CERES in Many-Valued Logics*

Matthias Baaz[1] and Alexander Leitsch[2]

[1] Institut für Computermathematik (E-118),
TU-Vienna, Wiedner Hauptstraße 8-10,
1040 Vienna, Austria
baaz@logic.at

[2] Institut für Computersprachen (E-185),
TU-Vienna, Favoritenstraße 9,
1040 Vienna, Austria
leitsch@logic.at

Abstract. CERES is a method for cut-elimination in classical logic which is based on resolution. In this paper we extend CERES to CERES-m, a resolution-based method of cut-elimination in Gentzen calculi for arbitrary finitely-valued logics. Like in the classical case the core of the method is the construction of a resolution proof in finitely-valued logics. Compared to Gentzen-type cut-elimination methods the advantage of CERES-m is a twofold one: 1. it is easier to define and 2. it is computationally superior and thus more appropriate for implementations and experiments.

1 Introduction

The core of classical cut-elimination methods in the style of Gentzen [8] consists of the permutation of inferences and of the reduction of cuts to cuts on the immediate subformulas of the cut formula. If we switch from two- valued to many-valued logic, the reduction steps become intrinsically tedious and opaque [3] in contrast to the extension of CERES to the many-valued case, which is straightforward.

We introduce CERES-m for correct (possible partial) calculi for m-valued first order logics based on m-valued connectives, distributive quantifiers [7] and arbitrary atomic initial sequents closed under substitution. We do not touch the completeness issue of these calculi, instead we derive clause terms from the proof representing the formulas which are ancestor formulas of the cut formulas; the evaluation of these clause terms guarantees the existence of a resolution refutation as core of a proof with atomic cuts only. This resolution refutation is extended to a proof of the original end-sequent by adjoining cut-free parts of the original proof. Therefore, it is sufficient to refute the suitably assembled components of the initial sequents using a m-valued theorem prover [2].

* supported by the Austrian Science Fund (FWF) proj. no P16264-N05

F. Baader and A. Voronkov (Eds.): LPAR 2004, LNAI 3452, pp. 1–20, 2005.

2 Definitions and Notation

Definition 1 (language). *The alphabet Σ consists of an infinite supply of variables, of infinite sets of n-ary function symbols and predicate symbols er σ contains a set W of truth symbols denoting the truth values of the logic, a finite number of connectives $\circ_1, \ldots, \circ_m$ of arity $n_1, \ldots, n_m$, and a finite number of quantifiers $Q_1, \ldots, Q_k$.*

Definition 2 (formula). *An atomic formula is an expression of the form $P(t_1, \ldots, t_n)$ where P is an n-ary predicate symbol in Σ and $t_1, \ldots, t_n$ are terms over Σ. Atomic formulas are formulas.*

If $\circ$ is an n-ary connective and $A_1, \ldots, A_n$ are formulas then $\circ(A_1, \ldots, A_n)$ is a formula.

If Q is quantifier in Σ and x is a variable then $(Qx)A$ is a formula.

Definition 3 (signed formula). *Let $w \in W$ and A be a formula. Then $w\colon A$ is called a signed formula.*

Definition 4 (sequent). *A sequent is a finite sequence of signed formulas. The number of signed formulas occurring in a sequent S is called the* length *of S and is denoted by $l(S)$. $\hat{S}$ is called the* unsigned version *of S if every signed formula $w\colon A$ in S is replaced by A. The length of unsigned versions is defined in the same way. A sequent S is called* atomic *if $\hat{S}$ is a sequence of atomic formulas.*

Remark 1. Note that the classical sequent $(\forall x)P(x) \vdash Q(a)$ can be written as $\mathbf{f}\colon (\forall x)P(x), \mathbf{t}\colon Q(a)$.

m-valued sequents are sometimes written as m-sided sequents. We refrain from this notation, because it denotes a preferred order of truth values, which even in the two-valued case might induce unjustified conclusions.

Definition 5 (axiom set). *A set $\mathcal{A}$ of atomic sequents is called an axiom set if $\mathcal{A}$ is closed under substitution.*

The calculus we are defining below is capable of formalizing any finitely valued logic. Concerning the quantifiers we assume them to be of distributive type [7]. Distribution quantifiers are functions from the non-empty sets of truth-values to the set of truth values, where the domain represents the situation in the structure, i.e. the truth values actually taken.

Definition 6. *Let $A(x)$ be a formula with free variable x. The* distribution *$Distr(A(x))$ of $A(x)$ is the set of all truth values in W to which $A(x)$ evaluates (for arbitrary assignments of domain elements to x).*

Definition 7. *Let q be a mapping $2^W \to W$. In interpreting the formula $(Qx)A(x)$ via q we first compute $Distr(A(x))$ and then $q(Distr(A(x)))$, which is the truth value of $(Qx)A(x)$ under the interpretation.*

In the calculus defined below the distinction between quantifier introductions with (strong) and without eigenvariable conditions (weak) are vital.

Definition 8. *A* strong quantifier *is a triple* (V, w, w') *(for* $V \subseteq W$*) s.t.* $(Qx)A(x)$ *evaluates to* w *if* $Distr(A(x)) \subseteq V$ *and to* w' *otherwise. A* weak quantifier *is a triple* (u, w, w') *s.t.* $(Qx)A(x)$ *evaluates to* w *if* $u \in Distr(A(x))$*, and to* w' *otherwise.*

Remark 2. Strong and weak quantifiers are dual w.r.t. to set complementation. In fact to any strong quantifier there corresponds a weak one and vice versa. Like in classical logic we may speak about weak and strong occurrences of quantifiers in sequents and formulas.

Note that strong and weak quantifiers define merely a subclass of distribution quantifiers. Nevertheless the following property holds:

Proposition 1. *Any distributive quantifier can be expressed by strong and weak quantifiers and many valued associative, commutative and idempotent connectives (which are variants of conjunction and disjunction).*

Definition 9 (LM-type calculi). *We define an* LM*-type calculus* **K***. The initial sequents are (arbitrary) atomic sequents of an axiom set* $\mathcal{A}$*. In the rules of* **K** *we always mark the auxiliary formulas (i.e. the formulas in the premiss(es) used for the inference) and the principal (i.e. the inferred) formula using different marking symbols. Thus, in our definition, classical* $\wedge$*-introduction to the right takes the form*

$$\frac{\Gamma, \mathbf{t}\colon A^{+} \quad \Gamma, \mathbf{t}\colon B^{+}}{\Gamma, \mathbf{t}\colon A \wedge B^{*}}$$

If $\Pi \vdash \Gamma, \Delta$ *is a sequent then* $\Pi \vdash \Gamma, \Delta^{+}$ *indicates that all signed formulas in* Δ *are auxiliary formulas of the defined inference.* $\Gamma \vdash \Delta, w\colon A^{*}$ *indicates that* $A\colon w^{*}$*is the principal formula (i.e. the inferred formula) of the inference.*

Auxiliary formulas and the principal formula of an inference are always supposed to be rightmost. Therefore we usually avoid markings as the status of the formulas is clear from the notation.

logical rules:

Let $\circ$ *be an* n*-nary connective.For any* $w \in W$ *we have an introduction rule* $\circ\colon w$ *of the form*

$$\frac{\Gamma, \Delta_1^{+} \quad \dots \quad \Gamma, \Delta_m^{+}}{\Gamma, w\colon \circ(\pi(\hat{\Delta}_1, \dots, \hat{\Delta}_m, \hat{\Delta}))^{*}}\ \circ\colon w$$

where $l(\Delta_1, \dots, \Delta_m, \Delta) = n$ *(the* Δ_i *are sequences of signed formulas which are all auxiliary signed formulas of the inference) and* $\pi(S)$ *denotes a permutation of a sequent* S*.*

Note that, for simplicity, we chose the additive version of all logical introduction rules.

