CERES in Second-Order Logic *

Stefan Hetzl[1], Alexander Leitsch[1], Daniel Weller[1], and
Bruno Woltzenlogel Paleo[1]

{hetzl, leitsch, weller, bruno}@logic.at
Institute of Computer Languages (E185),
Vienna University of Technology,
Favoritenstraße 9, 1040 Vienna, Austria

Abstract. This work defines an extension CERES^2 of the first-order cut-elimination method CERES to the subclass of sequent calculus proofs in second-order logic using quantifier-free comprehension. This extension is motivated by the fact that cut-elimination can be used as a tool to extract information from real mathematical proofs, and often a crucial part of such proofs is the definition of sets by formulas. This is expressed by the comprehension axiom scheme, which is representable in second-order logic. At the core of CERES^2 lies the production of a set of clauses CL(φ) from a proof φ that is always unsatisfiable. From a resolution refutation γ of CL(φ), an essentially cut-free proof can be constructed. The main theoretical obstacle in the extension of CERES to second-order logic is the construction of this cut-free proof from γ. This issue is solved for the subclass considered in this paper. Moreover, we discuss the problems that have to be solved to extend CERES^2 to the complete class of second-order proofs. Finally, the method is applied to a simple mathematical proof that involves induction and comprehension and the resulting proof is analyzed.

1 Introduction

The discipline of *proof mining* deals with the extraction of information from formal proofs. Different methods have been applied successfully (see [1], [2]). This work considers the approach of using cut-elimination to extract new proofs from known ones. In particular, it is well known that in first-order logic cut-elimination produces proofs that are analytic in the sense that all formulas used in the proof will be subformulas of the proved theorem, eliminating the use of auxiliary notions that have no direct connection to the theorem. In second-order logic, the notion of analyticity has to be adapted to this slightly weaker form: all formulas used in a cut-free proof in second-order logic either are subformulas of the proved theorem, or they are replaced by weakly quantified second-order variables by the use of comprehension (i.e. they are used to define a set). In other words, formulas of second-order logic can be viewed as frames, and cut-free proofs of such formulas will only contain (subformulas of) instances of these frames.

* Supported by the Austrian Science Fund (project P19875)

The first-order cut-elimination method CERES (cut-elimination by resolution) has several advantages over the traditional reductive cut-elimination methods: firstly, the reductive methods are subsumed by CERES (i.e. every proof obtained by a reductive method can also be obtained by CERES, see [2]), and secondly, a non-elementary speed-up over Gentzen's method by the use of CERES is possible (see [3]). The CERES method has been implemented in the `CERES` system[1].

An inherent limitation of the CERES method (and indeed of all first-order cut-elimination procedures) is that proofs that use comprehension cannot be handled in a straightforward way, as comprehension is essentially a second-order property. This motivates the extension of CERES to CERES^2, a cut-elimination method for second-order logic, which will be able to handle proofs that make use of comprehension in a natural way. The subclass of proofs we are considering here is the class of proofs where comprehension is restricted to quantifier-free formulas. This choice is motivated in part by the fact that converting a resolution refutation to a sequent calculus proof in the presence of arbitrary comprehension (and, therefore, skolemization) is problematic.

2 The second-order language

Here, we consider a fragment of higher-order logic based on Church's simply typed λ-calculus [4] and fix the set of *base types* $BT := \{\iota, o\}$, where ι denotes the type of individuals and o the boolean type. The set $\mathcal{T}$ of *types* is built in the usual inductive way over the BT. In contrast to second-order logic as it is defined in e.g. [5], we include in the language more objects of order ≤ 2 to allow skolemization, although quantification is restricted to individuals and unary predicates on individuals (i.e. variables of types ι and $\iota \to o$).

We assume given a set of symbols S together with a function $\tau : S \mapsto \mathcal{T}$ assigning types to symbols, where S can be partitioned into the sets V (individual variables), CS (individual constants), FS^n (function symbols), PC^n (predicate constants), PV (unary predicate variables) s.t.

1. For all $x \in V$, $\tau(x) = \iota$,
2. for all $c \in CS$, $\tau(c) = \iota$,
3. for all $f \in FS^n$, $n \geq 1$: $\tau(f) = t_1 \to \ldots \to t_n \to \iota$ where for $1 \leq i \leq n$, $t_i = \iota$ or $t_i = \iota \to o$,
4. for all $P \in PC^n$, $n \geq 0$: $\tau(P) = t_1 \to \ldots \to t_n \to o$ where for $1 \leq i \leq n$, $t_i = \iota$ or $t_i = \iota \to o$,
5. for all $X \in PV$, $\tau(X) = \iota \to o$.

We additionally require that each of these partitions is countably infinite. We define $PC := \bigcup_{i \geq 0} PC^i$ and $FS := \bigcup_{i \geq 1} FS^i$. The set of *expressions* $\mathcal{E}$ is defined inductively in the usual way over the set of symbols together with the symbols $\neg, \wedge, \vee, \to, \exists, \forall, \lambda, ., (,)$ (keeping in mind the restriction on the order of the types and on the types of the quantified variables). We use infix notation for familiar function symbols and predicates (e.g. $+, =$).

[1] `http://www.logic.at/ceres`

Definition 1. *The* set of second-order formulas *or simply* formulas $SOF := \{F \mid F \in \mathcal{E}, \tau(F) = o\}$. *If* $F \in SOF$, $F \equiv P(t_1, \ldots, t_n)$, $P \in PC \cup PV$, *then* F *is called* atomic.

For atomic formulas $P(t_1, \ldots, t_n)$ we may also write $t_1 \in P(t_2, \ldots, t_n)$. We define the set of *lambda terms* $LT := \{t \mid t \in \mathcal{E}, t \equiv \lambda x.F, \tau(F) = o\}$ and the set of *terms* $T := \{t \mid t \in \mathcal{E}, \tau(t) = \iota\}$. *Polarity* of subexpressions w.r.t. formulas and sequents, *strong* and *weak* quantifiers, the *scope* of quantifiers, *closed* formulas, β-reduction are defined as usual. We assume a variable convention (i.e. variables are renamed appropriately to avoid conflicts).

3 The calculus LKDe^2

In this section, we define the sequent calculus **LKDe^2**. It consists of the following rules:

1. propositional

$$\frac{\Gamma \vdash \Delta, A \quad \Pi \vdash \Lambda, B}{\Gamma, \Pi \vdash \Delta, \Lambda, A \wedge B} \wedge : r$$

$$\frac{A, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta} \wedge : l1 \qquad \frac{A, \Gamma \vdash \Delta}{B \wedge A, \Gamma \vdash \Delta} \wedge : l2$$

$$\frac{A, \Gamma \vdash \Delta \quad B, \Pi \vdash \Lambda}{A \vee B, \Gamma, \Pi \vdash \Delta\Lambda} \vee : l$$

$$\frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A \vee B} \vee : r1 \qquad \frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, B \vee A} \vee : r2$$

$$\frac{\Gamma \vdash \Delta, A \quad B, \Pi \vdash \Lambda}{A \to B, \Gamma, \Pi \vdash \Delta, \Lambda} \to : l \qquad \frac{A, \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \to B} \to : r$$

$$\frac{A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg A} \neg : r \qquad \frac{\Gamma \vdash \Delta, A}{\neg A, \Gamma \vdash \Delta} \neg : l$$

2. first-order

$$\frac{\Gamma \vdash \Delta, A\{x \leftarrow \alpha\}}{\Gamma \vdash \Delta, (\forall x)A} \forall : r \qquad \frac{A\{x \leftarrow t\}, \Gamma \vdash \Delta}{(\forall x)A, \Gamma \vdash \Delta} \forall : l$$

$$\frac{\Gamma \vdash \Delta, A\{x \leftarrow t\}}{\Gamma \vdash \Delta, (\exists x)A} \exists : r \qquad \frac{A\{x \leftarrow \alpha\}, \Gamma \vdash \Delta}{(\exists x)A, \Gamma \vdash \Delta} \exists : l$$

For the $\forall : r$ and the $\exists : l$ rules the variable α must not occur in Γ nor in Δ nor in A.
For the $\forall : l$ and the $\exists : r$ rules the term t must not contain a variable that is bound in A.

3. second-order

$$\frac{\Gamma \vdash \Delta, A\{X \leftarrow \Theta\}}{\Gamma \vdash \Delta, (\forall X)A}\ \forall^2 : r \qquad \frac{A\{X \leftarrow \lambda x.F\}, \Gamma \vdash \Delta}{(\forall X)A, \Gamma \vdash \Delta}\ \forall^2 : l$$

$$\frac{\Gamma \vdash \Delta, A\{X \leftarrow \lambda x.F\}}{\Gamma \vdash \Delta, (\exists X)A}\ \exists^2 : r \qquad \frac{A\{X \leftarrow \Theta\}, \Gamma \vdash \Delta}{(\exists X)A, \Gamma \vdash \Delta}\ \exists^2 : l$$

For the $\forall^2 : r$ and the $\exists^2 : l$ rules the predicate variable Θ must not occur in Γ nor in Δ nor in A.
For the $\forall^2 : l$ and the $\exists^2 : r$ rules the formula F must not contain variables that are bound in A, and $A\{X \leftarrow \lambda x.F\}$ is A after replacing all occurrences of X with $\lambda x.F$ and reducing to β-normal form.

4. equality

$$\frac{\Gamma \vdash \Delta, s = t \quad \Pi \vdash \Lambda, A[s]_\Xi}{\Gamma, \Pi \vdash \Delta, \Lambda, A[t]_\Xi} = (\Xi) : r1 \qquad \frac{\Gamma \vdash \Delta, s = t \quad A[s]_\Xi, \Pi \vdash \Lambda}{A[t]_\Xi, \Gamma, \Pi \vdash \Delta, \Lambda} = (\Xi) : l1$$

$$\frac{\Gamma \vdash \Delta, t = s \quad \Pi \vdash \Lambda, A[s]_\Xi}{\Gamma, \Pi \vdash \Delta, \Lambda, A[t]_\Xi} = (\Xi) : r2 \qquad \frac{\Gamma \vdash \Delta, t = s \quad A[s]_\Xi, \Pi \vdash \Lambda}{A[t]_\Xi, \Gamma, \Pi \vdash \Delta, \Lambda} = (\Xi) : l2$$

where Ξ is a set of positions in A, and s, t are terms.

5. structural

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A}\ w : r \qquad \frac{\Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}\ w : l$$

$$\frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}\ c : r \qquad \frac{A, A, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}\ c : l$$

$$\frac{\Gamma_1, A_1, A_2, \Gamma_2 \vdash \Delta}{\Gamma_1, A_2, A_1, \Gamma_2 \vdash \Delta}\ \pi : l \qquad \frac{\Gamma \vdash \Delta_1, A_1, A_2, \Delta_2}{\Gamma \vdash \Delta_1, A_2, A_1, \Delta_2}\ \pi : r$$

$$\frac{\Gamma \vdash \Delta, A \quad A, \Pi \vdash \Lambda}{\Gamma, \Pi \vdash \Delta, \Lambda}\ cut$$

6. definitions

$$\frac{A(t_1, \ldots, t_n), \Gamma \vdash \Delta}{P(t_1, \ldots, t_n), \Gamma \vdash \Delta}\ \mathrm{def}_P : l \qquad \frac{\Gamma \vdash \Delta, A(t_1, \ldots, t_n)}{\Gamma \vdash \Delta, P(t_1, \ldots, t_n)}\ \mathrm{def}_P : r$$

where P is a new constant predicate symbol, the *defining predicate* of A.

As axioms we allow the usual tautological sequents $A \vdash A$ for an atomic formula A as well as arbitrary atomic sequents without second-order variables (which is useful for conveniently axiomatizing a background theory). Additionally, if $\mathcal{C}$ is a set of atomic sequents, then we say that π is *an* $\mathbf{LKDe^2}$*-proof from* $\mathcal{C}$ if for every initial sequent S of π, S is either an axiom, or S is in $\mathcal{C}$. For formula occurrences α in π, we will say that α *goes into the end-sequent (into a cut)* if

there exists a formula occurrence β such that α is an ancestor of β and β occurs in the end-sequent (is a cut-formula occurrence). For rule applications ρ, we say that ρ goes into the end-sequent (into a cut) if the main formula occurrence of ρ goes into the end-sequent (into a cut). Sometimes, when it is convenient, we will use the additive rules $\vee : r$, $\wedge : l$ — these can of course be derived using the multiplicative rules together with contractions and permutations.

4 The second-order resolution calculus

In this section, we briefly present the resolution calculus we will need for the CERES^2 method. Note that in second-order logic, in contrast to first-order logic, clauses are not closed under substitution, so the transformation of a formula to clause form has to be incorporated into the calculus, instead of being used just in a preprocessing step.

To use a resolution calculus with CERES^2, it must be possible to use the resolution refutation of a particular set of clauses (the characteristic clause set, see Section 5) as the skeleton of an **LKDe^2**-proof that contains no non-atomic cuts. Intuitively, the following requirements arise:

1. Only literals (i.e. atomic formulas and their negations) may be resolved.
2. It must be possible to produce a propositional resolution refutation from instances of the refuted set of clauses.

