Towards Uniform Certification in QBF

Leroy Chew
TU Wien, Austria

Friedrich Slivovsky
TU Wien, Austria

Abstract
We pioneer a new technique that allows us to prove a multitude of previously open simulations in QBF proof complexity. In particular, we show that extended QBF Frege p-simulates clausal proof systems such as IR-Calculus, IRM-Calculus, Long-Distance Q-Resolution, and Merge Resolution. These results are obtained by taking a technique of Beyersdorff et al. (JACM 2020) that turns strategy extraction into simulation and combining it with new local strategy extraction arguments.

This approach leads to simulations that are carried out mainly in propositional logic, with minimal use of the QBF rules. Our proofs therefore provide a new, largely propositional interpretation of the simulated systems. We argue that these results strengthen the case for uniform certification in QBF solving, since many QBF proof systems now fall into place underneath extended QBF Frege.

2012 ACM Subject Classification Theory of computation → Proof complexity

Keywords and phrases QBF, Proof Complexity, Verification, Frege, Extended Frege, Strategy Extraction

1 Introduction
The problem of evaluating Quantified Boolean Formulas (QBF), an extension of propositional satisfiability (SAT), is a canonical PSPACE-complete problem [36, 1]. Many tasks in verification, synthesis and reasoning have succinct QBF encodings [35], making QBF a natural target logic for automated reasoning. As such, QBF has seen considerable interest from the SAT community, leading to the development of a variety of QBF solvers (e.g., [29, 19, 32, 20, 30]).

The underlying algorithms are often highly nontrivial, and their implementation can lead to subtle bugs [9]. While formal verification of solvers is typically impractical, trust in a solver’s output can be established by having it generate a proof trace that can be externally validated. This is already standard in SAT solving with the DRAT proof system [39], for which even formally verified checkers are available [15]. A key requirement for standard proof formats like DRAT is that they simulate all current and emerging proof techniques.

Currently, there is no decided-upon checking format for QBF proofs (although there have been some suggestions [22, 18]). The main challenge of finding such an universal format, is that QBF solvers are so radically different in their proof techniques, that each solver basically works in its own proof system. For instance, solvers based on CDCL and (some) clausal abstraction solvers can generate proofs in Q-resolution (Q-Res) [25] or long-distance Q-resolution (LD-Q-Res) [2], while the proof system underlying expansion based solvers combines instantiation of universally quantified variables with resolution (∀Exp+Res) [21]. Variants of the latter system have been considered: IR-calc (Instantiation Resolution) admits instantiation with partial assignments, and IRM-calc (Instantiation Resolution Merge) additionally incorporates elements of long-distance Q-resolution [7].
A universal checking format for QBF ought to simulate all of these systems. A good candidate for such a proof system has been identified in extended QBF Frege (eFrege + ∀red): Beyersdorff et al. showed [6] that a lower bound for eFrege + ∀red would not be possible without a major breakthrough.

In this work, we show that eFrege + ∀red does indeed p-simulate IR-calc, IRM-calc, Merge Resolution (M-Res) and LQU+-Res (a generalisation of LD-Q-Res), thereby establishing eFrege + ∀red and any stronger system (e.g., QRAT [18] or G [28]) as potential universal checking formats in QBF. As corollaries, we obtain (known) simulations of ∀Exp+Res [23] and LD-Q-Res [24] by QRAT, as well as a (new) simulation of IR-calc by QRAT, answering a question recently posed by Chede and Shukla [10]. A simulation structure with many of the known QBF proof systems and our new results is given in Figure 1.

![Hasse diagram for polynomial simulation order of QBF calculi](image)

**Figure 1** Hasse diagram for polynomial simulation order of QBF calculi [7, 3, 6, 18, 12, 2, 38, 13, 5]. In this diagram all proof systems below the first line are known to have strategy extraction, and all below the second line have an exponential lower bound. G and QRAT have strategy extraction if and only if P = PSPACE.

Our proofs crucially rely on a property of QBF proof systems known as strategy extraction. Here, “strategy” refers to winning strategies of a set of PSPACE two-player games (see Section 2 for more details) each of which corresponds exactly to some QBF. A proof system is said to have strategy extraction if a strategy for the two-player game associated with a QBF can be computed from a proof of the formula in polynomial time. Balabanov and Jiang discovered [2] that Q-Resolution admitted a form of strategy extraction where a circuit computing a winning strategy could be extracted in linear time from the proofs. Strategy extraction was subsequently proven for many QBF proof systems (cf. Figure 1): the expansion based systems ∀Exp+Res [7], IR-calc [7] and IRM-calc [7], Long-Distance Q-Resolution [16], including with dependency schemes [16], Merge Resolution [5], Relaxing Stratex [11] and C-Frege + ∀red systems including eFrege + ∀red [6]. Strategy extraction also gained notoriety because it became a method to show Q-resolution lower bounds [7]. Beyersdorff et al. [6, 8] generalised this approach to more powerful proof systems, allowing them to establish a tight correspondence between lower bounds for eFrege + ∀red and two major open problems in circuit complexity and propositional proof complexity: they showed that proving a lower bound for eFrege + ∀red is equivalent to either proving a lower bound for P/poly or a lower bound for propositional eFrege. Chew conjectured [12] that this meant...
that all the aforementioned proof systems that had strategy extraction were very likely to
be simulated by $\text{eFrege} + \forall \text{red}$ and showed an outline of how to use strategy extraction to
obtain the corresponding simulations.

We follow this outline in proving simulations for multiple systems by $\text{eFrege} + \forall \text{red}$. While
the strategy extraction for expansion based systems [7] has been known for a while using
the technique from Goultiaeva et. al [17], there currently is no intuitive way to formalise
this strategy extraction into a simulation proof. Here we specifically studied a new strategy
extraction technique given by Schlaipfer et al. [34], that creates local strategies for each
$\forall \text{Exp+Res}$ line. Inductively, we can affirm each of these local strategies and prove the full
strategy extraction this way. This local strategy extraction technique is based on arguments
of Suda and Gleiss [37], which allow it to be generalised to the expansion based system
$\text{IRM-calc}$. We thus manage to prove a simulation for $\forall \text{Exp+Res}$ and generalise it to $\text{IR-calc}$
and then to $\text{IRM-calc}$. We also show a much more straight-forward simulation of $\text{M-Res}$ and
an adaptation of the $\text{IRM-calc}$ argument to $\text{LQU}^\rightarrow \text{-Res}$.

The remainder of the paper is structured as follows. In Section 2 we go over general
preliminaries and the definition of $\text{eFrege} + \forall \text{red}$. The remaining sections are each dedicated
to simulations of different calculi by $\text{eFrege} + \forall \text{red}$. In Section 3 we begin with a simulation
of $\text{M-Res}$ as a relatively easy example. In Section 4 we show for expansion based systems,
how both an interpretation by in propositional logic and a local strategy is possible and
why that leads to a simulation by $\text{eFrege} + \forall \text{red}$. For $\text{IR-calc}$ we state the essential lemmas of
the proof and for $\text{IRM-calc}$ we detail which modifications are needed. In Section 5 we study
the strongest CDCL proof system $\text{LQU}^\rightarrow \text{-Res}$ and explain why it is also simulated by $\text{eFrege} + \forall \text{red}$, using a similar argument to $\text{IRM-calc}$.

## 2 Preliminaries

### 2.1 Quantified Boolean Formulas

A Quantified Boolean Formula (QBF) is a propositional formula augmented with Boolean
quantifiers $\forall, \exists$ that range over the Boolean values $\bot, \top$ (the same as $0, 1$). Every propositional
formula is already a QBF. Let $\phi$ be a QBF. The semantics of the quantifiers are that:

$$\forall x \phi(x) \equiv \phi(\bot) \land \phi(\top) \quad \text{and} \quad \exists x \phi(x) \equiv \phi(\bot) \lor \phi(\top).$$

When investigating QBF in computer science we want to standardise the input formula. In a prenex QBF, all quantifiers appear outermost in a (quantifier) prefix, and are followed
by a propositional formula, called the matrix. If every propositional variable of the matrix is
bound by some quantifier in the prefix we say the QBF is a closed prenex QBF. We often
want to standardise the propositional matrix, and so we can take the same approach as seen
often in propositional logic. A literal is a propositional variable ($x$) or its negation ($\neg x$ or $\bar{x}$). A clause is a disjunction of literals. Since disjunction is idempotent, associative and
commutative we can think of a clause simultaneously as a set of literals. The empty clause
is just false. A conjunctive normal form (CNF) is a conjunction of clauses. Again, since
conjunction is idempotent, associative and commutative a CNF can be seen as set of clauses.
The empty CNF is true, and a CNF containing an empty clause is false. Every propositional
formula has an equivalent formula in CNF, we therefore restrict our focus to closed $\text{PCNF}$
QBFs, that is closed prenex QBFs with CNF matrices.
2.2 QBF Proof Systems

2.2.1 Proof Complexity

A proof system [14] is a polynomial-time checking function that checks that every proof maps to a valid theorem. Different proof systems have varying strengths, in one system a theorem may require very long proofs, in another the proofs could be considerably shorter. We use proof complexity to analyse the strength of proof systems [26]. A proof system is said to have an $\Omega(f(n))$-lower bound, if there is a family of theorems such that shortest proof (in number of symbols) of the family are bounded below by $\Omega(f(n))$ where $n$ is the size (in number of symbols) of the theorem. Proof system $p$ is said to simulate proof system $q$ if there is a fixed polynomial $P(x)$ such that for every $q$-proof $\pi$ of every theorem $y$ there is a $p$-proof of $y$ no bigger than $P(|\pi|)$ where $|\pi|$ denotes the size of $\pi$. A stricter condition, proof system $p$ is said to $p$-simulate proof system $q$ if there is a polynomial-time algorithm that takes $q$-proofs to $p$-proofs preserving the theorem.

2.2.2 Extended Frege+∀-Red

Frege systems are “text-book” style proof systems for propositional logic. They consist of a finite set of axioms and rules where any variable can be replaced by any formula (so each rule and axiom is actually a schema). A Frege system needs also to be sound and complete. Frege systems are incredibly powerful and can handle simple tautologies with ease. No lower bounds are known for Frege systems and all Frege systems are p-equivalent [14, 33]. For these reasons we can assume all Frege-systems can handle simple tautologies and syllogisms without going into details.

Extended Frege (eFrege) takes a Frege system and allows the introduction of new variables that do not appear in any previous line of the proof. These variables abbreviate formulas. The rule works by introducing the axiom of $v \leftrightarrow f$ for new variable $v$ (not appearing in the formula $f$). Alternatively one can consider eFrege as the system where lines are circuits instead of formulas.

Extended Frege is a very powerful system, it was shown [27, 4] that any propositional proof system $f$ can be simulated by $\text{eFrege} + |\phi||$ where $\phi$ is a polynomially recognisable axiom scheme. The QBF analogue is $\text{eFrege} + \forall\text{red}$, which adds the reduction rule to all existing eFrege rules [6]. $\text{eFrege} + \forall\text{red}$ is refutationally sound and complete for closed prenex QBFs. The reduction rules allows one to substitute a universal variable in a formula with 0 or with 1 as long as no other variable appearing in that formula is right of it in the prefix. Extension variables now must appear in the prefix and must be quantified right of the variables used to define it, we can consider them to be defined immediately right of these variables as there is no disadvantage to this.

2.3 QBF Strategies

With a closed prenex QBF $\Pi\phi$, the semantics of a QBF has an alternative definition in games. The two-player QBF game has an $\exists$-player and a $\forall$-player. The game is played in order of the prefix $\Pi$ left-to-right, whoever’s quantifier appears must assign the quantified variable to $\bot$ or $\top$. The existential player is trying to make the matrix $\phi$ become true. The universal player is trying to make the matrix become false. $\Pi\phi$ is true if and only if there winning strategy for the $\exists$ player. $\Pi\phi$ is false if and only if there winning strategy for the $\forall$ player.
A strategy for a false QBF is a set of functions $f_u$ for each universal variable $u$ on variables left of $u$ in the prefix. In a winning strategy the propositional matrix must evaluate to false when every $u$ is replaced by $f_u$. A QBF proof system has strategy extraction if there is a polynomial time program that takes in a refutation $\pi$ of some QBF $\Psi$ and outputs circuits that represent the functions of a winning strategy.

A policy is similarly defined as a strategy but with partial functions for each universal variables instead of a fully defined function.