In the introduction rules for quantifiers we distinguish strong *and* weak *introduction rules. Any strong quantifier rule* $Q\colon w$ *(for a strong quantifier* (V, w, w')*) is of the form*

$$\frac{\Gamma, u_1\colon A(\alpha)^+, \ldots, u_m\colon A(\alpha)^+}{\Gamma, w\colon (Qx)A(x)^*}\; Q\colon w$$

where α *is an eigenvariable not occurring in* Γ*, and* $V = \{u_1, \ldots, u_m\}$*.*

Any weak quantifier rule (for a weak quantifier (u, w, w')*) is of the form*

$$\frac{\Gamma, u\colon A(t)^+}{\Gamma, w\colon (Qx)A(x)^*}\; Q\colon w$$

where t *is a term containing no variables which are bound in* $A(x)$*. We say that* t *is* eliminated *by* $Q\colon w$*.*

We need define a special n*-ary connective for every strong quantifier in order to carry out skolemization. Indeed if we skip the introduction of a strong quantifier the* m *(possibly* $m > 1$*) auxiliary formulas must be contracted into a single one* after *the removal of the strong quantifier (see definition of skolemization below). Thus for every rule*

$$\frac{\Gamma, u_1\colon A(\alpha_1)^+, \ldots, u_m\colon A(\alpha_m)^+}{\Gamma, w\colon (Qx)A(x)^*}\; Q\colon w$$

we define a propositional rule

$$\frac{\Gamma, u_1\colon A(t)^+, \ldots, u_m\colon A(t)^+}{\Gamma, w\colon A(t)^*}\; c_Q\colon w$$

This new operator c_Q *can be eliminated by the de-skolemization procedure afterwards.*

structural rules:

The structural rule of weakening is defined like in **LK** *(but we need only one weakening rule and may add more then one formula).*

$$\frac{\Gamma}{\Gamma, \Delta}\; w$$

for sequents Γ *and* Δ*.*

To put the auxiliary formulas on the right positions we need permutation rules of the form

$$\frac{F_1, \ldots, F_n}{F_{\pi(1)}, \ldots, F_{\pi(n)}}\; \pi$$

where π *is a permutation of* $\{1, \ldots, n\}$ *and the* F_i *are signed formulas .*

Instead of the usual contraction rules we define an n-contraction rule for any $n \geq 2$ *and* $F_1 = \ldots = F_n = F$*:*

$$\frac{\Gamma, F_1, \ldots, F_n}{\Gamma, F}\ c:n$$

In contrast to **LK** *we do not have a single cut rule, but instead rules* $cut_{ww'}$ *for any* $w, w' \in W$ *with* $w \neq w'$*. Any such rule is of the form*

$$\frac{\Gamma, w\colon A \quad \Gamma', w'\colon A}{\Gamma, \Gamma'}\ cut_{ww'}$$

Definition 10 (proof). *A* proof *of a sequent* S *from an axiom set* $\mathcal{A}$ *is a directed labelled tree. The root is labelled by* S*, the leaves are labelled by elements of* $\mathcal{A}$*. The edges are defined according to the inference rules (in an n-ary rule the children of a node are labelled by the antecedents, the parent node is labelled by the consequent). Let* N *be a node in the proof* ϕ *then we write* $\phi.N$ *for the corresponding subproof ending in* N*. For the number of nodes in* ϕ *we write* $\|\phi\|$*.*

Definition 11. *Let* **K** *be an* LM*-type calculus. We define* $\mathcal{P}[\mathbf{K}]$ *as the set of all* **K***-proofs.* $\mathcal{P}^i[\mathbf{K}]$ *is the subset of* $\mathcal{P}[\mathbf{K}]$ *consisting of all proofs with cut-complexity* $\leq i$ *(*$\mathcal{P}^0[\mathbf{K}]$ *is the set of proofs with at most atomic cuts).* $\mathcal{P}^\emptyset[\mathbf{K}]$ *is the subset of all cut-free proofs.*

Example 1. We define $W = \{0, u, 1\}$ and the connectives as in the 3-valued Kleene logic, but introduce a new quantifier D ("D" for determined) which gives true iff all truth values are in $\{0, 1\}$. We only define the rules for $\vee$ and for D, as no other operators occur in the proof below.

$$\frac{0\colon A, 1\colon A \quad 0\colon B, 1\colon B \quad 1\colon A, 1\colon B}{1\colon A \vee B}\ \vee\colon 1$$

$$\frac{u\colon A, u\colon B}{u\colon A \vee B}\ \vee\colon u \qquad \frac{0\colon A, 0\colon B}{0\colon A \vee B}\ \vee\colon 0$$

$$\frac{0\colon A(\alpha), 1\colon A(\alpha)}{1\colon (Dx)A(x)}\ D\colon 1 \qquad \frac{u\colon A(t)}{0\colon (Dx)A(x)}\ D\colon 0$$

where α is an eigenvariable and t is a term containig no variables bound in $A(x)$. Note that $D\colon 1$ is a strong, and $D\colon 0$ a weak quantifier introduction. The formula $u\colon (Dx)A(x)$ can only be introduced via weakening.

For the notation of proofs we frequently abbreviate sequences of structural rules bei $*$; thus $\pi^* + \vee\colon u$ means that $\vee\colon u$ is performed and permutations before and/or afterwards. This makes the proofs more legible and allows to focus on the logically relevant inferences. As in the definition of LM-type calculi we mark the auxiliary formulas of logical inferences and cut by $+$, the principle ones by $*$.

Let ϕ be the following proof

$$\frac{\phi_1 \quad \phi_2}{0\colon (Dx)((P(x)\vee Q(x))\vee R(x)), 1\colon (Dx)P(x)}\ cut$$

where $\phi_1 =$

$$\dfrac{\dfrac{\dfrac{\dfrac{\begin{matrix}(\psi')\\ 0\colon P(\alpha)\vee Q(\alpha),\ u\colon P(\alpha)\vee Q(\alpha),\ 1\colon P(\alpha)\vee Q(\alpha)\end{matrix}}{0\colon P(\alpha)\vee Q(\alpha),\ u\colon P(\alpha)\vee Q(\alpha),\ u\colon R(\alpha)^{*},\ 1\colon P(\alpha)\vee Q(\alpha)}\ \pi^{*}+w}{0\colon A(\alpha)\vee Q(\alpha),\ u\colon (P(\alpha)\vee Q(\alpha))\vee R(\alpha)^{+*},\ 1\colon P(\alpha)\vee Q(\alpha)}\ \vee\colon u}{0\colon (Dx)((P(x)\vee Q(x))\vee R(x))^{*},\ 0\colon P(\alpha)\vee Q(\alpha)^{+},\ 1\colon P(\alpha)\vee Q(\alpha)^{+}}\ \pi^{*}+D\colon 0}{0\colon (Dx)((P(x)\vee Q(x))\vee R(x)),\ 1\colon (Dx)(P(x)\vee Q(x))^{*}}\ D\colon 1$$

and $\phi_2 =$

$$\dfrac{\dfrac{\dfrac{\dfrac{0\colon P(\beta),\ u\colon P(\beta),\ 1\colon P(\beta)}{0\colon P(\beta),\ 1\colon P(\beta),\ u\colon P(\beta)^{+},\ u\colon Q(\beta)^{*+}}\ \pi^{*}+w}{0\colon P(\beta),\ u\colon P(\beta)\vee Q(\beta)^{*+},\ 1\colon P(\beta)}\ \pi^{*}+\vee\colon u}{0\colon (Dx)(P(x)\vee Q(x))^{*},\ 0\colon P(\beta)^{+},\ 1\colon P(\beta)^{+}}\ \pi^{*}+D\colon 0}{0\colon (Dx)(P(x)\vee Q(x)),\ 1\colon (Dx)P(x)^{*}}\ D\colon 1$$

