Cut-elimination for Provability Logic *GL* Resolved

Rajeev Goré and Revantha Ramanayake

Computer Sciences Laboratory
The Australian National University, Canberra.
`{ rajeev.gore, revantha }@rsise.anu.edu.au`

September 2, 2008

The modal provability logic *GL*

- Let K denote the basic propositional modal logic
- $GL = K + \Box(\Box A \supset A) \supset \Box A$ (Löb's axiom)
- characterised by Kripke frames satisfying transitivity and no ∞-R-chains (we cannot have $w_1 R w_2 \ldots w_n R w_{n+1} R \ldots$)
- Interpreting $\Box A$ as "A is provable in Peano arithmetic", *GL* is sound and complete wrt formal provability interpretation in Peano arithmetic
- Hence the name *provability logic*
- (Sambin and Valentini, 1982) proposed the sequent rule

$$\frac{\Box X, X, \Box B \Rightarrow B}{\Box X \Rightarrow \Box B} \; GLR$$

where B is a formula and X is formula set
$\Box B$ is called the *diagonal formula*

The set based sequent calculus GLS_{set} for GL

Initial sequents: $A \Rightarrow A$ for each formula A

Logical rules:

$$\frac{X \Rightarrow Y, A}{X, \neg A \Rightarrow Y}\ L\neg \qquad \frac{A, X \Rightarrow Y}{X \Rightarrow Y, \neg A}\ R\neg$$

$$\frac{A_i, X \Rightarrow Y}{A_1 \wedge A_2, X \Rightarrow Y}\ L\wedge \qquad \frac{X \Rightarrow Y, A_1 \qquad X \Rightarrow Y, A_2}{X \Rightarrow Y, A_1 \wedge A_2}\ R\wedge$$

$$\frac{A_1, X \Rightarrow Y \qquad A_2, X \Rightarrow Y}{A_1 \vee A_2, X \Rightarrow Y}\ L\vee \qquad \frac{X \Rightarrow Y, A_i}{X \Rightarrow Y, A_1 \vee A_2}\ R\vee$$

$$\frac{X \Rightarrow Y, A \qquad B, U \Rightarrow W}{A \supset B, X, U \Rightarrow Y, W}\ L\supset \qquad \frac{A, X \Rightarrow Y, B}{X \Rightarrow Y, A \supset B}\ R\supset$$

Modal rule:

$$\frac{\Box X, X, \Box A \Rightarrow A}{\Box X \Rightarrow \Box A}\ GLR$$

Structural rules:

$$\frac{X \Rightarrow Y}{A, X \Rightarrow Y}\ LW \qquad \frac{X \Rightarrow Y}{X \Rightarrow Y, A}\ RW$$

$$\frac{X \Rightarrow Y, A \qquad A, U \Rightarrow W}{X, U \Rightarrow Y, W}\ cut$$

Cut-elimination versus semantic completeness

The cut-rule is:

$$\frac{X \Rightarrow Y, A \qquad A, U \Rightarrow W}{X, U \Rightarrow Y, W}\ cut$$

Does not support backward proof search. Cut-free calculus yields simple consistency proof.

- Semantic completeness of the calculus minus cut is well known
- Cut-elimination (CE): exhibiting a constructive procedure transforming a given derivation τ into a cutfree derivation τ' with identical end-sequent
- Cut-elimination may or may not hold depending on the form of the sequent rules

Cut-elimination for *GL* - a brief history

- Leivant (1981) suggests a proof of CE, counter-example given by Valentini (1982)
- new proof of CE for GLS_{set} proposed by Valentini (1983) — induction on $degree \cdot \omega^2 + width \cdot \omega + cutheight$
- Subsequently Borga (1983) and Sasaki (2001) present new proofs
- All the above proofs are for *set*-based sequent calculi
- In 2001, Moen claimed that Valentini's cut-elimination procedure does not terminate for certain derivations in a multiset-based version GLS_{multi} of GLS_{set}
- Moen formalises Valentini's proof using reduction sequences and appeals to the Church–Rosser property to obtain his (non)termination result

