On Sequent Systems and Resolution for QBFs*

Uwe Egly

Institut für Informationssysteme 184/3, Technische Universität Wien,
Favoritenstrasse 9–11, A-1040 Vienna, Austria
uwe@kr.tuwien.ac.at

Abstract. Quantified Boolean formulas generalize propositional formulas by admitting quantifications over propositional variables. We compare proof systems with different quantifier handling paradigms for quantified Boolean formulas (QBFs) with respect to their ability to allow succinct proofs. We analyze cut-free sequent systems extended by different quantifier rules and show that some rules are better than some others.

Q-resolution is an elegant extension of propositional resolution to QBFs and is applicable to formulas in prenex conjunctive normal form. In Q-resolution, there is no explicit handling of quantifiers by specific rules. Instead the forall reduction rule which operates on single clauses inspects the global quantifier prefix. We show that there are classes of formulas for which there are short cut-free tree proofs in a sequent system, but any Q-resolution refutation of the negation of the formula is exponential.

1 Introduction

Quantified resolution (or Q-resolution) [10] is a relatively inconspicuous calculus. It was introduced as an elegant extension of resolution to process quantified Boolean formulas (QBFs) in prenex conjunctive normal form. Although there are only a few QBF solvers directly based on Q-resolution, it has gained an enormous practical importance as a subcalculus in modern DPLL solvers with clause learning. Moreover, an early proposal for a uniform proof format [9] is based on resolution. Nowadays many QBF solvers produce Q-resolution proofs and certificate generation [1] can be based on them.

Sequent calculi [7] are well explored proof systems, which are not restricted to specific normal forms. Variants of these calculi like tableau systems are widely used in (first-order) theorem proving for classical and non-classical logics, where often no clausal normal form is available. Variants of sequent calculi are available for QBFs and used for a variety of purposes [4,11]. Even some solvers not based on prenex conjunctive normal form like `qpro` [6] implement proof search in a restricted variant of a sequent calculus, and a look at a high-level description of its main procedure indicates that it is not too far away from DPLL.

* The work was partially supported by the Austrian Science Foundation (FWF) under grant S11409-N23. We thank the referees for valuable comments.

A. Cimatti and R. Sebastiani (Eds.): SAT 2012, LNCS 7317, pp. 100–113, 2012.

Initially driven by the $P =? NP$ question [5], propositional proof systems are well studied and compared with respect to their relative efficency, i.e., their ability to allow for succinct proofs. In this paper, we compare Q-resolution and sequent systems for QBFs. The crucial difference between systems for SAT and systems for quantified SAT (QSAT) is Boolean quantification in the latter, which allows for more succinct problem representations. As we will see later, there are different methods to handle quantifiers like the rules implementing semantics directly, rules inspired by first-order logic, or a completely different technique to handle quantifiers in Q-resolution. It turns out that the way how quantifiers are handled strongly influence proof complexity.

Contributions. First we consider *cut-free* propositional sequent systems extended by different quantifier rules. We show that these rules have increasing strength by providing formula classes which can be used for exponential separations. Second we partially solve the problem stated in [4] whether in sequent systems with restricted cuts, the quantifier rule introducing propositional formulas can be polynomially simulated by the one introducing variables. We show this for all tree-like systems except the one with only propositional cuts. Third we show an exponential separation between *cut-free tree-like* sequent systems and *arbitrary* Q-resolution. This result is surprising because the first system is extremely weak, whereas the second one does not have to obey the tree restriction and has an atomic cut (the resolution rule) in addition. It turns out that the relative strength comes from the more powerful quantifier rules of the sequent system.

Structure. In Sect. 2, we introduce necessary concepts. Section 3 presents sequent systems and Q-resolution. Different quantifier rules are compared in Sect. 4. In Sect. 5, we present an exponential separation between cut-free tree-like sequent systems and arbitrary Q-resolution. We show that the latter cannot polynomially simulate the former. Concluding remarks are presented in Sect. 6.

2 Preliminaries

We assume basic familiarity with the syntax and semantics of propositional logic. We consider a propositional language based on a set $\mathcal{PV}$ of Boolean variables and truth constants $\top$ (true) and $\bot$ (false), both of which are not in $\mathcal{PV}$. A variable or a truth constant is called *atomic*. We use connectives from $\{\neg, \wedge, \vee, \rightarrow\}$ and $A \leftrightarrow B$ is a shorthand for $(A \rightarrow B) \wedge (B \rightarrow A)$. A *clause* is a disjunction of literals. *Tautological clauses* contain a variable and its negation and the *empty clause* is denoted by $\Box$. Propositional formulas are denoted by capital Latin letters like A, B, C possibly annotated with subscripts, superscripts or primes.

We extend the propositional language by Boolean quantifiers. Universal ($\forall$) and existential ($\exists$) quantification is allowed within a QBF. QBFs are denoted by Greek letters. Observe that we allow non-prenex formulas, i.e., quantifiers may occur deeply in a QBF and not only in an initial quantifier prefix. An example for a non-prenex formula is $\forall p\,(p \rightarrow \forall q \exists r\,(q \wedge r \wedge s))$, where p, q, r and s are variables. Moreover, free variables (like s) are allowed, i.e., there might be occurrences of variables in the formula for which we have no quantification. Formulas without

free variables are called *closed*; otherwise they are called *open*. The *universal* (*existential*) closure of φ is $\forall x_1 \ldots \forall x_n \varphi$ ($\exists x_1 \ldots \exists x_n \varphi$), for which we often write $\forall \boldsymbol{X} \varphi$ ($\exists \boldsymbol{X} \varphi$) if $\boldsymbol{X} = \{x_1, \ldots, x_n\}$ is the set of all free variables in φ. A formula in *prenex conjunctive normal form* (PCNF) has the form $Q_1 p_1 \ldots Q_n p_n\, A$, where $Q_1 p_1 \ldots Q_n p_n$ is the *quantifier prefix*, $Q_i \in \{\forall, \exists\}$ and A is the (propositional) *matrix* which is in CNF. The *size* of a formula φ, *size*(φ), is the number of occurrences of connectives or quantifiers.

Let Σ_0^q and Π_0^q both denote the set of propositional formulas. For $i > 0$, Σ_i^q is the set of all QBFs whose prenex forms starts with $\exists$ and which have $i-1$ quantifier alternations. Π_i^q is the dual of Σ_i^q and $\Sigma_{i-1}^q \subseteq \Pi_i^q$ as well as $\Pi_{i-1}^q \subseteq \Sigma_i^q$ holds. We refer to [11] for more details.