we have to define ψ' as our axiom set must be atomic. We set

$$\psi' = \psi(A,B)\{A \leftarrow P(\alpha), A \leftarrow Q(\alpha)\}$$

and define
$\psi(A,B) =$

$$\dfrac{\dfrac{\dfrac{S,0\colon A,1\colon A \quad S,0\colon B,1\colon B \quad S,1\colon A,1\colon B}{0\colon A,\ u\colon A,u\colon B,\ 1\colon A\vee B}\ \vee\colon 1 \qquad \dfrac{T,0\colon A,1\colon A \quad T,0\colon B,1\colon B \quad T,1\colon A,1\colon B}{0\colon B,\ u\colon A,u\colon B,\ 1\colon A\vee B}}{0\colon A\vee B,\ u\colon A,u\colon B,\ 1\colon A\vee B}\ \vee\colon 0}{0\colon A\vee B,\ u\colon A\vee B,\ 1\colon A\vee B}\ \pi^{*}+\vee\colon u$$

For $S = 0\colon A,\ u\colon A, u\colon B$ and $T = 0\colon B,\ u\colon A, u\colon B$. It is easy to see that the end sequent is valid as the axioms contain $0\colon A,\ u\colon A, 1\colon A$ and $0\colon B,\ u\colon B, 1\colon B$ as subsequents.

Definition 12 (W-clause). *A W-clause is an atomic sequent (where W is the set of truth symbols). The empty sequent is called empty clause and is denoted by $\Box$.*

Let S be an W-clause. S' is called a renamed variant of S if $S' = S\eta$ for a variable permutation η.

Definition 13 (W-resolution). *We define a resolution calculus R_W which only depends on the set W (but not on the logical rules of* **K***). R_W operates on W-clauses; its rules are:*

1. *$res_{ww'}$ for all $w, w' \in W$ and $w \neq w'$,*
2. *w-factoring for $w \in W$,*
3. *permutations.*

Let $S\colon \Gamma, w\colon A$ and $S'\colon \Gamma', w'\colon A'$ (where $w \neq w'$) be two W-clauses and $S''\colon \Gamma'', w'\colon A''$ be a variant of S' s.t. S and S' are variable disjoint. Assume that $\{A, B'\}$ are unifiable by a most general unifier σ. Then the rule $res_{ww'}$ on S, S' generates a resolvent R for

$$R = \Gamma\sigma, \Gamma''\sigma.$$

Let $S\colon \Gamma, w\colon A_1, \ldots, w\colon A_m$ be a clause and σ be a most general unifier of $\{A_1, \ldots, A_m\}$. Then the clause

$$S'\colon \Gamma\sigma, w\colon A_1\sigma$$

is called a w-factor of S.

A W-resolution proof of a clause S from a set of clauses $\mathcal{S}$ is a directed labelled tree s.t. the root is labelled by S and the leaves are labelled by elements of $\mathcal{S}$. The edges correspond the applications of w-factoring (unary), permutation (unary) and $res_{ww'}$ (binary).

It is proved in [1] that W-resolution is complete. For the LM-type calculus we only require soundness w.r.t. the underlying logic. So from now on we assume that **K** is sound.

Note that we did not define clauses as sets of signed literals; therefore we need the permutation rule in order to "prepare" the clauses for resolution and factoring.

Definition 14 (ground projection). *Let γ be a W-resolution proof and $\{x_1, \ldots, x_n\}$ be the variables occurring in the indexed clauses of γ. Then, for all ground terms $t_1, \ldots, t_n$, $\gamma\{x_1 \leftarrow t_1, \ldots, x_1 \leftarrow t_n\}$ is called a ground projection of γ.*

Remark 3. Ground projections of resolution proofs are ordinary proofs in **K**; indeed factoring becomes n-contraction and resolution becomes cut.

Definition 15 (ancestor relation). *Let*

$$\frac{S_1\colon \Gamma, \Delta_1^+ \quad \ldots \quad S_m\colon \Gamma, \Delta_m^+}{S\colon \Gamma, w\colon A^*}\ x$$

be a an inference in a proof ϕ; let μ be the occurrence of the principal signed formula $w\colon A$ in S and ν_{ij} be the occurrence of the j-th auxiliary formula in S_i. Then all ν_{ij} are ancestors of μ.

The ancestor relation in ϕ is defined as the reflexive and transitive closure of the above relation.

By $S(N, \Omega)$ ($\bar{S}(N, \Omega)$) we denote the subsequent of S at the node N of ϕ consisting of all formulas which are (not) ancestors of a formula occurrence in Ω.

Example 2. Let $\psi(A,B)$ as in Example 1:

$$\cfrac{\cfrac{S,0\colon A,1\colon A \quad S,0\colon B,1\colon B \quad S,1\colon A,1\colon B}{0\colon A^{\dagger},\ u\colon A,u\colon B,\ 1\colon A\vee B}\ \vee\colon 1 \qquad \cfrac{T,0\colon A,1\colon A \quad T,0\colon B,1\colon B \quad T,1\colon A,1\colon B}{0\colon B^{\dagger},\ u\colon A,u\colon B,\ 1\colon A\vee B}}{\cfrac{0\colon A\vee B^{\dagger},\ u\colon A,u\colon B,\ 1\colon A\vee B}{0\colon A\vee B^{\dagger},\ u\colon A\vee B,\ 1\colon A\vee B}\ \pi^{*}+\vee\colon u}\ \vee\colon 0$$

Let N_0 be the root of $\psi(A,B)$ and μ be the occurrence of the first formula $(0\colon A\vee B)$ in N. The formula occurrences which are ancestors of μ are labelled with †. The marking is not visible in S and T where the ancestors occur. In the antecedent N_1,N_2 of the binary inference $\vee\colon 0$ we have $S(N_1,\{\mu\})=0\colon A$ and $S(N_2,\{\mu\})=0\colon B$.

3 Skolemization

As CERES-m (like CERES [6] and [5]) augments a ground resolution proof with cut-free parts of the original proof related only to the end-sequent, eigenvariable conditions in these proof parts might be violated. To get rid of this problem, the endsequent of the proof and the formulas, which are ancestors of the end-sequent have to be skolemized, i.e eigenvariables have to be replaced by suitable Skolem terms. To obtain a skolemization of the end-sequent, we have to represent (analyze) distributive quantifiers in terms of strong quantifiers (covering exclusively eigenvariables) and weak quantifiers (covering exclusively terms). This was the main motivation for the choice of our definition of quantifiers in Definition 9. The strong quantifiers are replaced by Skolem functions depending on the weakly quantified variables determined by the scope. Note that distributive quantifiers are in general mixed, i.e. they are neither weak nor strong, even in the two-valued case.

3.1 Skolemization of Proofs

Definition 16 (skolemization). *Let $\Delta\colon\Gamma, w\colon A$ be a sequent and $(Qx)B$ be a subformula of A at the position λ where Qx is a maximal strong quantifier in $w\colon A$. Let $y_1,\ldots,y_m$ be free variables occurring in $(Qx)B$, then we define*

$$sk(\Delta)=\Gamma, w\colon A[B\{x\rightarrow f(y_1,\ldots,y_m)\}]_{\lambda}$$

where f is a function symbol not occurring in Δ.

If $w\colon A$ contains no strong quantifier then we define $sk(\Delta)=\Delta$.

A sequent S is in Skolem form *if there exists no permutation S' of S s.t. $sk(S')\neq S'$. S' is called a Skolem form of S if S' is in Skolem form and can be obtained from S by permutations and the operator sk.*

The skolemization of proofs can be defined in a way quite similar to the classical case (see [4]).