Requirement 1 stems from the fact that CERES^2 is a cut-elimination method, and the resolution rule will be translated to the cut rule in **LKDe^2**. Requirement 2 is due to the fact that substitution is integrated in the resolution calculus, while this is not the case with **LKDe^2**.

The resolution calculus we are considering here is a restricted version of the higher-order resolution calculus defined by P.B. Andrews in [6].

Definition 2. *We define a* clause *as a sequent* $C := A_1, \ldots, A_n \vdash B_1, \ldots, B_m$ *with* A_i, B_i *atomic.*

In this paper, the transformation to conjunctive normal form (CNF) is the standard transformation that preserves logical equivalence.

Definition 3. *Let* F *be a quantifier-free formula. Let* $\mathrm{CNF}(F) \equiv F_1 \wedge \ldots \wedge F_n$ *and for all* $1 \leq i \leq n$ *define* L_i^+ *(*L_i^-*) as the set consisting of the atom formulas occurring positively (negatively) in* F_i*. If* $L_i^- = \{A_1, \ldots, A_k\}$ *and* $L_i^+ = \{B_1, \ldots, B_l\}$*, then define the clause* C_i *as the atomic sequent* $A_1, \ldots, A_k \vdash B_1, \ldots, B_l$*. Then the* clause form $\mathcal{C}$ *of* F *is defined as the set* $\mathcal{C} = \{C_1, \ldots, C_n\}$*.*

Let $S \equiv F_1, \ldots, F_n \vdash G_1, \ldots, G_m$ *be a quantifier-free sequent, then the clause form of* S *is defined as the clause form of* $(F_1 \wedge \ldots \wedge F_n) \rightarrow (G_1 \vee \ldots \vee G_m)$*.*

A substitution is a pair of mappings: The first maps variables to terms, while the second maps predicate variables to lambda terms. The result of the application of a substitution σ to an expression e is e after replacing all variables by the respective terms and all predicate variables by the respective lambda terms and

reducing to β-normal form, this will be denoted by $e\sigma$. A substitution is called quantifier-free if all the (lambda-)terms are quantifier-free.

Definition 4. *We define the application of a quantifier-free substitution σ to a set of clauses $\mathcal{C} = \{C_1, \ldots, C_n\}$, denoted $\mathcal{S}(\mathcal{C}, \sigma)$, as the clause form of the set of quantifier-free sequents $\{C_1\sigma, \ldots, C_n\sigma\}$. Note that this includes transformation to CNF, therefore $|\mathcal{S}(\mathcal{C}, \sigma)| \geq |\mathcal{C}|$.*

With this definition, we can state the rules of our resolution calculus.

Definition 5. *In the following, C, D are clauses.*

1. *C is called* instance *of D if there exists a quantifier-free substitution σ s.t. $C \in \mathcal{S}(\{D\}, \sigma)$.*
2. *C is called* p-reduct *of D if C is D after omission of some multiply occuring atomic formulas on either side of the sequent.*
3. *Let $C \equiv \Gamma, L \vdash \Delta$ and $D \equiv \Gamma' \vdash L, \Delta'$, then the clause $\Gamma, \Gamma' \vdash \Delta, \Delta'$ is called a* resolvent *of $\{C, D\}$.*

Definition 6. *Let $C \equiv \Gamma \vdash \Delta, s = t$, $D \equiv \Pi \vdash \Lambda, F$ be clauses, s, t terms and $=$ a distinguished constant predicate. Then the clause $\Gamma, \Pi \vdash \Lambda, \Delta, F[t]$ (or $\Gamma, \Pi \vdash \Lambda, \Delta, F[s]$) where $F[t]$ is the result of replacing some occurrences of s by t in F ($F[s]$ is defined symmetrically) is the result of* paramodulation *of $\{C, D\}$. For $D \equiv F, \Pi \vdash \Lambda$ paramodulation is defined analogously.*

With this, we can define the notion of a deduction in this calculus:

Definition 7. *Let $\mathcal{C}$ be a set of clauses and let C be a clause. A sequence $C_1, \ldots, C_n$ is called an* R-deduction *of C from $\mathcal{C}$ if it fulfills the following conditions:*

1. *$C_n \equiv C$,*
2. *for all $i = 1, \ldots, n$:*
   (a) *$C_i \in \mathcal{C}$ or*
   (b) *C_i is an instance or a p-reduct of C_j for some $j < i$ or*
   (c) *C_i is a resolvent of $\{C_j, C_k\}$ for some $j, k < i$ or*
   (d) *C_i is the result of paramodulation of $\{C_j, C_k\}$ for $j, k < i$.*

An R-deduction of the empty sequent $\vdash$ from $\mathcal{C}$ is called an R-refutation of $\mathcal{C}$.

To see how this calculus can be used to prove a theorem, consider the following example.

Example 1. We want to prove $(\forall x)(\neg 0 < x \rightarrow 0 = x)$ in a theory of arithmetic. We use the second-order induction axiom, an axiom for the successor function s, an axiom for the transitivity of the predicate $<$, and an axiom for the reflexivity of the predicate $=$ (the other properties of $=$ are expressed by the paramodulation rule). After negation of the theorem and transformation to clause form,

this yields the set of clauses

$$\begin{array}{ll}
\mathcal{C} = \{ \vdash x < s(x) & (AX1) \\
\quad x < y, y < z \vdash x < z & (AX2) \\
\quad X(0) \vdash X(x), X(f(X)) & (IND1) \\
\quad X(0), X(s(f(X))) \vdash X(x) & (IND2) \\
\quad \vdash x = x, & (REF) \\
\quad 0 < a \vdash, & (CONC1) \\
\quad 0 = a \vdash \} & (CONC2)
\end{array}$$

where $(IND1)$, $(IND2)$ correspond to the induction axiom and $(CONC1)$, $(CONC2)$ correspond to the negated theorem. We denote $T \equiv \lambda x.0 = x \vee 0 < x$, then using

$$\sigma = \langle \{x \leftarrow a\}, \{X \leftarrow T\} \rangle ,$$

we produce the set of clauses $\mathcal{S}(\{(IND1)\}, \sigma) =$

$$\begin{array}{l}
\{\ 0 = 0 \vdash 0 = a, 0 < a, 0 = f(T), 0 < f(T);\ (1) \\
\ \ 0 < 0 \vdash 0 = a, 0 < a, 0 = f(T), 0 < f(T)\}\ (2)
\end{array}$$

from which we choose the instance (1) which we resolve with $(CONC2)$, this yields

$$(C1) : 0 = 0 \vdash 0 < a, 0 = f(T), 0 < f(T)$$

From (REF) we get the instance $\vdash 0 = 0$, resolving with $(C1)$ we get

$$(C2) : \vdash 0 < a, 0 = f(T), 0 < f(T)$$

and resolving $(C2)$ with $(CONC1)$ yields

$$(C3) : \vdash 0 = f(T), 0 < f(T)$$

Again using σ we obtain the set of clauses $\mathcal{S}(\{(IND2)\}, \sigma) =$

$$\begin{array}{l}
\{\ 0 = 0, 0 = s(f(T)) \vdash 0 = a, 0 < a;\ (1) \\
\ \ 0 < 0, 0 = s(f(T)) \vdash 0 = a, 0 < a;\ (2) \\
\ \ 0 = 0, 0 < s(f(T)) \vdash 0 = a, 0 < a;\ (3) \\
\ \ 0 < 0, 0 < s(f(T)) \vdash 0 = a, 0 < a;\ (4)
\end{array}$$

from which we choose the instance (3) and resolve it with $(CONC1)$, $(CONC2)$ and an instance of (REF) to get

$$(C4) : 0 < s(f(T)) \vdash$$

Now we resolve $(C4)$ with an instance of $(AX2)$ to obtain

$$(C5) : 0 < y, y < s(f(T)) \vdash$$

and resolve $(C5)$ with $(AX1)$ and get

$$(C6) : 0 < f(T) \vdash$$

From $(C6)$ and $(C3)$ we get the resolvent

$$(C7) : \vdash 0 = f(T)$$

and from paramodulation with $(C4)$ we get

$$(C8) : 0 < s(0) \vdash$$

Now resolving $(C8)$ and $(AX1)$ yields

$$\vdash$$

and we have proved $(\forall x)(\neg 0 < x \rightarrow 0 = x)$.

Finally, we state some lemmas that show that R-deductions can be transformed to **LKDe²**-proofs. These will be useful for showing the effectiveness of the CERES^2 method in the next section.

Lemma 1. *Let C be a clause and σ be a quantifier-free substitution. Then we can construct an* **LKDe²***-proof of $C\sigma$ from $\mathcal{S}(\{C\}, \sigma)$ containing quantifier-free cuts only.*

Proof. As σ is quantifier-free, $C\sigma$ can be considered as a first-order sequent $\Gamma \vdash \Delta$. Let $\mathcal{S}(\{C\}, \sigma) = \{\Gamma_1 \vdash \Delta_1, \ldots, \Gamma_n \vdash \Delta_n\}$. For $\Sigma = F_1, \ldots, F_j$, define $\neg\Sigma = \neg F_1, \ldots, \neg F_j$, $\bigvee \Sigma = F_1 \vee \ldots \vee F_j$. Then by the definition of transformation to clause form, $\Pi \equiv \bigvee \neg\Gamma \vee \bigvee \Delta$ is logically equivalent to $\Lambda \equiv (\bigvee \neg\Gamma_1 \vee \bigvee \Delta_1) \wedge \ldots \wedge (\bigvee \neg\Gamma_n \vee \bigvee \Delta_n)$, so there is a proof of $\Lambda \vdash \Pi$. Clearly there is a proof of $\Pi, \Gamma \vdash \Delta$. There is a proof of $\vdash \Lambda$ from $\mathcal{S}(\{C\}, \sigma)$, we show this by induction on the number of conjuncts in Λ:

1. $\Lambda \equiv \bigvee \neg\Gamma_1 \vee \bigvee \Delta_1$. Then $\mathcal{S}(\{C\}, \sigma) = \{\Gamma_1 \vdash \Delta_1\}$. By repeated applications of $\neg : r$, we can prove $\vdash \neg\Gamma_1, \Delta_1$ from $\mathcal{S}(\{C\}, \sigma)$. By repeated applications of $\vee : r$, we get $\vdash \bigvee \neg\Gamma_1 \vee \bigvee \Delta_1$.
2. $\Lambda \equiv (\bigvee \neg\Gamma_1 \vee \bigvee \Delta_1) \wedge \ldots \wedge (\bigvee \neg\Gamma_{n+1} \vee \bigvee \Delta_{n+1})$, so $\mathcal{S}(\{C\}, \sigma) = \{\Gamma_1 \vdash \Delta_1, \ldots, \Gamma_{n+1} \vdash \Delta_{n+1}\}$. By (IH) we have a proof of $\vdash (\bigvee \neg\Gamma_1 \vee \bigvee \Delta_1) \wedge \ldots \wedge (\bigvee \neg\Gamma_n \vee \bigvee \Delta_n)$ from $\{\Gamma_1 \vdash \Delta_1, \ldots, \Gamma_n \vdash \Delta_n\}$. To get the desired proof, use

$$\dfrac{\vdash (\bigvee \neg\Gamma_1 \vee \bigvee \Delta_1) \wedge \ldots \wedge (\bigvee \neg\Gamma_n \vee \bigvee \Delta_n) \qquad \dfrac{\dfrac{\Gamma_{n+1} \vdash \Delta_{n+1}}{\vdash \neg\Gamma_{n+1}, \Delta_{n+1}}\neg : r}{\vdash \bigvee \neg\Gamma_{n+1} \vee \bigvee \Delta_{n+1}}\vee : r}{\vdash (\bigvee \neg\Gamma_1 \vee \bigvee \Delta_1) \wedge \ldots \wedge (\bigvee \neg\Gamma_n \vee \bigvee \Delta_n) \wedge (\bigvee \neg\Gamma_{n+1} \vee \bigvee \Delta_{n+1})}\wedge : r$$

Putting things together, we get a proof π with quantifier-free cuts

$$\dfrac{\dfrac{\vdash \Lambda \qquad \Lambda \vdash \Pi}{\vdash \Pi}\,cut \qquad \Pi, \Gamma \vdash \Delta}{\Gamma \vdash \Delta}\,cut$$

As required, π is a proof from $\mathcal{S}(\{C\}, \sigma)$.