### 3 Extended Frege+$\forall$-Red p-simulates M-Res

In this section we show a first example of how the $e\text{Frege}+\forall\text{red}$ simulation argument works in practice for systems that have strategy extraction. Merge resolution provides a straightforward example because the strategies themselves are very suitable to be managed in propositional logic. In later theorems where we simulate calculi like IR-calc and IRM-calc, representing strategies is much more of a challenge.

#### 3.1 Merge Resolution

Merge resolution (M-Res) was first defined by Beyersdorff, Blinkhorn and Mahajan [5]. Its lines combines clausal information with a merge map, for each universal variable. Merge maps give a “local” strategy which when followed forces the clause to be true or the original CNF to be false.

##### 3.1.1 Definition of Merge Resolution

Each line of an M-Res proof consists of a clause on existential variables and partial universal strategy functions for universal variables. These functions are represented by merge maps, which are defined as follows. For universal variable $u$, let $E_u$ be the set of existential variables left of $u$ in the prefix. A non-trivial merge map $M^u_i$ is a collection of nodes in $[i]$, where the construction function $M^u_i(j)$ is either in $\{\bot, \top\}$ for leaf nodes or $E_u \times [j] \times [j]$ for internal nodes. The root $r(u, i)$ is the highest value of all the nodes $M^u_i$. The strategy function $h^{u}_{i,j} : \{0,1\}^{E_u} \rightarrow \{0,1\}$ maps assignments of existential variables $E_u$ in the dependency set of $u$ to a value for $u$. The function $h^{u}_{i,t}$ for leaf nodes $t$ is simply the truth value $M^u_i(t)$. For internal nodes $a$ with $M^u_i(a) = (y, b, c)$, we should interpret $h^{u}_{i,a}$ as “If $y$ then $h^u_{i,b}$, else $h^u_{i,c}$”. In summary the merge map $M^u_i(j)$ is a representation of the strategy given by function $h^{u}_{i,r(u, i)}$.

The merge resolution proof system inevitably has merge maps for the same universal variable interact, and we have two kinds of relations on pairs of merge maps.

- **Definition 1.** Merge maps $M^u_j$ and $M^u_k$ are said to be consistent if $M^u_i(i) = M^u_k(i)$ for each node $i$ appearing in both $M^u_j$ and $M^u_k$.

- **Definition 2.** Merge maps $M^u_j$ and $M^u_k$ are said to be isomorphic if there exists a bijection $f$ from the nodes of $M^u_j$ to the nodes of $M^u_k$ such that if $M^u_j(a) = (y, b, c)$ then $M^u_k(f(a)) = (y, f(b), f(c))$ and if $M^u_j(t) = p \in \{\bot, \top\}$ then $M^u_k(f(t)) = p$.

With two merge maps $M^u_j$ and $M^u_k$, we define two operations as follows:

- **Select**($M^u_j, M^u_k$) returns $M^u_j$ if $M^u_k$ is trivial (representing a “don’t care”), or $M^u_j$ and $M^u_k$ are isomorphic and returns $M^u_k$ if $M^u_j$ is trivial and not isomorphic to $M^u_k$. If neither $M^u_j$ or $M^u_k$ is trivial and the two are not isomorphic then the operation fails.
Towards Uniform Certification in QBF

We now state the main result of this section.

Definition of extension variables.

Proofs in M-Res consist of lines, where every line is a pair \((C_i, \{M^u_i | u \in U\})\).

Axiom: \(C_i = \{l | l \in C, \text{var}(l) \in E\}\) is the existential subset of some clause \(C\) where \(C\) is a clause in the matrix. If universal literals \(u, \bar{u}\) do not appear in \(C\), let \(M^u_i\) be trivial.

If universal variable \(u\) appears in \(C\) then let \(i\) be the sole node of \(M^u_i\) with \(M^u_i(i) = \perp\). Likewise if \(\neg u\) appears in \(C\) then let \(i\) be the sole node of \(M^u_i\) with \(M^u_i(i) = \top\).

Resolution: Two lines \((C_j, \{M^u_j | u \in U\})\) and \((C_k, \{M^u_k | u \in U\})\) can be resolved to obtain a line \((C_i, \{M^u_i | u \in U\})\) if there is literal \(\neg x \in C_j\) and \(x \in C_k\) such that \(C_i = C_j \cup C_k \setminus \{\neg x\}\), and every \(M^u_i\) can either be defined as \(\text{Select}(M^u_j, M^u_k)\), when \(M^u_j\) and \(M^u_k\) are isomorphic or one is trivial, or as \(\text{Merge}(x, M^u_j, M^u_k)\) when \(x < u\) and \(M^u_j\) and \(M^u_k\) are consistent.

### 3.2 Simulation of Merge Resolution

We now state the main result of this section.

#### Theorem 3.

\(\text{eFrege} + \forall \text{red} \) simulates M-Res.

For a false QBF \(\neg \phi\) refuted by M-Res, the final set of merge maps represent a falsifying strategy for the universal player, the strategy can be asserted by a proposition \(S\) that states that all universal variables are equivalent to their strategy circuits. It then should be the case that if \(\phi\) is true, \(S\) must be false, a fact that can be proved propositionally, formally \(\phi \vdash \neg S\).

To build up to this proof we can inductively find a local strategy \(S_i\) for each clause \(C_i\) that appears in an M-Res line \((C_i, \{M^u_i(x)\})\) such that \(\phi \vdash S_i \rightarrow C_i\). Elegantly, \(S_i\) really just a circuit expressing that each \(u \in U\) takes its value in \(M^u_i\) (if non-trivial). Extension variables are used to represent these local strategy circuits and so the proof ends up as a propositional extended Frege proof.

The final part of the proof is the technique suggested by Chew [12] which was originally used by Beyersdorff et al. [6]. That is, to use universal reduction starting from the negation of a universal strategy and arrive at the empty clause.

**Proof.**

Definition of extension variables. We create new extension variables for each node in every non-trivial merge map appearing in a proof. \(s^u_{i,j}\) is created for the node \(j\) in merge map \(M^u_i\). \(s^u_{t,o}\) is defined as a constant when \(t\) is leaf node in \(M^u_i\). Otherwise \(s^u_{i,a}\) is defined as \(s^u_{i,a} := (y \land s^u_{i,b}) \lor (\neg y \land s^u_{i,c})\), when \(M^u_i(j) = (y, b, c)\). Because \(y\) has to be before \(u\) in the prefix, \(s^u_{i,j}\) is always defined before universal variable \(u\).

**Induction Hypothesis.** It is easy for \(\text{eFrege}\) to prove \(\bigwedge_{u \in U_i}(u \leftrightarrow s^u_{i,r(u,i)} \rightarrow C_i)\), where \(r(u, i)\) is the index of the root node of Merge map \(M^u_i\). \(U_i\) is the subset of \(U\) for which \(M^u_i\) is non-trivial.
Base Case: Axiom. Suppose \( C_i \) is derived by axiom download of clause \( C \). If \( u \) has a strategy, it is because it appears in a clause and so \( u \leftrightarrow s_{i,u}^u \), where \( s_{i,u}^u \leftrightarrow c_u \) for \( c_u \in \top, \bot \), \( c_u \) is correctly chosen to oppose the literal in \( C \) so that \( C_i \) is just the simplified clause of \( C \) replacing all universal \( u \) with their \( c_u \). This is easy for \texttt{eFerge} to prove.

Inductive Step: Resolution. If \( C_j \) is resolved with \( C_k \) to get \( C_i \) with pivots \( \neg x \in C_j \) and \( x \in C_k \), we first show \( \bigwedge_{u \in U_i} (u \leftrightarrow s_{i,r(u,i)}^u) \rightarrow C_j \) and \( \bigwedge_{u \in U_i} (u \leftrightarrow s_{i,r(u,i)}^u) \rightarrow C_k \), where \( r(u,i) \) is the root index of the Merge map for \( u \) on line \( i \). We resolve these together.

To argue that \( \bigwedge_{u \in U_i} (u \leftrightarrow s_{i,r(u,i)}^u) \rightarrow C_j \) we prove by induction that we can replace \( u \leftrightarrow s_{i,r(u,i)}^u \) with \( u \leftrightarrow s_{i,r(u,i)}^u \) one by one.

Induction Hypothesis. \( U_i \) is partitioned into \( W \) the set of adjusted variables and \( V \) the set of variables yet to be adjusted.

\[
\left( \bigwedge_{u \in W \cap U_i} (v \leftrightarrow s_{j,r(u,j)}^v) \right) \land \left( \bigwedge_{u \in W \cap U_j} (v \leftrightarrow s_{j,r(u,j)}^v) \right) \rightarrow C_j
\]

Base Case. \( \left( \bigwedge_{v \in W \cap U_i} (v \leftrightarrow s_{j,r(u,j)}^v) \right) \rightarrow C_j \)

Inductive Step. Starting with \( \left( \bigwedge_{v \in W \cap U_i} (v \leftrightarrow s_{j,r(u,j)}^v) \right) \land \left( \bigwedge_{v \in W \cap U_j} (v \leftrightarrow s_{j,r(u,j)}^v) \right) \rightarrow C_j \) We pick \( u \in V \) to show \( (u \leftrightarrow s_{i,r(u,i)}^u) \land (\bigwedge_{v \in W \cap U_i} (v \leftrightarrow s_{j,r(u,j)}^v)) \land (\bigwedge_{v \in W \cap U_j} (v \leftrightarrow s_{j,r(u,j)}^v)) \rightarrow C_j \) We have four cases:

1. Select chooses \( M_i^u = M_j^u \)
2. Select chooses \( M_i^u = M_k^u \) because \( M_i^u \) is trivial
3. Select chooses \( M_i^u = M_k^u \) because there is an isomorphism \( f \) that maps \( M_j^u \) to \( M_k^u \).
4. Merge so that \( M_i^u \) is the merge of \( M_j^u \) and \( M_k^u \) over pivot \( x \)

In (1) we prove inductively from the leaves to the root that \( s_{i,r(u,i)}^u \leftrightarrow s_{j,r(u,j)}^u \). Eventually, we end up with \( s_{r(u,i)}^u \leftrightarrow s_{r(u,j)}^u \). Then \( (u \leftrightarrow s_{i,r(u,i)}^u) \) can be replaced by \( (u \leftrightarrow s_{i,r(u,i)}^u) \).

In (2) we are simply weakening the implication as \( (u \leftrightarrow s_{i,r(u,i)}^u) \) never appeared before.

In (3) we prove inductively from the leaves to the root that \( s_{i,f(t)}^u = s_{k,f(t)}^u = s_{j,x}^u \). Eventually, we end up with \( s_{i,f(t)}^u = s_{k,f(t)}^u = s_{j,x}^u \). Then \( (u \leftrightarrow s_{i,r(u,i)}^u) \) can be replaced by \( (u \leftrightarrow s_{i,f(t)}^u) \). As \( f \) is an isomorphism \( f(r(u,j)) = r(u,k) \) and because \( Select \) is used \( r(u,k) = r(u,j) \). Therefore we have \( (u \leftrightarrow s_{i,r(u,i)}^u) \).

In (4) we prove inductively that for each node \( t \) in \( M_j^u \) we have \( (s_{i,t}^u \leftrightarrow s_{j,t}^u) \). This is true in all leaf nodes as \( s_{i,t}^u \) and \( s_{j,t}^u \) have the same constant value. For intermediate nodes \( a, b \), \( s_{i,a}^u := (y \land s_{i,b}^u) \lor (\neg y \land s_{j,c}^u) \) where \( b \) and \( c \) are other nodes. Since \( M_i^u \) is consistent with \( M_j^u \) then \( s_{i,a}^u := (y \land s_{i,b}^u) \lor (\neg y \land s_{j,c}^u) \) and since \( s_{i,b}^u \leftrightarrow s_{j,b}^u \) and \( s_{j,c}^u \leftrightarrow s_{j,c}^u \) by induction hypothesis, we have \( s_{i,a}^u \leftrightarrow s_{j,a}^u \). Eventually we have \( s_{i,t}^u \leftrightarrow s_{j,t}^u \). However we need to replace \( s_{i,t}^u \) with \( s_{j,t}^u \), not \( s_{i,t}^u \). For this we use the definition of merging that \( x \rightarrow (s_{i,t}^u \leftrightarrow s_{j,t}^u) \) and so we have \( (s_{i,t}^u \leftrightarrow s_{j,t}^u) \lor \neg x \) but the \( \neg x \) is absorbed by the \( C_j \) in right hand side of the implication.