Building sequents from multisets

- the crucial question for sets is membership so $\{A\}$ and $\{A, A\}$ are the same set
- *multisets*: order not important, number of occurrences important. So $\{A\}$ and $\{A, A\}$ are different multisets
- using sequents built from sets 'hides' instances of the contraction rule. Eg: GLS_{set} (left) versus GLS_{multi} (right)

$$\frac{P \wedge Q, P, X \Rightarrow Y}{P \wedge Q, X \Rightarrow Y} L\wedge \qquad \frac{\dfrac{P \wedge Q, P, X \Rightarrow Y}{P \wedge Q, P \wedge Q, X \Rightarrow Y} L\wedge}{P \wedge Q, X \Rightarrow Y} LC(P \wedge Q)$$

- more formal to account for all contraction rules

The sequent calculus GLS_{multi}

- GLS_{multi} uses sequents built from multisets
- initial sequents, logical, modal, structural rules have same form as GLS_{set}
- ... although the X, Y represent multisets now
- Also the following contraction rules are required:

$$\frac{A, A, X \Rightarrow Y}{A, X \Rightarrow Y}\ LC \qquad \frac{X \Rightarrow Y, A, A}{X \Rightarrow Y, A}\ RC$$

Moen claims failure of Valentini's procedure

Claim: Valentini's procedure does not terminate for certain proofs in GLS_{multi} (Moen, 2001)

Consequences:

- "When an explicit rule of contraction is added . . . the reduction . . . needs further justification" (Negri, 2005). Presents a proof of CE for a *non-standard* calculus $G3GLS$ using labelled formulae of the form $x : A$
- ". . . the author was informed . . . [no] accepted syntactic cut elimination proof . . . for a standard sequent formulation" (Mints, 2006). Presents a new proof, not based on Valentini's procedure.
- ". . . my cut-elimination procedure seems not to be working in this case (Anders Moen found a non-terminating elimination in this case)" (Valentini, 2007) [personal correspondence]

So where is the problem?

Valentini's procedure is complicated so the source of the problem is not easy to find.

Is the problem with:

- Valentini's original proof for GLS_{set}?
- extending Valentini's proof to a multiset sequent calculus?
- Moen's claim that Valentini's procedure does not always terminate for GLS_{multi}?

So where is the problem?

Is the problem with:

- Valentini's original proof for GLS_{set}?
  No, the proof is essentially correct
- extending Valentini's proof to a multiset sequent calculus?
  Not really. The proof can be made to work. The case of contractions above cut requires special attention
- Moen's work that implies that Valentini's transformation does not always terminate?
  Yes, there is an error in Moen's work

To clarify these issues, the cut-elimination proof must be placed in a formal setting

Definitions

Definition

A *derivation* is an initial sequent or an application of a logical, modal or structural rule to derivations concluding its premises.

Definition

The *degree* $d(A)$ of a formula A.

1. $d(P) = 1$ for a propositional variable P
2. $d(A \wedge B) = d(A \vee B) = d(A \supset B) = d(A) + d(B) + 1$
3. $d(\neg A) = d(A) + 1$
4. $d(\Box A) = d(A) + 1$.

Definitions (cont.)

Definition

The *height* $h(\tau)$ of a derivation τ:

1. $h(A \Rightarrow A) = 1$ (initial sequent)
2. $h(\frac{\tau_1}{X \Rightarrow Y}) = s(\tau_1) + 1$ (unary rule)
3. $h(\frac{\tau_1 \quad \tau_2}{X \Rightarrow Y}) = \max(s(\tau_1), s(\tau_2)) + 1$ (binary rule)

Definition

The *cut-height* of an instance of the cut-rule with premise derivations τ_1 and τ_2 is the sum of the heights $s(\tau_1)$ and $s(\tau_2)$ of the premise derivations

Sambin Normal Form

A derivation is in Sambin Normal Form when:

- the last rule is the cut rule with cutfree premises
- the cut-formula is principal by *GLR* in both premises

$$\dfrac{\dfrac{\dfrac{\{\pi\}_1^r}{\Box X, X, \Box B \overset{k}{\Rightarrow} B}}{\Box X \overset{k+1}{\Rightarrow} \Box B}\,GLR \qquad \dfrac{\dfrac{\{\sigma\}_1^s}{\Box B, B, \Box U, U, \Box D \overset{l}{\Rightarrow} D}}{\Box B, \Box U \overset{l+1}{\Rightarrow} \Box D}\,GLR}{\Box X, \Box U \Rightarrow \Box D}\,cut(\Box B)$$

where Π and Ω are cutfree

cut-height is $(k+1)+(l+1)$. degree of cut-formula is $d(\Box B)$.

