Generic Methods for Formalising Sequent Calculi Applied to Provability Logic

Jeremy Dawson and Rajeev Goré

Logic and Computation Group
School of Computer Science
College of Engineering and Computer Science
Australian National University
Canberra ACT 0200, Australia
http://users.rsise.anu.edu.au/~jeremy/
http://users.rsise.anu.edu.au/~rpg/

October 7, 2010

Outline

Introduction

Formalisation of cut-admissibility for the GLS sequent system

- cut-admissibility applies for many sequent systems
- proofs can be tedious — details omitted ("other cases are similar")
- we try to get common elements of the proofs for re-use
- provability logic has unusual features (*GL* rule has formula on both sides of $\vdash$), proof more complex
- previous proofs wrong, or allegedly so but actually OK
- formalised proof in Isabelle/HOL confirms the result, omits no details, and uses many lemmas applicable for other logics

Sequents and Multisets, Sets and Provability Logic

- sequents $\Gamma \vdash \Delta$ where Γ and Δ are "collections" of formulae
- Our "collections" are multisets (unordered, but repetitions counted)
- Tree-shaped derivations, conclusion at the bottom
- Tree branches where rule has > 1 premise, leaf where rule has no premises

Provability Logic

- explicit weakening and contraction rules
- usual (additive) rules for $\neg, \wedge, \vee, \rightarrow$
- additional rule *GLR* which characterises **GL**:

$$\frac{\Box X, X, \Box B \vdash B}{\Box X \vdash \Box B}\ GLR \text{ or } GLR(B) \text{ or } GLR(X, B)$$

- in our formalisation, cut or multicut rules not part of GLS

$$(\text{cut})\ \frac{\Gamma \vdash A, \Delta \qquad \Gamma, A \vdash \Delta}{\Gamma \vdash \Delta}$$

$$(\text{multicut})\ \frac{\Gamma' \vdash A^n, \Delta' \qquad \Gamma'', A^m \vdash \Delta''}{\Gamma', \Gamma'' \vdash \Delta', \Delta''}$$

Derivability Predicates and their Induction Principles

An inference rule is a list of premises and a conclusion. Then

- `derrec rls prems` is the set of sequents derivable using rules `rls` from the set `prems` of premises.

The induction principle (simplified) from the definition of `derrec` :

$$\frac{x \in derrec\ rls\ prems \qquad \forall c \in prems.\ P\ c \qquad \forall (ps, c) \in rls.\ (\forall p\ in\ ps.\ P\ p) \Rightarrow P\ c}{P\ x}$$

Induction on two derivations

Induction for a property of two derivations (eg cut-admissibility!)

$$\frac{cl \in derrec\ rlsl\ \{\} \qquad cr \in derrec\ rlsr\ \{\} \qquad \forall (lps, lc) \in rlsl.\ \forall (rps, rc) \in rlsr.\ (\forall lp \in lps.\ P\ lp\ rc) \wedge (\forall rp \in rps.\ P\ lc\ rp) \Rightarrow P\ lc\ rc}{P\ cl\ cr}$$

To prove $P(\mathcal{C}_l, \mathcal{C}_r)$, the induction hypothesis is that $P(\mathcal{P}_{li}, \mathcal{C}_r)$ and $P(\mathcal{C}_l, \mathcal{P}_{rj})$ hold for all i and j:

$$\frac{\dfrac{\mathcal{P}_{l1} \ldots \mathcal{P}_{ln}}{\mathcal{C}_l}\rho_l \qquad \dfrac{\mathcal{P}_{r1} \ldots \mathcal{P}_{rm}}{\mathcal{C}_r}\rho_r}{?}\ (cut\ ?)$$

The Induction Pattern in Cut-Admissibility Proofs

Definition of gen_step2ssr

In the diagram below, to prove $P(\mathcal{C}_l, \mathcal{C}_r)$, the induction hypothesis is that $P(\mathcal{P}_{li}, \mathcal{C}_r)$ and $P(\mathcal{C}_l, \mathcal{P}_{rj})$ hold for all i and j:

$$\frac{\dfrac{\mathcal{P}_{l1} \ldots \mathcal{P}_{ln}}{\mathcal{C}_l}\mathcal{R}_l \qquad \dfrac{\mathcal{P}_{r1} \ldots \mathcal{P}_{rm}}{\mathcal{C}_r}\mathcal{R}_r}{?}\ (cut\ ?)$$

`gen_step2ssr` expresses that property P holds, given appropriate inductive hypotheses, for last rules on each side $\mathcal{R}_l$ and $\mathcal{R}_r$.
P might be that cut-admissibility holds for cut-formula A, rule set `rls`, assuming it holds for smaller cut-formulae