Finalise Inner Induction. At the end of this inner induction, we have \( \bigwedge_{u \in U_i} (u \leftrightarrow s_{i,r(u,i)}^u) \rightarrow C_j \) and symmetrically \( \bigwedge_{u \in U_i} (u \leftrightarrow s_{i,r(u,i)}^u) \rightarrow C_k \). We can then prove \( \bigwedge_{u \in U_i} (u \leftrightarrow s_{i,r(u,i)}^u) \rightarrow C_j \).

Finalise Outer Induction. Note that we have done three nested inductions on the nodes in a merge maps, on the the universal variables, and then on the lines of an \texttt{M-Res} proof. Nonetheless, this gives a linear size \texttt{eFerge} proof in the number of nodes appearing in the proof. In \texttt{M-Res} the final line will be the empty clause and its merge maps. The induction gives us \( \bigwedge_{u \in U_i} (u \leftrightarrow s_{i,t}^u) \rightarrow \perp \). In other words, if \( U_l = \{y_1, \ldots, y_n\} \), where \( y_i \) appears before \( y_{i+1} \) in the prefix, \( \bigwedge_{i=1}^n (y_i \oplus s_{i,t}^u(y_{i+1})) \).
We derive \((0 \oplus s_{y_i}^{n-k+1}) \lor \lor_{i=1}^{n-k+1} (y_i \oplus s_{y_i}^{n-k+1})\) from reduction of \(\lor_{i=1}^{n-k+1} (y_i \oplus s_{y_i}^{n-k+1})\). We can resolve both with the easily proved tautology \(\lor_{i=1}^{n-k+1} (y_i \oplus s_{y_i}^{n-k+1})\). We continue this until we reach the empty disjunction.

### 4 Extended Frege+∀-Red p-simulates Expansion Based Systems

#### 4.1 Expansion-Based Resolution Systems

The idea of an expansion based QBF proof system is to utilise the semantic identity: 
\[ \forall u \phi(u) = \phi(0) \land \phi(1) \]

to replace universal quantifiers and their variables with propositional formulas. With 
\[ \forall u \exists x \phi(u) = \exists x \phi(0) \land \exists x \phi(1) \]

the variables from \(\exists x \phi(0)\) and from \(\exists x \phi(1)\) are actually different variables. The way to deal with this while maintaining prenex normal form is to introduce annotations that distinguish one variable from another.

**Definition 4.**

1. An extended assignment is a partial mapping from the universal variables to \(\{0, 1, *\}\). We denote an extended assignment by a set or list of individual replacements i.e. \(0/u, */v\) is an extended assignment.
2. An annotated clause is a clause where each literal is annotated by an extended assignment to universal variables.
3. For an extended assignment \(\sigma\) to universal variables we write \([\text{restrict}_{\sigma}(l)]\) to denote an annotated literal where \([\text{restrict}_{\sigma}(l)] = \{c/u \in \sigma \mid \text{lv}(u) < \text{lv}(l)\}\).
4. Two (extended) assignments \(\tau\) and \(\mu\) are called contradictory if there exists a variable \(x \in \text{dom}(\tau) \cap \text{dom}(\mu)\) with \(\tau(x) \neq \mu(x)\).

#### 4.1.1 Definitions

The most simple way to use expansion would be to expand all universal quantifiers and list every annotated clause. The first expansion based system we consider, \(\forall \text{Exp+Res}\), has a mechanism to avoid a this potential exponential explosion in some (but not all) cases. An annotated clause is created and then checked to see if it could be obtained from expansion. This way a refutation can just use an unsatisfiable core rather than all clauses from a fully expanded matrix.

\[
\{[\text{restrict}_{\tau}(l)] \mid l \in C, l \text{ is existential}\} \cup \{\tau(l) \mid l \in C, l \text{ is universal}\} \quad \text{(Axiom)}
\]

\(C\) is a clause from the matrix and \(\tau\) is an assignment to all universal variables.

\[
\begin{align*}
C_1 \cup \{x^\tau\} & \quad C_2 \cup \{\neg x^\tau\} \\
\hline
C_1 \cup C_2 & \quad \text{(Res)}
\end{align*}
\]

**Figure 2** The rules of \(\forall \text{Exp+Res}\) (adapted from [21]).

The drawback of \(\forall \text{Exp+Res}\) is that one might end up repeating almost the same derivations over and over again if they vary only in changes in the annotation which make little difference in that part of the proof. This was used to find a lower bound to \(\forall \text{Exp+Res}\) for a family of formulas easy in system \(Q-\text{Res}\) [21]. To rectify this, IR-calc improved on \(\forall \text{Exp+Res}\) to allow a
delay to the annotations in certain circumstances. Annotated clauses now have annotations with “gaps” where the value of the universal variable is yet to be set. When they are set there is the possibility of choosing both assignments without the need to rederive the annotated clauses with different annotations.

**Definition 5.** Given two partial assignments (or partial annotations) \( \alpha \) and \( \beta \). The completion \( \alpha \circ \beta \), is a new partial assignment, where

\[
\alpha \circ \beta (u) = \begin{cases} 
\alpha (u) & \text{if } u \in \text{dom}(\alpha) \\
\beta (u) & \text{if } u \in \text{dom}(\beta) \setminus \text{dom}(\alpha) \\
\text{unassigned} & \text{otherwise}
\end{cases}
\]

For \( \alpha \) an assignment of the universal variables and \( C \) an annotated clause we define

\[
\text{inst}(\alpha, C) := \bigvee_{l \in C} \text{restrict}(l \circ \alpha).
\]

Annotation \( \alpha \) here gives values to unset annotations where one is not already defined. Because the same \( \alpha \) is used throughout the clause, the previously unset values gain consistent annotations, but mixed annotations can occur due to already existing annotations.

\[
\{ \text{restrict}(l) \mid l \in C, l \text{ is existential} \} \quad \text{(Axiom)}
\]

\( C \) is a non-tautological clause from the matrix. \( \tau = \{0/u \mid u \text{ is universal in } C\} \), where the notation \( 0/u \) for literals \( u \) is shorthand for \( 0/x \) if \( u = x \) and \( 1/x \) if \( u = \neg x \).

\[
\frac{x^\tau \lor C_1}{C_1 \cup C_2} \quad \text{(Resolution)}
\]

\[
\frac{\neg x^\tau \lor C_2}{C} \quad \text{(Instatiation)}
\]

\( \tau \) is an assignment to universal variables with \( \text{rng}(\tau) \subseteq \{0, 1\} \).

**Figure 3** The rules of IR-calc [7].

The definition of IR-calc is given in Figure 3. Resolved variables have to match exactly, including that missing values are missing in both pivots. However, non-contradictory but different annotations may still be used for a later resolution step after the instantiation rule is used to make the annotations match the annotations of the pivot.

### 4.1.2 Local Strategies and Policies

The work from Schlaipfer et al. [34] creates a conversion of each annotated clause \( C \) into a propositional formula \( \text{con}(C) \) defined in the original variables of \( \phi \) (so without creating new annotated variables). \( C \) appearing in a proof asserts that there is some (not necessarily winning) strategy for the universal player to force \( \text{con}(C) \) to be true under \( \phi \). The idea is that for each line \( C \) in an \( \forall \text{Exp}+\text{Res} \) refutation of \( \Pi \phi \) there is some local strategy \( S \) such that \( S \land \phi \rightarrow \text{con}(C) \).

The construction of the strategy is formed from the structure of the proof and follows the semantic ideas of Suda and Gleiss [37], in particular the **Combine** operation for resolution. The extra work by Schlaipfer et al. is that the strategy circuits (for each \( u \)) can be constructed in polynomial time, and can be defined in variables left of \( u \) in the prefix.

Let \( u_1 \ldots u_n \) be all universal variables in order. For each line in an \( \forall \text{Exp}+\text{Res} \) proof we have a strategy which we will here call \( S \). For each \( u_i \) there is an extension variable \( \text{Val}_S \), before \( u_i \), that represents the value assigned to \( u_i \) by \( S \) (under an assignment of existential
variables). Using these variables, we obtain a propositional formula representing the strategy as $S = \bigwedge_{i=1}^{n} u_i \leftrightarrow \text{Val}_S^{i}$. Additionally, we define a conversion of annotated logic in $\forall \text{Exp} + \text{Res}$ to propositional logic as follows. For annotations $\tau$ let $\text{anno}(\tau) = \bigwedge_{1/u_i \in \tau} u_i \wedge \bigwedge_{0/u_i \in \tau} \bar{u}_i$. We convert annotated literals as $\text{con}(l^\tau) = l \wedge \text{anno}(\tau)$ and clauses as $\text{con}(C) = \bigvee_{l \in C} \text{con}(l)$.

### 4.2 Simulating IR-calc

The conversion needs to be revised for IR-calc. In particular the variables not set in the annotations need to be understood. The solution is to basically treat unset as a third value, although in practice this requires new $\text{Set}^{i}$ variables (left of $u_i$) which state that the ith universal variable is set by policy $S$. We include these variables in our encoding of policy $S$ and let $S = \bigwedge_{i=1}^{n} \text{Set}^{i}_S \rightarrow (u_i \leftrightarrow \text{Val}^{i}_S)$. The conversion of annotations, literals and clauses also has to be changed. For annotations $\tau$ let

$$\text{anno}_{x,S}(\tau) = \bigwedge_{1/u_i \in \tau} (\text{Set}^{i}_S \wedge u_i) \wedge \bigwedge_{0/u_i \in \tau} (\text{Set}^{i}_S \wedge \bar{u}_i) \wedge \bigwedge_{u_i \notin \text{dom}(\tau)} \neg \text{Set}^{i}_S.$$

Let $\text{con}_{S}(l^\tau) = l \wedge \text{anno}_{x,S}(\tau)$ and $\text{con}_{S}(C) = \bigvee_{l \in C} \text{con}_{S}(l)$ similarly to before, we just reference a particular policy $S$. This means that we again want $S \wedge \phi \rightarrow \text{con}_{S}(C)$ for each line, note that $\text{Set}^{i}$ variables are defined in their own way.

The most crucial part of simulating IR-calc is that after each application of the resolution rule we can obtain a working policy.

**Lemma 6.** Suppose, there are policies $L$ and $R$ such that $L \rightarrow \text{con}_{L}(C_1 \lor \neg x^\tau)$ and $R \rightarrow \text{con}_{R}(C_1 \lor x^\tau)$ then there is a policy $B$ such that $B \rightarrow \text{con}_{B}(C_1 \lor C_2)$ can be obtained in a short eFregé proof.

The proof of the simulation of IR-calc relies on Lemma 6. To prove this we have to first give the precise definitions of the policy $B$ based on policies $L$ and $R$. Schlaipfer et al.’s work [34] is used to crucially make sure the strategy $B$, respects the prefix ordering.

#### 4.2.1 Building the Strategy

We start to define $\text{Val}^{i}_B$ and $\text{Set}^{i}_B$ on lower $i$ values first. In particular we will always start with $1 \leq i \leq m$ where $u_m$ is the rightmost universal variable still before $x$ in the prefix. Starting from $i=0$, the initial segments of $\text{con}_{x,L}(\tau)$ and $\text{con}_{x,R}(\tau)$ may eventually reach such a point $j$ where one is contradicted. Before this point $L$ and $R$ are detailing the same strategy (they may differ on $\text{Val}^{i}$ but only when $\text{Set}^{i}$ is false) so $B$ can be played as both simultaneously as $L$ and $R$. Without loss of generality, as soon as $L$ contradicts $\text{anno}_{x,L}(\tau)$, we know that $\text{con}_{L}(x^\tau)$ is not satisfied by $L$ and thus it makes sense for $B$ to copy $L$, at this point and the rest of the strategy as it will satisfy $\text{con}_{B}(C_1)$. It is entirely possible that we reach $i=m$ and not contradict either $\text{con}_{x,L}(\tau)$ or $\text{con}_{x,R}(\tau)$. Fortunately after this point in the game we now know the value the existential player has chosen for $x$. We can use the $x$ value to decide whether to play $B$ as $L$ (if $x$ is true) or $R$ (if $x$ is false).