The main case — a derivation in SNF

$$\dfrac{\dfrac{\dfrac{\{\pi\}_1^r}{\Box X, X, \Box B \overset{k}{\Rightarrow} B}}{\Box X \overset{k+1}{\Rightarrow} \Box B}\, GLR \qquad \dfrac{\dfrac{\{\sigma\}_1^s}{\Box B, B, \Box U, U, \Box D \overset{l}{\Rightarrow} D}}{\Box B, \Box U \overset{l+1}{\Rightarrow} \Box D}\, GLR}{\Box X, \Box U \Rightarrow \Box D}\, cut(\Box B)$$

A naive transformation to eliminate cut:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\{\pi\}_1^r}{\Box X, X, \Box B \overset{k}{\Rightarrow} B}}{\Box X \overset{k+1}{\Rightarrow} \Box B}\, GLR \qquad \dfrac{\dfrac{\{\pi\}_1^r}{\Box X, X, \Box B \overset{k}{\Rightarrow} B} \qquad \dfrac{\{\sigma\}_1^s}{\Box B, B, \Box U, U, \Box D \overset{l}{\Rightarrow} D}}{\Box X, X, \Box B, \Box U, U, \Box D \overset{[k,l]+1}{\Rightarrow} D}\, cut_1}{\Box X, X, \Box X, \Box U, U, \Box D \Rightarrow D}\, cut_2}{\Box X, X, \Box U, U, \Box D \Rightarrow D}\, LC^*(\Box X)}{\Box X, \Box U \Rightarrow \Box D}\, GL$$

Cut-height is $k + l$ (cut_1) and $(k+1) + ([k,l]+1)$ (cut_2)
Problem with cut_2 ! (possibly greater than before)

A successful transformation for SNF

Transform derivation in SNF to:

$$
\dfrac{
\dfrac{\{\pi'\}_1^t}{\Box X, X \Rightarrow {\color{red}B}}
\qquad
\dfrac{
\dfrac{\dfrac{\{\pi\}_1^r}{\Box X, X, \Box B \overset{k}{\Rightarrow} B}}{\Box X \overset{k+1}{\Rightarrow} {\color{red}\Box B}}\,GLR
\qquad
\dfrac{\{\sigma\}_1^s}{{\color{red}\Box B}, B, \Box U, U, \Box D \overset{l}{\Rightarrow} D}
}{\Box X, {\color{red}B}, \Box U, U, \Box D \Rightarrow D}\,cut_1
}{
\dfrac{\dfrac{\Box X, \Box X, X, \Box U, U, \Box D \Rightarrow D}{\Box X, X, \Box U, U, \Box D \Rightarrow D}\,LC^*(\Box X)}{\Box X, \Box U \Rightarrow \Box D}\,GLR
}\,cut_2
$$

where $\{\pi'\}_1^t$ is some cut-free derivation.

- cut_1 has cut-height $(k+1)+l$
- cut_2 has smaller degree of cut-formula

New task: given a derivation of $\Box X, X, \Box B \Rightarrow B$ obtain a cutfree derivation of $\Box X, X \Rightarrow B$

A sketch of the proof

- identify the number n of occurrences of the following schema, where no GLR rule occurrences appear between GLR_1 and the endseqent.

$$\dfrac{\dfrac{\Box G, G, \Box B, B, \Box C \Rightarrow C}{\Box G, \Box B \Rightarrow \Box C}\; GLR_1}{\underset{\vdots \quad (GLR\text{-free})}{}\over \Box X, X, \Box B \Rightarrow B}$$

- If $n = k + 1$, each occurrence of the above schema is deleted using appropriate transformation
- Intuition:

$$\dfrac{\Box C \Rightarrow \Box C}{\Box G, \Box B, \Box C \Rightarrow \Box C}\; LW(\Box G, \Box B)$$

- now need to remove the $\Box C$ in the antecedent!

