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

Abstract
Recently Beyersdorff, Bonacina, and Chew [9] 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 [9], denoted EF + ∀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 G1 p-simulates EF + ∀red and that G1 is strictly stronger under standard complexity-theoretic hardness assumptions.

Secondly, we show a correspondence of EF + ∀red to bounded arithmetic: EF + ∀red can be seen as the non-uniform propositional version of intuitionistic S2 1. Specifically, intuitionistic S2 1 proofs of arbitrary statements in prenex form translate to polynomial-size EF + ∀red proofs, and EF + ∀red is in a sense the weakest system with this property.

Finally, we show that unconditional lower bounds for EF + ∀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 EF + ∀red naturally unites the central problems from circuit and proof complexity.

Technically, our results rest on a formalised strategy extraction theorem for EF + ∀red akin to witnessing in intuitionistic S2 1 and a normal form for EF + ∀red proofs.

Categories and Subject Descriptors F.2.2 [Analysis of algorithms and problem complexity]: Nonnumerical Algorithms and Problems—Complexity of proof procedures

General Terms Proof complexity, bounded arithmetic, quantified Boolean formulas

Keywords QBF proof systems, sequent calculus, Frege systems, intuitionistic logic, strategy extraction, lower bounds, simulations

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 [19]), to first-order logic (theories of bounded arithmetic [18, 30]), as well as to practical SAT- and QBF-solving [14].

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. [6]) 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 [23, 34] and formal verification. 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, 7, 8, 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 [24]) and axiom-rule based systems known as Frege or Hilbert-type calculi [19]. In propositional logic, both Gentzen and Frege systems are equivalent from a proof complexity point of view [19, 30].

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 Krajiček and Pudlák [31], of which we use slightly modified versions G1 and G1 ∗ due to Cook and Morioka [17]. These systems are known to be strictly more powerful than QBF resolution [22], 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 [12, 17, 31]. This correspondence allows to translate first-order formulas into sequences of QCAs, and indeed first-order proofs in S2 1 or T2 1 to polynomial-size G1 ∗ or G1 proofs, respectively [17, 31], thus providing the main tool to construct short propositional proofs.

On the other hand, QBF Frege systems were only developed very recently [9]. Their definition is very elegant, adding to classical Frege just one single ∀red rule for managing quantifiers, leading to the QBF system Frege + ∀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 + ∀red can be calibrated by allowing different classes of formulas (or more directly Boolean circuits [27]) as their underlying objects. With a technique [7, 9] 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 on AC2[p]-Frege + ∀red. In sharp contrast, the strongest lower bound in the propositional world holds for AC2[-]
Frege [1, 32, 33], while lower bounds for the stronger $AC^0[p]$-Frege systems 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 QBF Frege also admit a correspondence to bounded arithmetic? Can we push lower bounds even beyond the current state-of-the-art bound for $AC^0[p]$-Frege from [9]? 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 [19]. 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 $\text{Frege} + \forall \text{red}$ and $\text{EF} + \forall \text{red}$, forming QBF analogues of the classical Frege and extended Frege system $\text{EF}$ from [19].

For these four systems the following picture emerges (cf. Figure 1): We prove that $G_1$ $p$-simulates $\text{EF} + \forall \text{red}$ (Theorem 5.1) and $G_0$ simulates $\text{Frege} + \forall \text{red}$ under a 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 $\text{EF} + \forall \text{red}$ is strictly weaker than $G_1$ (Theorems 3.1, 3.3). Moreover, $\text{EF} + \forall \text{red}$ is incomparable to both $G_0$ and $G_0^i$ (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 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 [18, 30]. Here we show such a correspondence between $\text{EF} + \forall \text{red}$ and first-order intuitionistic logic $IS^2_2$, introduced in [13, 21]. For this first-order arithmetic formulas are translated into sequences of QBFs [31].

Our main result on the correspondence states that translations of arbitrarily complex prenex theorems in $IS^2_2$ admit polynomial-size $\text{EF} + \forall \text{red}$ proofs (Theorem 7.1). Informally, this says that all $IS^2_2$ consequences can be efficiently derived in $\text{EF} + \forall \text{red}$, and moreover, $\text{EF} + \forall \text{red}$ is the weakest system with this property.

The second facet of the correspondence is that $IS^2_2$ can prove the correctness of $\text{EF} + \forall \text{red}$ in a suitable encoding (Theorem 7.2), and in a certain sense $\text{EF} + \forall \text{red}$ is the strongest proof system that is provably sound in the theory $IS^2_2$.

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 [9]. This strategy extraction result states that for formulas provable in $\text{EF} + \forall \text{red}$ one can compute witnesses for all existential quantifiers with Boolean circuits that can be efficiently extracted from the $\text{EF} + \forall \text{red}$ proof.

We provide two formalisations for this result: one in first-order logic, where we formalise strategy extraction in $IS^2_1$ (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 $IS^2_2$.

Although intuitionistic bounded arithmetic was already developed by Buss in the mid ’80’s [13], no QBF counterpart of this theory was found so far—in sharp contrast to most other arithmetic theories [18]. As we show here, the missing piece in the puzzle is the recent QBF Frege system $\text{EF} + \forall \text{red}$.

Indeed, the appealing link between $IS^2_2$ and $\text{EF} + \forall \text{red}$ comes via their witnessing properties: similarly as $\text{EF} + \forall \text{red}$ has strategy extraction for arbitrarily complex QBFs [9], the theory $IS^2_2$ admits a witnessing theorem for arbitrary first-order formulas [21].

### C. Characterising lower bounds for QBF Frege.

The main question left open by the recent advances in strong QBF lower bounds [9] is whether unconditional lower bounds can be obtained for $\text{Frege} + \forall \text{red}$ or even $\text{EF} + \forall \text{red}$. 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 $P$ ($\text{poly}$) 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 central 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 $G^i_0$ 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 Frege + red, thus highlighting that Frege + red is indeed a natural and important system.