The semantics of propositional logic is based on an *evaluation function* indexed by a *variable assignment* I for free variables. The semantics is extended to quantifiers by $\nu_I(Qp\,\varphi) = \nu_I(\varphi\{p/\top\} \circ \varphi\{p/\bot\})$, where $\circ = \vee$ if $Q = \exists$, and $\circ = \wedge$ if $Q = \forall$. We denote by $\varphi\{p/\psi\}$ the replacement of all (free) occurrences of p by ψ in φ.

A *quantified propositional proof system* is a surjective PTIME-computable function F from the set of strings over some finite alphabet to the set of valid QBFs. Every string α is then a proof of $F(\alpha)$. Let P_1 and P_2 be two proof systems. Then P_1 *polynomially simulates* (p-simulates) P_2 if there is a polynomial p such that for every natural number n and every formula φ, the following holds. If there is a proof of φ in P_2 of size n, then there is a proof of φ (or a suitable translation of it) in P_1 whose size is less than $p(n)$.

3 Calculi for Quantified Boolean Formulas

We first discuss sequent calculi [7] with different alternative quantifier rules. Later Q-resolution [10] is introduced which is applicable to QBFs in PCNF.

3.1 Sequent Calculi for Quantified Boolean Formulas

Sequent calculi do not work directly on formulas but on sequents. A *sequent* S is an ordered pair of the form $\Gamma \vdash \Delta$, where Γ and Δ are finite sequences of formulas. Γ is the *antecedent* of S, and Δ is the *succedent* of S. A formula occurring in one of Γ or Δ is called a *sequent formula* (of S). We write "$\vdash \Delta$" or "$\Gamma \vdash$" whenever Γ or Δ is empty, respectively. The meaning of a sequent $\Phi_1, \ldots, \Phi_n \vdash \Psi_1, \ldots, \Psi_m$ is the same as the meaning of $(\bigwedge_{i=1}^n \Phi_i) \rightarrow (\bigvee_{i=1}^m \Psi_i)$. The *size* of S, *size*(S), is the sum over the size of all sequent formulas in S.

We introduce the axioms and the rules in Fig. 1. In the *strong quantifier rules* $\exists l_e$ and $\forall r_e$, q has to satisfy the *eigenvariable* (EV) *condition*, i.e., q does not occur as a free variable in the conclusion of these rules. In the *weak quantifier rules* $\forall l$ and $\exists r$, no free variable of Ψ is allowed to become bound in $\Phi\{p/\Psi\}$. For instance, this restriction forbids the introduction of x for y in the (false) QBF $\exists y \forall x\,(x \leftrightarrow y)$. Without this restriction, the true QBF $\forall x\,(x \leftrightarrow x)$ would result.

In the following, we instantiate the quantifier rules as follows. If the formula Ψ in $\forall l$ and $\exists r$ is restricted to a propositional formula, we call the quantifier

$$\Phi \vdash \Phi \ \text{Ax} \qquad \bot \vdash \ \bot l \qquad \vdash \top \ \top r$$

$$\frac{\Gamma \vdash \Delta}{\Phi^*, \Gamma \vdash \Delta}\ wl \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \Phi^*}\ wr$$

$$\frac{\Gamma_1, \Phi^+, \Psi^+, \Gamma_2 \vdash \Delta}{\Gamma_1, \Psi^*, \Phi^*, \Gamma_2 \vdash \Delta}\ el \qquad \frac{\Gamma \vdash \Delta_1, \Phi^+, \Psi^+, \Delta_2}{\Gamma \vdash \Delta_1, \Psi^*, \Phi^*, \Delta_2}\ er$$

$$\frac{\Gamma_1, \Phi^+, \Phi^+, \Gamma_2 \vdash \Delta}{\Gamma_1, \Phi^*, \Gamma_2 \vdash \Delta}\ cl \qquad \frac{\Gamma \vdash \Delta_1, \Phi^+, \Phi^+, \Delta_2}{\Gamma \vdash \Delta_1, \Phi^*, \Delta_2}\ cr$$

$$\frac{\Gamma \vdash \Delta, \Phi^+}{(\neg\Phi)^*, \Gamma \vdash \Delta}\ \neg l \qquad \frac{\Phi^+, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, (\neg\Phi)^*}\ \neg r$$

$$\frac{\Phi^+, \Psi^+, \Gamma \vdash \Delta}{(\Phi \wedge \Psi)^*, \Gamma \vdash \Delta}\ \wedge l \qquad \frac{\Gamma \vdash \Delta, \Phi^+ \quad \Gamma \vdash \Delta, \Psi^+}{\Gamma \vdash \Delta, (\Phi \wedge \Psi)^*}\ \wedge r$$

$$\frac{\Phi^+, \Gamma \vdash \Delta \quad \Psi^+, \Gamma \vdash \Delta}{(\Phi \vee \Psi)^*, \Gamma \vdash \Delta}\ \vee l \qquad \frac{\Gamma \vdash \Delta, \Phi^+, \Psi^+}{\Gamma \vdash \Delta, (\Phi \vee \Psi)^*}\ \vee r$$

$$\frac{\Gamma \vdash \Delta, \Phi^+ \quad \Psi^+, \Gamma \vdash \Delta}{(\Phi \to \Psi)^*, \Gamma \vdash \Delta}\ \to l \qquad \frac{\Phi^+, \Gamma \vdash \Delta, \Psi^+}{\Gamma \vdash \Delta, (\Phi \to \Psi)^*}\ \to r$$

$$\frac{\Gamma \vdash \Delta, \Phi\{p/q\}^+}{\Gamma \vdash \Delta, (\forall p \Phi)^*}\ \forall r_e \qquad \frac{\Phi\{p/q\}^+, \Gamma \vdash \Delta}{(\exists p \Phi)^*, \Gamma \vdash \Delta}\ \exists l_e$$

$$\frac{\Phi\{p/\Psi\}^+, \Gamma \vdash \Delta}{(\forall p \Phi)^*, \Gamma \vdash \Delta}\ \forall l \qquad \frac{\Gamma \vdash \Delta, \Phi\{p/\Psi\}^+}{\Gamma \vdash \Delta, (\exists p \Phi)^*}\ \exists r$$

Fig. 1. Axioms and inference rules for sequent calculi. *Principal formulas* are marked by *, *auxiliary formulas* by $^+$, the other (unmarked) formulas are *side formulas*.

rules $\forall l_f$ and $\exists r_f$. If only variables or truth constants are allowed, then the index f is replaced by v. Finally, if Ψ is further restricted to truth constants, then the index is s. We define three different sequent calculi $\mathsf{Gqx e}$ ($\mathsf{x} \in \{\mathsf{s}, \mathsf{v}, \mathsf{f}\}$) for QBFs possessing the quantifier rules with index x and $\forall r_e$ and $\exists l_e$. A fourth calculus, Gqss, is defined by adopting $\forall l_s$ and $\exists r_s$ together with the following two rules.