Lemma 2. *Let $C \equiv \Gamma \vdash \Delta$ be a clause, $\mathcal{D}$ be a set of clauses, ψ be a* $\mathbf{LKDe^2}$*-proof of $\Gamma, \Pi \vdash \Lambda, \Delta$ from $\mathcal{D}$ with only quantifier-free cuts, let σ be a quantifier-free substitution whose domain contains no variable which occurs free in $\Pi \cup \Lambda$ and let $\Gamma^* \vdash \Delta^* \in \mathcal{S}(\{C\}, \sigma)$. Then we can construct an* $\mathbf{LKDe^2}$*-proof ψ^* of $\Gamma^*, \Pi \vdash \Lambda, \Delta^*$ from $\mathcal{S}(\mathcal{D}, \sigma)$ with only quantifier-free cuts and with $|\psi^*| \leq |\psi| + \rho(|\Gamma\sigma \vdash \Delta\sigma|)$, where ρ is exponential if σ substitutes for a predicate variable in $\mathcal{D}$, and polynomial otherwise.*

Proof. The proof ψ^* has the following form:

$$\begin{array}{c} (\psi'\sigma) \\ \Gamma\sigma, \Pi \vdash \Lambda, \Delta\sigma \\ \vdots\ (a) \\ \Pi \vdash \Lambda, \bigwedge \Gamma\sigma \rightarrow \bigvee \Delta\sigma \\ \vdots\ (b) \\ \Pi \vdash \Lambda, \mathrm{NNF}(\bigwedge \Gamma\sigma \rightarrow \bigvee \Delta\sigma) \\ \vdots\ (c) \\ \Gamma^*, \Pi \vdash \Lambda, \Delta^* \end{array}$$

First, we obtain $\psi'\sigma$ from ψ: Let $\mathcal{D} = \{C_1, \ldots, C_n\}$, then when we apply σ to ψ, this yields a proof of $\Gamma\sigma, \Pi \vdash \Lambda, \Delta\sigma$ where every initial sequent is either an axiom, or of the form $A\sigma \vdash A\sigma$, or $C_i\sigma$ for some $1 \leq i \leq n$. We have to replace the latter two kinds of initial sequents by proofs to obtain the proof $\psi'\sigma$ from $\mathcal{S}(\mathcal{D}, \sigma)$:

1. We replace initial sequents of the form $A\sigma \vdash A\sigma$ by their respective proofs from atomic initial sequents and
2. apply Lemma 1 to initial sequents of the form $C_i\sigma$ to obtain proofs of $C_i\sigma$ from $\mathcal{S}(\{C_i\}, \sigma)$. We replace the initial sequents by the respective proofs.

This yields the desired proof $\psi'\sigma$ from $\mathcal{S}(\mathcal{D}, \sigma)$. We will now describe the steps (a-c) in detail:

(a) By a series of $\wedge$: l- and $\vee$: r-, followed by an $\rightarrow$: r-rule.

(b) For any formula F there is a proof χ_F of $F \vdash \mathrm{NNF}(F)$ based on the well-known rewrite rules of (i) replacing implication by negation and disjunction, (ii) the de Morgan-laws and (iii) double negation elimination. Phase (b) consists of a single cut against such a proof.

(c) For every negation normal form F and clause $\Gamma^* \vdash \Delta^* \in \mathrm{CNF}(F)$, there exists a proof $\chi_F^{\Gamma^* \vdash \Delta^*}$ of $F, \Gamma^* \vdash \Delta^*$. $\chi_F^{\Gamma^* \vdash \Delta^*}$ is constructed as follows:
If $F = G \wedge H$, then $\Gamma^* \vdash \Delta^* \in \mathrm{CNF}(G)$ or $\Gamma^* \vdash \Delta^* \in \mathrm{CNF}(H)$. Define

$$\chi_{G \wedge H}^{\Gamma^* \vdash \Delta^*} \quad := \quad \dfrac{\begin{array}{c}(\chi_G^{\Gamma^* \vdash \Delta^*}) \\ G, \Gamma^* \vdash \Delta^*\end{array}}{G \wedge H, \Gamma^* \vdash \Delta^*}\ \wedge\text{: l1}$$

in the first case and use $\wedge$: l2 analogously in the second case. If $F = G \vee H$, then $\Gamma^* = \Gamma_1^* \cup \Gamma_2^*$ and $\Delta^* = \Delta_1^* \cup \Delta_2^*$ s.t. $\Gamma_1^* \vdash \Delta_1^* \in \mathrm{CNF}(G)$ and

$\Gamma_2^* \vdash \Delta_2^* \in \mathrm{CNF}(H)$. Define

$$\chi_{G\vee H}^{\Gamma^*\vdash\Delta^*} := \dfrac{(\chi_G^{\Gamma_1^*\vdash\Delta_1^*}) \quad (\chi_H^{\Gamma_2^*\vdash\Delta_2^*})}{G,\Gamma_1^* \vdash \Delta_1^* \quad H,\Gamma_2^* \vdash \Delta_2^*} \vee\colon \mathrm{l}$$

If $F = \neg G$, then G is an atom, $\Gamma^* = \{G\}$, $\Delta^* = \emptyset$ and define

$$\chi_{\neg G}^{G\vdash} := \dfrac{G \vdash G}{\neg G, G \vdash} \neg\colon \mathrm{l}$$

If F is an atom, then $\Gamma^* = \emptyset$, $\Delta^* = \{F\}$ and therefore $F, \Gamma^* \vdash \Delta^*$ is already an axiom. Phase (c) consists of a single cut against $\chi_{\mathrm{NNF}(\bigwedge \Gamma\sigma\to\bigvee\Delta\sigma)}^{\Gamma^*\vdash\Delta^*}$.

The total size of ψ^* is $|\psi\sigma| = |\psi|$ plus $O(|\Gamma\sigma \vdash \Delta\sigma|)$ for each of the three phases, plus a number exponential in the size of σ in case we have to apply Lemma 1.

Lemma 3. *Let R be an R-deduction of $\Gamma \vdash \Delta$ from a set of clauses $\mathcal{C}$. Then there exists an* **LKDe²***-proof ψ of $\Gamma \vdash \Delta$ from $\mathcal{D}$ containing quantifier-free cut-formulas only, where $\mathcal{D} = \{D \mid D \in \mathcal{S}(\mathcal{C}, \sigma)$ for some quantifier-free $\sigma\}$.*

Proof. By induction on the size of R, letting $\mathcal{C} = \{C_1, \ldots, C_n\}$:

1. $|R| = 0$. Then $R = C_i$ for some $1 \le i \le n$. Take ψ as the initial sequent C_i.
2. $|R| = m + 1$. Let $R = A_1, \ldots, A_{m+1}$. Distinguish:
   (a) A_{m+1} is an instance of A_i under a quantifier-free substitution σ (for some $1 \le i \le m$). By (IH) we have an **LKDe²**-proof ψ of A_i from $\mathcal{D} = \{D \mid D \in \mathcal{S}(\mathcal{C}, \mu)$ for some quantifier-free $\mu\}$. We apply Lemma 2 to obtain a proof ψ' of A_{m+1} from $\mathcal{S}(\mathcal{D}, \sigma)$. Clearly, $\mathcal{S}(\mathcal{D}, \sigma)$ consists of quantifier-free instances of clauses in $\mathcal{C}$ and we can take ψ' as the desired **LKDe²**-proof.
   (b) A_{m+1} is a p-reduct of A_i for some $1 \le i \le m$. Then

   $$A_i \equiv B_1, \ldots, B_1, B_2, \ldots, B_2, \ldots, B_k, \ldots, B_k \vdash C_1, \ldots, C_1, \ldots, C_l, \ldots, C_l$$

   and A_{m+1} is A_i after omission of some $B_1, \ldots, B_k, C_1, \ldots, C_l$ such that at least one atom remains in every group. By (IH), we have an **LKDe²**-proof ψ of A_i fulfilling our conditions, so clearly we can take

   $$\dfrac{\begin{array}{c}\psi\\ A_i\end{array}}{A_{m+1}}\, c : *$$

   as the desired proof.
   (c) A_{m+1} is a resolvent of $\{C_j, C_k\}$ for some $1 \le j \le m$, $1 \le k \le m$. So if $C_j \equiv \Gamma \vdash \Delta, A$, $C_k \equiv A, \Pi \vdash \Lambda$, then $A_{m+1} \equiv \Gamma, \Pi \vdash \Delta, \Lambda$ and by (IH), we have proofs ψ_1 of C_j and ψ_2 of C_k fulfilling our conditions. So as the desired proof we may take

$$\dfrac{\begin{array}{cc}\psi_1 & \psi_2\\ \Gamma \vdash \Delta, A & A, \Pi \vdash \Lambda\end{array}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{cut}$$

(d) A_{m+1} is the result of paramodulation of $\{C_j, C_k\}$ for some $1 \leq j \leq m$, $1 \leq k \leq m$. Analogous to the previous case, using the equality rules of **LKDe²** instead of cut.

Example 2. Consider the following R-deduction of $P(t), Q(t) \vdash P(s)$ from

$$\mathcal{C} = \{T, t \in X \vdash s \in X;\ \vdash T\},$$

where $\sigma = \{X \leftarrow \lambda x.P(x) \wedge Q(x)\}$:

$$\dfrac{\dfrac{\vdash T \qquad T, t \in X \vdash s \in X}{t \in X \vdash s \in X}\ \text{res}}{P(t), Q(t) \vdash P(s)}\ \text{inst } \sigma$$

First, we convert the application of resolution to an application of cut, yielding the proof ψ:

$$\dfrac{\vdash T \qquad T, t \in X \vdash s \in X}{t \in X \vdash s \in X}\ \text{cut}$$

Using Lemma 2, from ψ we obtain a proof φ of $P(t), Q(t) \vdash P(s)$. For step (a), we obtain the proof $\psi_{\rightarrow}$:

$$\dfrac{\dfrac{\vdash T \qquad \dfrac{\dfrac{T, P(t), Q(t) \vdash P(s) \qquad T, P(t), Q(t) \vdash Q(s)}{T, P(t), Q(t) \vdash P(s) \wedge Q(s)}\ \wedge : r}{T, P(t) \wedge Q(t) \vdash P(s) \wedge Q(s)}\ \wedge : l}{P(t) \wedge Q(t) \vdash P(s) \wedge Q(s)}\ \text{cut}}{\vdash P(t) \wedge Q(t) \rightarrow P(s) \wedge Q(s)}\ \rightarrow : r$$

Step (b) yields the proof $\xi_{P(t)\wedge Q(t)\rightarrow P(s)\wedge Q(s)}$:

$$\dfrac{\dfrac{\dfrac{\dfrac{P(t) \vdash P(t) \qquad Q(t) \vdash Q(t)}{P(t), Q(t) \vdash P(t) \wedge Q(t)}\ \wedge : r}{\vdash P(t) \wedge Q(t), \neg P(t), \neg Q(t)}\ \neg : r \qquad \dfrac{\dfrac{P(s) \vdash P(s) \qquad Q(s) \vdash Q(s)}{P(s), Q(s) \vdash P(s) \wedge Q(s)}\ \wedge : r}{P(s) \wedge Q(s) \vdash P(s) \wedge Q(s)}\ \wedge : r}{P(t) \wedge Q(t) \rightarrow P(s) \wedge Q(s) \vdash \neg P(t), \neg Q(t), P(s) \wedge Q(s)}\ \rightarrow : l}{P(t) \wedge Q(t) \rightarrow P(s) \wedge Q(s) \vdash \neg P(t) \vee \neg Q(t) \vee (P(s) \wedge Q(s))}\ \vee : r$$

In step (c), we compute $\xi^{P(t),Q(t)\vdash P(s)}_{\text{NNF}(P(t)\wedge Q(t)\rightarrow P(s)\wedge Q(s))}$:

$$\dfrac{\dfrac{\dfrac{P(t) \vdash P(t)}{\neg P(t), P(t) \vdash}\ \neg : l \qquad \dfrac{Q(t) \vdash Q(t)}{\neg Q(t), Q(t) \vdash}\ \neg : l}{\neg P(t) \vee \neg Q(t), P(t), Q(t) \vdash}\ \vee : l \qquad \dfrac{P(s) \vdash P(s)}{P(s) \wedge Q(s) \vdash P(s)}\ \wedge : l_1}{\neg P(t) \vee \neg Q(t) \vee (P(s) \wedge Q(s)), P(t), Q(t) \vdash P(s)}\ \vee : l$$

Putting these proofs together we obtain φ:

$$\dfrac{\dfrac{\psi_{\rightarrow} \qquad \xi_{P(t)\wedge Q(t)\rightarrow P(s)\wedge Q(s)}}{\vdash \neg P(t) \vee \neg Q(t) \vee (P(s) \wedge Q(s))}\ \text{cut} \qquad \xi^{P(t),Q(t)\vdash P(s)}_{\text{NNF}(P(t)\wedge Q(t)\rightarrow P(s)\wedge Q(s))}}{P(t), Q(t) \vdash P(s)}\ \text{cut}$$

which is the desired **LKDe²**-proof of $P(t), Q(t) \vdash P(s)$ from $\mathcal{S}(\mathcal{C}, \sigma)$.

5 The CERES^2 cut-elimination method

We now define the CERES^2 method, which will turn out to be a cut-elimination method for **LKDe^2**-proofs using quantifier-free comprehension.

Definition 8. *Let (R) be a weak second-order quantifier rule*

$$\frac{A\{X \leftarrow \lambda x.F\}, \Gamma \vdash \Delta}{(\forall X)A, \Gamma \vdash \Delta}\ \forall^2 : l \qquad \frac{\Gamma \vdash \Delta, A\{X \leftarrow \lambda x.F\}}{\Gamma \vdash \Delta, (\exists X)A}\ \exists^2 : r$$

then (R) is called quantifier-free if F does not contain quantifiers. We call an **LKDe^2***-proof π a* **QFC***-proof if all its weak second-order quantifier rule applications are quantifier-free.*

Note that as we allow non-tautological axioms, it is not in general possible to eliminate all cuts. This leads to the following notion: An **LKDe^2**-proof π is called in *atomic cut normal form (ACNF)* if all cut-formulas of π are atomic.