Technically, this result uses a normal form that we achieve for $\text{Frege} + \forall \text{red}$ proofs: these can be decomposed into a classical Frege proof followed by a number of $\forall \text{red}$ steps (Theorem 6.1). We further show that even $\forall \text{red}$ 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 $S^2_2$ and Frege, and Section 6 derives from this a normalisation of $\text{EF} + \forall \text{red}$ proofs. This enables us to show the correspondence between the theory $IS^2_2$ and $\text{EF} + \forall \text{red}$ in Section 7. Finally, in Section 8 we give the characterization of $\text{Frege} + \forall \text{red}$ and $\text{EF} + \forall \text{red}$...
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 $P/poly$ of functions computed by polynomial-size Boolean circuits and the class $NC^1$ of functions computed by polynomial-size circuits of logarithmic depth (cf. [35]). We say that a function is hard for $P/poly$ if it is not computable by a sequence of polynomial-size circuits.

By $FP^{O[\log n]}$ we denote the set of functions computed by a polynomial-time Turing machine making at most $O(\log n)$ queries to a $\Sigma^p_2$-oracle. $FP^{O[\log n]}$ is defined analogously but without the restriction on the number of queries.

2.2 Notions from proof complexity

Proof systems. According to [19] a proof system for a language $L$ is a polynomial-time onto function $P : \{0,1\}^* \rightarrow L$. Each string $\phi \in L$ is a theorem and if $P(\pi) = \phi$, $\pi$ is a proof of $\phi$ in $P$. Given a polynomial-time function $P : \{0,1\}^* \rightarrow \{0,1\}^*$ the fact that $P((0,1)^n) \subseteq L$ is the soundness property for $L$ and the fact that $P((0,1)^n) \supseteq L$ is the completeness property for $L$.

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

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

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

Frege systems. Frege proof systems are the common 'textbook' proof systems for propositional logic based on axioms and rules [19]. The lines in a Frege proof are propositional formulas built from propositional variables $x_i$ and Boolean connectives $\neg$, $\land$, and $\lor$. A Frege system comprises a finite set of axiom schemes and rules, e.g., $\phi \lor \neg \phi$ is an 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 [19] and [30, 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 [27], where $C$-Frege directly operates with circuits from the set $C$ using a finite set of derivation Frege rules. For example, if there are no restrictions on $C$ then $C$-Frege is $p$-equivalent to the extended Frege system $EF$, cf. [27]. If $C$ is restricted to formulas, i.e., $C = NC^1$, then $C$-Frege is just Frege. Throughout the paper, whenever we speak of EF we indeed mean $P/poly$-Frege and Frege stands for $NC^1$-Frege.

Sequent calculus. Gentzen’s sequent calculus [24] is another classical proof system, both for first-order and propositional logic (cf. [30]). Propositional sequent calculus $LK$ operates with sequents $\Gamma \rightarrow \Delta$ with the semantic meaning $\bigwedge_{\phi \in \Gamma} \phi \models \bigvee_{\psi \in \Delta} \psi$. An important rule in $LK$ is the cut rule

$$\Gamma \rightarrow \Delta, A, \Gamma \rightarrow \Delta$$

where $A$ is called the cut formula.

$LK$ is well known to be $p$-equivalent to Frege (cf. [30]).

2.3 Quantified Boolean formulas

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

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

Often it is useful to think of a QBF $\bigwedge_{i} Q_i x_i \ldots Q_k x_k \phi$ as a game between the universal and the existential player. In the $i$-th step of the game, the player $Q_i$ assigns values to all the variables $x_i$. The existential player wins the game if the matrix $\phi$ evaluates to 1 under the assignment constructed in the game. The universal player wins iff the matrix $\phi$ 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 [26], [2, Sec. 4.2.2].

2.4 Sequent calculi for QBF

Quantified propositional calculus $Q$, as defined by Cook and Morioka [17], extends Gentzen’s classical propositional sequent calculus $LK$, cf. [30, Chapter 4.3], by allowing quantified propositional formulas in sequents and by adopting the following extra quantification rules for $\forall$-introduction

$$\phi(x/\psi), \Gamma \rightarrow \Delta \quad \forall x \phi, \Gamma \rightarrow \Delta \quad (\forall-l)$$

and $\exists$-introduction

$$\phi(x/p), \Gamma \rightarrow \Delta \quad \exists x \phi, \Gamma \rightarrow \Delta \quad (\exists-l)$$

For the rules $\forall$-l and $\exists$-l, $\phi(x/\psi)$ 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 $\exists$-r must not occur free in the bottom sequent.

For $i \geq 0$, $G_i$ is a subsystem of $G$ with cuts restricted to prenex $\Sigma_p^i \cup \Pi_p^i$-formulas. $G_0^*$ denotes the subsystem of $G_i$ allowing only tree-like proofs.

The systems $G$ and $G_i$ were originally introduced slightly differently, cf. [29–31], not restricting the formulas $\psi$ in $\forall$-l and $\exists$-r to be quantifier-free, and defining $G_i$ as the system $G$ allowing only $\Sigma_p^i$-formulas in sequents. Hence, $G_0^*$‘s could not prove all true QBFs. We will, however, use the redefinition of these systems by Cook and Morioka [17].
Notably, (for Cook and Morioka’s definition) Jerabek and Nguyen [28] showed that the system $G_i$ with cuts restricted to prenex $\Sigma_i^n$-formulas is $\pi$-equivalent to $G_i$ with cuts restricted to prenex $\Pi_i^n$-formulas and $\pi$-equivalent to $G_i$ with cuts restricted to (not necessarily prenex) $\Sigma_i^n \cup \Pi_i^n$-formulas. Moreover these equivalences hold as well for the tree-like versions of these systems.

Cook and Morioka [17] also proved that their definition of $G_i$ is $\pi$-equivalent to $G_i$ from [31] for $i \geq 0$ and prenex $\Sigma_i^n \cup \Pi_i^n$-formulas (so by [28] also for non-prefix ones).