The Induction Pattern in Cut-Admissibility Proofs

- We defined a predicate `gen_step2ssr` (see the paper, Defnition 1), which says that you can prove the inductive step at a point in the derivation
- We proved a lemma which says that if this property holds throughout a tree for a property P, then P holds (Theorem 1)
- Then we proved that this predicate `gen_step2ssr` holds for the case where the cut-formula A is parametric on the left, subject to certain conditions: a result applicable to many cut-elimination proofs (Theorem 2)

Introduction Sequents, Multisets, Sets and Provability Logic Reasoning About Derivations and Derivability Capturing the Core of

The proof of Goré & Ramanayake, and our proof

The proof of Goré & Ramanayake

- Proves admissibility of (*cut*) (we prove admissibility of (*multicut*))
- Induction on height of derivation and on "width"
- Induction on size of cut-formula.

In contrast, in our proof

- we prove admissibility of (*multicut*)
- Induction on "fact of" derivation and on `del0` (approximates to ∂^0, related to width)
- Well-founded induction on immediate subformula relation

Introduction Sequents, Multisets, Sets and Provability Logic Reasoning About Derivations and Derivability Capturing the Core of

Deep and Shallow Embeddings — Derivations

- Deep or shallow embeddings of *derivations*, *rules* and *variables*.
- *shallow* means that a feature in the logic is identified with the same feature of Isabelle/HOL

Derivations:

- Deep: the actual derivation tree is a data structure in HOL

```
datatype 'a dertree = Der 'a ('a dertree list)
    | Unf 'a (* unfinished leaf not proved *)
```

  there is a predicate which tests whether each node of an derivation tree is an instance of a rule
- Shallow: no derivation tree data structure, but an inductive definition in HOL saying what formulae are derivable; (the course of a proof, in HOL, of a formula, could be described by a derivation tree)

Introduction Sequents, Multisets, Sets and Provability Logic Reasoning About Derivations and Derivability Capturing the Core of

Using a deep embedding — explicit derivation trees

To define `del0` on a derivation we need an explicit derivation tree

A *valid* tree is one whose inferences are in the set of rules and which as a whole has no premises.

Lemma

Sequent $X \vdash Y$ is derivable, shallowly, from the empty set of premises using rules `rls` (ie, is in `derrec rls {}`) iff some explicit derivation tree `dt` is valid wrt. `rls` and has a conclusion $X \vdash Y$.

```
"(?a : derrec ?rls {}) =
   (EX dt. valid ?rls dt & conclDT dt = ?a)"
```

can "mix and match" a deep embedding (derivation trees) with a shallow embedding (inductively defined sets of derivable sequents)

Introduction Sequents, Multisets, Sets and Provability Logic Reasoning About Derivations and Derivability Capturing the Core of

Defining `del0`

Definition (`del0`)

For derivation tree `dt` and formula B, define `del0` B `dt`:

- if the bottom rule of `dt` is $GLR(Y, A)$ (for *any* Y, A), then `del0` B `dt` is 1 (0) if $\Box B$ is (is not) in the antecedent of the conclusion of `dt`
- if the bottom rule of `dt` is not GLR, then `del0` B `dt` is obtained by summing `del0` B `dt'` over all premise subtrees `dt'` of `dt`.

ie, you go up each branch of an explicit derivation tree until you find an instance of the GLR rule, and count 1 where B is in Y

$$\frac{\Box Y, Y, \Box A \vdash A}{\Box Y \vdash \Box A}$$

Introduction Sequents, Multisets, Sets and Provability Logic Reasoning About Derivations and Derivability Capturing the Core of

The Proof

Lemma

If μ is a valid derivation tree with conclusion $\Box X, X, \Box B \vdash B$, and `del0` B $\mu = 0$, then $\Box X, X \vdash B$ is derivable.

Proof.

Applying the GLR rule to the $\Box X, X, \Box B \vdash B$ gives $\Box X \vdash \Box B$. Tracing upwards, change each $\Box B$ to $\Box X$ in the usual way. Contraction is not problematic since we use, as the inductive hypothesis, that *all* occurrences of $\Box B$ can be replaced by $\Box X$. □

Introduction Sequents, Multisets, Sets and Provability Logic Reasoning About Derivations and Derivability Capturing the Core of

Defining `muxbn`

$$\dfrac{\mu\left\{\dfrac{\dfrac{\Pi_l}{\Box X, X, \Box B \vdash B}}{\Box X \vdash \Box B}\right. GLR(B) \qquad \dfrac{\Pi_r}{\Box B^k, Y \vdash Z}\,\rho}{\Box X, Y \vdash Z}\ (multicut\ ?)$$

Figure: A multicut on cut formula $\Box B$ where $\Box B$ is left-principal via GLR

Definition (`muxbn`)

`muxbn` B n holds iff: for all instances of Figure 1 (for fixed B) such that `del0` B $\mu \leq n$, the multicut in Figure 1 is admissible.