$$\frac{\Gamma \vdash \Delta, (\Phi\{p/\top\} \wedge \Phi\{p/\bot\})^+}{\Gamma \vdash \Delta, (\forall p \Phi)^*}\ \forall r_s \qquad \frac{(\Phi\{p/\top\} \vee \Phi\{p/\bot\})^+, \Gamma \vdash \Delta}{(\exists p \Phi)^*, \Gamma \vdash \Delta}\ \exists l_s$$

All the calculi introduced above are *cut-free*, i.e., the *cut rule*

$$\frac{\Gamma_1 \vdash \Delta_1, \Phi^+ \qquad \Phi^+, \Gamma_2 \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ cut$$

is not part of the calculus. For $i \geq 0$ and $\mathsf{G} \in \{\mathsf{Gqss}, \mathsf{Gqse}, \mathsf{Gqve}, \mathsf{Gqfe}\}$, G_i is G extended by cut, where the cut formula Φ is restricted to be a $\Pi_i^q \cup \Sigma_i^q$ formula.

A *sequence* proof α of a sequent S (the *end sequent*) in G is a sequence $S_1, \ldots, S_m$ of sequents such that $S_m = S$ and, for every S_i ($1 \leq i \leq m$), S_i is

either an axiom of G, the conclusion of an application of a unary inference from G with premise S_j, or the conclusion of an application of a binary inference from G with premises S_j, S_k $(j, k < i)$. Proofs in G are called G proofs. If α is a proof of $\vdash \Phi$, then α is a proof of the *formula* Φ. A proof α is called *tree-like* or a *tree proof*, if every sequent in α is used at most once as a premise. The *length*, $l(\alpha)$, of α is the number m of sequents occurring in α and its size is $\sum_{i=1}^{m} size(S_i)$.

We denote by G^* the version of G which permits only tree proofs. They are assumed to be in *free variable normal form* (FVNF) [2,4], to which they can be translated efficiently. A tree proof α is in FVNF, if (i) no free variable from the end sequent is used as an EV, and (ii) every other free variable z occurring in α is used exactly once as an EV and appears in α only in sequents above the application of $\exists l_e$ or $\forall r_e$ which introduced z.

Later, we have to trace formula occurrences through a tree proof. The means to do this is an *ancestor* relation between formula occurrences in a tree proof [2]. We first define *immediate descendants* (IDs). If Φ is an auxiliary formula of any rule R except exchange or cut, then Φ's ID is the principal formula of R. For the exchange rules el and er, the ID of Φ or Ψ in the premise is Φ or Ψ, respectively, in the conclusion. An occurrence of the cut formula does not have any ID. If Φ is a side formula at position i in $\Gamma, \Gamma_1, \Gamma_2, \Delta, \Delta_1, \Delta_2$ of the premise(s), then Φ's ID is the same formula at the same position of the same sequence in the conclusion. Now, Φ is an *immediate ancestor* of Ψ iff Ψ is an ID of Φ. The *ancestor relation* is the reflexive and transitive closure of the immediate ancestor relation.

G is *sound* and *complete*, i.e., a sequent S is valid iff it has a G proof. We will consider variants of our tree calculi without exchange rules and where sequents consists of multisets instead of sequences. Since the multiset and the sequence version are p-equivalent, it is sufficient to consider the multiset version.

The calculus in Fig. 1 is a cut-free variant of calculi proposed by Krajíček and Pudlák (KP) (cf, e.g., [11]). In the calculi KP_i, only $\Sigma_i^q \cup \Pi_i^q$ formulas can occur in a proof. Cook and Morioka [4] modified the KP calculi by allowing arbitrary QBFs as sequent formulas, but restricting cut formulas to $\Sigma_i^q \cup \Pi_i^q$ formulas. Moreover, $\forall l$ and $\exists r$ are replaced by $\forall l_f$ and $\exists r_f$.[1] They show in [4] that any of their system G_i $(i > 0)$ is p-equivalent to the corresponding system KP_i for proving formulas from $\Sigma_i^q \cup \Pi_i^q$. G_i is complete for QBFs (in contrast to KP_i).

3.2 The Q-resolution Calculus

The quantified resolution calculus, Q-res, is an extension of propositional resolution to QBFs [10]. There is no explicit handling of quantifiers by specific rules. Instead the $\forall$ reduction rule which operates on single clauses inspects the global quantifier prefix. As we will see, this processing of quantifiers results in a relatively weak calculus with respect to the ability to produce succinct refutations.

The input for Q-res is a (closed) QBF in PCNF. Quantifier blocks are numbered from left to right in increasing order and bound variables from quantifier

[1] The restriction to *propositional* formulas is necessary. For unrestricted QBFs, the hierarchy of calculi would "collapse" to G_1.

$$\frac{C_1 \vee x \vee C_2 \quad C_3 \vee \neg x \vee C_4}{C_1 \vee C_2 \vee C_3 \vee C_4}\ \exists\mathsf{PR} \qquad \frac{C_1 \vee \ell \vee C_2 \vee \ell \vee C_3}{C_1 \vee \ell \vee C_2 \vee C_3}\ \mathsf{PF} \qquad \frac{C_5 \vee k \vee C_6}{C_5 \vee C_6}\ \forall\mathsf{R}$$

C_1 to C_6 are clauses, x is an $\exists$ variable and ℓ a literal. $C_5 \vee k \vee C_6$ is non-tautological and k is a $\forall$ literal with level i. Any $\exists$ literal in $C_5 \vee C_6$ has a level smaller than i.

Fig. 2. The rules of the Q-resolution calculus

block i have level i. Literal occurrences in the CNF inherit the level from their variable in the quantifier prefix. Q-res consists of the *propositional resolution rule* $\exists$PR over existential literals, the *factoring rule* PF and the $\forall$ *reduction rule* $\forall$R, all of which are shown in Fig. 2. The following is Theorem 2.1 in [10].

Theorem 1. *A QBF φ in PCNF is false iff $\square$ can be derived from φ by* Q-res.

A Q-res refutation can be in tree form as well as in sequence form. The *length* of a Q-res refutation is the number of clauses in it. The *size* of a Q-res refutation is the sum of the sizes of its clauses.

4 Comparing Different Quantifier Rules

We compare Gqss, Gqse, Gqve and Gqfe with respect to p-simulation. Let $\mathsf{G} \in \{\mathsf{Gqse}, \mathsf{Gqve}, \mathsf{Gqfe}\}$. We reproduce Definition 6 and Lemma 3 from [4] below.