On propositional formulas $G_0$ is $\pi$-equivalent to Frege and $G_1$ is $\pi$-equivalent to the Extended Frege system EF, cf. [30].

Finally, the systems $G_i$ and $G_i^*$ have quite constructive witnessing properties. Whenever there are polynomial-size $G_i^*$ proofs of formulas $\exists y A_n(x, y)$ for $A_n(x, y) \in \Sigma_i^n$ there exist polynomial-size circuits $C_n$ witnessing the existential quantifiers, i.e., the formula $A_n(x, C_n(x))$ holds, cf. [17, Theorem 7]. In case of $G_0$ the circuits witnessing $\Sigma_i^n$-formulas are from NC$^1$, cf. [17, Theorem 9]. The witnessing theorems can be generalized to systems $G_i^*$ and $G_i$ for $i \geq 1$ w.r.t. $\Sigma_i^n$-formulas and witnessing functions corresponding to higher levels of the polynomial hierarchy.

2.5 Frege systems for QBF

An alternative way to define reasoning with QBFs was given in [9] by using systems denoted as C-Frege + $\forall$ red. C-Frege + $\forall$ red is a refutational proof system augmenting the classical C-Frege system by a $\forall$ red rule. Formally, a C-Frege + $\forall$ red refutation of a QBF $Q \phi$ with quantifier prefix $Q$ is a sequence of circuits $L_1, \ldots, L_i \subset C$ where $L_i = \phi$, $L_i = \emptyset$, and each $L_i$ is derived from previous $L_i$’s using the inference rules of C-Frege or the following $\forall$ red rule

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

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

In principle, variables not quantified in the prefix of a QBF might appear in its C-Frege + $\forall$ red refutation as consequences of 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 $C$, we denote C-Frege + $\forall$ red as EF + $\forall$ red. If $C$ is restricted to formulas, we speak of Frege + $\forall$ red.

Note that C-Frege + $\forall$ red is essentially a refutational substitution Frege system SF, cf. [30], 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 $\pi$-equivalent proof system denoted C-Frege + $\forall$ red$$_{0,1}$.

A characteristic property we will work with the language $L = \{ 0, S, +, \cdot, \leq, 1, \lfloor x \rfloor, \lfloor x \rfloor, \# \}$ where the function $\lfloor x \rfloor$ is intended to mean ‘the length of the binary representation of $x$’ and $x \# y = 2^{\lfloor |x| \rfloor + |y|}$. 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 $\Sigma_0^n (= \Pi_0^n = \Delta_0^n)$ we denote the set of all formulas in the language $L$ with all quantifiers sharply bounded. For $i \geq 0$, the sets $\Sigma_{i+1}$ and $\Pi_{i+1}$ are defined inductively. $\Sigma_{i+1}$ is the closure of $\Pi_i$ under bounded existential and sharply bounded quantifiers, and $\Pi_{i+1}$ is the closure of $\Sigma_i$ 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 $i > 0$, $\Delta_i^n$ denotes $\Sigma_i^n \cap \Pi_i^n$.

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

Buss [12] introduced theories of bounded arithmetic $S_1$, $T_2$ for $i \geq 1$ in the language $L$. The axioms of $S_1$ consist of a set of basic axioms defining properties of symbols from $L$, cf. [30], and length induction $\Sigma_0^n$-LIND, which is the following schema for $\Sigma_0^n$-formulas $A$ (or equivalently, for $A \in \Pi_0^n$, in which case we speak of $\Pi_0^n$-LIND):

$$A(0) \land \forall x (A(x) \rightarrow A(x+1)) \rightarrow \forall x A(x)\tag{1}$$

Theories $T_2^1$ are defined similarly, but here the induction scheme is

$$A(0) \land \forall x (A(x) \rightarrow A(x+1)) \rightarrow \forall x A(x)\tag{2}$$

for $A \in \Sigma_1^n$, $T_2^1$ proves the totality of $FP_{\Sigma_1}$ functions, cf. [30, Theorem 6.1.2]. More precisely, for any $f \in FP_{\Sigma_1}$ there is a $\Sigma_1^{i+1}$-formula $f(x) = y$ such that $T_2^1 \vdash \forall x \exists y f(x) = y$. In the same way, $S_2^1$ proves the totality of functions in $FP_{\Pi_1}$ ($O(\log n)$), cf. [30, Theorem 6.2.2]. By Parikh’s theorem, $T_2^1 \vdash \exists y f(x) = y$ implies $T_2^1 \vdash \exists y (|y| \leq p(|x|) \land f(x) = y)$ for some polynomial $p$, and the same is true for $S_2^1$ (cf. [12]).

$S_2^1$ can be seen as a first-order non-uniform version of $G_i^*$, $i \geq 1$.

Firstly, for $j \geq 1$ any $\Sigma_1^n$-formula $\phi(x)$ can be translated into a sequence $\langle \phi(x) \rangle^n$ of $\Sigma_1^n$-formulas, where $n$ denotes the size of the input $x$ in binary (cf. [30, Definition 9.2.1]). Then, for $i \geq 1$, whenever $S_2^1 \vdash A$ for $A \in \Sigma_i^n$, there is a polynomial $p$ such that formulas $\langle A \rangle^n$ have $G_i^*$-proofs of size $p(n)$. This also holds for $T_2^1$ in place of $S_2^1$ if $G_i^*$ is replaced by $G_i$. The ability to use arbitrary $j$ is due to Cook and Morioka [17, Theorem 3] who generalized a standard result, cf. [30, Theorem 9.2.6], which worked for $j = 1$.