Definition 17 (skolemization of K-proofs). *Let* $\mathbf{K}$ *be an* LM*-type calculus. We define a transformation of proofs which maps a proof* ϕ *of* S *from* $\mathcal{A}$ *into a proof* $sk(\phi)$ *of* S' *from* $\mathcal{A}'$ *where* S' *is the Skolem form of* S *and* $\mathcal{A}'$ *is an instance of* $\mathcal{A}$*.*

Locate an uppermost logical inference which introduces a signed formula $w{:}\,A$ *which is not an ancestor of a cut and contains a strong quantifier.*

(a) The formula is introduced by a strong quantifier inference:

$$\frac{\begin{array}{c}\psi[\alpha]\\ S'{:}\,\Gamma, u_1{:}\,A(\alpha)^+, \ldots, u_m{:}\,A(\alpha)^+\end{array}}{S{:}\,\Gamma, w{:}\,(Qx)A(x)^*}\ Q{:}\,w$$

in ϕ *and* N', N *be the nodes in* ϕ *labelled by* S', S*. Let* P *be the path from the root to* N'*, locate all weak quantifier inferences* ξ_i *(i=1,…,n) on* P *and all terms* t_i *eliminated by* ξ_i*. Then we delete the inference node* N *and replace the derivation* ψ *of* N' *by*

$$\frac{\begin{array}{c}\psi[f(t_1,\ldots,t_n)]\\ S'{:}\,\Gamma, u_1{:}\,A(f(t_1,\ldots,t_n))^+, \ldots, u_m{:}\,A(f(t_1,\ldots,t_n))^+\end{array}}{S_0{:}\,\Gamma, w{:}\,A(f(t_1,\ldots,t_n))^*}\ c_Q : w$$

where f *is a function symbol not occurring in* ϕ *and* c_Q *is the connective corresponding to* Q*. The sequents on* P *are adapted according to the inferences on* P*.*

(b) The formula is inferred by a propositional inference or by weakening (within the principal formula $w{:}\,A$*) then we replace* $w{:}\,A$ *by the Skolem form of* $w{:}\,A$ *where the Skolem function symbol does not occur in* ϕ*.*

Let ϕ' *be the proof after such a skolemization step. We iterate the procedure until no occurrence of a strong quantifier is an ancestor of an occurrence in the end sequent. The resulting proof is called* $sk(\phi)$*. Note that* $sk(\phi)$ *is a proof from the* same *axiom set* $\mathcal{A}$ *as* $\mathcal{A}$ *is closed under substitution.*

Definition 18. *A proof* ϕ *is called* skolemized *if* $sk(\phi) = \phi$*.*

Note that skolemized proofs may contain strong quantifiers, but these are ancestors of cut, in the end-sequent there are none.

Example 3. Let ϕ be the proof from Example 1:

$$\frac{\phi_1 \quad \phi_2}{0{:}\,(Dx)((P(x) \vee Q(x)) \vee R(x)), 1{:}\,(Dx)P(x)}\ cut$$

where $\phi_1 =$

$$\frac{\dfrac{\dfrac{\dfrac{\begin{array}{c}(\psi')\\ 0{:}\,P(\alpha) \vee Q(\alpha),\ u{:}\,P(\alpha) \vee Q(\alpha),\ 1{:}\,P(\alpha) \vee Q(\alpha)\end{array}}{0{:}\,P(\alpha) \vee Q(\alpha),\ u{:}\,P(\alpha) \vee Q(\alpha),\ u{:}\,R(\alpha)^*,\ 1{:}\,P(\alpha) \vee Q(\alpha)}\ \pi^* + w}{0{:}\,A(\alpha) \vee Q(\alpha),\ u{:}\,(P(\alpha) \vee Q(\alpha)) \vee R(\alpha)^{+*},\ 1{:}\,P(\alpha) \vee Q(\alpha)}\ \vee{:}\,u}{0{:}\,(Dx)((P(x) \vee Q(x)) \vee R(x))^*,\ 0{:}\,P(\alpha) \vee Q(\alpha)^+,\ 1{:}\,P(\alpha) \vee Q(\alpha)^+}\ \pi^* + D{:}\,0}{0{:}\,(Dx)((P(x) \vee Q(x)) \vee R(x)),\ 1{:}\,(Dx)(P(x) \vee Q(x))^*}\ D{:}\,1$$

and $\phi_2 =$

$$\cfrac{\cfrac{\cfrac{\cfrac{0\colon P(\beta),\ u\colon P(\beta),\ 1\colon P(\beta)}{0\colon P(\beta),\ 1\colon P(\beta),\ u\colon P(\beta)^+,\ u\colon Q(\beta)^{*+}}\ \pi^* + w}{0\colon P(\beta),\ u\colon P(\beta) \vee Q(\beta)^{*+},\ 1\colon P(\beta)}\ \pi^* + \vee\colon u}{0\colon (Dx)(P(x) \vee Q(x))^*,\ 0\colon P(\beta)^+,\ 1\colon P(\beta)^+}\ \pi^* + D\colon 0}{0\colon (Dx)(P(x) \vee Q(x)),\ 1\colon (Dx)P(x)^*}\ D\colon 1$$

The proof is not skolemized as the endsequent contains a strong quantifier occurrence in the formula $1\colon (Dx)P(x)$. This formula comes from the proof ϕ_2. Thus we must skolemize ϕ_2 and adapt the end sequent of ϕ. It is easy to verify that $sk(\phi_2) =$

$$\cfrac{\cfrac{\cfrac{\cfrac{0\colon P(c),\ u\colon P(c),\ 1\colon P(c)}{0\colon P(c),\ 1\colon P(c),\ u\colon P(c)^+,\ u\colon Q(c)^{*+}}\ \pi^* + w}{0\colon P(c),\ u\colon P(c) \vee Q(c)^{*+},\ 1\colon P(c)}\ \pi^* + \vee\colon u}{0\colon (Dx)(P(x) \vee Q(x))^*,\ 0\colon P(c)^+,\ 1\colon P(c)^+}\ \pi^* + D\colon 0}{0\colon (Dx)(P(x) \vee Q(x)),\ 1\colon P(c)^*}\ c_{D-1}$$

Then $sk(\phi) =$

$$\cfrac{\phi_1 \quad sk(\phi_2)}{0\colon (Dx)((P(x) \vee Q(x)) \vee R(x)), 1\colon P(c)}\ cut$$

Note that ϕ_1 cannot be skolemized as the strong quantifiers in ϕ_1 are ancestors of the cut in ϕ.

3.2 De-Skolemization of Proofs

Skolem functions can be replaced by the original structure of (strong and weak) quantifiers by the following straightforward algorithm at most exponential in the maximal size of the original proof and of the CERES-m proof of the Skolemized end sequent: Order the Skolem terms (terms, whose outermost function symbol is a Skolem function) by inclusion.The size of the proof resulting from CERES-m together with the number of inferences in the original proof limits the number of relevant Skolem terms. Always replace a maximal Skolem term by a fresh variable, and determine the formula F in the proof, for which the corresponding strong quantifier should be introduced. In re-introducing the quantifier we eliminate the newly introduced connectives c_Q. As the eigenvariable condition might be violated at the lowest possible position, where the quantifier can be introduced (because e.g. the quantified formula has to become part of a larger formula by an inference) suppress all inferences on F such that F occurs as side formula besides the original end-sequent. Then perform all inferences on F. This at most triples the size of the proof (a copy of the proof together with suitable contractions might be necessary).