To build the circuitry for $\text{Val}^{i}_B$ and $\text{Set}^{i}_B$ we will introduce other circuits that will act as intermediate. First we will use constants $\text{Set}^{i}_B$ and $\text{Val}^{i}_B$ that make $\text{anno}_{x,S}(\tau)$ equivalent to $\bigwedge_{u_i \in \text{ws}} (\text{Set}^{i}_B \leftrightarrow \text{Set}^{i}_S) \wedge \text{Set}^{i}_B \rightarrow (u_i \leftrightarrow \text{Val}^{i}_B)$. This mainly makes our notation easier. Next we will define circuits that represent two strategies being equivalent up to the ith universal variable. This is a generalisation of what was seen in the local strategy extraction for $\forall \text{Exp} + \text{Res}$ [34].

$$\text{Eq}^{0}_{f=g} := 1, \text{Eq}^{i+1}_{f=g} := \text{Eq}^{i+1}_{f=g} \land ((\text{Set}^{i}_f \leftrightarrow \text{Set}^{i}_g) \land (\text{Set}^{i}_f \rightarrow (\text{Val}^{i}_f \leftrightarrow \text{Val}^{i}_g))).$$
We specifically use this for a trigger variable that tells you which one of $L$ and $R$ differed from $\tau$ first.

$$\text{Dif}_L^0 := 0 \quad \text{and} \quad \text{Dif}_R^0 := \text{Dif}_L^{i-1} \lor (\text{Eq}_{R=\tau} \lor (\text{Set}_L^i \lor \text{Val}_L^i))$$

$$\text{Dif}_R^0 := 0 \quad \text{and} \quad \text{Dif}_R^i := \text{Dif}_R^{i-1} \lor (\text{Set}_R^i \lor (\text{Val}_R^i \lor \text{Val}_L^i))$$

Note that $\text{Dif}_L^i$ and $\text{Dif}_R^i$ can both be true but only if they start to differ at the same point.

Suda and Gleiss’s Combine operation allows one to construct a bottom policy $B$ that chooses between the left and right policies.

**Definition 7** (Definition of resolvent policy for IR-calc). For $0 \leq i \leq m$, define $\text{Val}_B^i$ and $\text{Set}_B^i$ such $\text{Val}_B^i$ and $\text{Set}_B^i$ if

$$\neg \text{Dif}_L^i \land (\text{Dif}_R^i \lor (\neg \text{Set}_L^i \land \text{Set}_R^i) \lor (\text{Set}_L^i \land \text{Set}_R^i \land (\text{Val}_L^i \lor \text{Val}_R^i)))$$

and $\text{Val}_B^i$ and $\text{Set}_B^i$ are defined otherwise.

For $i > m$, define $\text{Val}_B^i$ and $\text{Set}_B^i$ such $\text{Val}_B^i$ and $\text{Set}_B^i$ if

$$\neg \text{Dif}_L^m \land (\text{Dif}_R^m \lor x)$$

and $\text{Val}_B^i$ and $\text{Set}_B^i$ are defined otherwise.

We will now define variables $B_L$ and $B_R$. These say that $B$ is choosing $L$ or $R$, respectively. These variables can appear rightmost in the prefix, as they will be removed before reduction takes place. The purpose of $B_L$ (resp. $B_R$) is that $\text{con}_B$ becomes the same as $\text{con}_L$ (resp. $\text{con}_R$).

- $B_L := \bigwedge_{i=1}^m (\text{Set}_B^i \leftrightarrow \text{Set}_L^i) \land (\text{Set}_B^i \rightarrow (\text{Val}_B^i \leftrightarrow \text{Val}_L^i))$
- $B_R := \bigwedge_{i=1}^m (\text{Set}_B^i \leftrightarrow \text{Set}_R^i) \land (\text{Set}_B^i \rightarrow (\text{Val}_B^i \leftrightarrow \text{Val}_R^i))$

We have not fully defined $B$ here. The important points are that $B$ is set up so that it either takes values in $L$ or $R$, i.e. $B \rightarrow B_L \lor B_R$, specifically we need that whenever the propositional formula $\text{anno}_{x,B}(\tau)$ is satisfied, $B = B_L$ when $x$, and $B = B_R$ when $\neg x$. The variables $\text{Set}_B^i$ and $\text{Val}_B^i$ that comprise the policy are carefully constructed to come before $u_i$. A number of technical lemmas involving all these definitions is necessary for the simulation.

**Lemma 8.** For $0 < j < m$ the following propositions have short derivations in Extended Frege:

- $\text{Dif}_L^j \rightarrow \bigvee_{i=1}^j \text{Dif}_L^i \land \neg \text{Dif}_L^{j-1}$
- $\text{Dif}_R^j \rightarrow \bigvee_{i=1}^j \text{Dif}_R^i \land \neg \text{Dif}_R^{j-1}$
- $\neg \text{Eq}_{f=g} \rightarrow \bigvee_{i=1}^j \neg \text{Eq}_{f=g} \land \neg \text{Eq}_{f=g}$. For $f, g \in \{L, R, \tau\}$.

**Lemma 9.** For $0 \leq i \leq j \leq m$ the following propositions that describe the monotonicity of $\text{Dif}$ have short derivations in Extended Frege:

- $\text{Dif}_L^i \rightarrow \text{Dif}_L^j$
- $\text{Dif}_R^i \rightarrow \text{Dif}_R^j$
- $\neg \text{Eq}_{f=g} \rightarrow \neg \text{Eq}_{f=g}$

**Lemma 10.** For $0 \leq i \leq j \leq m$ the following propositions describe the relationships between the different extension variables and have short derivations in Extended Frege:

- $\text{Eq}_{L=\tau} \rightarrow \neg \text{Dif}_L$
- $\text{Dif}_L \land \neg \text{Dif}_L^{j-1} \rightarrow \text{Eq}_{L=\tau}^{i-1}$
- $\text{Dif}_L \land \neg \text{Dif}_L^{j-1} \rightarrow \neg \text{Dif}_R^{i-1}$
Towards Uniform Certification in QBF

- \text{Eq}_{R=L}^i \rightarrow \neg \text{Diff}_{L}^i_R
- \text{Diff}_{R}^i \land \neg \text{Diff}_{L}^{i-1} \rightarrow \text{Eq}_{L=R}^{i-1}
- \text{Diff}_{R}^i \land \neg \text{Diff}_{L}^{i-1} \rightarrow \neg \text{Diff}_{L}^{i-1}

\begin{itemize}
  \item \textbf{Lemma 11.} For any \( 0 \leq i \leq m \) the following propositions are true and have short Extended Frege proofs.
  \begin{itemize}
    \item \( L \land \text{Diff}_{L}^i \rightarrow \neg \text{anno}_{x,L}(\tau) \)
    \item \( R \land \text{Diff}_{R}^i \rightarrow \neg \text{anno}_{x,R}(\tau) \)
  \end{itemize}

  \item \textbf{Lemma 12.} For any \( 1 \leq j \leq m \) the following propositions are true and have a short Extended Frege proof.
  \begin{itemize}
    \item \( \neg \text{Diff}_{L}^j \land \neg \text{Diff}_{R}^j \rightarrow \text{Eq}_{L}^j \)
    \item \( \neg \text{Diff}_{L}^i \land \neg \text{Diff}_{R}^j \rightarrow \text{Eq}_{R}^i \)
    \item \( \neg \text{Diff}_{L}^j \land \neg \text{Diff}_{R}^j \rightarrow (\text{Set}_{R}^{j} \leftrightarrow \text{Set}_{L}^{j}) \)
    \item \( \neg \text{Diff}_{L}^j \land \neg \text{Diff}_{R}^j \rightarrow (\text{Val}_{B}^{j} \leftrightarrow \text{Val}_{R}^{j}) \)
    \item \( \neg \text{Diff}_{L}^j \land \neg \text{Diff}_{R}^j \rightarrow (\text{Set}_{B}^{j} \leftrightarrow \text{Set}_{R}^{j}) \)
    \item \( \neg \text{Diff}_{L}^j \land \neg \text{Diff}_{R}^j \rightarrow (\text{Val}_{B}^{j} \leftrightarrow \text{Val}_{R}^{j}) \)
  \end{itemize}

  \item \textbf{Lemma 13.} For any \( 0 \leq i \leq m \) the following propositions are true and have short Extended Frege proofs.
  \begin{itemize}
    \item \( \text{Diff}_{L}^i \rightarrow (\text{Val}_{B}^{i} \leftrightarrow \text{Val}_{L}^{i}) \land (\text{Set}_{B}^{i} \leftrightarrow \text{Set}_{L}^{i}) \)
    \item \( \neg \text{Diff}_{L}^i \land \text{Diff}_{R}^i \rightarrow (\text{Val}_{B}^{i} \leftrightarrow \text{Val}_{R}^{i}) \land (\text{Set}_{B}^{i} \leftrightarrow \text{Set}_{R}^{i}) \)
  \end{itemize}

  \item \textbf{Lemma 14.} The following propositions are true and have short Extended Frege proofs.
  \begin{itemize}
    \item \( B \land \text{Diff}_{L}^0 \rightarrow B_L \)
    \item \( B \land \neg \text{Diff}_{L}^0 \land \text{Diff}_{R}^m \rightarrow B_R \)
  \end{itemize}

  \item \textbf{Lemma 15.} The following propositions are true and have short Extended Frege proofs.
  \begin{itemize}
    \item \( B \land \neg \text{Diff}_{L}^m \land \neg \text{Diff}_{R}^m \rightarrow B_L \lor \neg x \)
    \item \( B \land \neg \text{Diff}_{L}^m \land \neg \text{Diff}_{R}^m \rightarrow B_R \lor x \)
  \end{itemize}

  \item \textbf{Lemma 16.} The following proposition is true and has a short Extended Frege proof.
  \( B \rightarrow B_L \lor B_R \)

  \textbf{Proof.} This roughly says that \( B \) either is played entirely as \( L \) or is played as \( R \). We can prove this by combining Lemmas 14 and 15, it essentially is a case analysis in formal form. \( \blacksquare \)

  \item \textbf{Lemma 17.} The following propositions are true and have short Extended Frege proofs.
  \begin{itemize}
    \item \( B \land \text{anno}(\tau) \land x \rightarrow B_L \)
    \item \( B \land \text{anno}(\tau) \land \neg x \rightarrow B_R \)
  \end{itemize}

  \textbf{Proof.} We start with \( B \land \neg \text{Diff}_{L}^m \land \neg \text{Diff}_{R}^m \rightarrow B_L \lor \neg x \) and \( B \land \neg \text{Diff}_{L}^m \land \neg \text{Diff}_{R}^m \rightarrow B_R \lor x \). It remains to remove \( \neg \text{Diff}_{L}^m \land \neg \text{Diff}_{R}^m \) from the left hand side. This is where we use \( L \land \text{Diff}_{L}^j \rightarrow \neg \text{anno}_{L}(\tau) \) and \( R \land \text{Diff}_{R}^j \rightarrow \neg \text{anno}_{R}(\tau) \) from Lemma 11. These can be simplified to \( B \land B_L \land \text{Diff}_{L}^j \rightarrow \neg \text{anno}_{B}(\tau) \) and \( B \land B_R \land \text{Diff}_{R}^j \rightarrow \neg \text{anno}_{R}(\tau) \). The \( B_L \) and \( B_R \) can be removed by using \( B \land \text{Diff}_{L}^j \rightarrow B_L \) and \( B \land \neg \text{Diff}_{L}^m \land \text{Diff}_{R}^m \rightarrow B_R \) and we can end up with \( B \rightarrow \neg \text{anno}_{B}(\tau) \lor (\neg \text{Diff}_{L}^m \land \neg \text{Diff}_{R}^m) \) we can use this to resolve out \( (\neg \text{Diff}_{L}^m \land \neg \text{Diff}_{R}^m) \) and get \( B \land \text{anno}(\tau) \land x \rightarrow B_L \) and \( B \land \text{anno}(\tau) \land \neg x \rightarrow B_R \). \( \blacksquare \)