If $A \in \Pi_1^n$, we abuse notation and also denote by $\|A\|^n$ the propositional formulas obtained as in $\|A\|^n$, but leaving the universally quantified variables free. $S_2^1 \vdash A$ for $A \in \Pi_1^n$ implies that $S_2^1$ proved the existence of polynomial-size $G_i^*$-proofs of propositional formulas $\|A\|^n$, cf. [30, 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 EF + $\forall$ red. Our first conditional result shows that there are $\Sigma_2^n$-formulas with polynomial-size $G_i^*$ proofs but no polynomial-size EF + $\forall$ red proofs, and this result generalises to stronger systems.
Theorem 3.1. Let \( i \geq 1 \). Assume \( f \in \text{FP}_{\Sigma_i}^{\Sigma_i} \) is hard for \( P/\text{poly} \). Then formulas \( \exists y (|y| \leq p(|x|) \wedge f(x) = y) \) of \( p \) are a polynomial and \( f(x) = y \) is expressed by a \( \Sigma_{i+1}^p \) formula, have polynomial-size \( G_1 \) proofs and require super-polynomial-size \( \text{EF} + \forall \text{red} \) proofs. If \( f \in \text{FP}_{\Sigma_i}^{\Sigma_i}[O(\log n)] \) then \( G_1 \) can be replaced by \( G_1^* \).

Proof. As \( \Sigma^P_2 \) proves the totality of \( \text{FP}_{\Sigma_i}^{\Sigma_i} \) functions \([12]\), it proves the totality of \( f \) and the proof can be transformed into a sequence of polynomial-size \( G_1 \) proofs \([17, 31]\). If the totality of \( f \) can be shown by polynomial-size proofs in \( \text{EF} + \forall \text{red} \), then, by the Strategy Extraction Theorem \([9]\), \( f \) is in \( P/\text{poly} \).

Similarly, \( \Sigma_2^P \) proves the totality of \( \text{FP}_{\Sigma_i}^{\Sigma_i}[O(\log n)] \) functions and such proofs translate into sequences of polynomial-size \( G_1^* \) proofs \([12, 17, 31]\).

It seems that the separation above of \( G_1^* \) and \( \text{EF} + \forall \text{red} \) by \( \Sigma_2^P \) formulas cannot be improved to \( \Sigma_2^P \) formulas as it is tight in the following sense. If we had \( \Sigma_2^P \) formulas \( \exists y \ A_n(x, y) \) with polynomial-size \( G_1 \) proofs but without polynomial-size \( \text{EF} + \forall \text{red} \) proofs, this would imply that \( f \) is not polynomially bounded: by the witnessing theorem for \( G_1 \), cf. \([17, \text{Theorem } 7]\), there would be polynomial-size circuits \( C_n \), such that formulas \( A_n(x, C_n(x)) \) are true, and so \( A_n(x, C_n(x)) \) would be hard to refute in \( \text{EF} \).

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

Definition 3.2. The bounded collection scheme \( \text{BB}(\phi) \) is the formula
\[
\exists i < |\alpha| \exists u < t(\alpha) \forall v < a \forall j < |\alpha| \phi(i, u) \rightarrow \phi(j, [w_i])
\]

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

Roughly, \( \text{BB}(\phi) \) says that \( u \)’s witnessing \( \phi(i, u) \) can be collected in a sequence \( w \):
\[
\forall v < a \exists u < t(\alpha) \forall j < |\alpha| \phi(j, [w_i]).
\]

Theorem 3.3. \( G_1 \) has polynomial-size proofs of \( \|\text{BB}(\phi)\|^{n_1} \) for all \( \phi \in \Sigma_1^p \). In contrast, there exists \( \phi \in \Sigma_1^p \) such that formulas \( \|\text{BB}(\phi)\|^{n_1} \) 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 \( \geq 1 - 1/n \).

Proof. The upper bound follows from the \( \Sigma_1^p \)-provability of \( \text{BB}(\phi) \) for \( \phi \in \Sigma_1^p \), cf. \([12, \text{Theorem } 14]\), and its transformation to \( G_1 \) proofs \([17, 31]\).

For the lower bound we will use a result by Cook and Thapen \([20]\) showing that Cook’s theory \( PV \) does not prove \( \text{BB}(\phi) \) for all \( \phi \in \Sigma_0 \) 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 \( \Sigma_1^p \) formula), and \( y \) encoding a sequence of \( n \) strings of length \( n \).

Assume that \( \text{EF} + \forall \text{red} \) has polynomial-size proofs of \( \|\text{BB}(\phi)\|^{n_1} \). By the Strategy Extraction Theorem \([9]\) there are polynomial-size circuits \( B, C \) such that
\[
\exists u < 2^n, f(u) = [y_i] \rightarrow \forall j < n, f([B(y)]_j) = [y_j].
\]

To invert \( f \) we proceed as follows. Given \( x \in \{0, 1\}^n \), pick randomly \( n \) strings \( s_i \in \{0, 1\}^n \) and let \( i_0 \) be a position (a nonuniform advice) such that \( \Pr_y[C(y) = i_0] \leq 1/n \) where \( y \)’s are sequences of \( n \) strings of length \( n \). Define \( y_{s, i} \) to be the sequence of elements \( z, f(s_1), \ldots, f(s_{n-1}) \) ordered so that \( y_{s, i}\) holds and by \( (1) \) the inverse of \( f \) on \( z \) is \( [B(y)]_{i_0} \).

While the previous two results exhibited formulas easy for \( G_1^* \) and hard for \( \text{EF} + \forall \text{red} \), we now show that even \( G_0 \) cannot prove \( \Sigma_2^p \) formulas hard for \( \text{EF} + \forall \text{red} \) (modulo hardness of factoring).

For this we use a result by Bonet, Pitassi, and Raz \([11]\), 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 \( \Sigma_2^p \) formulas with polynomial-size \( G_0^* \) proofs. However, assuming factoring of Blum integers is not computable by polynomial-size circuits, these formulas require \( \text{EF} + \forall \text{red} \) proofs of super-polynomial-size.