3.3 Re-introduction of Distributive Quantifiers

The distributive quantifiers are by now represented by a combination of strong quantifiers, weak quantifiers and connectives. A simple permutation of inferences in the proof leads to the immediate derivation in several steps of the representation of the distributive quantifier from the premises of the distributive quantifier inference. The replacement of the representation by the distributive quantifier is then simple.

4 CERES-m

As in the classical case (see [5] and [6]) we restrict cut-elimination to skolemized proofs. After cut-elimination the obtained proof can be re-skolemized, i.e. it can be transformed into a derivation of the original (unskolemized) end-sequent.

Definition 19. *Let* $\mathbf{K}$ *be an* LM*-type calculus. We define* $\mathcal{SK}[\mathbf{K}]$ *be the set of all skolemized proofs in* $\mathbf{K}$*.* $\mathcal{SK}^{\emptyset}[\mathbf{K}]$ *is the set of all cut-free proofs in* $\mathcal{SK}[\mathbf{K}]$ *and, for all* $i \geq 0$*,* $\mathcal{SK}^{i}[\mathbf{K}]$ *is the subset of* $\mathcal{SK}[\mathbf{K}]$ *containing all proofs with cut-formulas of formula complexity* $\leq i$*.*

Our goal is to transform a derivation in $\mathcal{SK}[\mathbf{K}]$ into a derivation in $\mathcal{SK}^{0}[\mathbf{K}]$ (i.e. we reduce all cuts to atomic ones). The first step in the corresponding procedure consists in the definition of a clause term corresponding to the sub-derivations of an $\mathbf{K}$-proof ending in a cut. In particular we focus on derivations of the cut formulas themselves, i.e. on the derivation of formulas having no successors in the end-sequent. Below we will see that this analysis of proofs, first introduced in [5], is quite general and can easily be generalized to LM-type calculi.

Definition 20 (clause term). *The signature of clause terms consists of that of* W*-clauses and the operators* $\oplus^n$ *and* $\otimes^n$ *for* $n \geq 2$*.*

- *(Finite) sets of* W*-clauses are clause terms.*
- *If* $X_1, \ldots, X_n$ *are clause terms then* $\oplus^n(X_1, \ldots, X_n)$ *is a clause term.*
- *If* $X_1, \ldots, X_n$ *are clause terms then* $\otimes^n(X_1, \ldots, X_n)$ *is a clause term.*

Clause terms denote sets of W-clauses; the following definition gives the precise semantics.

Definition 21. *We define a mapping* $|\ |$ *from clause terms to sets of* W*-clauses in the following way:*

$$|\mathcal{S}| = \mathcal{C} \quad \textit{for sets of } W\textit{-clauses } \mathcal{S},$$

$$|\oplus^n (X_1, \ldots, X_n)| = \bigcup_{i=1}^{n} |X_i|,$$

$$|\otimes^n (X_1, \ldots, X_n)| = \mathit{merge}(|X_1|, \ldots, |X_n|),$$

where

$$merge(\mathcal{S}_1, \dots, \mathcal{S}_n) = \{S_1 \dots S_n \mid S_1 \in \mathcal{S}_1, \dots S_n \in \mathcal{S}_n\}.$$

We define clause terms to be equivalent if the corresponding sets of clauses are equal, i.e. $X \sim Y$ *iff* $|X| = |Y|$*.*

Definition 22 (characteristic term). *Let* $\mathbf{K}$ *be an* LM*-type calculus,* ϕ *be a proof of* S *and let* Ω *be the set of all occurrences of cut formulas in* ϕ*. We define the* characteristic (clause) term $\Theta(\phi)$ *inductively:*

Let N *be the occurrence of an initial sequent* S' *in* ϕ*. Then* $\Theta(\phi)/N = \{S(N, \Omega)\}$ *(see Definition 15).*

Let us assume that the clause terms $\Theta(\phi)/N$ *are already constructed for all nodes* N *in* ϕ *with* $\mathrm{depth}(N) \leq k$*. Now let* N *be a node with* $\mathrm{depth}(\nu) = k + 1$*. We distinguish the following cases:*

(a) N *is the consequent of* M*, i.e. a unary rule applied to* M *gives* N*. Here we simply define*

$$\Theta(\varphi)/N = \Theta(\varphi)/M.$$

(b) N *is the consequent of* $M_1, \dots, M_n$*, for* $n \geq 2$*, i.e. an* n*-ary rule* x *applied to* $M_1, \dots, M_n$ *gives* N*.*

(b1) *The auxiliary formulas of* x *are ancestors of* Ω*, i.e. the formulas occur in* $S(M_i, \Omega)$ *for all* $i = 1, \dots, n$*. Then*

$$\Theta(\phi)/N = \oplus^n(\Theta(\varphi)/M_1, \dots, \Theta(\varphi)/M_n).$$

(b2) *The auxiliary formulas of* x *are not ancestors of* Ω*. In this case we define*

$$\Theta(\phi)/N = \otimes^n(\Theta(\varphi)/M_1, \dots, \Theta(\varphi)/M_n).$$

Note that, in an n*-ary inference, either all auxiliary formulas are ancestors of* Ω *or none of them.*

Finally the characteristic term $\Theta(\phi)$ *of* ϕ *is defined as* $\Theta(\phi)/N_0$ *where* N_0 *is the root node of* ϕ*.*

Definition 23 (characteristic clause set). *Let* ϕ *be proof in an* LM*-type calculus* $\mathbf{K}$ *and* $\Theta(\phi)$ *be the characteristic term of* ϕ*. Then* $\mathrm{CL}(\phi)$*, defined as* $\mathrm{CL}(\phi) = |\Theta(\phi)|$*, is called the characteristic clause set of* ϕ*.*

Remark 4. If ϕ is a cut-free proof then there are no occurrences of cut formulas in ϕ and $\mathrm{CL}(\phi) = \{\Box\}$.

Example 4. Let ϕ' be the skolemized proof defined in Example 3. It is easy to verify that the characteristic clause set $\mathrm{CL}(\phi')$ is

$$\begin{array}{l}\{u\colon P(c),\\ 0\colon P(\alpha),\ 0\colon P(\alpha),\ 1\colon P(\alpha)\\ 0\colon P(\alpha),\ 0\colon Q(\alpha),\ 1\colon Q(\alpha)\\ 0\colon P(\alpha),\ 1\colon P(\alpha),\ 1\colon Q(\alpha)\\ 0\colon Q(\alpha),\ 0\colon P(\alpha),\ 1\colon P(\alpha)\\ 0\colon Q(\alpha),\ 0\colon Q(\alpha),\ 1\colon Q(\alpha)\\ 0\colon Q(\alpha),\ 1\colon P(\alpha),\ 1\colon Q(\alpha)\}.\end{array}$$

The set $\mathrm{CL}(\phi')$ can be refuted via W-resolution for $W = \{0, u, 1\}$. A W-resolution refutation is ($0f$ stands for 0-factoring) $\gamma =$

$$\dfrac{\dfrac{\dfrac{0\colon P(\alpha),\ 0\colon P(\alpha),\ 1\colon P(\alpha) \quad u\colon P(c)}{0\colon P(c),\ 0\colon P(c)}\ res_{1u}}{0\colon P(c)}\ 0f \qquad u\colon P(c)}{\Box}\ res_{0u}$$

A ground projection of γ (even the only one) is $\gamma' = \gamma\{\alpha \leftarrow c\} =$

$$\dfrac{\dfrac{\dfrac{0\colon P(c),\ 0\colon P(c),\ 1\colon P(c) \quad u\colon P(c)}{0\colon P(c),\ 0\colon P(c)}\ cut_{1u}}{0\colon P(c)}\ c \qquad u\colon P(c)}{\Box}\ cut_{0u}$$

Obviously γ' is a proof in $\mathbf{K}$.