  \textbf{Proof of Lemma 6.} Since \( B \land B_L \rightarrow L \) and \( B \land B_R \rightarrow R \), \( L \rightarrow \text{conv}(C_1 \lor \neg x) \) and \( R \rightarrow \text{conv}(C_2 \lor x) \) imply \( B \land B_L \rightarrow \text{conv}(C_1 \lor C_2) \lor \text{anno}_{B}(\tau) \), \( B \land B_R \rightarrow \text{conv}(C_1 \lor C_2) \lor \text{anno}_{r,B}(\tau) \), \( B \land B_L \rightarrow \text{conv}(C_1 \lor C_2) \lor \neg x \) and \( B \land B_R \rightarrow \text{conv}(C_1 \lor C_2) \lor x \).
We combine $B \rightarrow B_L \lor B_R$ with $B \land B_L \rightarrow \text{con}_B(C_1 \lor C_2) \lor \text{anno}_x.B(\tau)$ (removing $B_L$) and $B \land B_R \rightarrow \text{con}_B(C_1 \lor C_2) \lor \text{anno}_x.B(\tau)$ (removing $B_R$) to gain $B \rightarrow \text{con}_B(C_1 \lor C_2) \lor \text{anno}_x.B(\tau)$. Next, we derive $B \rightarrow \text{con}_B(C_1 \lor C_2) \lor \neg \text{anno}_x.B(\tau)$. Policy $B$ is set up so that $B \land \text{anno}_x.B(\tau) \land x \rightarrow B_L$ and $B \land \text{anno}_x.B(\tau) \land \neg x \rightarrow B_R$ have short proofs. We resolve these, respectively, with $B \land \text{anno}_x.B(\tau) \land x \rightarrow B_L$ and $B \land \text{anno}_x.B(\tau) \land \neg x \rightarrow B_R$, to obtain $B \land \text{anno}_x.B(\tau)$ and $B \rightarrow \text{con}_B(C_1 \lor C_2)$, which can be rewritten as $B \rightarrow \text{con}_B(C_1 \lor C_2) \lor \neg \text{anno}_x.B(\tau)$. Putting these together allows us to remove $B_L$ and $B_R$, deriving $B \land \text{anno}_x.B(\tau) \rightarrow \text{con}_B(C_1 \lor C_2)$, which can be rewritten as $B \rightarrow \text{con}_B(C_1 \lor C_2) \lor \neg \text{anno}_x.B(\tau)$, which resolve to get $B \rightarrow \text{con}_B(C_1 \lor C_2)$. ◁

**Theorem 18.** $\text{eFrege} + \forall \text{red}$ $p$-simulates $\text{IR-calc}$.

**Proof.** We prove by induction that every annotated clause $C$ appearing in an IR-calc proof has a local policy $S$ such that $\phi \vdash_{\text{eFrege}} S \rightarrow \text{con}_S(C)$ and this can be done in a polynomial-size proof.

**Axiom.** Suppose $C \in \phi$ and $D = \text{inst}(C, \tau)$ for partial annotation $\tau$. We construct policy $B$ such that $B \rightarrow \text{con}_B(D)$.

$$
\begin{align*}
\text{Set}^j_B = & \begin{cases} 1 & \text{if } u_j \in \text{dom}(\tau) \\ 0 & \text{if } u_j \notin \text{dom}(\tau) \end{cases}, \\
\text{Val}^j_B = & \begin{cases} 1 & \text{if } 1/u_j \in \tau \\ 0 & \text{if } 0/u_j \in \tau \end{cases}
\end{align*}
$$

**Instantiation.** Suppose we have an instantiation step for $C$ on a single universal variable $u_i$ using instantiation $0/u_i$, so the new annotated clause is $D = \text{inst}(C, 0/u_i)$. From the induction hypothesis $T \rightarrow \text{con}_T(C)$ we will develop $B$ such that $B \rightarrow \text{con}_B(D)$.

$$
\begin{align*}
\text{Set}^j_B = & \begin{cases} 1 & \text{if } j = i \\ \text{Set}^j_B & \text{if } j \neq i \end{cases}, \\
\text{Val}^j_B = & \begin{cases} \text{Val}^j_T \land \text{Set}^j_T & \text{if } j = i \\ \text{Val}^j_T & \text{if } j \neq i \end{cases}
\end{align*}
$$

Val$^j_B \land \text{Set}^j_B$ becomes Val$^j_B \lor \neg \text{Set}^j_B$ for instantiation by $1/u_j$. Either case means $B$ satisfies the same annotations anno as $T$ appearing in our converted clauses $\text{con}_B(C)$ and $\text{con}_B(D)$, proving the rule as an inductive step.

**Resolution.** See Lemma 6.

**Contradiction.** At the end of the proof we have $T \rightarrow \text{con}_T(\bot)$. $T$ is a policy, so we turn it into a full strategy $B$ by having for each $i$: Val$_B^i \leftrightarrow (\text{Val}^i_T \land \text{Set}^i_T)$ and $\text{Set}^j_B = 1$. Effectively this instantiates $\bot$ by the assignment that sets everything to 0 and we can argue that $B \rightarrow \text{con}_B(\bot)$ although $\text{con}_B(\bot)$ is just the empty clause. So we have $\neg B$. But $\neg B$ is just $\bigvee_{i=1}^{n-k}(u_i \oplus \text{Val}^i_B)$. Furthermore, just as in Schlipf’s work, we have been careful with the definitions of the extension variables Val$^i_B$ so that they are left of $u_i$ in the prefix. In $\text{eFrege} + \forall \text{red}$ we can use the reduction rule (this is the first time we use the reduction rule). We show an inductive proof of $\bigvee_{i=1}^{n-k}(u_i \oplus \text{Val}^i_B)$ for increasing $k$ eventually leaving us with the empty clause. This essentially is where we use the $\forall$-Red rule. Since we already have $\bigvee_{i=1}^{n-k}(u_i \oplus \text{Val}^i_B)$ we have the base case and we only need to show the inductive step.

We derive from $\bigvee_{i=1}^{n+1-k}(u_i \oplus \text{Val}^i_B)$ both $(0 \oplus \text{Val}^B_{n-k+1}) \lor \bigvee_{i=1}^{n-k}(u_i \oplus \text{Val}^B_B)$ and $(1 \oplus \text{Val}^B_{n-k+1}) \lor \bigvee_{i=1}^{n-k}(u_i \oplus \text{Val}^B_B)$ from reduction. We can resolve both with the easily proved tautology $(0 \leftrightarrow \text{Val}^B_{n-k+1}) \lor (1 \leftrightarrow \text{Val}^B_{n-k+1})$ which allows us to derive $\bigvee_{i=1}^{n-k}(u_i \oplus \text{Val}^B_B)$.

We continue this until we reach the empty disjunction. ◁
Corollary 19. eFrege + ∀red p-simulates ∀Exp + Res.

While this can be proven as a corollary of the simulation of IR-calc, a more direct simulation can be achieved by defining the resolvent strategy by removing the Set\(^i\) variables (i.e. by considering them as always true).

4.3 Simulating IRM-calc

4.3.1 Definition

IRM-calc was designed to compress annotated literals in clauses in order simulate LD-Q-Res. Like that system it uses the \(\ast\) symbol, but since universal literals do not appear in an annotated clause, the \(\ast\) value is added to the annotations, \(0/u, 1/u, \ast/u\) being the first three possibilities in an extended annotation (the fourth being when \(u\) does not appear in the annotation).

Axiom and instantiation rules as in IR-calc in Figure 3.

\[
\begin{align*}
\frac{x^\tau \land \xi \lor C_1}{\text{inst}(\sigma, C_1) \cup \text{inst}(\xi, C_2)} \quad \text{(Resolution)}
\end{align*}
\]

\(\text{dom}(\tau), \text{dom}(\xi) \text{ and } \text{dom}(\sigma)\) are mutually disjoint. \(\text{rng}(\tau) = \{0, 1\}\)

\[
\frac{C \lor b^\mu \lor b^\sigma}{C \lor b^k} \quad \text{(Merging)}
\]

\(\text{dom}(\mu) = \text{dom}(\sigma). \quad \xi = \{c/u \mid c/u \in \mu, c/u \in \sigma\} \cup \{\ast/u \mid c/u \in \mu, d/u \in \sigma, c \neq d\}\)

Figure 4 The rules of IRM-calc.

The rules of IRM-calc as given in Figure 4, become more complicated as a result of the \(\ast/u\). In particular resolution is no longer done between matching pivots but matching is done internally in the resolution steps. This is to prevent variables resolving with matching \(\ast\) annotations. Allowing such resolution steps would be unsound in general, as these \(\ast\) annotations show that the universal variables are set according to some function, but when appearing in two different literals the functions could be completely different. Resolutions where one pivot literal has a \(\ast/u\) annotation means that the other pivot literal must not have \(u\) in its annotation’s domain. The intuition is that the unset \(u\) is given a \(\ast\) value during the resolution but it can be controlled to be exactly the same \(\ast\) as in the other pivot. A \(0/u, 1/u\) or \(\ast/u\) value cannot be given a new \(\ast\) value so cannot match the other \(\ast/u\) annotation.

It is in IRM-calc where the positive Set literals introduced in the simulation of IR-calc become useful. In most ways \(\text{Set}^i_S\) asserts the same things as \(\ast/u_i\), that \(u_i\) is given a value, but this value does not have to be specified.

4.3.2 Conversion, Policies and Simulation

The first major change from IR-calc is that while \(\text{con}_S\) worked on three values in IR-calc, in IRM-calc we effectively run in four values \(\text{Set}^i_S, \neg \text{Set}^i_S, \text{Set}^i_S \land u_i\) and \(\text{Set}^i_S \land \neg u_i\). \(\text{Set}^i_S\) is the new addition deliberately ambiguous as to whether \(u_i\) is true or false. Readers familiar with the \(\ast\) used in IRM-calc may notice why \(\text{Set}^i_S\) works as a conversion of \(\ast/u_i\), as \(\text{Set}^i_S\) is just saying our policy has given a value but it may be different values in different circumstances.
Like in the case of IR-calc, most work needs to be done in the IRM-calc resolution steps, although here it is even more complicated. A resolution step in IRM-calc is in two parts. Firstly $C_1 \lor \neg x^{\tau \upharpoonright \sigma}$, $C_2 \lor x^{\tau \upharpoonright \bar{\sigma}}$ are both instantiated (but by $\ast$ in some cases), secondly they are resolved on a matching pivot. We simplify the resolution steps so that $\sigma$ and $\xi$ only contain $\ast$ annotations, for the other constant annotations that would normally be found in these steps suppose we have already instantiated them in the other side so that they now appear in $\tau$ (this does not affect the resolvent).

Again we assume that there are policies $L$ and $R$ such that $L \rightarrow \text{con}_L(C_1 \lor \neg x^{\tau \upharpoonright \sigma})$ and $R \rightarrow \text{con}_R(C_2 \lor x^{\tau \upharpoonright \bar{\sigma}})$. We know that if $L$ falsifies $\text{anno}_{x,L}(\tau \upharpoonright \sigma)$ then $\text{con}_L(C_1)$ and likewise if $R$ falsifies $\text{anno}_{x,R}(\tau \upharpoonright \xi)$ then $\text{con}_R(C_1)$ is satisfied. These are the safest options, however this leaves cases when $L$ satisfies $\text{anno}_{x,L}(\tau \upharpoonright \sigma)$ and $R$ satisfies $\text{anno}_{x,R}(\tau \upharpoonright \xi)$ but $L$ and $R$ are not equal. This happens either when $\text{Set}_L^1$ and $\neg \text{Set}_R^1$ both occur for $\ast/u_i \in \sigma$ or when $\neg \text{Set}_L^1$ and $\text{Set}_R^1$ both occur for $\ast/u_i \in \xi$.

This would cause issues if $B$ had to choose between $L$ and $R$ to satisfy $\text{con}_B(C_1 \lor C_2)$. Fortunately, we are not trying to satisfy $\text{con}_B(C_1 \lor C_2)$ but $\text{con}_B(\text{inst}(\xi, C_1) \lor \text{inst}(\sigma, C_2))$, so we have to choose between a policy that will satisfy $\text{con}_B(\text{inst}(\xi, C_1))$ and a policy that will satisfy $\text{con}_B(\text{inst}(\sigma, C_2))$. By borrowing values from the opposite policy we obtain a working new policy that does not have to choose between left and right any earlier than we would have for IR-calc.

- **Theorem 20.** eFrege$\forall$red simulates IRM-calc.
- **Corollary 21.** eFrege$\forall$red simulates LD-Q-Res.

## 5 Extended Frege+$\forall$-Red p-simulates LQU$^+$-Res

### 5.1 QCDCL Resolution Systems

The most basic and important CDCL system is $Q$-resolution ($Q$-Res) by Kleine Büning et al. [25]. Long-distance resolution ($LD$-$Q$-Res) appears originally in the work of Zhang and Malik [40] and was formalized into a calculus by Balabanov and Jiang [2]. It merges complementary literals of a universal variable $u$ into the special literal $u^\ast$. These special literals prohibit certain resolution steps. $QU$-resolution ($QU$-Res) [38] removes the restriction from $Q$-Res that the resolved variable must be an existential variable and allows resolution of universal variables. $LQU^+$-Res [3] extends LD-Q-Res by allowing short and long distance resolution pivots to be universal, however, the pivot is never a merged literal $z^\ast$. $LQU^+$-Res encapsulates Q-Res, LD-Q-Res and QU-Res.