Proof. In \([11]\) it is shown that there are propositional formulas \( A_0(x, y) \), \( A_1(x, z) \) with common variables \( x \) such that \( A_0(x, y) \lor A_1(x, z) \) 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 \([30]\) and so it is possible to derive in \( G_0^* \) the sequents in Figure 2.

Therefore, the \( \Sigma_2^p \) formulas
\[
\exists y, u ((A_0(x, y) \lor b) \lor (A_1(x, u) \land \lnot b))
\]

have polynomial-size \( G_0 \) proofs.

If these formulas had polynomial-size \( \text{EF} + \forall \text{red} \) proofs, then, by the Strategy Extraction Theorem \([9]\), there would be polynomial-size circuits computing \( b \) from \( x \) and thus recognizing which of \( A_0(x, y) \) or \( A_1(x, u) \) holds.

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 \( \text{EF} + \forall \text{red} \). Thus \( G_0 \) and \( G_1 \) appear to be incomparable to \( \text{EF} + \forall \text{red} \).

Theorem 3.5. If \( P/\text{poly} \neq \text{NC}^1 \) then there are \( \Sigma_2^p \) formulas with polynomial-size \( \text{EF} + \forall \text{red} \) proofs but without polynomial-size \( G_0 \) proofs.

Proof. Let \( f \) be a function in \( P/\text{poly} \). Then \( \text{EF} + \forall \text{red} \) has simple polynomial-size proofs of \( \Sigma_2^p \) 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 \( \text{EF} + \forall \text{red} \) proof refutes the propositional formula \( f(x) \neq y \) by gradually replacing each variable from \( y \) by the circuit it represents.

If the totality of \( f \) had polynomial-size \( G_0 \) proofs, by the \( \Sigma_2^p \) witnessing property, cf. \([17, \text{Theorem } 9]\), \( f \) would be in \( \text{NC}^1 \).

Notably, in Section 6 we show that Frege + \( \forall \text{red} \) and \( \text{EF} + \forall \text{red} \) 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 $EF + \forall$red we first formalize the Strategy Extraction Theorem from [9]. We provide two different formalizations, one in $S^1_2$ 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 $S^2_2$ proves the following. Assume that $\pi$ is an $EF + \forall$red refutation of a QBF $\psi$ 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 $\phi \in \Sigma^0_0$. Then $A(\pi)$ outputs $n$ circuits $C_i(x_1), \ldots, C_n(x_1, \ldots, x_n, y_1, \ldots, y_{n-1})$ defining a winning strategy for the universal player on formula $\psi$; that is,

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

**Proof.** We will inspect the original proof of the Strategy Extraction Theorem from [9], and point out that it essentially uses a $\Pi^1_2$-induction on the number of steps in the proof $\pi$, i.e., $\Pi^1_2$-LIND available in $S^2_2$.

Let $\pi = (L_1, \ldots, L_s)$ be an $EF + \forall$red refutation of the QBF $Q \phi$. The statement of the Formalized Strategy Extraction Theorem corresponds to the case $i = 0$. In the base case, $\phi_0$ contains a contradiction and the winning strategy can be defined as the set of trivial circuits $\{0, 0, \ldots, 0\}$.

Assume now that $\sigma$ is a winning strategy for $Q \phi_i$. If $L_i$ is derived by an EF rule, then we set $\sigma^{-1} := \sigma$.

Assume now that $L_i = L_j[u/B]$ is the result of an application of a $\forall$red rule on $L_j$ where $u$ is the rightmost variable in $L_j$. We define $C_i^{-1} := C_l$ if $u \neq y_i$, otherwise we set $C_i^{-1}(z) := \begin{cases} B(z) & \text{if } L_j[u/B](z) = 0, \\ C_l(z) & \text{if } L_j[u/B](z) = 1. \end{cases}$

This constructs circuits $C_i$ from $\pi_i$ by a standard $O(|\pi|)$-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 $Q \phi_i$. 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, $C_i^{-1}(z)$ is redefined only if $L_i[u/B](z) = 0$. For $z$ such that $L_j[u/B](z) = 1$, the strategy $\sigma^i$ has to work also for $Q \phi_{i-1}$. Therefore, $\sigma^{-1}$ is a winning strategy for the universal player on $Q \phi_{i-1}$.

The statement that a strategy $\sigma$ is winning for the universal player on $Q \psi$ is a $\Pi^0_1$ predicate (given $\pi$) expressible as a well-behaved $\Pi^1_2$-formula. The induction we used is on the number of steps in $\pi$. Hence, the presented proof is an $S^2_2$-proof.

The statement provable in $S^2_2$ in Theorem 4.1 is a $\Pi^0_1$ predicate expressible by a $\Pi^1_2$-formula. Consequently, translating the $S^2_2$ proof to EF, the extracted strategy is even EF-provably correct.

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

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

where $\phi \in \Sigma^0_0$, we can construct in time $|\pi|^{O(1)}$ an EF proof of

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

for some circuits $C_i$.

We will now show the same result as in the last corollary for $\mathcal{C}$-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 $C$ be the circuit class NC$^1$ or $\mathcal{P}$/$\mathcal{P}$oly. $1$ Given a $\mathcal{C}$-Frege + $\forall$red refutation $\pi$ of a QBF

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

where $\phi \in \Sigma^0_0$, we can construct in time $|\pi|^{O(1)}$ a $\mathcal{C}$-Frege proof of

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

for some circuits $C_i \in C$.

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

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

$$\pi_s := \emptyset, \pi_i := (L_{i+1}, \ldots, L_s) \text{ for } i < s \text{ and } \phi_0 := \phi, \phi_i := \phi \land L_1 \land \cdots \land L_i \text{ for } i > 0.$$
We will show by downward induction on \( i \), that from \( \pi_i \) it is possible to construct in linear time a winning strategy

\[
\sigma^i = \{ C^i_t(x_1), \ldots, C^i_n(x_1, \ldots, x_n, y_1, \ldots, y_{n-1}) \}
\]

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

\[
\bigwedge_{i=1}^{n} (y_i \leftrightarrow C^i_t(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})) \rightarrow \neg \phi_i(x_1, \ldots, x_n, y_1, \ldots, y_n)
\]
denoted \( \sigma^i(\phi_i) \) will have a C-Frege proof of size \( K|\pi_i|^K \) for a constant \( K \) depending only on the choice of the C-Frege system. The statement of the theorem corresponds to the case \( i = 0 \).