In Example 4 we have seen that the characteristic clause set of a proof is refutable by W-resolution. This is a general principle and the most significant property of cut-elimination by resolution.

Definition 24. *From now on we write Ω for the set of all occurrences of cut-formulas in ϕ. So, for any node N in ϕ $S(N, \Omega)$ is the subsequent of S containing the ancestors of a cut. $\bar{S}(N, \Omega)$ denotes the subsequent of S containing all non-ancestors of a cut.*

Remark 5. Note that for any sequent S occurring at a node N of ϕ, S is a permutation variant of $S(N, \Omega), \bar{S}(N, \Omega)$.

Theorem 1. *Let ϕ be a proof in an* LM*-calculus* $\mathbf{K}$*. Then there exists a W-resolution refutation of* $\mathrm{CL}(\phi)$.

Proof. According to Definition 22 we have to show that

$(*)$ for all nodes N in ϕ there exists a proof of $S(N, \Omega)$ from $\mathcal{S}_N$, where $\mathcal{S}_N$ is defined as $|\Theta(\phi)/N|$ (i.e. the set of clauses corresponding to N, see Definition 22). If N_0 is the root node of ϕ labelled by S then, clearly, no ancestor of a cut exists in S and so $S(N_0, \Omega) = \Box$. But by definition $\mathcal{S}_{N_0} = \mathrm{CL}(\phi)$. So we obtain a proof of $\Box$ from $\mathrm{CL}(\phi)$ in **K**. By the completeness of W-resolution there exists a W-resolution refutation of $\mathrm{CL}(\phi)$.

It remains to prove $(*)$:

Let N be a leaf node in ϕ. Then by definition of $\mathrm{CL}(\phi)$ $\mathcal{S}_N = \{S(N, \Omega)\}$. So $S(N, \Omega)$ itself is the required proof of $S(N, \Omega)$ from $\mathcal{S}_N$.

(IH):
Now assume inductively that for all nodes N of depth $\leq n$ in ϕ there exists a proof ψ_N of $S(N, \Omega)$ from $\mathcal{S}_N$.

So let N be a node of depth $n+1$ in ϕ. We distinguish the following cases:

(a) N is the consequent of M, i.e. N is the result of a unary inference in ϕ. That means $\phi.N =$

$$\frac{\phi.M}{S(N)}\ x$$

By (IH) there exists a proof ψ_M of $S(M, \Omega)$ from $\mathcal{S}_M$. By Definition 22 $\mathcal{S}_N = \mathcal{S}_M$. If the auxiliary formula of the last inference is in $S(M, \Omega)$ we define $\psi_N =$

$$\frac{\psi_M}{S'}\ x$$

Obviously S' is just $S(N, \Omega)$.
If the auxiliary formula of the last inference in $\phi.N$ is not in $S(M, \Omega)$ we simply drop the inference and define $\psi_N = \psi.M$. As the ancestors of cut did not change ψ_N is just a proof of $S(N, \Omega)$ from $\mathcal{S}_N$.

(b) N is the consequent of an n-ary inference for $n \geq 2$, i.e. $\phi.N =$

$$\frac{\phi.M_1 \quad \ldots \quad \phi.M_n}{S(N)}\ x$$

By (IH) there exist proofs ψ_{M_i} of $S(M_i, \Omega)$ from $\mathcal{S}_{M_i}$.

(b1) The auxiliary formulas of the last inference in $\phi.N$ are in $S(M_i, \Omega)$, i.e. the inference yields an ancestor of a cut. Then, by Definition 22

$$\mathcal{S}_N = \mathcal{S}_{M_1} \cup \ldots \cup \mathcal{S}_{M_n}.$$

Then clearly the proof ψ_N:

$$\frac{\psi_{M_1} \quad \ldots \quad \psi_{M_n}}{S'}\ x$$

is a proof of S' from $\mathcal{S}_N$ and $S' = S(N, \Omega)$.

(b2) The auxiliary formulas of the last inference in $\phi.N$ are not in $S(M_i, \Omega)$, i.e. the principal formula of the inference is not an ancestor of a cut. Then, by Definition 22

$$\mathcal{S}_N = merge(\mathcal{S}_{M_1}, \ldots, \mathcal{S}_{M_n}).$$

We write $\mathcal{S}_i$ for $\mathcal{S}_{M_i}$ and ψ_i for ψ_{M_i}, Γ_i for $S(M_i, \Omega)$ and define

$$\mathcal{D}_i = merge(\mathcal{S}_1, \ldots, \mathcal{S}_i),$$
$$\Delta_i = \Gamma_1, \ldots, \Gamma_i,$$

for $i = 1, \ldots, n$. Our aim is to define a proof ψ_N of $S(N, \Omega)$ from $\mathcal{S}_N$ where $\mathcal{S}_N = \mathcal{D}_n$.

We proceed inductively and define proofs χ_i of Δ_i from $\mathcal{D}_i$. Note that for $i = n$ we obtain a proof χ_n of $S(M_1, \Omega), \ldots, S(M_n, \Omega)$ from $\mathcal{S}_N$, and $S(N, \Omega) = S(M_1, \Omega), \ldots, S(M_n, \Omega)$. This is just what we want.

For $i = 1$ we define $\chi_1 = \psi_1$.

Assume that $i < n$ and we already have a proof χ_i of Δ_i from $\mathcal{D}_i$. For every $D \in \mathcal{S}_{i+1}$ we define a proof $\chi_i[D]$:

Replace all axioms C in χ_i by the derivation

$$\frac{C, D}{D, C}\ \pi$$

and simulate χ_i on the extended axioms (the clause D remains passive). The result is a proof $\chi'[D]$ of the sequent

$$D, \ldots, D, \Delta_i.$$

Note that the propagation of D through the proof is possible as no eigenvariable conditions can be violated, as we assume the original proof to be regular (if not then we may transform the ψ_i into proofs with mutually disjoint sets of eigenvariables) . Then we define $\chi_i[D]$ as

$$\frac{\chi'[D]}{\Delta_i, D}\ c^* + \pi$$

Next we replace every axiom D in the derivation ψ_{i+1} by the proof $\chi_i[D]$ and (again) simulate ψ_{i+1} on the end-sequents of the $\chi_i[D]$ where the Δ_i remain passive. Again we can be sure that no eigenvariable condition is violated and we obtain a proof ρ of

$$\Delta_i, \ldots, \Delta_i, \Gamma_{i+1}.$$

from the clause set $merge(\mathcal{D}_i, \mathcal{S}_{i+1})$ which is $\mathcal{D}_{i+1}$. Finally we define $\chi_{i+1} =$

$$\frac{\rho}{\Delta_i, \Gamma_{i+1}}\ \pi^* + c^*$$

Indeed, χ_{i+1} is a proof of Δ_{i+1} from $\mathcal{D}_{i+1}$. ◇

Like in the classical case ([6]) we define projections of the proof ϕ relative to clauses C in $\mathrm{CL}(\phi)$. The basic idea is the following: we drop all inferences which infer ancestors of a cut formula; the result is a cut-free proof of the end sequent extended by the clause C. Of course we do not obtain cut-elimination itself, but instead a cut free proof of the end sequent extended by a clause. These cut-free proofs are eventually inserted into a resolution proof, which eventually gives a proof with atomic cuts only.