Definition 1. *Let φ be a quantified QBF in prenex form and let S be the sequent $\vdash \varphi$. Let $\alpha(S)$ be a G_0 proof of S. Then any quantifier-free formula A in $\alpha(S)$ that occurs as the auxiliary formula of a quantifier inference is called an α-prototype of φ. Define the* Herbrand α-disjunction *to be the sequent $\vdash A_1, \ldots, A_m$, where $A_1, \ldots, A_m$, are all the α-prototypes of φ.*

Lemma 1. *Let φ be a quantified QBF in prenex form and let S be the sequent $\vdash \varphi$. Let $\alpha(S)$ be a G_0 proof of S. Then the Herbrand α-disjunction is valid and it has a purely propositional sequent proof of size polynomial in the size of $\alpha(S)$.*

In the construction of the proof of the Herbrand α-disjunction in Lemma 1, no (new) cut is introduced and the form of the proof is retained. Consequently, if $\alpha(S)$ is cut-free and tree-like, then so is the resulting propositional proof.

Proposition 1. *(1)* Gqss_0 *cannot p-simulate* Gqse^**, (2)* Gqse_0 *cannot p-simulate* Gqve^* *and (3)* Gqve_0 *cannot p-simulate* Gqfe^**.*

We show (3) in detail. Let $(F_n)_{n>0}$ be a sequence of propositional formulas of the form $\bigwedge_{i=1}^{n}((\neg x_i) \leftrightarrow y_i)$ and let φ_n be $\forall \boldsymbol{X}_n \exists \boldsymbol{Y}_n F_n$ with $\boldsymbol{X}_n = \{x_1, \ldots, x_n\}$ and $\boldsymbol{Y}_n = \{y_1, \ldots, y_n\}$. The size of φ_n is linear in n and it has a short proof in Gqfe^* of length linear in n. It can be obtained by (i) introducing eigenvariable c_i for x_i for all i $(1 \leq i \leq n)$, (ii) introducing formula $\neg c_i$ for y_i for all i $(1 \leq i \leq n)$ and (iii) proving $\bigwedge_{i=1}^{n}\big((\neg c_i) \leftrightarrow (\neg c_i)\big)$ with $O(n)$ sequents.

Next we show that any proof of φ_n in Gqve_0 is exponential in n. The key observation is that only the introduction of truth constants for y_i makes sense. Otherwise we obtain conjunctive subformulas of the form $(\neg c_i) \leftrightarrow v_i$ which are unprovable. Consequently, all $\exists r$ inferences introduce truth constants.

Let α_n be an arbitrary Gqve_0 proof of $\vdash \varphi_n$. By Lemma 1 we get a purely propositional Gqve_0 proof β_n of the valid Herbrand α_n-disjunction

$$\vdash F_{n,1}, \ldots, F_{n,m} \ .$$

Moreover, the size of β_n is polynomially related to the size of α_n. We argue in the following that this disjunction consists of $m = 2^n$ formulas. Let S_n be the following set $\{F_n\{x_1/c_1, \ldots, x_n/c_n, y_1/t_1, \ldots, y_n/t_n\} \mid t_i \in \{\bot, \top\}\}$ of all possible substitution instances of F_n with 2^n elements. We show in the following that $\bigvee_{d \in D} d$ is not valid if $D \subset S_n$ holds. Then all elements of S_n have to occur in the Herbrand α_n-disjunction and the exponential lower bound follows.

Let C be an arbitrary instance $\bigwedge_{i=1}^{n} \big((\neg c_i) \leftrightarrow t_i\big)$ of F_n which is in S_n but not in D. Let I be any assignment that makes C true, i.e., each c_i is assigned to the dual of t_i by I. Now take an arbitrary $d \in D$ of the form $\bigwedge_{i=1}^{n} \big((\neg c_i) \leftrightarrow s_i\big)$. There must be an index k, $1 \leq k \leq n$, such that $s_k \neq t_k$. Then $(\neg c_k) \leftrightarrow s_k$ is false under I and so is d. Since d has been chosen arbitrarily, all elements of D are false under I and so is $\bigvee_{d \in D} d$. Consequently, all elements of S_n have to occur in the Herbrand α_n-disjunction and the exponential lower bound follows.

For (2), we can use a similar argumentation with $(G_n)_{n>0}$ instead of F_n, where G_n is of the form $\bigwedge_{i=1}^{n}(x_i \leftrightarrow y_i)$. For (1), the family of formula is $(\psi_n)_{n>1}$, where ψ_n is of the form $\exists x_n \forall y_n \ldots \exists x_1 \forall y_1 \, (x_n \vee y_n \vee \cdots \vee x_1 \vee y_1)$.

Looking at the structure of φ_n, one immediately realizes that the quantifiers can be pushed into the formula ("antiprenexed") in an equivalence-preserving way. This antiprenexed formula F'_n: $\bigwedge_{i=1}^{n}(\forall x_i \exists y_i((\neg x_i) \leftrightarrow y_i))$ has short proofs in Gqve^*, $\mathsf{Gqse}^*$and even in Gqss^*, mainly because $\forall x_i \exists y_i((\neg x_i) \leftrightarrow y_i)$ has a proof of constant length. A similar statement holds for the other two cases.

4.1 Using Eliminable Extensions to Simulate $\exists r_f/\forall l_f$ by $\exists r_v/\forall l_v$

We show in the following that the weak quantifier rules $\exists r_f$ and $\forall l_f$ in Gqfe_i^* can be simulated efficiently by $\exists r_v$ and $\forall l_v$ in Gqve_i^* for $i \geq 1$. The key idea is to use a quantified extension $\varepsilon(B)$ of the form $\exists x \, (x \leftrightarrow B)$ with B being a propositional formula. $\varepsilon(B)$ has a proof $\alpha(\varepsilon(B))$ in Gqve^* and Gqse^* of constant length.

Given a tree proof β_e of an end sequent S_e. For any occurrence of an inference $\forall l_f$ and $\exists r_f$ introducing non-atomic propositional formula B, we perform the following. Take an occurrence I of an inference $\exists r_f$ (the case of $\forall l_f$ is similar) and a globally new variable q, not occurring in β_e and not introduced as a new variable before. Employ the ancestor relation for I's auxiliary formula $\Phi\{p/B\}$ and get all highest sequents with occurrences of the sequent formula B originating from I. Start from the next lower sequent of these highest positions downwards until the conclusion of I and put $F(B) = q \leftrightarrow B$ into the antecedent of each sequent. If there is already a copy there, then do nothing. If there are strong

quantifier rules, then there is *no* violation of the EV condition because we add only a globally new variable; all the variables from B have been already present in the sequent before.

Employing the ancestor relation again and starting from $\Phi\{p/B\}$, we replace any formula $\Psi\{p/B\}$ by $\Psi\{p/q\}$ in sequents containing $F(B)$. This includes a replacement of B by q. Perform the above procedure for each of the w occurrences of $\forall l_f$ and $\exists r_f$. We have not increased the number of sequents yet, but there are $O(w)$ additional formulas in any sequent.