In the base case, \( \phi_i \) contains a contradiction so the winning strategy can be defined as the set of trivial circuits \( \{ 0, 1 \} \) and it is trivially provably correct.

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

If \( L_i \) is derived by a 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 \( C^i_{t+1} := C^i_t \) if \( u \neq y_i \), otherwise set

\[
C^i_{t+1}(z) := \begin{cases} 
B(z) & \text{if } L_j[u/B](z) = 0 \\
C^i_t(z) & \text{if } L_j[u/B](z) = 1.
\end{cases}
\]

This constructs strategies \( \sigma^i \) from \( \pi \) by a \( D|\pi| \)-time algorithm for a constant \( D \). W.l.o.g., \( D < K \). In fact, circuits \( C^i_t \) are in \( C \).

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

If \( L_i \) is derived by a C-Frege rule, then \( \sigma^i \) also witnesses \( \neg \phi_{i-1} \) because

\[
\neg L_i \rightarrow \neg (L^1_i \land \cdots \land L^k_i)
\]

for some conjuncts \( L^1_i, \ldots, L^k_i \) in \( \phi_{i-1} \). Note that \( C^{i-1}_{t} \)'s are then \( C^{i}_{t} \)'s. The implications

\[
\neg \phi_i \rightarrow \neg \phi_{i-1} \\
\sigma^i(\phi_i) \land (\neg \phi_i \rightarrow \neg \phi_{i-1}) \rightarrow \sigma^{i-1}(\phi_{i-1})
\]

(2)

can be derived by a fixed sequence of C-Frege rules depending only on the choice of C-Frege. Thus, the common size of 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 C-Frege proof of size \( \leq K(s+1-(i-1))|\pi_{i-1}|^K + K_1|\pi_{i-1}|^{K_1} \leq K(s+1-(i-1))|\pi_{i-1}|^K \) where \( K_1 > K_0 \) depends again on a fixed sequence of C-Frege rules needed to derive \( \sigma^{i-1}(\phi_{i-1}) \) from (2) 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 \( u = y_i \). Then there is a fixed sequence of C-Frege rules deriving implications

\[
\sigma^i(\phi_i) \land \neg L_j[u/B] \rightarrow C^{i}_{t} = B \land \sigma^{i-1}(\phi_{i-1}) \\
\sigma^i(\phi_i) \land L_j[u/B] \rightarrow C^{i}_{t} = C^{i}_{t} \land \sigma^{i-1}(\phi_{i-1}).
\]

The total size of both C-Frege derivations is \( K_0|\pi_{i-1}|^{K_0} \) where \( K_0 \) depends on the choice of C-Frege and the size of \( C^{i}_{t} \)'s. The size of all \( C^{i}_{t} \)'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 C-Frege proof of size \( \leq K(s+1-(i-1))|\pi_{i-1}|^{K} + K_1|\pi_{i-1}|^{K_1} \leq K(s+1-(i-1))|\pi_{i-1}|^{K} \) where as before \( K_1 \) depends on a fixed sequence of 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 [30]. 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 \( EF + \forall \)red.

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

\[
\bigwedge_{i=1}^{n} (y_i \leftrightarrow C^i_t(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})) \rightarrow \neg \phi(x_1, \ldots, x_n, y_1, \ldots, y_n)
\]

for certain circuits \( C_i \).

Claim 1. There is a \( |\pi|^{O(1)} \)-size \( G^*_1 \) proof of the following sequent

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

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. [30]), the EF proof obtained above can be turned into a \( |\pi|^{O(1)} \)-size \( G^*_1 \)-proof of the formula

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

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

\[
\neg \left( \bigwedge_{i=1}^{n} y_i = C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1}) \right) \rightarrow \neg \phi.
\]

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

\[
\bigwedge_{i=1}^{n} (y_i = C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})) \rightarrow \neg \phi.
\]

Finally, \( G^*_1 \) derives the sequent we want by 'not introducing' \( \land \) in the antecedent. This proves the claim.

Applying \( \exists \)-r and \( \exists \)-l introductions, \( G^*_1 \) then derives

\[
\Gamma, \exists y_n \ (y_n = C_n(x_1, \ldots, x_n, y_1, \ldots, y_{n-1})) \rightarrow \exists y_n \neg (\phi(x_1, \ldots, x_n, y_1, \ldots, y_n))
\]

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

As \( G^*_1 \) proves efficiently \( \exists y \ (y = C(x)) \) for any circuit \( C \), we can cut \( \exists y_n \ (y_n = C_n(x_1, \ldots, x_n, y_1, \ldots, y_{n-1})) \) out of the antecedent and derive

\[
\{ y_i = C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1}) \}_{i=1}^{n-1} \rightarrow \exists y_n \neg \phi.
\]

Now, we use \( \forall \)-r introduction to obtain

\[
\{ y_i = C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1}) \}_{i=1}^{n-1} \rightarrow \forall x_n \exists y_n \neg \phi.
\]

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 \( |\pi|^{O(1)} \).
To introduce the quantifier prefix of $\psi$ in the previous proof we needed to cut $\Sigma^*_2$-formulas. We would like to use a similar proof to simulate Frege + $\forall$red and Frege + $\forall$red by $G_0$. However, $G_0$ is allowed to cut only $\Sigma^*_2$-formulas. Therefore we obtain just a simulation of Frege + $\forall$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 Frege + $\forall$red refutation of a QBF $\psi$ 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 $\phi \in \Sigma^*_n$, $t(\pi)$ is a $G_0$ proof of the sequent

$$\forall x_1 \exists y_2 \ldots \forall x_n \exists y_n \bigwedge_{i=1}^{n} y_i = C_i(x_1, \ldots, x_n, y_1, \ldots, y_n) \rightarrow \neg \psi$$

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 Frege + $\forall$red refutation $\pi$ of a QBF $\psi$ can be transformed in time $|\pi|^{O(1)}$ into a Frege proof of

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

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

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

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

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

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 Frege + $\forall$red and EF + $\forall$red proofs. Firstly, we show that any EF + $\forall$red refutation can be efficiently rewritten as an EF derivation followed essentially just by $\forall$red rules, and the same normalisation applies to Frege + $\forall$red. Secondly, we show that in the $\forall$red rule it is sufficient to only substitute constants.

