-principle. *Combinatorica*, 14(4):417–433, 1994.

[2] S. Arora and B. Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009.

[3] V. Balabanov, M. Widl, and J.-H. R. Jiang. QBF resolution systems and their proof complexities. In *SAT'14*, pages 154–169, 2014.

[4] P. Beame and T. Pitassi. Propositional proof complexity: Past, present, and future. In G. Paun, G. Rozenberg, and A. Salomaa, editors, *Current Trends in Theoretical Computer Science: Entering the 21st Century*, pages 42–70. World Scientific Publishing, 2001.

[5] M. Benedetti and H. Mangassarian. QBF-based formal verification: Experience and perspectives. *JSAT*, 5(1-4):133–191, 2008.

[6] O. Beyersdorff. On the correspondence between arithmetic theories and propositional proof systems – a survey. *Mathematical Logic Quarterly*, 55(2):116–137, 2009.

[7] O. Beyersdorff, I. Bonacina, and L. Chew. Lower bounds: From circuits to QBF proof systems. In *Proc. ACM Conference on Innovations in Theoretical Computer Science (ITCS'16)*, pages 249–260. ACM, 2016.

[8] O. Beyersdorff, L. Chew, and M. Janota. Proof complexity of resolution-based QBF calculi. In *Proc. Symposium on Theoretical Aspects of Computer Science (STACS'15)*, pages 76–89. LIPIcs, 2015.

[9] O. Beyersdorff, L. Chew, M. Mahajan, and A. Shukla. Feasible interpolation for QBF resolution calculi. In *Proc. International Colloquium on Automata, Languages, and Programming (ICALP'15)*, pages 180–192. Springer, 2015.

[10] O. Beyersdorff, L. Chew, M. Mahajan, and A. Shukla. Are short proofs narrow? QBF resolution is not simple. In *Proc. Symposium on Theoretical Aspects of Computer Science (STACS'16)*, 2016.

[11] O. Beyersdorff and O. Kutz. Proof complexity of non-classical logics. In N. Bezhanishvili and V. Goranko, editors, *Lectures on Logic and Computation - ESSLLI 2010*

/ESSLLI 2011, Selected Lecture Notes, pages 1–54. Springer-Verlag, Berlin Heidelberg, 2012.

[12] M. L. Bonet, T. Pitassi, and R. Raz. On interpolation and automatization for Frege systems. *SIAM Journal on Computing*, 29(6):1939–1967, 2000.

[13] S. R. Buss. *Bounded Arithmetic.* Bibliopolis, Napoli, 1986.

[14] S. R. Buss. The polynomial hierarchy and intuitionistic bounded arithmetic. In *Proc. Structure in Complexity Theory Conference*, pages 77–103, 1986.

[15] S. R. Buss. Towards NP-P via proof complexity and search. *Ann. Pure Appl. Logic*, 163(7):906–917, 2012.

[16] S. R. Buss and G. Mints. The complexity of the disjunction and existential properties in intuitionistic logic. *Annals of Pure and Applied Logic*, 99(1–3):93–104, 1999.

[17] S. A. Cook. Feasibly constructive proofs and the propositional calculus. In *Proc. 7th Annual ACM Symposium on Theory of Computing*, pages 83–97, 1975.

[18] S. A. Cook and T. Morioka. Quantified propositional calculus and a second-order theory for NC^1. *Arch. Math. Log.*, 44(6):711–749, 2005.

[19] S. A. Cook and P. Nguyen. *Logical Foundations of Proof Complexity.* Cambridge University Press, 2010.

[20] S. A. Cook and R. A. Reckhow. The relative efficiency of propositional proof systems. *The Journal of Symbolic Logic*, 44(1):36–50, 1979.

[21] S. A. Cook and N. Thapen. The strength of replacement in weak arithmetic. *ACM Trans. Comput. Log.*, 7(4):749–764, 2006.

[22] S. A. Cook and A. Urquhart. Functional interpretations of feasibly constructive arithmetic. *Ann. Pure Appl. Logic*, 63(2):103–200, 1993.

[23] U. Egly. On sequent systems and resolution for QBFs. In *Theory and Applications of Satisfiability Testing (SAT'12)*, pages 100–113, 2012.

[24] U. Egly, M. Kronegger, F. Lonsing, and A. Pfandler. Conformant planning as a case study of incremental QBF solving. In *Artificial Intelligence and Symbolic Computation (AISC'14)*, pages 120–131, 2014.

[25] G. Gentzen. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39:68–131, 1935.

[26] K. Ghasemloo and J. Pich. A note on natural proofs and intuitionism. available at karlin.mff.cuni.cz/∼pich/natcons.pdf, 2013.

[27] A. Goultiaeva, A. Van Gelder, and F. Bacchus. A uniform approach for generating proofs and strategies for both true and false QBF formulas. In *IJCAI*, pages 546–553, 2011.

[28] E. Jeřábek. Dual weak pigeonhole principle, Boolean complexity, and derandomization. *Annals of Pure and Applied Logic*, 129:1–37, 2004.

[29] E. Jerábek and P. Nguyen. Simulating non-prenex cuts in quantified propositional calculus. *Math. Log. Q.*, 57(5):524–532, 2011.

[30] J. Krajícek and G. Takeuti. On induction-free provability. *Ann. Math. Artif. Intell.*, 6(1-3):107–125, 1992.

[31] J. Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, volume 60 of *Encyclopedia of Mathematics and Its Applications*. Cambridge University Press, Cambridge, 1995.

[32] J. Krajíček and P. Pudlák. Quantified propositional calculi and fragments of bounded arithmetic. *Zeitschrift für mathematische Logik und Grundlagen der Mathematik*, 36:29–46, 1990.

[33] J. Krajíček, P. Pudlák, and A. Woods. Exponential lower bounds to the size of bounded depth Frege proofs of the pigeonhole principle. *Random Structures and Algorithms*, 7(1):15–39, 1995.

[34] R. Parikh. Existence and feasibility in arithmetic. *J. Symb. Log.*, 36(3):494–508, 1971.

[35] T. Pitassi, P. Beame, and R. Impagliazzo. Exponential lower bounds for the pigeonhole principle. *Computational Complexity*, 3:97–140, 1993.

[36] J. Rintanen. Asymptotically optimal encodings of conformant planning in QBF. In *AAAI*, pages 1045–1050. AAAI Press, 2007.

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

ECCC ISSN 1433-8092

http://eccc.hpi-web.de