We are going to correct the inference tree. We check all sequents with sequent formulas of the form $F(B)$ whether binary rules are violated, like, e.g., in the left inference figure below for the case of $\wedge r$. It is replaced by the correct right figure. ($F(B_1)$ and $F(B_2)$ are replaced by F_1, F_2 for space reasons).

$$\frac{F_1, F_2, \Gamma \vdash \Delta, \Phi_1\{p/q\} \quad \Gamma \vdash \Delta, \Phi_2}{F_1, F_2, \Gamma \vdash \Delta, \Phi_1\{p/q\} \wedge \Phi_2} \qquad \frac{F_1, F_2, \Gamma \vdash \Delta, \Phi_1\{p/q\} \quad \dfrac{\Gamma \vdash \Delta, \Phi_2}{F_1, F_2, \Gamma \vdash \Delta, \Phi_2}\, wl*}{F_1, F_2, \Gamma \vdash \Delta, \Phi_1\{p/q\} \wedge \Phi_2}$$

We have to perform two additional corrections, namely (i) to get rid of $F(B)$ immediately below the conclusion of I and (ii) to correct the situation when B originating from I occurs as a principal formula in a propositional inference or as a formula in an axiom of the original proof β_e. For the former, we use

$$\frac{\alpha(\varepsilon(B)) \qquad \dfrac{\dfrac{q \leftrightarrow B,\, \Gamma \vdash \Delta,\, \Phi\{p/q\}}{q \leftrightarrow B,\, \Gamma \vdash \Delta,\, \exists p\, \Phi}\, \exists r_v}{\exists x\,(x \leftrightarrow B),\, \Gamma \vdash \Delta,\, \exists p\, \Phi}\, \exists l_e}{\vdash \exists x\,(x \leftrightarrow B) \qquad \Gamma \vdash \Delta, \exists p\, \Phi}\, cut$$

with a cut on a Σ_1^q-formula. Let us consider (ii) where B is the principal formula of a propositional inference. Below is one possible case for $B = B_1 \vee B_2$.

$$\frac{F(B),\, \Gamma \vdash \Delta,\, B_1, B_2}{F(B),\, \Gamma \vdash \Delta,\, q}\, \vee r \qquad \frac{\dfrac{F(B),\, \Gamma \vdash \Delta,\, B_1, B_2}{F(B),\, \Gamma \vdash \Delta,\, B}\, \vee r \qquad \overset{\alpha}{B, q \leftrightarrow B \vdash q}}{\dfrac{F(B),\, F(B),\, \Gamma \vdash \Delta,\, q}{F(B),\, \Gamma \vdash \Delta,\, q}\, cl}\, cut$$

cl is needed if $F(B)$ is required in the left branch. The case for the axiom is simpler. Finally, wl inferences are introduced to remove $q \leftrightarrow B$.

During the proof manipulations, we have added to each sequent $O(w)$ formulas. Moreover, by correcting the binary inferences, we added $O(w)$ sequents for any sequent in the original proof. For each occurrence of B and each of the w occurrences of the quantifier rules, we added a deduction of length $O(1)$ In total, we obtain a polynomial increase in length and size.

5 Exponential Separation of Q-res and Gqve*

We stepwisely construct a family $(\varphi_n)_{n>1}$ of closed QBFs φ_n for which (1) there exists short proofs in Gqve*, but (2) any Q-resolution refutation of $\neg\varphi_n$ has length exponential in n. We use the traditional approaches, namely a refutational approach with resolution and an affirmative approach with sequent systems.

5.1 The Construction of φ_n

We start with a version of the well-known pigeon hole formula in *disjunctive* normal form. The formula for n holes and $n+1$ pigeons is given by

$$\left(\bigvee_{i=1}^{n+1}\bigwedge_{j=1}^{n}\neg x_{i,j}\right)\vee\left(\bigvee_{j=1}^{n}\bigvee_{1\leq i_1<i_2\leq n+1}(x_{i_1,j}\wedge x_{i_2,j})\right)\ .$$

Let $\mathsf{DPHP}_n^{X_n}$ denote this formula over the variables in $X_n=\{x_{1,1},\ldots,x_{n+1,n}\}$. Variable $x_{i,j}$ is intended to denote that pigeon i is sitting in hole j. The usual (unsatisfiable) version of the pigeon hole formula in CNF, $\mathsf{CPHP}_n^{X_n}$, is given by

$$\left(\bigwedge_{i=1}^{n+1}(\bigvee_{j=1}^{n}x_{i,j})\right)\wedge\left(\bigwedge_{j=1}^{n}\bigwedge_{1\leq i_1<i_2\leq n+1}(\neg x_{i_1,j}\vee\neg x_{i_2,j})\right)\ .$$

The number of clauses in $\mathsf{CPHP}_n^{X_n}$ is $l_n=(n+1)+n^2(n+1)/2$, $size(\mathsf{CPHP}_n^{X_n})$ is $O(n^3)$, and $\mathsf{CPHP}_n^{X_n}$ is obtained from $\neg\mathsf{DPHP}_n^{X_n}$ by shifting negations inwards using de Morgan's laws and eliminating double negations. Intuitively, we want to show that the refutation problem corresponding to the negation of the formula

$$\forall X_n\exists Y_n\big(\mathsf{DPHP}_n^{Y_n}\rightarrow\mathsf{DPHP}_n^{X_n}\big)\tag{1}$$

results only in Q-res refutations of length exponential in n. A short Gqve* proof of (1) exists which mainly relies on a unification property, namely that (i) $\forall r_e$ introduces eigenvariables C_n for X_n and (ii) $\exists r_v$ introduces exactly the same variables C_n for Y_n, therefore unifying the two versions of DPHP_n. As we will see later, this instantiation property of $\exists r_v$ is important to get a short proof.

A problem occurs if we want to translate the provability problem of (1) into a refutation problem of its negation. Clausifying the disjunctive normal form $\mathsf{DPHP}_n^{Y_n}$ using distributivity laws results in an exponential number of (tautological) clauses. We slightly modify the formula to be considered by introducing new variables of the form $z_{i_1,i_2,j}$ for disjuncts in $\mathsf{DPHP}_n^{Y_n}$. This procedure is in the spirit of the well-known Tseitin translation [13]. We use the "one polarity optimization" of [12]. For the first $n+1$ disjuncts of the form $\bigwedge_{j=1}^{n}\neg y_{i,j}$ with $1\leq i\leq n+1$, we use variables $z_{1,0,0},\ldots,z_{n+1,0,0}$. For the second part, for any $1\leq j\leq n$ and the $n(n+1)/2$ disjuncts, we use

$$z_{1,2,j},\ldots,z_{1,n+1,j},z_{2,3,j},\ldots,z_{2,n+1,j},\ldots,z_{n,n+1,j}\ .\tag{2}$$

The set of these variables for DPHP_n is denoted by Z_n. Due to this construction, we can speak about the conjunction corresponding to the variable $z_{i_1,i_2,j}$.