A sketch of the proof (cont.)

If $n = 0$ then the $\Box B$ formula occurrence in the endsequent of τ has either been introduced by

1. $LW(\Box B)$. In this case delete the $LW(\Box B)$ rule. Or,
2. the initial sequent $\Box B \Rightarrow \Box B$. Substitute with the following:

$$\dfrac{\dfrac{\{\pi\}_1^r}{\Box X, X, \Box B \Rightarrow B}}{\Box X \Rightarrow \Box B}\ GLR$$

- *width*: the number of occurrences of the schema
- proof uses induction on width

Why a formal approach is necessary

- to maintain integrity of induction, we need to ensure new (ie introduced) cuts have width $< n$
- especially since for a given derivation of $\Box X, X, \Box B \Rightarrow B$, the transformed derivation $\Box X, X \Rightarrow B$ introduces many new cuts,
- we need to make sure that elimination of a topmost cut does not increase width of any introduced lower cuts.

Identifying the parametric ancestors of the diagonal formula

We trace the diagonal formula in the premise of the *GLR* rule:

Example. (diagonal formula is $\Box\Box A$ here)

$$\dfrac{\dfrac{\dfrac{\dfrac{\{\pi\}_1^r}{\Box C, C, \Box\Box A, \Box A, \Box A \Rightarrow A}}{\Box C, {\color{red}(\Box\Box A)^\circ} \Rightarrow \Box A}\,GLR \qquad \dfrac{\dfrac{\{\sigma\}_1^s}{\Box D \Rightarrow \Box A}}{\Box D, {\color{red}(\Box\Box A)^\circ} \Rightarrow \Box A}\,LW}{\Box C \lor \Box D, {\color{red}(\Box\Box A)^*} \Rightarrow \Box A}\,L\lor}{\Box(\Box C \lor \Box D), \Box C \lor \Box D, {\color{red}(\Box\Box A)^*} \Rightarrow \Box A}\,LW$$

- non-final parametric ancestors of $\Box\Box B$ annotated with $*$
- final parametric ancestors annotated with $\circ$

Definition of width

Define $\partial^\circ(\Box B, \tau)$ as the number of instances of the *GLR* rule in τ whose conclusion contains an occurrence of $(\Box B)^\circ$. Eg:

$$\dfrac{\Box C, C, \Box\Box A, \Box A, \Box A \Rightarrow A}{\Box C, {\color{red}(\Box\Box A)}^\circ \Rightarrow \Box A} \; GLR$$

Let cut_0 be a topmost cut as shown below:

$$\dfrac{\dfrac{\dfrac{\{\pi\}_1^r}{\Box X, X, \Box B \Rightarrow B}}{\Box X \Rightarrow \Box B} \; GLR \qquad \dfrac{\{\sigma\}_1^s}{\Box B, U \Rightarrow W}}{X, U \Rightarrow Y, W} \; cut_0$$

Define $width(cut_0)$ as $\partial^\circ\left(\Box B, \dfrac{\{\pi\}_1^r}{\Box X, X, (\Box B)^* \Rightarrow B}\right)$

Defining stub-derivations

- a stub-derivation $d[stub]$ is a derivation where some premise derivation has been “removed” and replaced with stub. It has the form

$$\frac{\text{stub}}{X \Rightarrow Y}\,\rho \qquad \frac{\text{stub} \qquad \Pi}{X \Rightarrow Y}\,\rho \qquad \frac{\Pi \qquad \text{stub}}{X \Rightarrow Y}\,\rho$$

- We say that stub-derivation $d[stub]$ and derivation d' are *compatible* when

$$\frac{d'}{\mathcal{S}}\,\rho \qquad \frac{d' \qquad \Pi}{\mathcal{S}}\,\rho \qquad \frac{\Pi \qquad d'}{\mathcal{S}}\,\rho$$

is a legal derivation

- We write the above derivation as $d[\text{stub}] \leftarrow d'$

Interaction between width and stub-derivations

- motivation: to keep track of width as we substitute premise derivations inside a given derivation