We will now prove a lemma that shows that strong quantifiers can be removed from a sequent in a proof by replacing the corresponding variables by skolem terms. First, we define skolemization:

Definition 9. *We define the* skolemization operator sk^-. *Let F be a closed formula, then define*

$$\mathrm{sk}^-(F) = \begin{cases} F & \text{if } F \text{ does not contain strong quantifiers,} \\ \mathrm{sk}^-(F_{(Qy)}\{y \leftarrow f(x_1,\ldots,x_n)\}) & \text{if } y \in V \text{ and } (Qy) \text{ is in the scope of the weak quantifiers } (Q_1x_1),\ldots,(Q_nx_n) \text{ (appearing in this order),} \\ \mathrm{sk}^-(F_{(Qy)}\{y \leftarrow \lambda z.z \in P(x_1,\ldots,x_n)\}) & \text{if } y \in PV \text{ and } (Qy) \text{ is in the scope of the weak quantifiers } (Q_1x_1),\ldots,(Q_nx_n) \text{ (appearing in this order),} \end{cases}$$

where $F_{(Qy)}$ denotes F after omission of (Qy), f,P do not occur in F, (Qy) is a strong quantifier and if for $1 \leq i \leq n$, $\tau(x_i) = t_i$, then $\tau(P) = \iota \to t_1 \to \ldots \to t_n \to o$ and $\tau(f) = t_1 \to \ldots \to t_n \to \iota$.

This definition is made for formulas F not containing defined atoms. In the case of F containing such atoms, the definition above has to be extended in the following way: every defined atom P is replaced by a new defined atom $P^{\mu}_{x_1,\ldots,x_n}$, where $\mu \in \{+,-\}$ denotes the polarity of P in F and $x_1,\ldots,x_n$ is the list of the weakly quantified variables whose quantifiers dominate P.

In any case, let S be the closed sequent $A_1,\ldots,A_n \vdash B_1,\ldots,B_m$, and let $F \equiv (A_1 \wedge \ldots \wedge A_n) \to (B_1 \vee \ldots \vee B_m)$. If $\mathrm{sk}^-(F) \equiv (A'_1 \wedge \ldots \wedge A'_n) \to (B'_1 \vee \ldots \vee B'_m)$, then $\mathrm{sk}^-(S) = A'_1,\ldots,A'_n \vdash B'_1,\ldots,B'_m$.

Example 3. Consider the formula $F \equiv (\forall X)((\exists Y)t \in Y \rightarrow (\exists Z)(s \in Z \wedge r \in X))$, then

$$\mathrm{sk}^-(F) \equiv t \in P_2 \rightarrow ((\exists Z)s \in Z \wedge r \in P_3)$$

A path in an $\mathbf{LKDe^2}$-proof is defined in the usual way. For the replacement of a subformula B at position λ by C in A we write $A[C]_\lambda$.

Lemma 4. *Let ψ be a proof of S, then we can construct a proof of* $\mathrm{sk}^-(S)$.

Proof. This proof is based on the proof of the proposition for first-order logic in [7]. Let $S \equiv \Gamma \vdash \Delta$ and assume S contains a positive occurrence of $(\forall X)A$. Then this quantifier has been introduced in one of the following ways in ψ:

$$\text{(a)} \quad \frac{\Pi \vdash \Lambda, B}{\Pi \vdash \Lambda, B \vee C} \vee : r$$

s.t. $(\forall X)A$ occurs as a subformula of C. Let $\rho[B \vee C]$ be the path connecting $\Pi \vdash \Lambda, B \vee C$ with S. Let $A\{X \leftarrow \lambda z.z \in P(x_1, \ldots, x_n)\}$ be the subformula in $\mathrm{sk}^-(S)$ corresponding to $(\forall X)A$ in S (i.e. its skolemization). Then define $C' \equiv C[(\forall X)A(X)/A(\lambda z.z \in P(x_1, \ldots, x_n))]_\xi$, where ξ is the position of $(\forall X)A$ in C and replace $\rho[B \vee C]$ by $\rho[B \vee C']$. This will not violate any eigenvariable conditions, as $x_1, \ldots, x_n$ are all weakly quantified variables.

$$\text{(b)} \quad \frac{B, \Pi \vdash \Lambda}{B \wedge C, \Pi \vdash \Lambda} \wedge : l$$

s.t. $(\forall X)A$ occurs as a subformula of C. Analogous to (a).

$$\text{(c)} \quad \frac{\Pi \vdash \Lambda}{\Pi \vdash \Lambda, B} w : r$$

s.t. $(\forall X)A$ occurs as a subformula of B. Analogous to (a).

$$\text{(d)} \quad \frac{\Pi \vdash \Lambda}{B, \Pi \vdash \Lambda} w : r$$

s.t. $(\forall X)A$ occurs as a subformula of B. Analogous to (a).

$$\text{(e)} \quad \frac{\varphi(\Theta)}{\Pi \vdash \Lambda, A(\Theta)} \forall^2 : r$$

Let $\rho[(\forall X)A(X)]$ be the path connecting $\Pi \vdash \Lambda, (\forall X)A(X)$ with S. Let $t_1, \ldots, t_n$ be the (lambda-)terms eliminated by introductions of weak quantifiers on $\rho[(\forall X)A(X)]$ that dominate the occurrence of $(\forall X)A(X)$. We introduce a new constant predicate symbol P of appropriate type and replace $\varphi(\Theta)$ by $\varphi(\lambda z.z \in P(t_1, \ldots, t_n))$. By the eigenvariable condition on Θ, this yields a valid proof of $\Pi \vdash \Lambda, A(\lambda z.z \in P(t_1, \ldots, t_n))$ (note that $t_1, \ldots, t_n$ cannot contain eigenvariables from the proof $\varphi(\Theta)$, as they cannot be present in $\Pi \vdash \Lambda, (\forall X)A(X)$ by the eigenvariable condition and $t_1, \ldots, t_n$ occur below this sequent). We remove the $\forall^2 : r$ rule and replace $\rho[(\forall X)A(X)]$ by $\rho[A(\lambda z.z \in P(t_1, \ldots, t_n))]$. By construction, the (lambda-)terms $t_1, \ldots, t_n$ will be eliminated one-by-one by the weak quantifier introduction rules on $\rho[A(\lambda z.z \in P(t_1, \ldots, t_n))]$, the occurrence of $(\forall X)A(X)$ in S will thus become $A(\lambda z.z \in P(x_1, \ldots, x_n))$, which is exactly the corresponding occurrence in $\mathrm{sk}^-(S)$.

In all cases, we have to take contractions and definition introductions into consideration: For the latter, we replace every definition introduction rule $\mathrm{def}_P : l$ by $\mathrm{def}_{P^-_{x_1,\ldots,x_n}} : l$ and $\mathrm{def}_P : r$ by $\mathrm{def}_{P^+_{x_1,\ldots,x_n}} : r$, where $P^\mu_{x_1,\ldots,x_n}$ is the corresponding skolemized defined predicate. Regarding the former: If there are two predecessors of the form $D \equiv C[(\forall X)A(X)]$ of the occurrence of $(\forall X)A(X)$ in S s.t. there is a contraction

$$\frac{F[D], F[D]\Lambda \vdash \Pi}{F[D], \Lambda \vdash \Pi}\, c : l$$

we have to introduce the same skolem symbol for both predecessors (as otherwise the contraction can not be applied anymore).

The cases for other quantifiers are handled analogously. Note that in this transformation, all tautological initial sequents $A \vdash A$ are still tautological although their structure changes: This is due to the restriction to atomic initial sequents and the eigenvariable condition. The only part of the transformation that changes the initial sequents is (e), here initial sequents of the form $A(\alpha) \vdash A(\alpha)$ are transformed to $A(t) \vdash A(t)$ in the first-order case and initial sequents of the form $t \in \Theta \vdash t \in \Theta$ are transformed to $t \in P(t_1, \ldots, t_n) \vdash t \in P(t_1, \ldots, t_n)$ in the second-order case.

Definition 10. *Let ψ be an* **LKDe²***-proof. If all strong quantifier rules in ψ go into cuts, then ψ is said to be in* skolem form*.*

The following proposition shows that from a **QFC**-proof, we can indeed obtain a proof in skolem form. Proofs in skolem form allow the definition of proof projections by leaving out rules from the proof, as no eigenvariable violations can occur by doing so. This will be necessary to construct sound proofs in Definition 11.

Proposition 1. *For every* **QFC***-proof ψ of S there exists a* **QFC***-proof ψ' of* $\mathrm{sk}^-(S)$ *in skolem form.*

Proof. We can obtain ψ' from ψ by applying Lemma 4 to S, this yields a proof of $\mathrm{sk}^-(S)$ s.t. all strong quantifiers go into cuts, as by assumption, ψ uses quantifier-free comprehension and therefore all strong quantifier rules in ψ going into the end-sequent will be removed by skolemization.

Note that in this context, skolemization indeed does preserve validity (in contrast to what is observed in [8]), because the proposition we just stated generates a proof of the skolemized formula from a proof of the unskolemized formula. As **LKDe²** is sound, the transformation is validity preserving.

We can now define the main parts of the CERES²-method: the characteristic clause set and the set of proof projections of a proof π. The former will be always unsatisfiable and give rise to a resolution refutation, while the latter will allow the resolution refutation to be transformed into a proof of the end-sequent of π.

Definition 11. *Let π be a* **QFC***-proof in skolem form. For each rule ρ in π, we define a set of cut-free* **QFC***-proofs, the set of* projections $\mathcal{P}_\rho(\pi)$ *of π, and a set of clauses, the* characteristic clause set $\mathrm{CL}_\rho(\pi)$ *of π, at the position ρ.*

– *If ρ is an initial sequent, let $\Gamma_1 \vdash \Delta_1$ be the part of it which consists of ancestors of cut formulas, let $\Gamma_2 \vdash \Delta_2$ be the part which consists of ancestors of the end-sequent of π and define*

$$\begin{aligned}\mathcal{P}_\rho(\pi) &:= \{\Gamma_1, \Gamma_2 \vdash \Delta_2, \Delta_1\}\\ \mathrm{CL}_\rho(\pi) &:= \{\Gamma_1 \vdash \Delta_1\}.\end{aligned}$$

– *If ρ is a unary rule with immediate predecessor ρ' with $\mathcal{P}_{\rho'}(\pi) = \{\psi_1, \ldots, \psi_n\}$, distinguish:*

(a) The active formulas of ρ are ancestors of cut formulas. Then

$$\mathcal{P}_\rho(\pi) := \mathcal{P}_{\rho'}(\pi)$$

(b) The active formulas of ρ are ancestors of the end-sequent. Then

$$\mathcal{P}_\rho(\pi) := \{\rho(\psi_1), \ldots, \rho(\psi_n)\}$$

where $\rho(\psi)$ is the proof that is obtained from ψ by applying ρ to its end-sequent. Note that by assumption, all strong quantifier rules go into cuts, so ρ cannot be a strong quantifier rule, so no eigenvariable violation can occur here.

In any case, $\mathrm{CL}_\rho(\pi) := \mathrm{CL}_{\rho'}(\pi)$.

– *Let ρ be a binary rule with immediate predecessors ρ_1 and ρ_2.*

(a) If the active formulas of ρ are ancestors of cut-formulas, let $\Gamma_i \vdash \Delta_i$ be the ancestors of the end-sequent in the conclusion sequent of ρ_i and define

$$\mathcal{P}_\rho(\pi) := \mathcal{P}_{\rho_1}(\pi)^{\Gamma_2 \vdash \Delta_2} \cup \mathcal{P}_{\rho_2}(\pi)^{\Gamma_1 \vdash \Delta_1}$$

where $P^{\Gamma\vdash\Delta} := \{\psi^{\Gamma\vdash\Delta} \mid \psi \in P\}$ and $\psi^{\Gamma\vdash\Delta}$ is ψ followed by weakenings adding $\Gamma \vdash \Delta$. For the characteristic clause set, define

$$\mathrm{CL}_\rho(\pi) := \mathrm{CL}_{\rho_1}(\pi) \cup \mathrm{CL}_{\rho_2}(\pi)$$

(b) If the active formulas of ρ are ancestors of the end-sequent, then

$$\mathcal{P}_\rho(\pi) := \mathcal{P}_{\rho_1}(\pi) \times \mathcal{P}_{\rho_2}(\pi).$$

where

$$P \times Q = \{\rho(\psi, \chi) \mid \psi \in P, \chi \in Q\}$$

and $\rho(\psi, \chi)$ is the proof that is obtained from the proofs ψ and χ by applying the binary rule ρ. For the characteristic clause set, define

$$\mathrm{CL}_\rho(\pi) := \mathrm{CL}_{\rho_1}(\pi) \times \mathrm{CL}_{\rho_2}(\pi)$$

where

$$\{\Gamma_1 \vdash \Delta_1, \ldots, \Gamma_m \vdash \Delta_m\} \times \{\Pi_1 \vdash \Lambda_1, \ldots, \Pi_n \vdash \Lambda_n\} = \{\Gamma_i, \Pi_j \vdash \Delta_i, \Lambda_j \mid i \leq m, j \leq n\}.$$

The set of projections *of* π, $\mathcal{P}(\pi)$ *is defined as* $\mathcal{P}_{\rho_0}(\pi)$, *and the* characteristic clause set *of* π, $\mathrm{CL}(\pi)$ *is defined as* $\mathrm{CL}_{\rho_0}(\pi)$, *where* ρ_0 *is the last rule of* π.