We construct the conjunctive normal form $\mathsf{TPHP}_n^{Y_n,Z_n}$ of $\mathsf{DPHP}_n^{Y_n,Z_n}$ as follows. First, we take the clause $D_n^{Z_n}=\bigvee_{z\in Z_n}\neg z$ over all variables in Z_n. The formula $P_n^{Y_n,Z_n}$ for the first $(n+1)$ disjuncts of $\mathsf{DPHP}_n^{Y_n}$ is of the form

$$\bigwedge_{i=1}^{n+1}\bigwedge_{j=1}^{n}(z_{i,0,0}\vee\neg y_{i,j})\ .$$

For the remaining $n^2(n+1)/2$ disjuncts of $\mathsf{DPHP}_n^{Y_n}$, we have the formula $Q_n^{Y_n,Z_n}$

$$\bigwedge_{j=1}^{n} \bigwedge_{1 \le i_1 < i_2 \le n+1} \big((z_{i_1,i_2,j} \vee y_{i_1,j}) \wedge (z_{i_1,i_2,j} \vee y_{i_2,j})\big) \ .$$

Then $\mathsf{TPHP}_n^{Y_n,Z_n}$ is $D_n^{Z_n} \wedge P_n^{Y_n,Z_n} \wedge Q_n^{Y_n,Z_n}$ and $size(\mathsf{TPHP}_n^{Y_n,Z_n})$ is $O(n^3)$. The family of formulas we consider in the following is $(\varphi_n)_{n>1}$, where φ_n is

$$\forall X_n \exists Y_n \forall Z_n \big(\mathsf{TPHP}_n^{Y_n,Z_n} \to \mathsf{DPHP}_n^{X_n}\big). \tag{3}$$

Formula (1) is equivalent to formula (3) because $\mathsf{DPHP}_n^{X_n}$ is valid. We show that

$$\mathsf{DPHP}_n^{Y_n} \equiv \exists Z_n \, \mathsf{TPHP}_n^{Y_n,Z_n} \tag{4}$$

holds.

$\Longrightarrow$: Let I be a model of $\mathsf{DPHP}_n^{Y_n}$, i.e., $I \models \mathsf{DPHP}_n^{Y_n}$ holds.

Case 1: There exists an index i such that $I \models \bigwedge_{j=1}^{n} \neg y_{i,j}$ holds. Therefore, $I \models \neg y_{i,1}, \ldots, I \models \neg y_{i,n}$ as well as $I \models \bigwedge_{j=1}^{n} z_{i,0,0} \vee \neg y_{i,j}$ hold. Let us extend I to an interpretation J such that $\mathsf{TPHP}_n^{Y_n,Z_n}$ is true under J. We set all $z_{k,l,m}$ from Z_n to true under J except $z_{i,0,0}$ which is set to false. Then $J \models D_n^{Z_n}$, $J \models P_n^{Y_n,Z_n}$ and $J \models Q_n^{Y_n,Z_n}$ hold.

Case 2: There exist indices i_1, i_2 and j such that $I \models y_{i_1,j} \wedge y_{i_2,j}$ holds. Then $I \models (z_{i_1,i_2,j} \vee y_{i_1,j}) \wedge (z_{i_1,i_2,j} \vee y_{i_2,j})$ holds. Again, we extend I to J such that $J \models \mathsf{TPHP}_n^{Y_n,Z_n}$ holds. We set all $z_{k,l,m}$ from Z_n to true under J except $z_{i_1,i_2,j}$ which is set to false. Then $J \models D_n^{Z_n}$, $J \models P_n^{Y_n,Z_n}$ and $J \models Q_n^{Y_n,Z_n}$ hold.

In both cases, there exists an extension J of I (which interprets all variables in Z_n), such that $J \models \mathsf{TPHP}_n^{Y_n,Z_n}$. Hence, $\exists Z_n \mathsf{TPHP}_n^{Y_n,Z_n}$ is true under I.

$\Longleftarrow$: Let I be an interpretation such that $I \models \exists Z_n \mathsf{TPHP}_n^{Y_n,Z_n}$ holds. Then there exists an extension J of I (which interprets all variables in Z_n), such that $J \models \mathsf{TPHP}_n^{Y_n,Z_n}$. Consequently $J \models D_n^{Z_n}$ holds and at least one z variable has to be false under J.

Case 1: There exists an index i such that $J \models \neg z_{i,0,0}$ holds. Since J satisfies $\bigwedge_{j=1}^{n}(z_{i,0,0} \vee \neg y_{i,j})$, J and also I make $\bigwedge_{j=1}^{n} \neg y_{i,j}$ true. Then $I \models \mathsf{DPHP}_n^{Y_n}$ holds.

Case 2: There exist indices i_1, i_2 and j such that $J \models \neg z_{i_1,i_2,j}$ holds. Since $J \models (z_{i_1,i_2,j} \vee y_{i_1,j}) \wedge (z_{i_1,i_2,j} \vee y_{i_2,j})$ also holds, $y_{i_1,j} \wedge y_{i_2,j}$ has to be true under J and I. Then $I \models \mathsf{DPHP}_n^{Y_n}$ holds.

We continue in the next subsection with the construction of a short proof of φ_n in Gqve^*. Afterwards, we show in Section 5.3 that any sequence Q-res refutation of $\neg\varphi_n$ possesses a number of clauses which is exponential in n.

5.2 Short Proofs of φ_n in Gqve^*

We provide a short proof of φ_n in Gqve^*. Observe that any proof of $\forall X_n \, \mathsf{DPHP}_n^{X_n}$ is exponential (see Theorem 5.3.5 in [3]).

Proposition 2. *Let $(\varphi_n)_{n>1}$ be a family of formulas where φ_n is given in (3). Then there exists a proof of $\vdash \varphi_n$ in* Gqve* *of size polynomial in n.*

We first show that sequents $S_{i_1,i_2,j}$ of the form

$$\neg z_{i_1,i_2,j}, P_n^{C_n,Z_n}, Q_n^{C_n,Z_n} \vdash \bigvee_{i=1}^{n+1} \bigwedge_{j=1}^{n} \neg c_{i,j}, \bigvee_{j=1}^{n} \bigvee_{1\le i_1<i_2\le n+1} (c_{i_1,j} \wedge c_{i_2,j})$$

are derivable using $O(n^3)$ sequents.

