

Syntactic Conditions for Invertibility in Sequent Calculi

Peter Chapman

School of Computer Science, University of St Andrews, Scotland.
Email: pc@cs.st-and.ac.uk

Abstract

Formalised proofs of Cut admissibility often rely on the invertibility of the rules of a sequent calculus. We will present some sufficient conditions for when a rule is invertible with respect to a calculus, which we illustrate with many examples. Appropriate definitions are given for rarely defined intuitive notions, such as a formula being principal for a rule. It must be noted we give purely *syntactic* criteria; no guarantees are given as to the suitability of the rules. We also formalise some of the results in the proof assistant *Isabelle*, as a means to automating Cut admissibility proofs.

1 Introduction

Several papers (Ciabattoni & Terui 2006b), (Ciabattoni & Terui 2006a), (Rasga 2007) have sought to give syntactic, or semantic, conditions for a calculus to ensure that it admits Cut. These conditions are often so difficult to check that it is often easier to prove that Cut is admissible directly. In this paper, we will present some easily checkable conditions which will ensure that a rule is invertible with respect to the calculus in which it is defined. These results will also be formalised in the proof assistant *Isabelle* (Nipkow et al. 2005), so that any future formalised proofs requiring the invertibility of rules can use our conditions to reduce the length, and complexity, of the proof. We will intersperse the informal reasoning with the formalised proof document, written in the *Isar* (Nipkow 2002) style of *Isabelle*. Any *Isabelle* notation will be explained where necessary. The first-order results are formalised using the package *Nominal Isabelle* (Tasson & Urban 2005), in which it is easy to reason about binding issues.

We build on (Dawson 2008), notably the idea that a rule in a (context-sharing) sequent calculus can be decomposed into two distinct parts. We will show that the lemmata in (Dawson 2008) are logical consequences of our lemmata.

1.1 Structure of the document

We will introduce some definitions in §2 which will help us define, rather abstractly, a sequent calculus, and some additional notions which we require. In §3, we will discuss the admissibility of weakening in a calculus, and prove some results about this. Following that, in §4 we give a full account, including the formalisation, of the sufficient conditions for a premiss to be derivable from the conclusion for a rule of a multisuccedent calculus, for both right rules (§4.1), and left rules (§4.2). We derive, as special cases, the conditions for invertibility in a single succedent calculus in §5, and in §6 show how the conditions in (Dawson

2008) are consequences of our conditions. In §7, we discuss extensions to first-order and modal logics, as well as other directions one could take in this area.

2 Definitions

In what follows, we have that $A, B, C \dots$ are formulae, and Γ, Δ, \dots are multisets of formulae. A *sequent* is represented¹ by $\Gamma \Rightarrow \Delta$. When we add a single formula to a multiset, we use the notation $\Gamma \oplus A$, but if the sequent is displayed in a tree, we will use the more standard “comma” notation. The two functions *antec* and *succ*, when applied to a sequent, extract the antecedent and succedent of a sequent, respectively.

Whilst it is important which connectives are used in formulae, it is more important that we can distinguish between compound formulae and atomic formulae (the reason for this will be explained in more detail at the appropriate time). A compound formula takes a constructor and a list of formulae, whereas an atomic formula has as its identifier a natural number (note that we are not, at this time, concerned with first order formulae):

datatype *form* = *At nat*
 | *Cpd string (form list)*

In our informal analysis, we will represent a compound formula as $\star_s(\vec{A})$ or $\circ_t(\vec{B})$, where \star_s is an s -ary connective, and \vec{A} has length s , for example.

Context sharing rules of a sequent calculus can be thought of as having two components. First, there is the *active* part of a rule, in which formulae are changed from the premisses to the conclusion, and the *passive* part of a rule, which does not change from premisses to conclusion. The latter part is really the context of the rule. As an example, consider the rule from **G3cp** for $L\supset$ (Troelstra & Schwichtenberg 2000):

$$\frac{\Gamma \Rightarrow A, \Delta \quad \Gamma, B \Rightarrow \Delta}{\Gamma, A \supset B \Rightarrow \Delta}$$

Here, the active part of the rule is

$$\frac{\Rightarrow A \quad B \Rightarrow}{A \supset B \Rightarrow}$$

whereas the passive part consists of Γ and Δ . Note that this is just the decomposition of the rule, neither part is a rule in its own right. We call the new rule the *extension* of the active part.