**Theorem 6.1.** Let $C$ be the circuit class $NC^1$ or $P/poly$. For any $C$-Frege + $\forall$red refutation $\pi$ of a QBF $\psi$ 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 $\phi \in \Sigma^*_n$, there is a $|\pi|^{O(1)}$-size $C$-Frege + $\forall$red refutation of $\psi$ starting with a $C$-Frege derivation of

$$\bigwedge_{i=1}^{n} (y_i \neq C_i(x_1, \ldots, x_n, y_1, \ldots, y_n))$$

from $\phi$ for some circuits $C_i$, followed by $n$ applications of the $\forall$red rule, gradually replacing the rightmost variable $y_i$ by circuit $C_i(x_1, \ldots, x_n, y_1, \ldots, y_{i-1})$ and cutting the inequality $y_i \neq C_i(x_1, \ldots, x_n, y_1, \ldots, y_{i-1})$ out of the disjunction (3).

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

$$\bigwedge_{i=1}^{n} (y_i \leftrightarrow C_i(x_1, \ldots, x_n, y_1, \ldots, y_n)) \rightarrow \neg \psi(x_1, \ldots, x_n, y_1, \ldots, y_n).$$

Having $\psi$ freely available in the refutation, $C$-Frege can derive (3) by applying the cut rule (derivable in $C$-Frege).

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

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

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

As the Frege (resp. EF) derivation can be efficiently replaced by a tree-like Frege (resp. EF) proof, cf. [30], and the rest of the $C$-Frege + $\forall$red refutation given above is tree-like we obtain the following.

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

6.1 Substituting constants in $\forall$red is sufficient

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

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

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

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

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

$$C_n(x_1, \ldots, x_n, y_1, \ldots, y_{n-1}) \neq c \lor$$

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

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

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

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

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

7. Intuitionistic logic corresponds to EF + $\forall$red

The main information on strong propositional and QBF systems stems from their correspondence to first-order theories of bounded arithmetic (cf. [5, 18, 30]). In this sense, $G^+_2$ corresponds to $S^2_2$ and $G_1$ to $T^2_2$ (cf. Section 2.6). Here we will establish such a correspondence between first-order intuitionistic logic and EF + $\forall$red.

In [13] Buss developed an intuitionistic version of $S^2_2$, denoted $IS^2_2$, and showed that for any formula $A$, $IS^2_2 \vdash \exists y A(x, y)$ 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 \( \text{EF} + \text{EFred} \). Using the formalized Strategy Extraction Theorem we can make the correspondence between these systems formal.\(^2\)

First, we recall the definition of \( IS_2^b \) by Cook and Urquhart [21]. It is equivalent to Buss’ original definition, cf. [13]. \( IS_2^b \) is a theory in the language \( L \) (like \( S_2^b \)), with underlying intuitionistic predicate logic, cf. [21], a set of basic axioms defining properties of symbols from \( L \), cf. [21], and a polynomial induction scheme for \( \Sigma_1^{b, n} \)-formulas \( A \):

\[
A(0) \land \forall x \left( A \left( \frac{x}{2} \right) \rightarrow A(x) \right) \rightarrow \forall x A(x).
\]

Here, \( \Sigma_1^{b, n} \)-formulas are \( \Sigma_1^b \)-formulas without negation and implication signs, \( S_2^b \) is \( \Sigma_1^b \)-conservative over \( IS_2^b \), cf. [21, Corollary 1.7].

We will also use Cook and Urquhart’s conservative extension of \( IS_2^b \) denoted \( IPV \), cf. [21, Chapter 4 and Theorem 4.12]. \( IPV \) is defined by adding intuitionistic predicate logic to Cook’s theory \( PV \), cf. [16]. The language of \( IPV \) consist of symbols for all polynomial-time functions. The hierarchy of formulas \( \Pi_1^1(PV) \) is defined analogously as in the case of \( A \in \Pi_1^1(PV) \). Consequently, \( IPV \vdash A \) for \( A \in \Pi_1^1(PV) \) implies that propositional formulas \( \|A\|_n \) have polynomial-size EF proofs, cf. [30, Theorem 9.2.7].

Cook and Urquhart [21, 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 \( IS_2^b \) and \( \text{EF} + \text{EFred} \). The correspondence consists of two parts (cf. [5]). For the first part we translate first-order formulas \( f \) into sequences of QBFs [31] and show that translations of provable \( IS_2^b \)-formulas have short \( \text{EF} + \text{EFred} \) proofs.

**Theorem 7.1.** If \( IS_2^b \) proves a statement \( T \) in prenex form, then there exist polynomial-size \( \text{EF} + \text{EFred} \) refutations of \( \| \neg T \|^n \).

**Proof.** By Cook and Urquhart’s improvements of Buss’ witnessing theorem, if \( IS_2^b \) 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 \( T' \in \Sigma_0^b \), there is an \( IPV \)-function \( f_1(x_1) \) such that \( IPV \vdash \forall x_1, x_2 \exists y_2 \ldots \forall x_n \exists y_n T'(x_1, \ldots, x_n, f_1(x_1), y_2, \ldots, y_n) \). 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 \( \Pi_1^1(PV) \) formula

\[
\bigwedge_{i=1}^n (y_i \leftrightarrow f_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})) \\
T'(x_1, \ldots, x_n, y_1, \ldots, y_n) \tag{4}
\]

and the formulas \( \| \neg T \|^n \) have polynomial-size \( \text{EF} \) proofs. \( \text{EF} + \text{EFred} \) can now refute \( \| \neg T \|^n \) in polynomial size by deriving \( \forall y \neg \neg T \).