Case 1: $z_{i_1,i_2,j}$ is of the form $z_{i,0,0}$ for $1 \le i \le n+1$. Take axioms and derive

$$\neg c_{i,1}, \ldots, \neg c_{i,n} \vdash \bigwedge_{j=1}^{n} \neg c_{i,j}$$

by applications of $\wedge r$ and wl using $O(n^2)$ sequents. Continue with the derived sequent by using axioms and applications of $\neg l$, weakening and $\vee l$ to generate

$$\neg z_{i,0,0}, z_{i,0,0} \vee \neg c_{i,1}, \ldots, z_{i,0,0} \vee \neg c_{i,n} \vdash \bigwedge_{j=1}^{n} \neg c_{i,j}$$

using $O(n^2)$ sequents. By applications of $\wedge l$ to the last sequent, we obtain

$$\neg z_{i,0,0}, \bigwedge_{j=1}^{n} (z_{i,0,0} \vee \neg c_{i,j}) \vdash \bigwedge_{j=1}^{n} \neg c_{i,j}$$

requiring further $O(n)$ sequents. Continue with weakening, $\wedge l$ and $\vee r$ to generate

$$\neg z_{i,0,0}, P_n^{C_n,Z_n}, Q_n^{C_n,Z_n} \vdash \bigvee_{i=1}^{n+1} \bigwedge_{j=1}^{n} \neg c_{i,j}, \bigvee_{j=1}^{n} \bigvee_{1\le i_1<i_2\le n+1} (c_{i_1,j} \wedge c_{i_2,j})$$

from the sequent above using $O(n)$ sequents. In total, the derivation of each of the $(n+1)$ sequents $S_{1,0,0}, \ldots, S_{n+1,0,0}$ requires $O(n^2)$ sequents, each of which consists of $O(n)$ sequent formulas.

Case 2: $z_{i_1,i_2,j}$ occurs as an element in (2). Start from axioms and derive

$$c_{i_1,j}, c_{i_2,j} \vdash c_{i_1,j} \wedge c_{i_2,j}$$

by weakenings and $\wedge r$ using $O(1)$ sequents. Take axioms and apply $\neg l$, weakening, $\vee l$ and $\wedge l$ to get from the sequent above

$$\neg z_{i_1,i_2,j}, (z_{i_1,i_2,j} \vee c_{i_1,j}) \wedge (z_{i_1,i_2,j} \vee c_{i_2,j}) \vdash c_{i_1,j} \wedge c_{i_2,j}$$

with $O(1)$ further sequents. Using $O(n^3)$ weakenings, $\wedge l$ and $\vee r$, we obtain

$$\neg z_{i_1,i_2,j}, P_n^{C_n,Z_n}, Q_n^{C_n,Z_n} \vdash \bigvee_{i=1}^{n+1} \bigwedge_{j=1}^{n} \neg c_{i,j}, \bigvee_{j=1}^{n} \bigvee_{1\le i_1<i_2\le n+1} (c_{i_1,j} \wedge c_{i_2,j}).$$

In total, we have to derive $n^2(n+1)/2$ sequents using at most a cubic number of sequents in each derivation. Each sequent has $O(n^3)$ sequent formulas.

This completes the case analysis. The sequent

$$D_n^{Z_n}, P_n^{C_n,Z_n}, Q_n^{C_n,Z_n} \vdash \bigvee_{i=1}^{n+1} \bigwedge_{j=1}^{n} \neg c_{i,j}, \bigvee_{j=1}^{n} \bigvee_{1 \le i_1 < i_2 \le n+1} (c_{i_1,j} \wedge c_{i_2,j})$$

can be derived from the $O(n^3)$ different sequents $S_{i_1,i_2,j}$ by repeated applications of $\vee l$ using $O(n^3)$ sequents. Then we can continue as follows.

$$\dfrac{\dfrac{\dfrac{D_n^{Z_n}, P_n^{C_n,Z_n}, Q_n^{C_n,Z_n} \vdash \bigvee_{i=1}^{n+1} \bigwedge_{j=1}^{n} \neg c_{i,j}, \bigvee_{j=1}^{n} \bigvee_{1 \le i_1 < i_2 \le n+1} (c_{i_1,j} \vee c_{i_2,j})}{D_n^{Z_n}, P_n^{C_n,Z_n}, Q_n^{C_n,Z_n} \vdash \mathsf{DPHP}_n^{C_n}} \vee r}{\vdash \mathsf{TPHP}_n^{C_n,Z_n} \to \mathsf{DPHP}_n^{C_n}} \wedge l, \wedge l}{\forall r_e, \exists r_v, \forall r_e} \to r$$
$$\vdash \forall X_n \exists Y_n \forall Z_n \big(\mathsf{TPHP}_n^{Y_n,Z_n} \to \mathsf{DPHP}_n^{X_n}\big)$$

Hence the overall number of sequents used to derive the indicated end sequent is $O(n^6)$. There are $O(n^3)$ sequent formulas in each sequent and each such formula is a subformula of φ_n. Therefore, we have a polynomial size proof of φ_n in Gqve^*.

5.3 Q-resolution Refutations of $\neg\varphi_n$

We reconsider φ_n from above. Since φ_n is valid iff $\neg\varphi_n$ is unsatisfiable, we use the latter and show it by Q-resolution. As we will see, any Q-resolution refutation of $\neg\varphi_n$ is exponential in n. Take $\neg\varphi_n$ and push negation inwards. Then we get

$$\neg\varphi_n \text{ is unsat iff } \exists X_n \forall Y_n \exists Z_n \big(\mathsf{TPHP}_n^{Y_n,Z_n} \wedge \mathsf{CPHP}_n^{X_n}\big) \text{ is unsat.}$$

Proposition 3. *Any* Q-res *refutation of* $\exists X_n \forall Y_n \exists Z_n \big(\mathsf{TPHP}_n^{Y_n,Z_n} \wedge \mathsf{CPHP}_n^{X_n}\big)$ *has exponential size.*

Since the two indicated CNFs $\mathsf{TPHP}_n^{Y_n,Z_n}$ and $\mathsf{CPHP}_n^{X_n}$ belong to completely different languages, no resolution is possible where one parent clause is from the one part and the other parent clause is from the other part. Therefore

$$\forall Y_n \exists Z_n \big(\mathsf{TPHP}_n^{Y_n,Z_n}\big) \text{ is unsat} \quad \text{or} \quad \exists X_n \big(\mathsf{CPHP}_n^{X_n}\big) \text{ is unsat.}$$

We first consider $\exists X_n \big(\mathsf{CPHP}_n^{X_n}\big)$ which is the existential closure of the purely propositional pigeon hole formula $\mathsf{CPHP}_n^{X_n}$ in conjunctive normal form. Only the propositional resolution rule is applicable because no $\forall$ variable occurs. By Haken's famous result [8], any resolution refutation of $\mathsf{CPHP}_n^{X_n}$ is exponential in n. Consequently, the same holds for any Q-res refutation of the same formula. Hence, $\exists X_n \big(\mathsf{CPHP}_n^{X_n}\big)$ is false and therefore unsatisfiable.