### 5.2 Conversion to Propositional Logic and Simulation

LQU$^+$-Res and IRM-calc are mutually incomparable in terms of proof strength, however both share enough similarities to get the simulation working. Once again we can use Set$^1$ variables to represent an $u_i^\ast$, and a $\neg$Set$^1_2$ to represent that policy $S$ chooses not to issue a value to $u_i$.

For any set of universal variables $U$, let $\text{anno}_{x,S}(U) = \bigwedge_{u_i \in U} \neg \text{Set}_S^1 \land \bigwedge_{u_i \in U} \text{Set}_S^1$. Note that we do not really need to add polarities to the annotations, these are taken into account by the clause literals. Literals $u$ and $\bar{u}$ do not need to be assigned by the policy, they are now treated as a consequence of the the CNF. Because they can be resolved we treat them like existential variables in the conversion. For universal variable $u_i$, $\text{con}_{S,C}(u_i) = u_i \land \neg \text{Set}_S^1 \land \text{anno}_{u_i,S}(\{ v | v^\ast \in C \})$ and $\text{con}_{S,C}(\neg u_i) = \neg u_i \land \neg \text{Set}_S^1 \land \text{anno}_{u_i,-S}(\{ v | v^\ast \in C \})$. We reserve Set$^1_2$ for starred literals as they cannot be removed. For existential literal $x,$
Towards Uniform Certification in QBF

\[ \text{con}_{S,C}(x) = x \land \text{anno}_x\{\{u \mid u^* \in C\}\}. \]

Finally, \( \text{con}_{S,C}(u^*) = \bot \), because we do not treat \( u^* \) as a literal but part of the “annotation” to literals right of it. Also, \( u^* \) cannot be resolved but it automatically reduced when no more literals are to the right of it. For clauses in \( \text{LQU}^+\text{-Res} \), we let \( \text{con}_S(C) = \bigvee_{l \in C} \text{con}_{S,C}(l) \). In summary, in comparison to \( \text{IRM-calc} \) the conversion now includes universal variables and gives them annotations, but removes polarities from the annotations. Policies still remain structured as they were for \( \text{IR-calc} \), with extension variables \( \text{Val}_i \) and \( \text{Set}_i \), where \( S = \bigwedge_{i=1}^n \text{Set}_i \rightarrow (u_i \leftrightarrow \text{Val}_i) \).

\[ \textbf{Theorem 22.} \text{eFrege + \forall red simulates \text{LQU}^+\text{-Res}.} \]

6 Conclusion

Our work reconciles many different QBF proof techniques under the single system \texttt{eFrege + \forall red}. Although \texttt{eFrege + \forall red} itself is likely not a good system for efficient proof checking, our results have implications for other systems that are more promising in this regard, such as \texttt{QRAT}, which inherits these simulations. In particular, \texttt{QRAT}’s simulation of \( \forall\text{Exp+Res} \) is upgraded to a simulation of \( \text{IRM-calc} \), and we do not even require the extended universal reduction rule. Existing \texttt{QRAT} checkers can be used to verify converted \texttt{eFrege + \forall red} proofs. Further, extended QU-resolution is polynomially equivalent to \texttt{eFrege + \forall red} [12], and has previously been proposed as a system for unified QBF proof checking [22]. Since our simulations split off propositional inference from a standardised reduction part at the end, another option is to use (highly efficient) propositional proof checkers instead. Our simulations use many extension variables that are known to negatively impact the checking time of existing tools such as \texttt{DRAT-trim}, but one may hope that they can be refined to become more efficient in this regard.

There are other proof systems, particularly ones using dependency schemes, such as \texttt{Q(Drrs)-Res} and \texttt{LD-Q(Drrs)-Res} that have strategy extraction [31]. Local strategy extraction and ultimately a simulation by \texttt{eFrege + \forall red} seem likely for these systems, whether it can be proved directly or by generalising the simulation results from this paper.

References


Towards Uniform Certification in QBF


A Appendix

A.1 Proof of Simulation of IR-calc

**Lemma 8.** For $0 < j \leq m$ the following propositions have short derivations in Extended Frege:

- $\text{Dif}_L^j \rightarrow \lor_{i=1}^j \text{Dif}_L^1 \land \neg \text{Dif}_L^{i-1}$
- $\text{Dif}_R^j \rightarrow \lor_{i=1}^j \text{Dif}_R^1 \land \neg \text{Dif}_R^{i-1}$
- $\neg \text{Eq}^j_{f=g} \rightarrow \lor_{i=1}^j \neg \text{Eq}^1_{f=g} \land \text{Eq}^{i-1}_{f=g}$. For $f, g \in \{L, R, \tau\}$.

**Proof.**

**Induction Hypothesis on** $j$. $\text{Dif}_L^j \rightarrow \lor_{i=1}^j \text{Dif}_L^1 \land \neg \text{Dif}_L^{i-1}$ has an $O(j)$-size proof.

**Base Case** $j = 1$. $\text{Dif}_L^1 \rightarrow \text{Dif}_L^1$ is a basic tautology that Frege can handle, $\text{Dif}_L^0$ is false by definition so Frege can assemble $\text{Dif}_L^1 \rightarrow \text{Dif}_L^1 \land \neg \text{Dif}_L^0$.

**Inductive Step** $j + 1$. $\neg \text{Dif}_L^1 \lor \text{Dif}_L^j$ and $\text{Dif}_L^{j+1} \rightarrow \text{Dif}_L^{j+1}$ are tautologies that Frege can handle. Putting them together we get $\text{Dif}_L^{j+1} \rightarrow \text{Dif}_L^{j+1} \land (\neg \text{Dif}_L^1 \lor \text{Dif}_L^j)$ and weaken to $\text{Dif}_L^{j+1} \rightarrow (\text{Dif}_L^{j+1} \land \neg \text{Dif}_L^1) \lor \text{Dif}_L^j$. Using the induction hypothesis, $\text{Dif}_L^1 \rightarrow \lor_{i=1}^j \text{Dif}_L^1 \land \neg \text{Dif}_L^{i-1}$, we can change this tautology to

$\text{Dif}_L^{j+1} \rightarrow (\lor_{i=1}^j \neg \text{Dif}_L^1) \lor \lor_{i=1}^j \text{Dif}_L^1 \land \neg \text{Dif}_L^{i-1}$

Note that since $\neg \text{Dif}_R^0, \text{Eq}^0_{L=\tau \land L}, \text{Eq}^0_{L=\tau \land R}$ are all true. The proofs for $\text{Dif}_R^1, \neg \text{Eq}^1_{f=g}$ and $\neg \text{Eq}^1_{R=\tau \land L}, \neg \text{Eq}^1_{R=\tau \land R}$ are identical modulo the variable names. ◀
Lemma 9. For $0 \leq i \leq j \leq m$ the following propositions that describe the monotonicity of $\text{Diff}$ have short derivations in Extended Frege:

\begin{itemize}
  \item $\text{Diff}^i_L \rightarrow \text{Diff}^j_L$
  \item $\text{Diff}^i_R \rightarrow \text{Diff}^j_R$
  \item $\neg \text{Eq}^j_{f=g} \rightarrow \neg \text{Eq}^j_{f=g}$
\end{itemize}

Proof. For $\text{Diff}_L$ and $\text{Diff}_R$, Induction Hypothesis on $j$. $\text{Diff}^i_L \rightarrow \text{Diff}^j_L$ has an $O(j)$ proof.

Base Case $j = i$. $\text{Diff}^j_L \rightarrow \text{Diff}^j_L$ is a tautology that Frege can handle.

Inductive Step $j + 1$. $\text{Diff}^{j+1}_L := \text{Diff}^j_L \lor A$ where expression $A$ depends on the domain of $u_{j+1}$. Therefore in all cases $\text{Diff}^j_L \rightarrow \text{Diff}^{j+1}_L$ is a straightforward corollary in Frege. Using the induction hypothesis $\text{Diff}^j_L \rightarrow \text{Diff}^k_L$ we can get $\text{Diff}^i_L \rightarrow \text{Diff}^{j+1}_L$. The proof is symmetric for $R$.

For $\neg \text{Eq}^j_{f=g}$, Induction Hypothesis on $j$. $\neg \text{Eq}^j_{f=g} \rightarrow \neg \text{Eq}^j_{f=g}$ has an $O(j)$ proof.

Base Case $j = i$. $\neg \text{Eq}^i_{f=g} \rightarrow \neg \text{Eq}^j_{f=g}$ is a tautology that Frege can handle.

Inductive Step $j + 1$. $\text{Eq}^{j+1}_f := \text{Eq}^j_{f=g} \land A$ where expression $A$ depends on the domain of $u_{j+1}$. Therefore in all cases $\neg \text{Eq}^j_{f=g} \rightarrow \neg \text{Eq}^{j+1}_f$ is a straightforward corollary in Frege.

Using the induction hypothesis $\neg \text{Eq}^i_{f=g} \rightarrow \neg \text{Eq}^{j+1}_f$ we can get $\neg \text{Eq}^j_{f=g} \rightarrow \neg \text{Eq}^{j+1}_f$.

Lemma 10. For $0 \leq i \leq j \leq m$ the following propositions describe the relationships between the different extension variables.

\begin{itemize}
  \item $\text{Eq}^i_{L=\tau} \rightarrow \neg \text{Diff}^i_L$
  \item $\text{Diff}^i_L \land \neg \text{Diff}^{i-1}_L \rightarrow \text{Eq}^{i-1}_{R=\tau}$
  \item $\text{Diff}^i_L \land \neg \text{Diff}^{i-1}_L \rightarrow \neg \text{Diff}^i_R$
  \item $\text{Eq}^{i}_{R=\tau} \rightarrow \neg \text{Diff}^i_L$
  \item $\text{Diff}^i_R \land \neg \text{Diff}^{i-1}_R \rightarrow \text{Eq}^{i-1}_{L=\tau}$
  \item $\text{Diff}^i_R \land \neg \text{Diff}^{i-1}_R \rightarrow \neg \text{Diff}^{i-1}_L$
\end{itemize}

Proof.

Induction Hypothesis on $i$. $\text{Eq}^i_{L=\tau} \rightarrow \neg \text{Diff}^i_L$ in an $O(i)$-size eFrege proof.

Base Case $i = 0$. $\text{Diff}^i_L$ is defined as $0$ so $\neg \text{Diff}^i_L$ is true and trivially implied by $\text{Eq}^i_{L=\tau}$.

Frege can manage this.

Inductive Step $i + 1$. If $\text{Set}^{i+1}_L$ is false then $\text{Eq}^i_{L=\tau}$ is equivalent to $\text{Eq}^i_{L=\tau} \land \neg \text{Diff}^{i+1}_L$ and $\neg \text{Diff}^{i+1}_L$ is equivalent to $\neg \text{Diff}^i_L \land \neg \text{Set}^{i+1}_L \lor \neg \text{Eq}^i_{L=\tau}$. If $\text{Set}^{i+1}_L$ is true then $\text{Eq}^i_{L=\tau}$ is equivalent to $\text{Eq}^i_{L=\tau} \land \text{Set}^{i+1}_L \land (\text{Val}^{i+1}_L \leftrightarrow \text{Val}^{i+1}_R)$ and $\neg \text{Diff}^{i+1}_L$ is equivalent to $\neg \text{Diff}^i_L \land \text{Set}^{i+1}_L \land (\text{Val}^{i+1}_L \leftrightarrow \text{Val}^{i+1}_R) \lor \neg \text{Eq}^i_{L=\tau}$. Therefore using the induction hypothesis $\text{Eq}^i_{L=\tau} \rightarrow \neg \text{Diff}^i_L$. Similarly for $R$.

The formulas $\text{Diff}^i_L \land \neg \text{Diff}^{i-1}_L \rightarrow \text{Eq}^i_{R=\tau}$ are simple corollaries of the inductive definition of $\text{Diff}^i_L$ and combined with $\text{Eq}^i_{R=\tau} \rightarrow \neg \text{Diff}^{i-1}_L$ we get $\text{Diff}^i_L \land \neg \text{Diff}^{i-1}_L \rightarrow \neg \text{Diff}^{i-1}_L$. Similarly if we swap $L$ and $R$.