We represent, in *Isabelle*, the active part of a rule using a list of sequents (for premisses), paired with a single sequent (the conclusion).

¹reserved symbols in *Isabelle* mean that, when we include output from a formal definition or lemma, the notation $\Gamma \Rightarrow^* \Delta$ is used instead

types $rule = sequent\ list * sequent$

We extend a sequent with another by adding combining their antecedents and succedents:

defs $extend-def :$
 $extend\ S1\ S2 \equiv$
 $(antec\ S1 + antec\ S2) \Rightarrow^* (succ\ S1 + succ\ S2)$

As an example, we have

$$extend\ (\Gamma \Rightarrow \Delta)\ (\Gamma' \Rightarrow \Delta') = \Gamma + \Gamma' \Rightarrow \Delta + \Delta'$$

We then extend a rule by using the extend function over the elements of the list of premisses, and also extending the conclusion:

defs $extendRule-def :$
 $extendRule\ S1\ R \equiv$
 $(map\ (extend\ S1)\ (fst\ R),\ extend\ S1\ (snd\ R))$

We focus on two kinds of rule, *axioms* and *single conclusion rules*. Axioms have no premisses, and both the antecedent and the succedent of the conclusion must contain some atomic formula $At\ i$. We guarantee this by creating a set of active parts with the following form, where $\{\#A\#\}$ is *Isabelle* notation for the multiset consisting of the object A .

inductive-set $idRules$ **where**
 $([], \{\#At\ i\ \#\} \Rightarrow^* \{\#At\ i\ \#\}) \in idRules$

Here our approach differs from that in (Dawson 2008). There, Dawson has that *any* formula can be part of an identity sequent, whereas we restrict ourselves to atomic formulae. Most calculi are sufficiently balanced so that a general axiom can be proved admissible (i.e. $A \Rightarrow A$ for any formula A), however not all calculi have this property. This restriction to atomic formulae in axioms, whilst more desirable from a theoretical view, has the drawback that we have to partially specify formulae. Thus, when we come to use these results in another *Isabelle* theory, we must specify connectives using the *Cpd* notation. For instance, we would define conjunction of A and B as $Cpd\ Conj\ [A, B]$.

Single conclusion rules must have a non-atomic formula in the active part of the conclusion, and furthermore this non-atomic formula must be the *only* formula in the active part of the conclusion. We guarantee this by creating a set of active parts with the following form, where $mset$ of a sequent is the multiset containing all formulae in the sequent.

inductive-set $scRules$ **where**
 $[mset\ c \equiv \{\#Cpd\ R\ Fs\ \#\};\ ps \neq []]$
 $\Rightarrow (ps, c) \in scRules$

A sequent calculus is thus defined by the extensions with contexts of some subset of all possible single conclusion rules, joined with every possible axiom. We will usually just talk about the single conclusion rules defining a calculus, with the understanding that the calculus contains all possible axioms.

These two rule sets define the active parts of rules. We build a third set of rules, built upon (any) underlying set of rules. These are the extensions of the initial set. If R was the initial set of rules, the extension of R is denoted R^* :

inductive-set $extRules :: rule\ set \Rightarrow rule\ set$ **for** $R :: rule\ set$
where
 $r \in R \Rightarrow extendRule\ S2\ r \in R^*$

The decomposition makes it straightforward to identify the *principal formula of a rule*, though; it is the only formula which appears in the conclusion of the active part of the rule. In the example above, we can clearly see that $A \supset B$ is principal for the rule. We can also define *principal on the left* and *principal*

on the right for a rule by noting whether the single formula in the conclusion of the active part of the rule is in the antecedent or succedent respectively. Note we can only define a formula being principal when there is a single formula in the conclusion of the active part of the rule. The approach we use will only work for calculi that can be decomposed in this manner. We show the definition of principal on the left, where $\{\#\}$ is the empty multiset.

inductive $leftPrincipal :: rule \Rightarrow form \Rightarrow bool$
where
 $C = (\{\#Cpd\ F\ Fs\ \#\} \Rightarrow^* \{\#\}) \Rightarrow$
 $leftPrincipal\ (Ps, C)\ (Cpd\ F\ Fs)$

As an example, $A \supset B$ is principal on the left for the rule shown on the previous page.