Note that for the soundness of this definition, we need the assumption that π is in skolem form: if this were not the case, violations of eigenvariable conditions could appear in the projections.

Example 4. Consider the proof ψ:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{a \in \Theta \vdash a \in \Theta}{\vdash a \in \Theta, a \notin \Theta}\neg : r \quad \dfrac{b \in \Theta \vdash b \in \Theta}{b \notin \Theta, b \in \Theta \vdash}\neg : l}{b \in \Theta, a \notin \Theta \to b \notin \Theta \vdash a \in \Theta}\to : l}{b \in \Theta, (\forall X)(a \in X \to b \in X) \vdash a \in \Theta}\forall^2 : l}{(\forall X)(a \in X \to b \in X) \vdash b \in \Theta \to a \in \Theta}\to : r}{(\forall X)(a \in X \to b \in X) \vdash (\forall X)(b \in X \to a \in X)}\forall^2 : r \quad \dfrac{\dfrac{\dfrac{b \in P \vdash b \in P \qquad a \in P \vdash a \in P}{b \in P \to a \in P, b \in P \vdash a \in P}\to : l}{b \in P \to a \in P \vdash b \in P \to a \in P}\to : r}{(\forall X)(b \in X \to a \in X) \vdash b \in P \to a \in P}\forall^2 : l}{(\forall X)(a \in X \to b \in X) \vdash b \in P \to a \in P}\,cut$$

where X, Θ are predicate variables, a, b are individual constants, and P is a predicate constant. Then

$$\begin{aligned}\mathrm{CL}(\psi) &= (\{\vdash a \in \Theta\} \times \{b \in \Theta \vdash\}) \cup \{\vdash b \in P\} \cup \{a \in P \vdash\} \\ &= \{b \in \Theta \vdash a \in \Theta;\ \ \vdash b \in P;\ \ a \in P \vdash\}\end{aligned}$$

and $\mathcal{P}(\psi)$ consists of the proofs

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{a \in \Theta \vdash a \in \Theta}{\vdash a \in \Theta, a \notin \Theta}\neg : r \quad \dfrac{b \in \Theta \vdash b \in \Theta}{b \notin \Theta, b \in \Theta \vdash}\neg : l}{b \in \Theta, a \notin \Theta \to b \notin \Theta \vdash a \in \Theta}\to : l}{b \in \Theta, (\forall X)(a \in X \to b \in X) \vdash a \in \Theta}\forall^2 : l}{b \in \Theta, (\forall X)(a \in X \to b \in X) \vdash b \in P \to a \in P, a \in \Theta}w : r$$

and

$$\dfrac{\dfrac{\dfrac{a \in P \vdash a \in P}{b \in P, a \in P \vdash a \in P}w : l}{a \in P \vdash b \in P \to a \in P}\to : r}{a \in P, (\forall X)(a \in X \to b \in X) \vdash b \in P \to a \in P}w : l$$

and

$$\dfrac{\dfrac{\dfrac{b \in P \vdash b \in P}{b \in P \vdash b \in P, a \in P}w : r}{\vdash b \in P \to a \in P, b \in P}\to : r}{(\forall X)(a \in X \to b \in X) \vdash b \in P \to a \in P, b \in P}w : l$$

We will now prove the main properties of CERES^2. The following lemmas are used to establish that for **QFC**-proofs π in skolem form, we can always find an R-refutation of $\mathrm{CL}(\pi)$.

Lemma 5. *Let* $\mathcal{C}$ *be a set of clauses,* π *be a regular* **QFC***-proof of* $\vdash$ *from* $\mathcal{C}$. *Then there exists a* **QFC***-proof* ψ *of* $\vdash$ *from a set of clauses* $\mathcal{D} = \{D \mid D \in \mathcal{S}(\mathcal{C}, \sigma)$ for some quantifier-free $\sigma\}$ *such that* ψ *consists of atomic cuts, contractions and permutations.*

Proof. As we know from e.g. [9], reductive cut-elimination in second-order logic terminates, so we can apply it to π to eliminate all non-atomic cuts and obtain a proof π' of $\vdash$. First, note that π' consists of atomic cut, contraction and permutation: weakening is automatically eliminated by cut-elimination. Denote the set of initial sequents of a proof φ by $init(\varphi)$. We will show that π' can be transformed into a proof ψ s.t. $init(\psi)$ consists of quantifier-free instances of clauses in $\mathcal{C}$. We can then take $\mathcal{D}$ as $init(\psi)$. We proceed by induction on the cut-elimination of π to obtain π'. As induction invariant, we take the following: π' can be transformed into a **QFC**-proof ψ s.t. $init(\psi)$ consists of quantifier-free instances of clauses in $\mathcal{C}$.

For the base case, we take $\psi = \pi$, so as $init(\pi) = init(\psi)$ and π uses quantifier free comprehension, the invariant holds.

1. The cut-eliminiation performs a rank reduction on π. Then the initial sequents of π and π' coincide, except when performing rank reduction over a contraction: Here, we perform adequate renamings of eigenvariables in π' to keep regularity and take $\psi = \pi'$. Clearly, $init(\psi)$ consists of $init(\pi)$ together with some renamed variants of clauses in $init(\pi)$, and the lambda terms of the weak second-order quantifier rules are not changed, so the proposition holds.
2. The cut-elimination performs a grade reduction on φ. Distinguish:
   (a) The grade reduction is performed on propositional rules. $init(\pi)$ and $init(\pi')$ coincide and we take $\psi = \pi'$, still the lambda terms of the weak second-order quantifier rules are not changed.
   (b) The grade reduction is performed on first-order quantifier rules. Let $x \leftarrow t$ be the substitution that is applied by the cut-elimination, then by regularity $init(\pi') = init(\pi)\{x \leftarrow t\}$. Again we take $\psi = \pi'$ and note that no quantifiers are introduced in any lambda terms of weak second-order quantifier rules, so the proposition holds.
   (c) The grade reduction is performed on second-order quantifier rules. Let $\sigma = \{X \leftarrow \lambda x.F\}$ be the substitution that is applied by the cut-elimination. By (IH), σ is quantifier-free. Let $init(\pi) = \{\Gamma_1 \vdash \Delta_1, \ldots, \Gamma_n \vdash \Delta_n\}$. Then

$$init(\pi') = \{(\Gamma_1 \vdash \Delta_1)\sigma, \ldots, (\Gamma_n \vdash \Delta_n)\sigma\}.$$

   By Lemma 1, for every $1 \leq i \leq n$, we have a proof of $(\Gamma_i \vdash \Delta_i)\sigma$ from $\mathcal{S}(\{\Gamma_i \vdash \Delta_i\}, \sigma)$. Take ψ to be π' where those leafs are replaced by the respective proofs, then

$$init(\psi) = \mathcal{S}(\{\Gamma_1 \vdash \Delta_1\}, \sigma) \cup \ldots \cup \mathcal{S}(\{\Gamma_n \vdash \Delta_n\}, \sigma)$$

   and the first part of the proposition holds. For the second part, note that as σ is quantifier-free and no new second-order quantifier rules are introduced in this step, all second-order quantifier rules are still quantifier-free.

Lemma 6. *Let π be a* **QFC***-proof in skolem form. Then there exists an R-refutation of* $\mathrm{CL}(\pi)$.

Proof. Analogous to the proof of unsatisfiability of $\mathrm{CL}(\pi)$ for first-order logic in [3] by removing all rules of π except the ancestors of the cuts, and removing all formula occurrences in π except the ancestors of cuts, we construct a **QFC**-proof ψ of $\vdash$ from $\mathrm{CL}(\pi)$. We apply Lemma 5 to obtain a **QFC**-proof γ of $\vdash$ from quantifier-free instances of $\mathrm{CL}(\pi)$ using atomic cut, contraction and permutation only. γ readily gives rise to an R-refutation of $\mathrm{CL}(\pi)$: First, derive the necessary instances used in γ from $\mathrm{CL}(\pi)$ using instantiation, then, whenever atomic cuts are used in γ, apply resolution, and whenever contractions are used in γ, apply p-reduction.

We are now ready to define the CERES^2 method and state our central result.

Definition 12. *Let π be a* **QFC***-proof of S. Then the* CERES^2 *method is the following algorithm:*

1. *Compute a* **QFC***-proof π_{sk} of* $\mathrm{sk}^-(S)$.
2. *Compute* $\mathrm{CL}(\pi_{sk})$, $\mathcal{P}(\pi_{sk})$.
3. *Compute an R-refutation γ of* $\mathrm{CL}(\pi_{sk})$.
4. *Convert γ into an* **LKDe²***-proof γ' of $\vdash$ from* $\mathrm{CL}(\pi_{sk})$.
5. *Plug instances of the proofs in $\mathcal{P}(\pi_{sk})$ into the leaves of γ' to obtain a proof ψ of* $\mathrm{sk}^-(S)$ *containing quantifier-free cuts only.*
6. *Perform quantifier-free cut-elimination on ψ to obtain a proof φ of* $\mathrm{sk}^-(S)$ *containing no non-atomic cuts.*

Let us remark here that in step 6, any method for cut-elimination for quantifier-free cuts can be used (e.g. reductive methods, "zero-th order" CERES). Furthermore, considering that the instantiations of quantifiers are the core information in a proof, one can even leave out this step as the instantiations in φ and ψ coincide.

Theorem 1. *Let π be a* **QFC***-proof of S. Then the* CERES^2 *method transforms π into an* **LKDe²***-proof φ of* $\mathrm{sk}^-(S)$ *such that φ is in atomic-cut normal form.*

Proof. Using Proposition 1, we convert π to π_{sk}. By Lemma 6, we can compute an R-refutation γ of $\mathrm{CL}(\pi_{sk})$. By Lemma 3, from γ we can construct an **LKDe²**-refutation γ' of $\mathrm{CL}(\pi_{sk})$. Every initial sequent of γ' is either a sequent $A \vdash A$, an axiom, or an instance C^* of some $C \in \mathrm{CL}(\pi_{sk})$ under a substitution σ. Let $C \equiv \Pi \vdash \Lambda$ and $\mathrm{sk}^-(S) \equiv \Gamma \vdash \Delta$, then by Definition 11 we have a cut-free **QFC**-proof ψ_C of $\Gamma, \Pi \vdash \Lambda, \Delta$. Let $C^* \equiv \Pi^* \vdash \Lambda^*$, then by Lemma 2, we can construct **LKDe²**-proofs ψ_{C^*} of $\Gamma, \Pi^* \vdash \Lambda^*, \Delta$ that contain quantifier-free cuts only. By plugging these proofs onto the leaves of γ' and adding contractions at the end, we obtain an **LKDe²**-proof of $\Gamma \vdash \Delta$ containing quantifier-free cuts only. By applying cut-elimination to this proof, we obtain the desired proof φ.

5.1 Extending CERES^2

This work defines a method for cut-elimination for **QFC**-proofs. A natural question is then, whether the method can be extended to stronger comprehension. In the previous section, it was stated that skolemization is an important technical tool in the context of the method, as it removes strong quantifier introduction rules and because of this allows the definition of proof projections without causing violations of eigenvariable conditions.

When considering comprehension involving quantifiers, proof skolemization has to be modified to achieve the same effect: it is not enough to skolemize the end-sequent, as strong quantifier rules may go into weak second-order quantifier rules and therefore, the corresponding strong quantifiers will not be present in the end-sequent.

A tempting idea is, then, to simply skolemize the formulas that disappear into weak second-order quantifier rules. This motivates the following definitions:

Definition 13. *Let (R) be a weak second-order quantifier rule*

$$\frac{A', \Gamma \vdash \Delta}{(\forall X)A, \Gamma \vdash \Delta}\, \forall^2 : l\ \lambda x.F$$

and let A^* be the formula obtained from A' by skolemizing the strong quantifiers that are eliminated by (R). (R) is called skolemizable *if there exists a formula F^* such that*

$$\frac{A^*, \Gamma \vdash \Delta}{(\forall X)A, \Gamma \vdash \Delta}\, \forall^2 : l\ \lambda x.F^*$$

is a valid rule application. For $\exists^2 : r$ the definition is analogous.