Lemma 1. *Let ϕ be a deduction in $\mathcal{SK}[\mathbf{K}]$ of a sequent S. Let C be a clause in $\mathrm{CL}(\phi)$. Then there exists a deduction $\phi[C]$ of C, S s.t. $\phi[C]$ is cut-free (in particular $\phi(C) \in \mathcal{SK}^{\emptyset}[\mathbf{K}]$) and $\|\phi[C]\| \leq 2 * \|\phi\|$.*

Proof. Let $\mathcal{S}_N$ be $|\Theta(\phi)/N|$ (like in the proof of Theorem 1). We prove that

($\star$) for every node N in ϕ and for every $C \in \mathcal{S}_N$ there exists a proof $T(\phi, N, C)$ of $C, \bar{S}(N, \Omega)$ s.t.
$$\|T(\phi, N, C)\| \leq 2\|\phi.N\|.$$

Indeed, it is sufficient to prove ($\star$): for the root node N_0 we have $S = \bar{S}(N_0, \Omega)$ (no signed formula of the end sequent is an ancestor of Ω), $\phi.N_0 = \phi$ and $\mathrm{CL}(\phi) = \mathcal{S}_{N_0}$; so at the end we just define $\phi[C] = T(\phi, N_0, C)$ for every $C \in \mathrm{CL}(\phi)$.

We prove $\star$ by induction on the depth of a node N in ϕ.

(IB) N is a leaf in ϕ.

Then, by definition of $\mathcal{S}_N$ we have $\mathcal{S} = \{S(N, \Omega)\}$ and $C\colon S(N, \Omega)$ is the only clause in $\mathcal{S}_N$. Let $\Gamma = \bar{S}(N, \Omega)$. Then $S(N)$ (the sequent labelling the node N) is a permutation variant of C, Γ and we define $T(\phi, N, C) =$

$$\frac{S(N)}{C, \Gamma}\ \pi$$

If no permutation is necessary we just define $T(\phi, N, C) = S(N)$. In both cases

$$\|T(\phi, N, C)\| \leq 2 = 2\|\phi.N\|.$$

(IH) Assume ($\star$) holds for all nodes of depth $\leq k$.

Let N be a node of depth $k + 1$. We distinguish the following cases:

(1) N is inferred from M via a unary inference x. By Definition of the clause term we have $\mathcal{S}_N = \mathcal{S}_M$. So any clause in $\mathcal{S}_N$ is already in $\mathcal{S}_M$.

(1a) The auxiliary formula of x is an ancestor of Ω. Then clearly $\bar{S}(N, \Omega) = \bar{S}(M, \Omega)$ and we define $T(\phi, N, C) = T(\phi, M, C)$. Clearly

$$\|T(\phi, N, C)\| = \|T(\phi, M, C)\| \leq_{(IH)} 2\|\phi.M\| < 2\|\phi.N\|.$$

(1b) The auxiliary formula of x is not an ancestor of Ω. Let $\Gamma = \bar{S}(M, \Omega), \Gamma' = \bar{S}(N, \Omega)$; thus the auxiliary formula of x is in Γ. By (IH) there exists a proof $\psi: T(\phi, M, C)$ of C, Γ and $\|\psi\| \leq 2\|\phi.M\|$. We define $T(\phi, N, C) =$

$$\cfrac{\begin{array}{c}(\psi)\\ C, \Gamma\end{array}}{C, \Gamma'}\ x$$

Note that x cannot be a strong quantifier inference as the proof ϕ is skolemized and there are no strong quantifiers in the end sequent. Thus $T(\phi, N, C)$ is well-defined. Moreover

$$\|T(\phi, N, C)\| = \|T(\phi, M, C)\| + 1 \leq_{(IH)} 2\|\phi.M\| + 1 < 2\|\phi.N\|.$$

(2) N is inferred from $M_1, \ldots, M_n$ via the inference x for $n \geq 2$. By (IH) there are proofs $T(\phi, M_i, C_i)$ for $i = 1, \ldots, n$ and $C_i \in \mathcal{S}_{M_i}$. Let $\bar{S}(M_i, \Omega) = \Gamma_i$ and $\bar{S}(N, \Omega) = \Gamma'_1, \ldots, \Gamma'_n$. We abbreviate $T(\phi, M_i, C_i)$ by ψ_i.

(2a) The auxiliary formulas of x are in $\Gamma_1, \ldots, \Gamma_n$. Let C be a clause in $\mathcal{S}_N$. Then, by definition of the characteristic clause set, $C = C_1, \ldots, C_n$ for $C_i \in \mathcal{S}_{M_i}$ ($\mathcal{S}_N$ is defined by merge). We define $T(\phi, N, C)$ as

$$\cfrac{\begin{array}{ccc}(\psi_1) & & (\psi_n)\\ C_1, \Gamma_1 & \ldots & C_n, \Gamma_n\end{array}}{C_1, \ldots, C_n, \Gamma'_1, \ldots, \Gamma'_n}\ x$$

By definition of $\|\ \|$ we have

$$\|\phi.N\| = 1 + \sum_{i=1}^{n} \|\phi.M_i\|,$$

$$\|\psi_i\| \leq 2\|\phi.M_i\| \text{ by (IH)}$$

Therefore

$$\|T(\phi, N, C)\| = 1 + \sum_{i=1}^{n} \|\psi_i\| \leq 1 + 2\sum_{i=1}^{n} \|\phi.M_i\| < 2\|\phi.N\|.$$

(2b) The auxiliary formulas of x are not in $\Gamma_1, \ldots, \Gamma_n$. Let C by a clause in $\mathcal{S}_N$. Then x operates on ancestors of cuts and $\mathcal{S}_N = \bigcup_{i=1}^{n} \mathcal{S}_{M_i}$, thus $C \in \mathcal{S}_{M_i}$ for some $i \in \{1, \ldots, n\}$. Moreover $\Gamma'_i = \Gamma_i$ for $i = 1, \ldots, n$. We define $T(\phi, N, C)$ as

$$\cfrac{\cfrac{\begin{array}{c}(\psi_i)\\ C, \Gamma_i\end{array}}{C, \Gamma_i, \Gamma_1, \ldots, \Gamma_{i-1}, \Gamma_{i+1}, \ldots, \Gamma_n}\ w}{C, \Gamma_1, \ldots, \Gamma_n}\ \pi$$

Then

$$\|T(\phi, N, C)\| \leq \|\psi_i\| + 2 < 2\|\phi.N\|.$$

This conclude the induction proof. ◇

Example 5. Let ϕ' be the proof from Example 3. We have computed the set $\mathrm{CL}(\phi')$ in example 4. We select the clause $C\colon 0\colon P(\alpha),\ 0\colon P(\alpha),\ 1\colon P(\alpha)$ and compute the projection $\phi'[C]$:

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{0\colon P(\alpha),\ u\colon P(\alpha),\ u\colon Q(\alpha),\ 0\colon P(\alpha),\ 1\colon P(\alpha)}{0\colon P(\alpha),\ 0\colon P(\alpha), 1\colon P(\alpha),\ u\colon P(\alpha),\ u\colon Q(\alpha)}\ \pi}{0\colon P(\alpha),\ 0\colon P(\alpha), 1\colon P(\alpha),\ u\colon P(\alpha)\vee Q(\alpha)}\ \vee\colon u}{0\colon P(\alpha),\ 0\colon P(\alpha), 1\colon P(\alpha),\ u\colon P(\alpha)\vee Q(\alpha),\ u\colon R(\alpha)}\ w}{0\colon P(\alpha),\ 0\colon P(\alpha), 1\colon P(\alpha),\ u\colon (P(\alpha)\vee Q(\alpha))\vee R(\alpha)}\ \vee\colon u}{0\colon P(\alpha),\ 0\colon P(\alpha), 1\colon P(\alpha),\ 0\colon (Dx)((P(x)\vee Q(x))\vee R(x))}\ D\colon 0}{0\colon P(\alpha),\ 0\colon P(\alpha), 1\colon P(\alpha),\ 0\colon (Dx)((P(x)\vee Q(x))\vee R(x)),\ 1\colon P(c)}\ w$$

Let ϕ be a proof of S s.t. $\phi \in \mathcal{SK}[\mathbf{K}]$ and let γ be a W-resolution refutation of $\mathrm{CL}(\phi)$. We define a ground projection γ' of γ which is a $\mathbf{K}$-proof of $\Box$ from instances of $\mathrm{CL}(\phi)$. This proof γ' can be transformed into a proof $\gamma'[\phi]$ of S from the axiom set $\mathcal{A}$ s.t. $\gamma'[\phi] \in \mathcal{SK}^0[\mathbf{K}]$ ($\gamma'[\phi]$ is a proof with atomic cuts). Indeed, γ' is the skeleton of the proof of S with atomic cuts and the real core of the end result; $\gamma'[\phi]$ can be considered as an application of γ' to (the projections of) ϕ.