Lemma

If multicut on B is admissible, then `muxbn` B 0 holds.

Introduction Sequents, Multisets, Sets and Provability Logic Reasoning About Derivations and Derivability Capturing the Core of

Proofs of `muxbn`

$$\dfrac{\mu\left\{\dfrac{\dfrac{\Pi_l}{\Box X, X, \Box B \vdash B}}{\Box X \vdash \Box B}\right. GLR(B) \qquad \dfrac{\Pi_r}{\Box B^k, Y \vdash Z}\,\rho}{\Box X, Y \vdash Z}\ (multicut\ ?)$$

Lemma

If multicut on B is admissible, then `muxbn` B 0 holds.

Proof.

$\Box X \vdash \Box B$ is derivable from $\Box X, X, \Box B \vdash B$ via $GLR(X, B)$. By Lemma 3, $\Box X, X \vdash B$ is derivable. The rest of the proof is by induction on the derivation of $\Box B^k, Y \vdash Z$, in effect, by tracing relevant occurrences of $\Box B$ up that derivation. If an inference $GLR(Y, C)$ is encountered, with B in Y, then a proof is constructed using the previous lemma □

From muxbn B n to muxbn B $(n+1)$

$$\dfrac{\mu\left\{\dfrac{\Pi_l}{\Box X, X, \Box B \vdash B}\right.}{\Box X \vdash \Box B}\; GLR(B)$$

Suppose del0 B $\mu = n+1$.
Since del0 B $\mu > 0$, the tree $\mu / \Box X \vdash \Box B$ contains one or more branches with a GLR rule, with $\Box B$ in the antecedent. (one such branch shown).

$$\dfrac{\dfrac{\dfrac{\Box G, G, \Box B^k, B^k, \Box A \vdash A}{\Box G, \Box B^k \vdash \Box A}\; GLR(A)}{\vdots}}{\dfrac{\Box X, X, \Box B \vdash B}{\Box X \vdash \Box B}\; GLR(X,B)}$$

From muxbn B n to muxbn B $(n+1)$

$$\dfrac{\dfrac{\dfrac{\Box G, G, \Box B^k, B^k, \Box A \vdash A}{\Box G, \Box B^k \vdash \Box A}\; GLR(A)\ \text{(delete this)}}{\vdots}}{\dfrac{\Box X, X, \Box B \vdash B}{\Box X \vdash \Box B}\; GLR(X,B)}$$

Delete top step, adjoin $\Box A$ on the left, extra weakening step:

$$\dfrac{\dfrac{\Box A, \Box G, \Box B^k \vdash \Box A}{\vdots}}{\dfrac{\dfrac{\Box A, \Box X, X, \Box B \vdash B}{\Box A, A, \Box X, X, \Box B \vdash B}\; (weakening)\ \text{(extra step)}}{\Box A, \Box X \vdash \Box B}\; GLR(B)}$$

Call this $\mu^A / \Box A, \Box X \vdash \Box B$, then del0 B $\mu >$ del0 B μ^A, so $\mu^A / \Box A, \Box X \vdash \Box B$ can be left branch of an admissible multicut.

Multicutting with $\Box A, \Box X \vdash \Box B$

We then, essentially, re-do the proof, using

- Admissible multicuts with $\Box A, \Box X \vdash \Box B$
- Admissible multicuts on cut-formula B

before the $GLR(A)$ step, so that the $GLR(A)$ step does not contribute to del0.
(Several steps manipulating proofs, see paper).
That is, given a derivation μ of $\Box X, X, \Box B \vdash B$ with del0 B $\mu = n+1$, we have a derivation μ' with del0 B $\mu' = n$.

Lemma

Assume that multicut-admissibility holds for cut-formula B, and that muxbn B n holds. Then muxbn B $(n+1)$ holds.

Now, since muxbn B 0 holds, repeated use of this Lemma gives that muxbn B n for all n.

The cut-admissibility theorem

Theorem

Multicut is admissible in GLS.

Proof.

Most of the proof is as usual for cut-elimination proofs, using induction on the size (or structure) of the cut-formula. The difficult case is with a multicut as in the Figure, which is handled by the previous lemma. □

Conclusion : value of the formalisation

- proofs usually tedious, with many details varying only slightly
- many cases or details usually omitted in paper proofs
- this may lead to erroneous proofs
- formal proof avoids this risk

Our formalisation includes:

- formalisation includes general treatment of derivation trees
- general theorem expressing the appropriate inductive principle
- general lemmas for many cases in this and other proofs