Lemma 11. For any $0 \leq i \leq m$ the following propositions are true and have short Extended Frege proofs.

\begin{itemize}
  \item $L \land \text{Diff}^i_L \rightarrow \neg \text{anno}_{x,L}(\tau)$
  \item $R \land \text{Diff}^i_R \rightarrow \neg \text{anno}_{x,R}(\tau)$
\end{itemize}
Proof. We primarily use the disjunction in Lemma 8 $\text{Diff}_L^i \rightarrow V_{i=1}^i \text{Diff}_L^i \land \neg \text{Diff}_L^{i-1}$.

In each disjunct $\text{Diff}_L^i \land \neg \text{Diff}_L^{i-1}$ we can say that the difference triggers at that point. We can represent that in a proposition that can be proven in \textit{eFrege}: $\text{Diff}_L^i \land \neg \text{Diff}_L^{i-1} \rightarrow ((\text{Set}_L^i \odot \text{Set}_L^i) \lor (\text{Set}_L^i \land (\text{Val}_L^i \odot \text{Val}_L^i)))$ If $L$ differs from $\tau$ on a $\text{Set}_L^i$ value we contradict $\text{anno}_{x,L}(\tau)$ in one of two ways: $L \land (\text{Set}_L^i \odot \text{Set}_L^i) \land \text{Set}_L^i \rightarrow \neg \text{Set}_L^i$ or $L \land (\text{Set}_L^i \odot \text{Set}_L^i) \land \neg \text{Set}_L^i \rightarrow \text{Set}_L^i$.

If $L$ differs from $\tau$ on a $\text{Val}_L^i$ value when $\text{Set}_L^i = \text{Set}_L^i = 1$ we contradict $\text{anno}_{x,L}(\tau)$ in one of two ways:

- $L \land \text{Set}_L^i \land \text{Set}_L^i \land (\text{Set}_L^i \rightarrow (\text{Val}_L^i \odot \text{Val}_L^i)) \land \text{Val}_L^i \rightarrow \neg \text{Val}_L^i \lor u_i$
- $L \land \text{Set}_L^i \land \text{Set}_L^i \land (\text{Set}_L^i \rightarrow (\text{Val}_L^i \odot \text{Val}_L^i)) \land \neg \text{Val}_L^i \rightarrow \text{Val}_L^i \land u_i$

When put together with the big disjunction this lends itself to a short \textit{eFrege} proof which is also symmetric for $R$.

\textbf{Lemma 12.} For any $1 \leq i \leq m$ the following propositions are true and have a short \textit{Extended Frege} proof.

\begin{itemize}
  \item $\neg \text{Diff}_L^i \land \neg \text{Diff}_R^i \rightarrow \text{Eq}_L^i$
  \item $\neg \text{Diff}_L^i \land \neg \text{Diff}_R^i \rightarrow \text{Eq}_R^i$
  \item $\neg \text{Diff}_L^i \land \neg \text{Diff}_R^i \rightarrow \text{Set}_B^i \leftrightarrow \text{Set}_L^i$
  \item $\neg \text{Diff}_L^i \land \neg \text{Diff}_R^i \rightarrow \text{Val}_B^i \leftrightarrow \text{Val}_L^i$
  \item $\neg \text{Diff}_L^i \land \neg \text{Diff}_R^i \rightarrow \text{Val}_B^i \leftrightarrow \text{Val}_L^i$
\end{itemize}

\textbf{Proof.} We first show $\neg \text{Eq}_{L=\tau}^i \rightarrow \neg \text{Eq}_{R=\tau}^{i-1} \lor \text{Diff}_L^i \lor \text{Diff}_R^i$ and $\neg \text{Eq}_{R=\tau}^i \rightarrow \neg \text{Eq}_{L=\tau}^{i-1} \lor \text{Diff}_L^i \lor \text{Diff}_R^i$.

\textbf{Induction Hypothesis on $j$.} $\neg \text{Diff}_L^j \land \neg \text{Diff}_R^j \rightarrow \text{Eq}_L^j$ and $\neg \text{Diff}_L^j \land \neg \text{Diff}_R^j \rightarrow \text{Eq}_R^j$.

\textbf{Base Case $j = 0$.} $\text{Eq}_{L=\tau}^j$ and $\text{Eq}_{R=\tau}^j$ are both true by definition so the implications automatically hold.

\textbf{Inductive Step $j$.} $\neg \text{Eq}_{L=\tau}^{j+1} \rightarrow \neg \text{Eq}_{L=\tau}^{j-1} \lor (\text{Set}_L^j \odot \text{Set}_L^j) \lor (\text{Set}_L^j \land (\text{Val}_L^j \odot \text{Val}_L^j))$, $\text{Set}_L^j \odot \text{Set}_L^j) \lor (\text{Set}_L^j \land (\text{Val}_L^j \odot \text{Val}_L^j)) \lor \text{Diff}_L^j \lor \neg \text{Eq}_{R=\tau}^{j-1}$ so we get $\neg \text{Eq}_{L=\tau}^j \rightarrow \neg \text{Eq}_{R=\tau}^{j-1} \lor \text{Diff}_L^j \lor \neg \text{Eq}_{R=\tau}^{j-1}$, which using the induction hypothesis can be generalised to $\neg \text{Eq}_{L=\tau}^j \rightarrow \text{Diff}_L^j \lor \text{Diff}_R^j$ which is equivalent to $\neg \text{Diff}_L^j \land \neg \text{Diff}_R^j \rightarrow \text{Eq}_L^j$. Similarly when swapping $L$ and $R$.

We can obtain the remaining propositions as corollaries by using the definition of Eq.

Nonetheless, $\text{Diff}_L^i$ and $\text{Diff}_R^i$ still end up being relevant to the choice of $\text{Val}_B^i$.

\textbf{Lemma 13.} For any $0 \leq i \leq m$ the following propositions are true and have short Extended Frege proofs.

\begin{itemize}
  \item $\text{Diff}_L^i \rightarrow (\text{Val}_B^i \leftrightarrow \text{Val}_L^i) \land (\text{Set}_B^i \leftrightarrow \text{Set}_L^i)$
  \item $\neg \text{Diff}_L^i \land \text{Diff}_R^i \rightarrow (\text{Val}_B^i \leftrightarrow \text{Val}_R^i) \land (\text{Set}_B^i \leftrightarrow \text{Set}_R^i)$
\end{itemize}

\textbf{Proof.} Suppose we want to prove $\text{Diff}_L^i \rightarrow (\text{Val}_B^i \leftrightarrow \text{Val}_L^i) \land (\text{Set}_B^i \leftrightarrow \text{Set}_L^i)$. We will assume the definition

$$\text{Diff}_L^i := \text{Diff}_L^{i-1} \lor (\text{Eq}_R^{i-1} \land ((\text{Set}_L^i \odot \text{Set}_L^i) \lor (\text{Set}_L^i \land (\text{Val}_L^i \odot \text{Val}_L^i))))$$
and show that following proposition is falsified

\[ \neg D_{L}^{i-1} \land (D_{L}^{j-1} \lor (\neg Set_{L}^{i} \land \neg Set_{L}^{j} \land Set_{R}^{i}) \lor (Set_{L}^{j} \land Set_{L}^{i} \land (Val_{L}^{i} \leftrightarrow Val_{L}^{j}))) \]

The first thing is that we only need to consider \( D_{L}^{i} \land \neg D_{L}^{i-1} \) as \( D_{L}^{i-1} \) already falsifies our proposition. Next we show \( \neg D_{L}^{i-1} \) is forced to be true in this situation. To do this we need Lemma 10 for \( D_{L}^{i} \land \neg D_{L}^{i-1} \rightarrow \neg D_{L}^{i-1} \).

Now we use \( D_{L}^{i} \land \neg D_{L}^{i-1} \rightarrow ((Set_{L}^{i} \lor Set_{L}^{j}) \lor (Set_{L}^{j} \land (Val_{L}^{i} \lor Val_{L}^{j}))) \), we break this down into three cases

1. \( D_{L}^{i} \land \neg D_{L}^{i-1} \land \neg Set_{L}^{i} \land Set_{L}^{j} \)
2. \( D_{L}^{i} \land \neg D_{L}^{i-1} \land Set_{L}^{i} \land \neg Set_{L}^{j} \)
3. \( D_{L}^{i} \land \neg D_{L}^{i-1} \land (Set_{L}^{i} \land (Val_{L}^{i} \lor Val_{L}^{j})) \)

1. \( D_{L}^{i} \land \neg D_{L}^{i-1} \) contradicts \( D_{L}^{i-1} \), \( Set_{L}^{i} \) contradicts \( (\neg Set_{L}^{i} \land \neg Set_{L}^{j} \land Set_{L}^{i}) \), and \( \neg Set_{L}^{i} \) contradicts \( (Set_{L}^{i} \land Set_{L}^{j} \land (Val_{L}^{i} \leftrightarrow Val_{L}^{j})) \).
2. \( D_{L}^{i} \land \neg D_{L}^{i-1} \) contradicts \( D_{L}^{i-1} \), \( Set_{L}^{i} \) contradicts \( (\neg Set_{L}^{i} \land \neg Set_{L}^{j} \land Set_{L}^{i}) \), and \( \neg Set_{L}^{i} \) contradicts \( (Set_{L}^{i} \land Set_{L}^{j} \land (Val_{L}^{i} \leftrightarrow Val_{L}^{j})) \).
3. \( D_{L}^{i} \land \neg D_{L}^{i-1} \) contradicts \( D_{L}^{i-1} \), \( Set_{L}^{j} \) contradicts \( (\neg Set_{L}^{i} \land \neg Set_{L}^{j} \land Set_{L}^{j}) \), \( (Val_{L}^{i} \lor Val_{L}^{j}) \) contradicts \( (Set_{L}^{i} \land Set_{L}^{j} \land (Val_{L}^{i} \leftrightarrow Val_{L}^{j})) \).

Since in all cases we contradict \( \neg D_{L}^{i-1} \land (D_{L}^{i-1} \lor (\neg Set_{L}^{i} \land \neg Set_{L}^{j} \land Set_{L}^{i}) \lor (Set_{L}^{j} \land Set_{L}^{i} \land (Val_{L}^{i} \leftrightarrow Val_{L}^{j}))) \) then as per definition \( (Val_{L}, Set_{R}) = (Val_{L}, Set_{L}) \). Using \( D_{L}^{i} \rightarrow (D_{L}^{i} \land \neg D_{L}^{i-1}) \lor D_{L}^{i-1} \) we get \( D_{L}^{i} \rightarrow (Val_{L, B} \leftrightarrow Val_{L, R}) \land (Set_{B} \leftrightarrow Set_{R}) \), in a polynomial number of Frege lines.

Now we suppose we want to prove the second proposition \( \neg D_{L}^{i} \land D_{R}^{m} \rightarrow (Val_{L, B} \leftrightarrow Val_{L, R}) \land (Set_{B} \leftrightarrow Set_{R}) \). We need \( \neg D_{L}^{i} \land D_{R}^{m} \) to satisfy \( \neg D_{L}^{i} \land (D_{L}^{i} \lor (\neg Set_{L}^{i} \land \neg Set_{L}^{j} \land Set_{L}^{i}) \lor (Set_{L}^{j} \land Set_{L}^{i} \land (Val_{L}^{i} \leftrightarrow Val_{L}^{j}))) \).

Lemma gives us that \( \neg D_{L}^{i} \rightarrow \neg D_{L}^{i-1} \). We can show that \( \neg D_{L}^{i-1} \land \neg D_{L}^{i-1} \rightarrow Eq_{L=\tau}^{i-1} \) using Lemma 15. This allows us to examine just the part where the difference is being triggered \( \neg D_{L}^{i} \land \neg D_{L}^{i-1} \rightarrow (Set_{L}^{i} \leftrightarrow Set_{L}^{i}) \land (Set_{L}^{j} \rightarrow (Val_{L}^{i} \leftrightarrow Val_{L}^{j})) \).