Theorem 2. *Let ϕ be a proof of S from $\mathcal{A}$ in $\mathcal{SK}[\mathbf{K}]$ and let γ' be a ground projection of a W-refutation of* $\mathrm{CL}(\phi)$. *Then there exists a proof $\gamma'[\phi]$ of S with $\gamma'[\phi] \in \mathcal{SK}^0[\mathbf{K}]$ and*

$$\|\gamma'[\phi]\| \leq \|\gamma'\|(2 * \|\phi\| + l(S) + 2).$$

Proof. We construct $\gamma'[\phi]$:

(1) Replace every axiom C in γ' by the projection $\phi[C]$. Then instead of C we obtain the proof $\phi[C]$ of C, S. For every occurrence of an axiom C in γ we obtain a proof of length $\leq 2 * \|\phi\|$ (by Lemma 1).

(2) Apply the permutation rule to all end sequents of the $\phi[C]$ and infer S, C. The result is a proof $\psi[C]$ with $\|\psi[C]\| \leq 2 * \|\phi\| + 1$.

(3) Simulate γ' on the extended sequents S, C, where the left part S remains passive (note that, according to our definition, inferences take place on the right). The result is a proof χ of a sequent $S, \ldots, S$ from $\mathcal{A}$ s.t.

$$\|\chi\| \leq \|\gamma'\| * (2 * \|\phi\| + 1) + \|\gamma\|.$$

Note that χ is indeed a $\mathbf{K}$-proof as all inferences in γ' are also inferences of $\mathbf{K}$.

(4) Apply one permutation and contractions to the end sequent of χ for obtaining the end sequent S. The resulting proof is $\gamma'[\phi]$, the proof we are searching for. As the number of occurrences of S in the end sequent is $\leq \|\gamma'\|$ the additional number of inferences is $\leq 1 + l(S) * \|\gamma'\|$. By putting things together we obtain

$$\|\gamma'[\phi]\| \leq \|\gamma'\|(2 * \|\phi\| + l(S) + 2).$$

◇

Looking at the estimation in Theorem 2 we see that the main source of complexity is the length of the W-resolution proof γ'. Indeed, γ (and thus γ') can be considered as the characteristic part of $\gamma'[\phi]$ representing the essence of cut-elimination. To sum up the procedure CERES-m for cut-elimination in any LM-type logic **K** cab be defined as:

Definition 25 (CERES-m).

input :$\phi \in \mathcal{P}[\mathbf{K}]$.
construct a Skolem form ϕ' *of* ϕ.
compute $\mathrm{CL}(\phi')$.
construct a W*-refutation* γ *of* $\mathrm{CL}(\phi')$.
compute a ground projection γ' *of* γ.
compute $\gamma'[\phi']$ $(\gamma'[\phi'] \in \mathcal{SK}^0[\mathbf{K}])$.
reskolemize $\gamma'[\phi']$ *to* ϕ'' $(\phi'' \in \mathcal{P}^0[\mathbf{K}])$.

Example 6. The proof ϕ from Example 1 has been skolemized to a proof ϕ' in Example 3. In Example 4 we have computed the characteristic clause set $\mathrm{CL}(\phi')$ and gave a refutation γ of $\mathrm{CL}(\phi')$ and a ground projection $\gamma' \colon \gamma\{\alpha \leftarrow c\}$. Recall γ':

$$\dfrac{\dfrac{\dfrac{0\colon P(c),\ 0\colon P(c),\ 1\colon P(c) \quad u\colon P(c)}{0\colon P(c),\ 0\colon P(c)}\,cut_{1u}}{0\colon P(c)}\,c \qquad u\colon P(c)}{\Box}\,cut_{0u}$$

and the instances $C'_1 = u\colon P(c)$ and $C'_2 = 0\colon P(c),\ 0\colon P(c),\ 1\colon P(c)$ of two signed clauses in $\mathrm{CL}(\phi')$ which defined the axioms of γ'. We obtain $\gamma'[\phi']$ by substituting the axioms C'_1, C'_2 by the projections $\phi[C'_1], \phi[C'_2]$ ($\phi[C'_2]$ is an instance of the projection computed in Example 5). The end sequent of ϕ' is

$$S\colon\ 0\colon (Dx)((P(x) \vee Q(x)) \vee R(x)), 1\colon P(c)$$

So we obtain $\gamma'[\phi'] =$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(\phi'[C'_2])}{0\colon P(c),\ 0\colon P(c),\ 1\colon P(c),\ S}}{S,\ 0\colon P(c),\ 0\colon P(c),\ 1\colon P(c)}\,\pi \quad \dfrac{\dfrac{(\phi[C'_1])}{u\colon P(c),\ S}}{S,\ u\colon P(c)}\,\pi}{S,\ S,\ 0\colon P(c),\ 0\colon P(c)}\,cut_{1u}}{S,\ S,\ 0\colon P(c)}\,c \qquad \dfrac{\dfrac{(\phi[C'_1])}{u\colon P(c),\ S}}{S,\ u\colon P(c)}\,\pi}{S,\ S,\ S}\,cut_{0u}}{S}\,c^*$$

5 Conclusion

Besides establishing a feasible cut-elimination method for many-valued first order logics the main aim of this paper is to demonstrate the stability of CERES w.r.t. cut elimination problems beyond classical first order logic. The authors are convinced, that this stability of CERES will it enable to incorporate intrinsic non-classical logics such as intuitionistic logic and possibly to extend CERES to the second order case, where inductive methods of cut-elimination fail by Gödel's Second Incompleteness Theorem.

References

1. M. Baaz, C. Fermüller: Resolution-Based Theorem Proving for Many-Valued Logics, *Journal of Symbolic Computation*, **19**(4), pp. 353-391, 1995.
2. M. Baaz, C. Fermüller, G. Salzer: Automated Deduction for Many-Valued Logics, in: Handbook of Automated Reasoning 2, eds. J. A. Robinson, A. Voronkov, Elsevier and MIT Press, pp. 1356-1402, 2001.
3. M. Baaz, C. Fermüller, R. Zach: Elimination of Cuts in First-order Finite-valued Logics, *J. Inform. Process. Cybernet. (EIK)*, **29**(6) , pp. 333-355, 1994.
4. M. Baaz, A. Leitsch: Cut normal forms and proof complexity, *Annals of Pure and Applied Logic*, **97**, pp. 127-177, 1999.
5. M. Baaz, A. Leitsch: Cut-Elimination and Redundancy-Elimination by Resolution, *Journal of Symbolic Computation*, **29**, pp. 149-176, 2000.
6. M. Baaz, A. Leitsch: Towards a Clausal Analysis of Cut-Elimination, *Journal of Symbolic Computation*, to appear.
7. W. A. Carnielli: Systematization of Finite Many-Valued Logics through the Method of Tableaux, *Journal of Symbolic Logic*, **52**(2), pp. 473-493, 1987.
8. G. Gentzen: Untersuchungen über das logische Schließen, *Mathematische Zeitschrift* **39**, pp. 405–431, 1934–1935.