For example, we can show

Theorem

Let $d[\mathrm{stub}]$ *be a stub-derivation and* d' *a derivation such that* $d[\mathrm{stub}]$ *and* d' *are compatible. Then*

$$\partial^{\circ}(B, d[\mathrm{stub}] \leftarrow d') = \partial^{\circ}(B, d[\mathrm{stub}]) + \partial^{\circ}(B, d')$$

if d'' is a derivation compatible with $d[\mathrm{stub}]$, and $\partial^{\circ}(B, d'') < \partial^{\circ}(B, d')$, we get

$$\partial^{\circ}(B, d[\mathrm{stub}] \leftarrow d'') < \partial^{\circ}(B, d[\mathrm{stub}] \leftarrow d')$$

Contractions above cut for boxed formulae

$$\dfrac{\dfrac{\Box X, X, \Box B \overset{k}{\Rightarrow} B}{\Box X \overset{k+1}{\Rightarrow} \Box B}\,GLR \qquad \dfrac{\dfrac{\dfrac{\Box B, \Box B, B, B, \Box U, U, \Box C \overset{l}{\Rightarrow} C}{\Box B, \Box B, \Box U \overset{l+1}{\Rightarrow} \Box C}\,GLR}{\Box B, \Box U \overset{l+2}{\Rightarrow} \Box C}\,LC(\Box B)}{\Box X, \Box U \Rightarrow \Box C}\,cut$$

is transformed to

$$\dfrac{\dfrac{\dfrac{\overset{\Sigma}{\Box X, X \Rightarrow B} \qquad \dfrac{\dfrac{\Box X \overset{k+1}{\Rightarrow} \Box B \qquad \dfrac{\Box B, \Box B, B, B, \Box U, U, \Box C \overset{l}{\Rightarrow} C}{\Box B, B, B, \Box U, U, \Box C \overset{l+1}{\Rightarrow} C}\,LC(\Box B)}{\Box X, B, B, \Box U, U, \Box C \Rightarrow C}\,cut_1(\Box B)}{\Box X, B, \Box U, U, \Box C \Rightarrow C}\,LC(B)}{\Box X, X, \Box X, \Box U, U, \Box C \Rightarrow C}\,cut_2(B)}{\dfrac{\Box X, X, \Box U, U, \Box C \Rightarrow C}{\Box X, \Box U \Rightarrow \Box C}\,GLR}\,LC^*(\Box X)$$

where $\Box X, X \Rightarrow B$ is obtained as described before.
cut_1 has lesser cut-height, cut_2 has smaller degree

Why Moen's argument is incorrect

Moen does not faithfully implement Valentini's procedure. He uses a transformation titled Val-II(core):

$$
\dfrac{
  \dfrac{
    \dfrac{\dfrac{\Pi}{\Box X, X, \Box B \overset{k}{\Rightarrow} B}}{\Box X \overset{k+1}{\Rightarrow} \Box B}\,GLR
    \qquad
    \dfrac{\Pi}{\Box X, X, \Box B \overset{k}{\Rightarrow} B}
  }{\Box X, \Box X, X \Rightarrow B}\,cut_{val}
  \qquad
  \dfrac{
    \dfrac{\dfrac{\Pi}{\Box X, X, \Box B \Rightarrow B}}{\Box X \Rightarrow \Box B}\,cut
    \qquad
    \dfrac{\Omega}{\Box B, B, \Box U, U, \Box D \Rightarrow D}
  }{\Box X, B, \Box U, U, \Box D \Rightarrow D}
}{
  \dfrac{
    \dfrac{\Box X, \Box X, \Box X, X, \Box U, U, \Box D \Rightarrow D}{\Box X, X, \Box U, U, \Box D \Rightarrow D}
  }{\Box X, \Box U \Rightarrow \Box D}\,LC^{*}(\Box X)
}\,cut
$$

In this transformation cut_{val} has

- degree same as before
- width same as before
- cut-height $(k+1)+k$ (possibly greater than before)

So cut_{val} cannot be eliminated by induction hypothesis !