Definition 14. *An* **LKDe^2***-proof ψ is called* skolemizable *if all weak second-order quantifier rules occurring in ψ that go into the end-sequent are skolemizable.*

Example 5. The following proof is not skolemizable:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(\beta,a)\vdash P(\beta,a)}{(\forall x)P(x,a)\vdash P(\beta,a)}\forall:l}{(\forall x)P(x,a)\vdash(\forall z)P(z,a)}\forall:r \quad \dfrac{\dfrac{P(\alpha,b)\vdash P(\alpha,b)}{(\forall z)P(z,b)\vdash P(\alpha,b)}\forall:l}{(\forall z)P(z,b)\vdash(\forall x)P(x,b)}\forall:r}{(\forall x)P(x,a),(\forall z)P(z,a)\to(\forall z)P(z,b)\vdash(\forall x)P(x,b)}\to:l}{(\forall x)P(x,a),(\forall X)(X(a)\to X(b))\vdash(\forall x)P(x,b)}\forall^2:l\ \lambda x.(\forall z)P(z,x)}{(\forall X)(X(a)\to X(b))\vdash(\forall x)P(x,a)\to(\forall x)P(x,b)}\to:r$$

Skolemization of the proof would yield

$$\dfrac{\dfrac{\dfrac{\dfrac{P(s_2,a)\vdash P(s_2,a)}{(\forall x)P(x,a)\vdash P(s_2,a)}\forall:l \quad \dfrac{P(s_1,b)\vdash P(s_1,b)}{(\forall z)P(z,b)\vdash P(s_1,b)}\forall:l}{(\forall x)P(x,a), P(s_2,a)\to(\forall z)P(z,b)\vdash P(s_1,b)}\to:l}{(\forall x)P(x,a), (\forall X)(X(a)\to X(b))\vdash P(s_1,b)}\forall^2:l\ \lambda x.(\forall z)P(z,x)}{(\forall X)(X(a)\to X(b))\vdash (\forall x)P(x,a)\to P(s_1,b)}\to:r$$

where the $\forall^2 : l$ rule application is clearly not sound.

Example 6. Proofs that use induction with an induction invariant that contains quantifiers (where the induction goes into the end-sequent) are not skolemizable. Take for example the proof

$$\dfrac{\Gamma, (\forall z)G(z,0)\wedge(\forall x)((\forall z)G(z,x)\to(\forall z)G(z,x'))\to(\forall x)(\forall z)G(z,x)\vdash\Delta}{\Gamma,(\forall X)(X(0)\wedge(\forall x)(X(x)\to X(x'))\to(\forall x)X(x))\vdash\Delta}\forall^2:l$$

where $A \equiv X(0)\wedge(\forall x)(X(x)\to X(x'))\to(\forall x)X(x)$. Here, X occurs in two polarities in A and $F \equiv \lambda x.(\forall z)G(z,x)$ contains quantifiers. Then

$$A^* \equiv G(s_1,0)\wedge(\forall x)((\forall z)G(z,x)\to G(s_2,x'))\to(\forall x)(\forall z)G(z,x)$$

and does not admit the introduction of the weak second-order quantifier.

We will now give a syntactic characterization of the skolemizable rules. For this, we need some definitions.

Definition 15. *Let X be a predicate variable and F be a formula. We say that X is* linear *in F if the number of occurrences of X in F is < 2. Let X be linear in F, then we call X* restricted *in F if*

1. *no weak quantifier dominates X or*
2. *exactly one weak quantifier (Qx) dominates X and X occurs as $x \in X$.*

Definition 16. *Let $(Qx)F$ be a quantified formula. The occurrence of (Qx) is called* non-dummy *if F contains x.*

Proposition 2. *Let (R) be a second-order quantifier rule as in Definition 13. (R) is skolemizable iff either*

1. *X is linear in A and if F contains non-dummy strong quantifiers w.r.t. $A\{X \leftarrow \lambda x.F\}$ then X is restricted in A or*
2. *X occurs only positively (negatively) in A and all non-dummy quantifier occurrences in F are weak (strong) quantifiers or*
3. *F does not contain non-dummy quantifiers.*

Proof. (R) is

$$\dfrac{A\{X\leftarrow\lambda x.F(x)\},\Gamma\vdash\Delta}{(\forall X)A,\Gamma\vdash\Delta}\forall^2:l$$

First, we will show that the given criteria imply skolemizability of (R). We will define the formula F^* that will be used for the rule application

$$\frac{A^*, \Gamma \vdash \Delta}{(\forall X)A, \Gamma \vdash \Delta}\ \forall^2 : l\ \lambda x.F^*$$

Either:

1. X is linear in A and if $F(x)$ contains non-dummy strong quantifiers w.r.t. $A\{X \leftarrow \lambda x.F\}$ then X is restricted in A. If X does not occur in A, then there is nothing to show, so assume X occurs as $t \in X$ at position ξ in A. Then $A\{X \leftarrow \lambda x.F(x)\} \equiv A[F(t)]_\xi$ and $A^* \equiv A[F'(t)]_\xi$ where $F'(t)$ is the skolemization of $F(t)$ in A. If F does not contain non-dummy strong quantifiers w.r.t. $A\{X \leftarrow \lambda x.F\}$, then $F'(t)$ is just $F(t)$ after dropping some quantifiers, and we can use $F^* \equiv F'(x)$. Otherwise, distinguish the cases
   (a) No weak quantifier dominates X. Then $F'(t)$ only contains variables that occur in $F(t)$, so $F'(t)$ does not contain any variable that is bound in A, therefore we may use $F^* \equiv F'(x)$.
   (b) Exactly one weak quantifier (Qz) dominates X and $t \equiv z$. We set $F^* \equiv F'(t)\{z \leftarrow x\}$, then $A\{X \leftarrow \lambda x.F^*\} \equiv A[F'(t)]_\xi$ and again F^* does not contain any variable that is bound in A.
2. X occurs only positively in A and all non-dummy quantifiers in $F(x)$ are weak. Then the skolemization of $F(x)$ in $A\{X \rightarrow \lambda x.F(x)\}$, call it $F'(x)$, is just $F(x)$ after dropping some empty strong quantifiers and we may use $F^* \equiv F'(x)$.
3. X occurs only negatively in A and all non-dummy quantifiers in $F(x)$ are strong. Analogous to the previous case.
4. $F(x)$ only contains empty quantifiers. Analogous to the previous cases.

For the other direction, we show that if the given criteria are not fulfilled, then (R) is not skolemizable. We proceed with a proof by contradiction. We may assume that F contains non-dummy quantifiers. We distinguish the cases

1. X is not linear in A. Assume X occurs at positions η_1,η_2 in A as $t_1 \in X$, $t_2 \in X$. Then at positions η_1, η_2 in $A\{X \leftarrow \lambda x.F\}$ we have subformula occurrences of $F(t_1)$, $F(t_2)$. There are the following subcases:
   (a) X occurs positively in A and F contains non-dummy strong quantifiers. Then the occurrences of $F(t_1)$, $F(t_2)$ are positive. F contains non-dummy strong quantifiers, so at the same relative positions in the skolemizations of $F(t_1)$, $F(t_2)$ we have skolem terms with different head symbols, say f_1, f_2. F^* cannot contain two terms with different heads at the same position, so they must be introduced in A^* by substitution when applying $\lambda x.F^*$ to t_1, t_2. But t_1, t_2 cannot contain f_1, f_2, because they are fresh symbols, and we arrive at a contradiction.
   (b) X occurs negatively in A and F contains non-dummy weak quantifiers. Analogous to the previous case.
   (c) F contains non-dummy strong and weak quantifiers. As X occurs in A, it does so either positively or negatively, so one of the above cases applies.

(d) X occurs positively and negatively in A. As F contains non-dummy quantifiers, it either contains strong or weak ones, so one of the above cases applies.

2. F contains non-dummy strong quantifiers w.r.t. $A\{X \leftarrow \lambda x.F\}$ and there are weak quantifiers dominating X in A and either
   (a) more than one weak quantifier dominates X or
   (b) exactly one quantifier (Qz) dominates X and X does not occur as $z \in X$ in A.

   Regarding (2a): Assume X occurs at position η as $t \in X$ in A, then at position η in $A\{X \leftarrow \lambda x.F\}$ we have the formula $F(t)$ that is dominated by more than one weak quantifier, say among them are (Qx_1), (Qx_2). F contains strongly quantified variables, so its skolemization will contain a skolem term $f(\ldots, x_1, \ldots, x_2, \ldots)$. F^* must not contain variables that are quantified in A, so x_1, x_2 must be introduced in f by substitution when applying $\lambda x.F^*$. But f is a new function symbol, so t cannot contain f, so if t contains both x_1 and x_2, then it has at the head some function symbol g, but the function symbol in the skolemization of F that is directly above x_1, x_2 is f, so we arrive at a contradiction.
   Regarding (2b): We may assume that exactly one weak quantifier dominates X. Let X occur at position η in A. Then X occurs as $t \in X$ with $t \neq z$. F contains non-dummy strong quantifiers w.r.t. $A\{X \leftarrow \lambda x.F\}$, so in the skolemization of F in $A\{X \leftarrow \lambda x.F\}$, there will be a skolem term $f(z, \ldots)$. In A, z is bound, so z must be introduced in f by substitution when applying $\lambda x.F^*$. But $t \neq z$, so if t contains z, it will be below some function symbol g, but z is directly below f, so we again have a contradiction.

For $\exists^2 : r$ the proof is symmetric.

Clearly, the class of skolemizable proofs includes the class of **QFC**-proofs, but it is not much larger.

So in extending the CERES^2 method to stronger comprehension, we will have to develop new techniques for dealing with projections containing strong quantifier rules. A promising approach is to use strong quantifier rules which introduce a quantifier not from a free variable but from a skolem term as in [8].

6 CERES^2 Example

We will now apply the CERES^2 method to a **QFC**-proof φ. The proof under consideration is a proof of the theorem $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$ by the least number principle. As axioms the proof uses the following axioms of arithmetic:

$$\begin{array}{ll}
\vdash x * 0 = 0, & \vdash 0 * x = 0, \\
\vdash x * y = y * x, & \vdash x + y = y + x, \\
\vdash x + (y + z) = (x + y) + z, & \vdash (x + y) + z = x + (y + z), \\
\vdash x * 1 = x, & \vdash x * (y + 1) = x + x * y, \\
\vdash x = x, & \vdash x * (y + z) = x * y + x * z
\end{array}$$

where x, y, z are arbitrary terms, and the following axioms that represent the recursive definition of the series:

$$\vdash \Sigma(n+1) = \Sigma(n) + (n+1) \; ; \vdash \Sigma(0) = 0$$

For the following, we define $2 \equiv 1+1$. In the proof, $\star$ denotes the ancestors of a cut, double lines indicate applications of propositional rules, and structural rules except cut are omitted.

$\varphi :=$

$$\dfrac{\begin{array}{cc} \varphi_1 & \varphi_2 \\ \vdots & \vdots \\ LNP \vdash IND^\star & IND^\star \vdash (\forall n) 2 * \Sigma(n) = n * (n+1) \end{array}}{LNP \vdash (\forall n) 2 * \Sigma(n) = n * (n+1)}\, cut$$

where

$$LNP \equiv (\forall Y)((\exists z) z \in Y \rightarrow 0 \in Y \vee (\exists z)(z \notin Y \wedge z+1 \in Y))$$
$$IND \equiv (\forall X)(0 \in X \wedge (\forall y)(y \in X \rightarrow y+1 \in X) \rightarrow (\forall y) y \in X)$$

This proof uses the fact that the least number principle implies induction as a lemma; the use of this lemma will be removed by application of the CERES^2 method, yielding a new proof that shows that the least number principle implies the theorem, without the use of induction.

The proof φ_1 specified below is exactly the proof of this lemma, and it is a formalization of the following argument: Assume the least number principle, and assume that for an arbitrary set $\mathcal{X}$, $0 \in \mathcal{X}$ and if $y \in \mathcal{X}$, then $y+1 \in \mathcal{X}$, and assume for contradiction that $\mathcal{X} \neq \mathbb{N}$. Then the set $\bar{\mathcal{X}} = \{x \mid x \notin \mathcal{X}\}$ (or $\lambda x.x \notin X$ in the lambda notation) is not empty, so by the least number principle either

1. $0 \in \bar{\mathcal{X}}$. But $0 \in \mathcal{X}$ by assumption, so $0 \notin \bar{\mathcal{X}}$.
2. There is a z s.t. $z \notin \bar{\mathcal{X}}$ and $z+1 \in \bar{\mathcal{X}}$. But then $z \in \mathcal{X}$ and by assumption $z+1 \in \mathcal{X}$, so $z+1 \notin \bar{\mathcal{X}}$.