We next consider $\forall Y_n \exists Z_n \mathsf{TPHP}_n^{Y_n,Z_n}$. Above we proved the following equivalence $\mathsf{DPHP}_n^{Y_n} \equiv \exists Z_n \mathsf{TPHP}_n^{Y_n,Z_n}$. Since $\mathsf{DPHP}_n^{Y_n}$ is valid, so is $\exists Z_n \mathsf{TPHP}_n^{Y_n,Z_n}$

and therefore $\forall Y_n \exists Z_n \left(\mathsf{TPHP}_n^{Y_n,Z_n}\right)$ is true. By the soundness and completeness of Q-resolution, no (non-tautological) clause with only universal literals can be derived. Hence, $\forall Y_n \exists Z_n \mathsf{TPHP}_n^{Y_n,Z_n}$ cannot provide any refutation.

In conclusion, any Q-res refutation of $\neg\varphi$ is exponential in n. Consider

$$\left(\mathsf{TPHP}_n^{X_n,Z_n} \wedge \mathsf{CPHP}_n^{X_n}\right) \tag{5}$$

which can be obtained by instantiating the quantifiers for Y_n properly. Interestingly, there exists a tree (Q-)resolution refutation of (the existential closure of) formula (5) of size polynomial in n, which identifies the simple way of handling quantifiers by $\forall$R to be the weak point in Q-res. Obviously, quantifier rules resulting an instantiation of the matrix formula can yield more succinct proofs.

From the above complexity analysis of Q-resolution refutations of $\neg\varphi$, a simple corollary can be drawn. Let us reconsider $\exists X_n \forall Y_n \exists Z_n \left(\mathsf{TPHP}_n^{Y_n,Z_n} \wedge \mathsf{CPHP}_n^{X_n}\right)$ to which we apply the QDPLL algorithm with clause learning. The only variables which are processed are from X_n because $\mathsf{CPHP}_n^{X_n}$ is unsatisfiable. Finding the conflicts results in learned clauses, which can be used to construct a Q-res refutation of the input formula as a witness for unsatisfiability. Since any Q-resolution refutation is exponential in n, so is the QDPLL refutation.[2]

6 Conclusion

We studied different techniques to handle quantification in QBFs. Integrated into a sequent calculus for propositional logic, all discussed combinations of quantifier rules yield sound and complete calculi, differing in their non-deterministic strength, i.e., their ability to represent proofs succinctly. We have seen that Q-res is a weaker calculus than sequent systems with reasonable quantifier rules. Although this result seems to be of limited relevance for practical applications, one should keep in mind that certificates (or solutions) are extracted from Q-res refutations produced by QBF solvers [1]. Since the size of the certificate corresponds to the size of the Q-res refutation, a more succinct proof could be beneficial.

We have identified instantiation as *the* feature for obtaining short proofs for our formulas. Neither the quantifier handling in Q-res nor semantically motivated quantifier rules possess this feature. Strong quantifier rules based on semantics are essentially binary inferences and in general not powerful enough in a cut-free sequent system. These rules require additional techniques like propagation of values, formula simplification, dependency directed backtracking, etc. to compensate their weakness. Such techniques can be integrated in sequent systems via restricted versions of cut or as additional inferences, cf. [6] for examples.

Although $\forall l_f$ and $\exists r_f$ are the rules with most non-deterministic power, they are not necessarily required for our problem formulas. They were actually proved with weaker rules $\forall l_v$ and $\exists r_v$ allowing only the introduction of variables (and truth constants). We provided some indication that, at least in some variants of sequent calculi like Gqve_i^* ($i \geq 1$), the weaker rules are sufficient. But a closer

[2] We learned this argument from F. Lonsing (private communication).

look reveals the practical problem of the $\forall l_f$ and $\exists r_f$ inferences, the simulation by extension and the simulation by cut (not discussed here): How does a good formula for the quantifier, the extension step or the cut rule look like?

References

1. Balabanov, V., Jiang, J.-H.R.: Resolution Proofs and Skolem Functions in QBF Evaluation and Applications. In: Gopalakrishnan, G., Qadeer, S. (eds.) CAV 2011. LNCS, vol. 6806, pp. 149–164. Springer, Heidelberg (2011)
2. Buss, S.: An introduction to proof theory. In: Handbook of Proof Theory, pp. 1–78. Elsevier, Amsterdam (1998)
3. Clote, P., Kranakis, E.: Boolean Functions and Models of Computation. Springer, Heidelberg (2002)
4. Cook, S.A., Morioka, T.: Quantified propositional calculus and a second-order theory for NC^1. Arch. Math. Log. 44(6), 711–749 (2005)
5. Cook, S.A., Reckhow, R.A.: On the lengths of proofs in the propositional calculus (preliminary version). In: STOC, pp. 135–148 (1974)
6. Egly, U., Seidl, M., Woltran, S.: A solver for QBFs in negation normal form. Constraints 14(1), 38–79 (2009)
7. Gentzen, G.: Untersuchungen über das logische Schließen. Mathematische Zeitschrift 39, 176–210, 405–431 (1935)
8. Haken, A.: The intractability of resolution. Theor. Comput. Sci. 39, 297–308 (1985)
9. Jussila, T., Biere, A., Sinz, C., Kroning, D., Wintersteiger, C.M.: A First Step Towards a Unified Proof Checker for QBF. In: Marques-Silva, J., Sakallah, K.A. (eds.) SAT 2007. LNCS, vol. 4501, pp. 201–214. Springer, Heidelberg (2007)
10. Kleine Büning, H., Karpinski, M., Flögel, A.: Resolution for quantified Boolean formulas. Inf. Comput. 117(1), 12–18 (1995)
11. Krajíček, J.: Bounded Arithmetic, Propositional Logic, and Complexity Theory. Encyclopedia of Mathematics and its Application, vol. 60. Cambridge University Press (1995)
12. Plaisted, D.A., Greenbaum, S.: A structure-preserving clause form translation. J. Symb. Comput. 2(3), 293–304 (1986)
13. Tseitin, G.S.: On the Complexity of Derivation in Propositional Calculus. In: Slisenko, A.O. (ed.) Studies in Constructive Mathematics and Mathematical Logic, Part II. Seminars in Mathematics, vol. 8, pp. 234–259. Steklov Mathematical Institute, Leningrad (1968)