Suppose the term \( (\neg Set_{L}^{i} \land \neg Set_{L}^{j} \land Set_{L}^{j}) \) is false, assuming \( D_{L}^{i-1} \) is also false, we have to show that \( (Set_{L}^{i} \land Set_{L}^{j} \land (Val_{L}^{i} \leftrightarrow Val_{L}^{j})) \) will be satisfied. We look at the three ways the term \( (\neg Set_{L}^{i} \land \neg Set_{L}^{j} \land Set_{L}^{j}) \) can be falsified and show that all the parts of the remaining term must be satisfied when assuming \( \neg D_{L}^{i} \land D_{R}^{m} \land \neg D_{L}^{i-1} \).

1. Set_{L}^{i}, in this case \( (Val_{L}^{i} \leftrightarrow Val_{L}^{j}) \) is active and Set_{L}^{i} is implied by \( (Set_{L}^{i} \leftrightarrow Set_{L}^{j}) \).
2. Set_{L}^{j}, Set_{L}^{i} is implied by \( (Set_{L}^{i} \leftrightarrow Set_{L}^{j}) \), then \( (Val_{L}^{i} \leftrightarrow Val_{L}^{j}) \) is active.
3. \( \neg Set_{L}^{j} \), then using D_{R}^{m} and \( \neg D_{R}^{i-1} \) we must Set_{j} (as this is the only allowed way Dif can trigger). Once again, \( (Val_{L}^{i} \leftrightarrow Val_{L}^{j}) \) is active and Set_{L}^{i} is implied by \( (Set_{L}^{i} \leftrightarrow Set_{L}^{j}) \).

Since our trigger formula is always satisfied when \( \neg D_{L}^{i} \land D_{R}^{m} \land \neg D_{L}^{i-1} \). It means that \( (Val_{L}, Set_{R}) = (Val_{L}, Set_{R}) \). Using \( D_{L}^{i} \rightarrow (D_{L}^{i} \land \neg D_{L}^{i-1}) \lor D_{L}^{i-1} \) we get \( \neg D_{L}^{i} \land D_{R}^{m} \rightarrow (Val_{L} \leftrightarrow Val_{R}) \land (Set_{B} \leftrightarrow Set_{R}) \), in a polynomial number of Frege lines. ✷

**Lemma 14.** The following propositions are true and have short Extended Frege proofs.

- \( B \land D_{L}^{m} \rightarrow B_{L} \)
- \( B \land \neg D_{R}^{i} \land D_{R}^{m} \rightarrow B_{R} \)

**Proof.** We use the disjunction \( D_{L}^{m} \rightarrow V_{j=1}^{m} D_{L}^{j} \lor \neg D_{L}^{j-1} \) So there is some \( j \) where this is the case.

For \( 1 \leq i < j \) observe that \( D_{L}^{j} \lor \neg D_{L}^{j-1} \rightarrow \neg D_{L}^{j-1} \). Now these negative literals propagate downwards. \( \neg D_{L}^{j-1} \land \neg D_{R}^{j-1} \rightarrow \neg D_{L}^{i} \land \neg D_{R}^{i} \) for \( 0 \leq i < j \) and \( \neg D_{L}^{i} \land \neg D_{R}^{i} \) means that \( B \) and \( L \) are consistent for those \( i \) as proven in Lemma 12.
Towards Uniform Certification in QBF

For \( j \leq k \leq m \), \( \text{Diff}_L^j \rightarrow \text{Diff}_L^k \) and \( \text{Diff}_L^k \) means \( B \) and \( L \) are consistent on those \( k \) as proven in Lemma 13.

For indices greater than \( m \), \( B \land \text{Diff}_L^m \) falsifies \( \sim \text{Diff}_L^m \land (\text{Diff}_R^m \lor \bar{x}) \), so \( B \) and \( R \) are consistent on those indices.

With the second proposition \( \text{Diff}_R^m \rightarrow \bigvee_{j=1}^m \text{Diff}_R^j \lor \sim \text{Diff}_R^{j-1} \) once again. So there is some \( j \) where this is the case. Note that \( \sim \text{Diff}_L^m \rightarrow \sim \text{Diff}_L^k \) for \( k \leq m \).

For \( 1 \leq i < j \), both \( \sim \text{Diff}_L^i \) and \( \sim \text{Diff}_R \) occur so then \( B \) and \( R \) are consistent for these values.

For \( j \leq k \leq m \), \( \text{Diff}_L^j \rightarrow \text{Diff}_R^k \) and \( \text{Diff}_R^k \land \sim \text{Diff}_R^i \) means \( B \) and \( R \) are consistent on those \( k \) as proven in Lemma 13.

For indices greater than \( m \), \( B \land \text{Diff}_R^m \land \sim \text{Diff}_L^m \) satisfies \( \sim \text{Diff}_L^m \land (\text{Diff}_R^m \lor \bar{x}) \), so \( B \) and \( R \) are consistent on those indices.

\[\text{Lemma 15.} \quad \text{The following propositions are true and have short Extended Frege proofs.}\]

- \( B \land \sim \text{Diff}_L^m \land \sim \text{Diff}_R^m \rightarrow B_L \lor \sim x \)
- \( B \land \sim \text{Diff}_L^m \land \sim \text{Diff}_R^m \rightarrow B_R \lor x \)

\textbf{Proof.} For indices \( 1 \leq i \leq m \), but since \( \sim \text{Diff}_L^m \rightarrow \sim \text{Diff}_L^i \) and \( \sim \text{Diff}_R^m \rightarrow \sim \text{Diff}_R^i \), Lemma 12 can be used to show that \( B \land \text{Diff}_L^m \land \text{Diff}_R^m \) leads to \( \text{Set}_{i_B}^i = \text{Set}_{i_L}^i = \text{Set}_{i_R}^i \) and \( \text{Val}_{i_B}^i = \text{Val}_{i_L}^i = \text{Val}_{i_R}^i \) whenever \( \text{Set}_{i_B}^i \) is also true. Extended Frege can prove \( O(m) \) many propositions expressing as such.

For \( i > m \), by definition \( B \land \sim \text{Diff}_L^m \land \sim \text{Diff}_R^m \land x \) gives \( \text{Set}_{i_B}^i = \text{Set}_{i_L}^i \) and \( \text{Val}_{i_B}^i = \text{Val}_{i_L}^i \). And \( B \land \sim \text{Diff}_L^m \land \sim \text{Diff}_R^m \land \sim x \) gives \( \text{Set}_{i_B}^i = \text{Set}_{i_R}^i \) and \( \text{Val}_{i_B}^i = \text{Val}_{i_R}^i \). The sum of this is that \( B \land \text{Diff}_L^m \land \text{Diff}_R^m \land x \rightarrow B_L \) and \( B \land \text{Diff}_L^m \land \text{Diff}_R^m \land \sim x \rightarrow B_R \).

\[\text{A.2 Local Strategy Extraction for Simulation of IRM-calc}\]

\[\text{A.2.1 Conversion}\]

\[\text{anno}_{x,s}(\tau) = \bigwedge_{i, u_i \in \tau} (\text{Set}_{i}^{s} \land u_i) \land \bigwedge_{j, u_j \in \tau} (\text{Set}_{j}^{\overline{u_j}} \land u_i) \land \bigwedge_{u_i \notin \text{dom}(\tau)} (\sim \text{Set}_{i}^{s}) \land \bigwedge_{u_i \notin \text{dom}(\tau)} \text{con}_{s}(x^t) = x \land \text{anno}_{x,s}(\tau), \text{con}_{s}(C_1) = \bigvee_{x^t \in C_1} \text{con}(x^t)\]

\[\text{A.2.2 Equivalence}\]

\[\text{Eq}_{f \neq g}^0 := 1, \quad \text{Eq}_{f \neq g}^{i-1} := \text{Eq}_{f \neq g}^{i-1} \land (\text{Set}_{j}^{s}) \land (\text{Set}_{j}^{t} \rightarrow (\text{Val}_{j}^{f} \leftrightarrow \text{Val}_{j}^{g}))) \quad \text{when } * / u_i \notin g\]

\[\text{Eq}_{f = g}^r := \text{Eq}_{f \neq g}^{i-1} \land (\text{Set}_{j}^{s} \leftrightarrow \text{Set}_{j}^{t}) \land (\text{Set}_{j}^{s} \rightarrow (\text{Val}_{j}^{f} \leftrightarrow \text{Val}_{j}^{g}))) \quad \text{when } * / u_i \notin g\]

\[\text{A.2.3 Difference}\]

\[\text{Diff}_{L}^{0} := 0 \quad \text{and} \quad \text{Diff}_{R}^{0} := 0\]

For \( u_i \notin \text{dom}(\tau \cup \sigma \cup \zeta) \), \( \text{Diff}_{L}^{i} := \text{Diff}_{L}^{i-1} \lor (\text{Eq}_{r \neq r \cup \bar{x}} \land (\text{Set}_{i}^{s})) \)

For \( u_i \in \text{dom}(\tau) \), \( \text{Diff}_{L}^{i} := \text{Diff}_{L}^{i-1} \lor (\text{Eq}_{r \neq r \cup \bar{x}} \land (\sim \text{Set}_{i}^{s} \lor \text{Val}_{i}^{f} \lor \text{Val}_{i}^{r})))\)

For \( u_i \in \text{dom}(\sigma) \), \( \text{Diff}_{L}^{i} := \text{Diff}_{L}^{i-1} \lor (\text{Eq}_{r \neq r \cup \bar{x}} \land (\sim \text{Set}_{i}^{s} \lor \text{Val}_{i}^{f} \lor \text{Val}_{i}^{r})))\)

For \( u_i \in \text{dom}(\zeta) \), \( \text{Diff}_{L}^{i} := \text{Diff}_{L}^{i-1} \lor (\text{Eq}_{r \neq r \cup \bar{x}} \land (\text{Set}_{i}^{s}))\)

\[\text{A.2.4 Policy Variables}\]

We define the policy variables \( \text{Val}_{i}^{f} \) and \( \text{Set}_{i}^{f} \) based on a number of cases, in all cases \( \text{Val}_{i}^{f} \) and \( \text{Set}_{i}^{f} \) are defined on variables left of \( u_i \).
For $u_i \not\in \text{dom}(\tau \sqcup \sigma \sqcup \xi)$, $u_i < x$,

$$(\text{Val}_B^i, \text{Set}_B^i) = \begin{cases} (\text{Val}_R^i, \text{Set}_R^i) & \text{if } \neg \text{Dif}_L^{i-1} \land (\text{Dif}_R^{i-1} \lor \neg \text{Set}_L^i) \\ (\text{Val}_L^i, \text{Set}_L^i) & \text{otherwise.} \end{cases}$$

For $u_i \in \text{dom}(\tau)$,

$$(\text{Val}_B^i, \text{Set}_B^i) = \begin{cases} (\text{Val}_R^i, \text{Set}_R^i) & \text{if } \neg \text{Dif}_L^{i-1} \land (\text{Dif}_R^{i-1} \lor (\text{Val}_L^i \leftrightarrow \text{Val}_R^i))) \\ (\text{Val}_L^i, \text{Set}_L^i) & \text{otherwise.} \end{cases}$$

For $\ast / u_i \in \sigma$,

$$(\text{Val}_B^i, \text{Set}_B^i) = \begin{cases} (0, 1) & \text{if } \neg \text{Dif}_L^{i-1} \land \text{Dif}_R^{i-1} \land \neg \text{Set}_R^i \\ (\text{Val}_R^i, \text{Set}_R^i) & \text{if } \neg \text{Dif}_L^{i-1} \land \text{Set}_R^i \land (\text{Dif}_R^{i-1} \lor \text{Set}_L^i) \\ (\text{Val}_L^i, \text{Set}_L^i) & \text{otherwise.} \end{cases}$$

For $\ast / u_i \in \xi$,

$$(\text{Val}_B^i, \text{Set}_B^i) = \begin{cases} (0, 1) & \text{if } \neg \text{Dif}_L^{i-1} \land \neg \text{Set}_L^i \\ (\text{Val}_R^i, \text{Set}_R^i) & \text{if } \neg \text{Dif}_L^{i-1} \land (\text{Dif}_R^{i-1} \lor \neg \text{Set}_L^i) \\ (\text{Val}_L^i, \text{Set}_L^i) & \text{otherwise.} \end{cases}$$

For $u_i > x$,

$$(\text{Val}_B^i, \text{Set}_B^i) = \begin{cases} (\text{Val}_R^i, \text{Set}_R^i) & \text{if } \neg \text{Dif}_L^m \land (\text{Dif}_R^m \lor \neg x) \\ (\text{Val}_L^i, \text{Set}_L^i) & \text{otherwise.} \end{cases}$$