So φ_1 is

$$\dfrac{\dfrac{\dfrac{\dfrac{y_0 \in X_0 \vdash y_0 \in X_0^\star}{\vdash (\forall y) y \in X_0^\star, (\exists z) z \notin X_0}\, \forall : r, \exists : r \qquad \varphi_1^1}{0 \in X_0^\star, (\forall y)(y \in X_0 \rightarrow y+1 \in X_0)^\star, LNP_\sigma \vdash (\forall y) y \in X_0^\star}\, \rightarrow : l}{LNP \vdash 0 \in X_0 \wedge (\forall y)(y \in X_0 \rightarrow y+1 \in X_0) \rightarrow (\forall y) y \in X_0^\star}\, \forall^2 : l\ \lambda x.x \notin X_0}{LNP \vdash IND^\star}\, \forall^2 : r$$

where

$$LNP_\sigma \equiv (\exists z) z \notin X_0 \rightarrow 0 \notin X_0 \vee (\exists z)(\neg z \notin X_0 \wedge z+1 \notin X_0)$$

The proof φ_1^1 is

$$\dfrac{\dfrac{}{0 \in X_0^\star \vdash 0 \in X_0}}{\dfrac{}{0 \in X_0^\star, 0 \notin X_0 \vdash}\,\neg : l} \qquad \dfrac{\dfrac{\dfrac{}{z_0 \in X_0 \vdash z_0 \in X_0^\star} \qquad \dfrac{}{z_0 + 1 \in X_0^\star \vdash z_0 + 1 \in X_0}}{z_0 \in X_0 \to z_0 + 1 \in X_0^\star, \neg z_0 \notin X_0 \wedge z_0 + 1 \notin X_0 \vdash}}{(\forall y)(y \in X_0 \to y + 1 \in X_0)^\star, (\exists z)(\neg z \notin X_0 \wedge z + 1 \notin X_0) \vdash}\,\exists, \forall : l$$

$$\dfrac{}{0 \in X_0^\star, (\forall y)(y \in X_0 \to y + 1 \in X_0)^\star, 0 \notin X_0 \vee (\exists z)(\neg z \notin X_0 \wedge z + 1 \notin X_0) \vdash}\,\vee : l$$

This completes the left hand side of the cut, showing that the least number principle implies induction. The right hand side of the cut is a formalization of the following induction proof of $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$: The induction base is trivial. For the induction step we want to show

$$\sum_{i=0}^{n+1} i = n + 1 + \sum_{i=0}^{n} i = \frac{(n+1)((n+1)+1)}{2}$$

By the induction hypothesis this reduces to showing

$$n + 1 + \frac{n(n+1)}{2} = \frac{(n+1)((n+1)+1)}{2}$$

which clearly holds.

The formalization of this argument is the proof φ_2:

$$\dfrac{\varphi_2^1 \qquad \dfrac{\dfrac{}{2 * \Sigma(n_0) = n_0 * (n_0 + 1)^\star \vdash 2 * \Sigma(n_0) = n_0 * (n_0 + 1)}}{(\forall x) 2 * \Sigma(x) = x * (x + 1)^\star \vdash (\forall n) 2 * \Sigma(n) = n * (n + 1)}\,\forall : r, \forall : l}{\dfrac{}{IND_\sigma^\star \vdash (\forall n) 2 * \Sigma(n) = n * (n + 1)}\,\forall^2 : l\ \lambda x. 2 * \Sigma(x) = x * (x + 1)}\,\to : l$$

where

$$IND_\sigma \equiv 2 * \Sigma(0) = 0 * (0 + 1) \wedge (\forall x)(2 * \Sigma(x) = x * (x + 1) \to 2 * \Sigma(x + 1) = (x + 1) * ((x + 1) + 1)) \to (\forall x) 2 * \Sigma(x) = x * (x + 1)$$

We continue with φ_2^1 — from this point on, we will omit $\star$ as all formula occurrences in the following proofs are cut ancestors:

$$\dfrac{\dfrac{\dfrac{}{\vdash \Sigma(0) = 0} \qquad \dfrac{\dfrac{}{\vdash 2 * 0 = 0} \qquad \dfrac{}{\vdash 0 = 0 * (0 + 1)}}{\vdash 2 * 0 = 0 * (0 + 1)}\,=: r_2}{\vdash 2 * \Sigma(0) = 0 * (0 + 1)}\,=: r_2 \qquad \varphi_2^2}{\vdash 2 * \Sigma(0) = 0 * (0 + 1) \wedge (\forall x)(2 * \Sigma(x) = x * (x + 1) \to 2 * \Sigma(x + 1) = (x + 1) * ((x + 1) + 1))}\,\wedge$$

Note that the left branch of φ_2^1 proves the induction base. The proof φ_2^2 will in turn show the induction step:

$$\dfrac{\dfrac{\dfrac{}{\vdash \Sigma(x_0 + 1) = \Sigma(x_0) + (x_0 + 1)} \qquad \varphi_1^=}{2 * \Sigma(x_0) = x_0 * (x_0 + 1) \vdash 2 * \Sigma(x_0 + 1) = (x_0 + 1) * ((x_0 + 1) + 1)}\,=: r_2}{\vdash (\forall x)(2 * \Sigma(x) = x * (x + 1) \to 2 * \Sigma(x + 1) = (x + 1) * ((x + 1) + 1))}\,\forall : r$$

We apply the distributivity of multiplication in $\varphi_1^=$:

$$\dfrac{\dfrac{}{\vdash 2 * (\Sigma(x_0) + (x_0 + 1)) = (2 * \Sigma(x_0) + 2 * (x_0 + 1))} \qquad \varphi_2^=}{2 * \Sigma(x_0) = x_0 * (x_0 + 1) \vdash 2 * (\Sigma(x_0) + (x_0 + 1)) = (x_0 + 1) * ((x_0 + 1) + 1)}\,=: r_2$$

and apply the induction hypothesis to the equation in $\varphi_2^{=}$:

$$\dfrac{\begin{array}{c}\varphi_3^{=}\\ \vdots\end{array}}{\dfrac{A \vdash A \qquad \vdash x_0 * (x_0+1) + 2 * (x_0+1) = (x_0+1) * ((x_0+1)+1)}{2 * \Sigma(x_0) = x_0 * (x_0+1) \vdash 2 * \Sigma(x_0) + 2 * (x_0+1) = (x_0+1) * ((x_0+1)+1)}} =: r_2$$

where $A \equiv 2 * \Sigma(x_0) = x_0 * (x_0+1)$. For lack of space we will not exhibit the proof $\varphi_3^{=}$, it is easy to see that it can be constructed using the axioms given above and equality rules. This completes the proof φ.

Skolemization of φ yields a proof φ_{sk} of the sequent

$$(\forall Y)((\exists z) z \in Y \rightarrow 0 \in Y \vee (f(Y) \notin Y \wedge f(Y)+1 \in Y)) \vdash 2 * \Sigma(s) = s * (s+1)$$

where f, s are the skolem symbols. In the proof, the skolem term $f(\lambda x.x \notin X_0)$ replaces the eigenvariable z_0 and the skolem term s replaces the eigenvariable n_0.

Remark 1. In all models of arithmetic and the left hand side of the sequent, a suitable interpretation of f will be a function $\gamma : P(\mathbb{N}) \mapsto \mathbb{N}$ such that for all $S \in P(\mathbb{N})$ with $S \neq \emptyset, 0 \notin S$, we have $\gamma(S) = \min(S) - 1$. This is an example for the natural interpretation of skolem symbols, which in practice is often possible.

The characteristic clause set $\mathrm{CL}(\varphi_{sk})$ can be written as:

$$\mathrm{CL}(\varphi_{sk}) = \mathrm{CL}(\varphi_{sk}^1) \cup \mathrm{CL}(\varphi_{sk}^2)$$

$$\begin{aligned}\mathrm{CL}(\varphi_{sk}^1) = &(\{0 \in X_0 \vdash\} \times \{\vdash f(\lambda x.x \notin X_0) \in X_0; f(\lambda x.x \notin X_0)+1 \in X_0\})\\ &\times \{\vdash y_0 \in X_0\}\end{aligned}$$

$$\begin{aligned}\mathrm{CL}(\varphi_{sk}^2) = &\{2 * \Sigma(s) = s * (s+1) \vdash\} \cup \{\vdash \Sigma(x_0+1) = \Sigma(x_0) + (x_0+1)\}\\ &\cup \{2 * \Sigma(x_0) = x_0 * (x_0+1) \vdash 2 * \Sigma(x_0) = x_0 * (x_0+1)\}\\ &\cup \{\vdash \Sigma(0) = 0\} \cup PAX_S\end{aligned}$$

where PAX_S is the set of axioms of arithmetic that are used in the proof φ_2^1. Modulo subsumption and tautology deletion, the characteristic clause set is:

$$\begin{aligned}CL(\varphi_{sk}) = \{\ & 0 \in X_0 \vdash f(\lambda x.x \notin X_0) \in X_0, y_0 \in X_0; && (I1)\\ & 0 \in X_0, f(\lambda x.x \notin X_0)+1 \in X_0 \vdash y_0 \in X_0; && (I2)\\ & 2 * \Sigma(s) = s * (s+1) \vdash; && (T1)\\ & \vdash \Sigma(x_0+1) = \Sigma(x_0) + (x_0+1); && (S1)\\ & \vdash \Sigma(0) = 0\} && (S2)\\ & \cup PAX'_S\end{aligned}$$

where PAX'_S is PAX_S after subsumption and tautology deletion.

6.1 Refutation of the characteristic clause set

We now define a resolution refutation of the characteristic clause set $CL(\varphi_{sk})$, using the resolution calculus from Section 4.

The clauses $(I1)$ and $(I2)$ correspond to the induction axiom, while the clause $(T1)$ is the negated theorem. For the refutation we will need the following instances of the induction clauses produced from the substitution $\sigma = \langle\{y_0 \leftarrow s\}, \{X_0 \leftarrow \lambda x.2 * \Sigma(x) = x * (x + 1)\}\rangle$:

$$(I1')\ 2 * \Sigma(0) = 0 * (0 + 1) \vdash 2 * \Sigma(f(T)) = f(T) * (f(T) + 1), 2 * \Sigma(s) = s * (s + 1)$$

$$(I2')\ 2 * \Sigma(0) = 0 * (0 + 1), 2 * \Sigma(f(T) + 1) = (f(T) + 1) * ((f(T) + 1) + 1) \vdash 2 * \Sigma(s) = s * (s + 1)$$

where $T \equiv \lambda x.\neg 2 * \Sigma(x) = x * (x + 1)$. We start by deriving the induction base using resolution, for this we need the clauses

$$(A1) \vdash 2 * 0 = 0\ ;\ (A2) \vdash 0 = 0 * (0 + 1)$$

Note that $(A1), (A2) \in PAX_S$. We now use paramodulation from $(S2)$ into $(A1)$ to derive

$$(IB1) \vdash 2 * \Sigma(0) = 0$$

Paramodulation from $(IB1)$ into $(A2)$ then yields

$$(IB) \vdash 2 * \Sigma(0) = 0 * (0 + 1)$$

We now resolve both $(I1')$ and $(I2')$ first with (IB) and then with $(T1)$ to obtain

$$(IH) \vdash 2 * \Sigma(f(T)) = f(T) * (f(T) + 1)$$
$$(IG)\ 2 * \Sigma(f(T) + 1) = (f(T) + 1) * ((f(T) + 1) + 1) \vdash$$

Note that (IH) corresponds to the induction hypothesis in the original proof, while (IG) is the negation of what was proved in the induction step. Towards a contradiction, we paramodulate (IG) with an instance of the second part of the definition of the series, $(S1)$, and get

$$(C1)\ 2 * (\Sigma(f(T)) + (f(T) + 1)) = (f(T) + 1) * ((f(T) + 1) + 1) \vdash$$

From clauses from PAX_S, it is easy to derive (using paramodulation exclusively) the clause

$$(C2) \vdash 2 * (\Sigma(x_0) + (x_0 + 1)) = 2 * \Sigma(x_0) + 2 * (x_0 + 1)$$

Paramodulation from an instance of $(C2)$ into $(C1)$ yields

$$(C3)\ 2 * \Sigma(f(T)) + 2 * (f(T) + 1) = (f(T) + 1) * ((f(T) + 1) + 1) \vdash$$

We can now use paramodulation to obtain from $(C3)$ and (IH) the clause

$$(C4)\ (f(T) * (f(T)+1)) + 2 * (f(T)+1) = (f(T)+1) * ((f(T)+1)+1) \vdash$$

which is a wrong arithmetical statement. From clauses in PAX_S it is now easy to derive the dual clause (modulo substitution)

$$(C5) \vdash x_0 * (x_0+1) + 2 * (x_0+1) = (x_0+1) * ((x_0+1)+1)$$

We can now resolve $(C4)$ with an instance of $(C5)$ to obtain the empty sequent and complete the refutation. Note that although the clauses used in the refutation correspond to the induction axiom, the proof constructed from the refutation will be a proof by the least number principle. This will become clear in the next section.

6.2 Interpretation of the ACNF

By the construction of the projections, the end-sequent of every projection contains the end-sequent of φ_{sk}. When combining the projections, we insert contractions at the end of the proof to contract the multiple occurrences of formulas introduced in this way. To ease the presentation of the ACNF, we drop weakenings that are later contracted in this way as they are redundant.

Additionally, the construction given in Lemma 2 leads to trivial cuts, as all the instances used in the refutation come from substitutions that do not contain logical connectives, which means that the transformation to clause form is trivial. These cuts are also left out in the following. Again, we will simply omit structural rules other than cut in the presentation.