\(^2\) It could be tempting to expect that an adequate counterpart to \( IS_2^b \) would be intuitionistic propositional logic. However, intuitionistic propositional logic admits the feasible interpolation property, cf. [15], while \( IS_2^b \) can (constructively) prove \( \forall x, A(x, y) \lor B(x, z) \), in principle, without the existence of an efficient interpolant. It is also known, cf. [25], that \( IS_2^b \vdash \exists y \forall x A(x, y) \lor \forall z B(x, z) \) 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 \( \text{EF} + \text{EFred} \) by QBFs. This is typically done by the reflection principle of a proof system \( P \), stating that whenever \( \phi \) has a \( P \)-proof (resp. a \( P \)-refutation), then \( \phi \) is true (resp. false).

Here, the Formalized Strategy Extraction Theorem allows us to express the reflection principle of \( \text{EF} + \text{EFred} \) by a \( \Pi_1^1 \)-formula \( \text{Ref}(\text{EF} + \text{EFred}) \). More precisely, we define \( \text{Ref}(\text{EF} + \text{EFred}) \) as the \( \Pi_1^1 \)-formula expressing that if \( \pi \) is a proof of a QBF, then circuits \( C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1}) \) 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.** \( IS_2^b \) proves \( \text{Ref}(\text{EF} + \text{EFred}) \).

**Proof.** The claim follows from Theorem 4.1 together with the \( \Sigma_0^b \)-conservativity of \( IS_2^b \) over \( IS_2^b \) [21].

Theorem 7.2 implies that \( \text{EF} + \text{EFred} \) is the weakest proof system that allows short proofs of all \( IS_2^b \) theorems, i.e., whenever Theorem 7.1 holds for a ‘decent’ proof system \( P \) in place of \( \text{EF} + \text{EFred} \), then \( P \) p-simulates \( \text{EF} + \text{EFred} \) on QBFs: If Theorem 7.1 holds for a proof system \( P \), then by Theorem 7.2, there are polynomial-size \( P \)-proofs of \( \| \text{Ref}(\text{EF} + \text{EFred}) \|^n \). Hence, if \( \pi \) is an \( \text{EF} + \text{EFred} \) 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.

On the other hand, \( \text{EF} + \text{EFred} \) is intuitively the strongest proof system for which \( IS_2^b \) provs 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, \( IS_2^b \) provability of the reflection principle for \( \Sigma_0^b \)-formulas for any fixed \( k \) implies the strategy extraction for the given proof system.)

8. Characterising QBF Frege lower bounds

We finally address the question of lower bounds for Frege + \text{EFred} or even \( \text{EF} + \text{EFred} \). 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 8.1.**

1. \( \text{EF} + \text{EFred} \) is not polynomially bounded if and only if \( \text{EF} \) is not polynomially bounded or \( \text{PSpace} \) \( \subseteq \text{Ppoly} \).

2. \( \text{Frege} + \text{EFred} \) is not polynomially bounded if and only if \( \text{Frege} \) is not polynomially bounded or \( \text{PSpace} \) \( \subseteq \text{NC}^1 \).\(^3\)

**Proof.** If \( \text{PSpace} \) \( \subseteq \text{Ppoly} \) then \( \text{EF} + \text{EFred} \) is not polynomially bounded by [9, Theorem 5.13]. Clearly, also if \( \text{EF} \) is not polynomially bounded then \( \text{EF} + \text{EFred} \) is not polynomially bounded.

In the opposite direction, assume that \( \text{EF} + \text{EFred} \) is not polynomially bounded. Then there is a sequence of true QBFs \( \psi_n \) such

\( f_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1}) \) and cutting all the disjuncts as in the proof of Theorem 6.1.

\(^3\) By \( \text{NC}^1 \) we mean non-uniform \( \text{NC}^1 \). Note that by the space hierarchy theorem it is known that \( \text{PSpace} \) \( \nsubseteq \text{uniform NC}^1 \), but this does not suffice for \( \text{Frege} + \text{EFred} \) lower bounds.
that $\neg Q\psi_n$ do not have polynomial-size refutations in $EF + \forall \text{red}$. 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 $\text{PSPACE} \not\subseteq \text{P/poly}$, we are done. Otherwise, there are polynomial-size circuits $C_i$ witnessing the existential quantifiers in $Q\psi_n$. That is, for any $x_1, \ldots, x_n, y_1, \ldots, y_n$,
\[
\forall i=1 \ldots n \ (y_i \leftrightarrow C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1}) \rightarrow \psi_n(x_1, \ldots, x_n, y_1, \ldots, y_n).
\]

We claim that (5) is a sequence of tautologies without polynomial-size $EF$ proofs. Otherwise, having $\neg \psi_n$, $EF$ can derive $\forall i, y_i \neq C_i(x_1, \ldots, x_i, y_1, \ldots, y_{i-1})$ by a polynomial-size proof, and so as in Theorem 6.1, $EF + \forall \text{red}$ can efficiently refute $\neg Q\psi_n$. The analogous argument works for item 2 of the theorem.

This result also essentially answers the main question left open in [9], whether a lower bound for Frege $+ \forall \text{red}$ can be shown by a different technique than the strategy extraction technique established in that paper. By Theorem 8.1, any such technique for Frege $+ \forall \text{red}$ 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 Frege $+ \forall \text{red}$ by $G_0^0$ in Theorem 5.2 can be made to work in the standard way, i.e., whether $G_0^0$ p-simulates Frege $+ \forall \text{red}$.

Acknowledgments

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

References