We use the following abbreviations:

$$\begin{array}{ll} A(x) & \equiv 2 * \Sigma(x) = x * (x+1) \\ A'(x) & \equiv 2 * \Sigma(x) \neq x * (x+1) \\ T & \equiv \lambda x.A'(x) \\ TH^{sk} & \equiv A(s) \\ LNP^{sk} & \equiv (\forall Y)((\exists z) z \in Y \rightarrow 0 \in Y \vee (f(Y) \notin Y \wedge f(Y)+1 \in Y)) \end{array}$$

LNP^{sk} expresses that for all sets $\mathcal{Y}$, if $\mathcal{Y}$ is not empty, then either 0 is in $\mathcal{Y}$ or the function f is such that $f(\mathcal{Y})$ is the predecessor of the least element of $\mathcal{Y}$.

With this in mind, we now give the $\mathbf{LKDe^2}$-proof ψ from step 5 in Definition 12 with regard to φ_{sk}, proceeding in a top-down way and alternating the formal proof parts with their respective informal interpretations.

$\varphi[(I1')] :=$

$$\dfrac{\dfrac{\dfrac{\dfrac{TH^{sk} \vdash TH^{sk}}{\vdash \neg TH^{sk}, TH^{sk}}\neg : r}{\vdash (\exists z)A'(z), TH^{sk}}\exists : r \qquad \dfrac{\dfrac{A(0) \vdash A(0)}{A(0), A'(0) \vdash}\neg : l \qquad \dfrac{\dfrac{A(f(T)) \vdash A(f(T))}{\neg A'(f(T)) \vdash A(f(T))}\neg : l, \neg : r}{\neg A'(f(T)) \wedge A'(f(T)+1) \vdash A(f(T))}\wedge : l_1}{A(0), A'(0) \vee (\neg A'(f(T)) \wedge A'(f(T)+1)) \vdash A(f(T))}\vee : l}{A(0), ((\exists z)A'(z) \rightarrow (A'(0) \vee (\neg A'(f(T)) \wedge A'(f(T)+1)))) \vdash TH^{sk}, A(f(T))}\rightarrow : l}{A(0), LNP^{sk} \vdash TH^{sk}, A(f(T))}\forall^2 : l\ \lambda x.A'(x)$$

Let $\mathcal{X} = \{x \mid A'(x)\}$ and $\bar{\mathcal{X}} = \{x \mid A(x)\}$ (note that $\mathcal{X}$ is the informal counterpart to T, and $s \in \bar{\mathcal{X}}$ is the informal version of the theorem). $\varphi[(I1')]$ shows that, assuming $0 \in \bar{\mathcal{X}}$ and LNP^{sk}, then either $s \in \bar{\mathcal{X}}$ or $f(\mathcal{X}) \in \bar{\mathcal{X}}$. It proceeds by the following case distinction:

1. $\mathcal{X}$ is empty. Then $\bar{\mathcal{X}}$ contains all elements, so in particular $s \in \bar{\mathcal{X}}$.
2. $\mathcal{X}$ is not empty. By applying LNP^{sk} to $\mathcal{X}$, we can distinguish the cases
   (a) $0 \in \mathcal{X}$. But then, $0 \notin \bar{\mathcal{X}}$, which contradicts our assumption.
   (b) $f(\mathcal{X})$ is the predecessor of the least number in $\mathcal{X}$. Then $f(\mathcal{X}) \notin \mathcal{X}$, and therefore $f(\mathcal{X}) \in \bar{\mathcal{X}}$.

$\varphi[(I2')] :=$

$$\dfrac{\dfrac{\dfrac{\dfrac{TH^{sk} \vdash TH^{sk}}{\vdash \neg TH^{sk}, TH^{sk}}\neg : r}{\vdash (\exists z)A'(z), TH^{sk}}\exists : r \qquad \dfrac{A(0) \vdash A(0)}{A(0), A'(0) \vdash}\neg : l \qquad \dfrac{\dfrac{A(f(T)+1) \vdash A(f(T)+1)}{A(f(T)+1), A'(f(T)+1) \vdash}\neg : l}{A(f(T)+1), \neg A'(f(T)) \wedge A'(f(T)+1) \vdash}\wedge : l_2}{A(0), A(f(T)+1), A'(0) \vee (\neg A'(f(T)) \wedge A'(f(T)+1)) \vdash}\vee : l}{A(0), A(f(T)+1), ((\exists z)A'(z) \rightarrow (A'(0) \vee (\neg A'(f(T)) \wedge A'(f(T)+1)))) \vdash TH^{sk}}\rightarrow : l}{A(0), A(f(T)+1), LNP^{sk} \vdash TH^{sk}}\forall^2 : l\ \lambda x.A'(x)$$

$\varphi[(I2')]$ shows that, assuming $0 \in \bar{\mathcal{X}}$, $f(\mathcal{X})+1 \in \bar{\mathcal{X}}$, and LNP^{sk}, then $s \in \bar{\mathcal{X}}$. The argument is the same as the argument of $\varphi[(I1')]$, except for case 2b: Assume that $f(\mathcal{X})$ is the predecessor of the least number in $\mathcal{X}$. Then $f(\mathcal{X}) + 1 \in \mathcal{X}$, which contradicts our assumption.

$\psi_{IB} :=$

$$\dfrac{\dfrac{\vdash \Sigma(0) = 0 \qquad \vdash 2 * 0 = 0}{\vdash 2 * \Sigma(0) = 0}=: r_2 \qquad \vdash 0 = 0 * (0+1)}{\vdash 2 * \Sigma(0) = 0 * (0+1)}=: r_2$$

Using basic arithmetic and the definition of $\Sigma(0)$, we show that $0 \in \bar{\mathcal{X}}$.

$\psi_{IG} :=$

$$\dfrac{\dfrac{\psi_{IB} \qquad \varphi[(I2')]}{2 * \Sigma(f(T)+1) = (f(T)+1) * (f(T)+1)+1), LNP^{sk} \vdash TH^{sk}}cut \qquad TH^{sk} \vdash TH^{sk}}{2 * \Sigma(f(T)+1) = (f(T)+1) * ((f(T)+1)+1), LNP^{sk} \vdash TH^{sk}}cut$$

From $0 \in \bar{\mathcal{X}}$ and what was proved in $\varphi[(I2')]$, we now know that $f(\mathcal{X}) + 1 \in \bar{\mathcal{X}}$ and LNP^{sk} imply $s \in \bar{\mathcal{X}}$.

$\psi_2 :=$

$$\dfrac{\vdash \Sigma(f(T)+1) = \Sigma(f(T)) + (f(T)+1) \qquad \psi_{IG}}{2 * (\Sigma(f(T)) + (f(T)+1)) = (f(T)+1) * ((f(T)+1)+1), LNP^{sk} \vdash TH^{sk}}=: l_1$$

$\psi_1 :=$

$$\dfrac{\psi_2 \qquad \vdash 2 * (\Sigma(f(T)) + (f(T)+1)) = 2 * \Sigma(f(T)) + 2 * (f(T)+1)}{2 * \Sigma(f(T)) + 2 * (f(T)+1) = (f(T)+1) + ((f(T)+1)+1), LNP^{sk} \vdash TH^{sk}}=: l_1$$

From the second part of the definition of Σ, it follows that $f(\mathcal{X}) + 1 \in \bar{\mathcal{X}}$ is equivalent to $2 * (\Sigma(f(\mathcal{X})) + (f(\mathcal{X}) + 1)) = (f(\mathcal{X}) + 1) * ((f(\mathcal{X}) + 1) + 1)$. This in turn is equivalent to

$$2 * \Sigma(f(\mathcal{X})) + 2 * (f(\mathcal{X}) + 1) = (f(\mathcal{X}) + 1) * ((f(\mathcal{X}) + 1) + 1).$$

$\psi_{IH} :=$

$$\dfrac{\dfrac{\psi_{IB} \qquad \varphi[(I1')]}{LNP^{sk} \vdash 2 * \Sigma(f(T)) = f(T) * (f(T) + 1), TH^{sk}}\, cut \qquad TH^{sk} \vdash TH^{sk}}{LNP^{sk} \vdash 2 * \Sigma(f(T)) = f(T) * (f(T) + 1), TH^{sk}}\, cut$$

From the fact that $0 \in \bar{\mathcal{X}}$ and what we showed in $\varphi[(I1')]$, we conclude that LNP^{sk} implies either $f(\mathcal{X}) \in \bar{\mathcal{X}}$ or $s \in \bar{\mathcal{X}}$. In the following, $\psi_=$ is a proof of

$$\vdash f(T) * (f(T) + 1) + 2 * (f(T) + 1) = (f(T) + 1) * ((f(T) + 1) + 1).$$

$\psi :=$

$$\dfrac{\psi_= \qquad \dfrac{\psi_{IH} \qquad \psi_1}{f(T) * (f(T) + 1) + 2 * (f(T) + 1) = (f(T) + 1) * ((f(T) + 1) + 1), LNP^{sk} \vdash TH^{sk}}\, =: l_1}{LNP^{sk} \vdash TH^{sk}}\, cut$$

Assume LNP^{sk}, then from ψ_{IH}, we know that either $f(\mathcal{X}) \in \bar{\mathcal{X}}$ or $s \in \bar{\mathcal{X}}$. If the latter holds, we are done, so assume the former holds. From ψ_1, we know then that

$$2 * \Sigma(f(\mathcal{X})) + 2 * (f(\mathcal{X}) + 1) = (f(\mathcal{X}) + 1) + ((f(\mathcal{X}) + 1) + 1)$$

implies the desired theorem, and by the definition $\bar{\mathcal{X}}$, we know that $2 * \Sigma(f(\mathcal{X})) = f(\mathcal{X}) * (f(\mathcal{X}) + 1)$, so the first equation is equivalent to

$$f(\mathcal{X}) * (f(\mathcal{X}) + 1) + 2 * (f(\mathcal{X}) + 1) = (f(\mathcal{X}) + 1) * ((f(\mathcal{X}) + 1) + 1).$$

But this equation is arithmetically valid, so we have shown that $s \in \bar{\mathcal{X}}$.

Reviewing the input proof from Section 6, we realize that the method of proof used there was an inductive argument showing that all numbers are in $\bar{\mathcal{X}}$. In the ACNF, this argument reappears as a proof by the least number principle (in the form of the proofs $\varphi[(I1')]$ and $\varphi[(I2')]$), showing directly that no numbers are in $\mathcal{X}$.

7 Conclusion

In this paper, we presented the extension of the cut-elimination method CERES from first-order logic to the class of **QFC**-proofs (in skolem form). Using CERES^2, we analyzed an example proof and discussed the resulting ACNF.

The benefits of CERES^2 over traditional cut-elimination methods are two-fold: Firstly, the characteristic clause set can be regarded as the kernel of the

proof with cuts and as such can provide valuable information that a human could not easily read off of a formal proof (for some evidence supporting this, see [10] and [11]). Secondly, due to the use of a resolution calculus at the core of CERES^2, theoretical and practical advances in higher-order theorem proving may enhance the power of the method. There is still much to be done:

1. We are working on extending CERES^2 to larger classes of proofs and
2. investigating the use of existing higher-order resolution calculi (see e.g. [12]) with CERES^2
3. For semi-automated application of the method, it will be necessary to replace the unrestricted substitution of our resolution calculus by unification (see e.g. [13]).
4. The existing ANSI C++ implementation of CERES is being extended to CERES^2. This will allow practical application of the method to larger and more interesting proofs.

References

1. Kohlenbach, U.: Effective bounds from ineffective proofs in analysis: an application of functional interpretation and majorization. Journal of Symbolic Logic **57**(4) (1992) 1239–1273
2. Baaz, M., Leitsch, A.: Towards a clausal analysis of cut-elimination. Journal of Symbolic Computation **41** (2006) 381–410
3. Baaz, M., Leitsch, A.: Cut-elimination and Redundancy-elimination by Resolution. Journal of Symbolic Computation **29**(2) (2000) 149–176
4. Church, A.: A formulation of the simple theory of types. Journal of Symbolic Logic **5**(2) (1940) 56–68
5. Boolos, G.S., Burgess, J.P., Jeffrey, R.C.: Computability and Logic. 4th edn. Cambridge University Press, Cambridge, UK (2002)
6. Andrews, P.B.: Resolution in Type Theory. Journal of Symbolic Logic **36**(3) (1971) 414–432
7. Baaz, M., Leitsch, A.: Cut normal forms and proof complexity. Annals of Pure and Applied Logic **97**(1–3) (1999) 127–177
8. Miller, D.A.: A compact representation of proofs. Studia Logica **46**(4) (1987) 347–370
9. Danos, V., Joinet, J.B., Schellinx, H.: A New Deconstructive Logic: Linear Logic. Journal of Symbolic Logic **62**(3) (1997) 755–807
10. Baaz, M., Hetzl, S., Leitsch, A., Richter, C., Spohr, H.: Ceres: An Analysis of Fürstenberg's Proof of the Infinity of Primes. to appear in Theoretical Computer Science (2008)
11. Hetzl, S.: Characteristic Clause Sets and Proof Transformations. PhD thesis, Vienna University of Technology (2007)
12. Benzmüller, C.: Comparing approaches to resolution based higher-order theorem proving. Synthese **133**(1–2) (2002) 203–335
13. Dowek, G.: Higher-order unification and matching. In: Handbook of automated reasoning. Elsevier Science Publishers B. V., Amsterdam, The Netherlands, The Netherlands (2001) 1009–1062