We now need the notion of *derivability*, and, because we are interested in height-preserving invertibility (in the first instance), we need the notion of *derivability at height n* . Axioms are derivable at height 0, and, should every premiss in a rule be derivable at height *at most* n , then the conclusion of the rule will be derivable at height $n + 1$. This is formalised as an inductive set of *derivs*, which are *(sequent, height)*-pairs, as follows:

inductive-set $derivable :: rule\ set \Rightarrow deriv\ set$
for $R :: rule\ set$
where
base:
 $[([], C) \in R] \Rightarrow (C, 0) \in derivable\ R$
step:
 $[r \in R; (fst\ r) \neq [];$
 $\forall p \in set\ (fst\ r). \exists n \leq m. (p, n) \in derivable\ R]$
 $\Rightarrow (snd\ r, m + 1) \in derivable\ R$

base and *step* name the two clauses of the definition. This definition uses bounded quantifiers, and so we need to cast the list of premisses to a set.

We now come to the definitions of invertibility. Intuitively, we say that a rule is invertible if given the conclusion of a rule, we can derive its premisses. We are most interested in the invertibility of the defining (also known as primitive) rules of the calculus. The notion we use is that of *strong admissibility* from (Dyckhoff & Negri 2000).

Definition 1 (Strong Admissibility) *The rule R given by*

$$\frac{S}{S'} R$$

is strongly admissible in a calculus if given an instance of a derivation with root S and height n , there is a corresponding instance of S' of height not more than n . \dashv

There is a corresponding notion of *admissibility* which drops the requirement that the derivation of S have height not greater than that of S' . This definition shows that we prove a rule is strongly admissible by taking an arbitrary instance of the rule, and showing that this instance has the necessary properties.

Definition 2 (Invertible rule) *For a calculus defined by a set of primitive rules \mathcal{R} , we say that a rule $R \in \mathcal{R}$ with premisses P_1, P_2, \dots, P_n and conclusion C , is invertible with respect to \mathcal{R} if, for each premiss P_i , the rule*

$$\frac{C}{P_i}$$

is strongly admissible.

If every such $R \in \mathcal{R}$ is invertible, we say that \mathcal{R} is invertible. \dashv

All of the strong admissibility results we prove require the strong admissibility of weakening (this is more commonly known as depth-preserving weakening). We will give a lemma that guarantees that weakening is depth-preserving, but require the following definition to do so, which can be found in (Negri 2005) and (Rasga 2007):

Definition 3 (Context Dependent Rules) A *context dependent rule* is a schematic rule which has side conditions which place restrictions upon the context of formulae allowable for instantiations of that rule. \dashv

Many rules with variable binding are context dependent rules, as is the usual rule for necessitation from the left in modal logic (Troelstra & Schwichtenberg 2000):

$$\frac{\Box \Gamma \Rightarrow A, \Diamond \Delta}{\Box \Gamma, \Gamma' \Rightarrow \Box A, \Diamond \Delta, \Delta'}$$

where here the side condition is that all formulae in the antecedent must be boxed.

3 Weakening

We have the following, simple result:

Lemma 1 (dp-Weakening) *If there are no context dependent rules in the calculus, then weakening is depth-preserving admissible.*

Proof. A routine induction. Since there are no context dependent rules, we know for instance there will be no stipulations of the form $|\Gamma| \leq n$ for some natural number n , or the requirement that all formulae be boxed (for example). So, it follows immediately that if $\Gamma \subseteq_m \Gamma'$, where \subseteq_m is the subset relation for multisets, and a rule was applicable with Γ , then it will be applicable with Γ' , because the active part of the rule is unaffected. \dashv

What does this tell us? The fact that there are *no* context dependent rules is very restrictive. In particular, it rules out lots of first order rules. This restriction can be relaxed, however for our purposes, we do not need to worry about this matter.

4 Multisuccedent Calculi

We have two sets of conditions, one for right rules being invertible, and one for left rules being invertible. After the proofs, we will give examples of rules which satisfy the conditions. The form of the lemmata may seem odd, however the additional multisets of formulae in the premisses come from the active part of the rule.

4.1 Right rules

Lemma 2 *The rule*

$$\frac{\Gamma \Rightarrow \star_s(\vec{B}), \Delta}{\Gamma + \Gamma' \Rightarrow \Delta + \Delta'}$$

is strongly admissible if $\Gamma' \Rightarrow \Delta'$ is a premiss of the active part of every rule with $\star_s(\vec{B})$ principal on the right.

This is formalised as follows, where the assumption labelled b is that which says “ $\Gamma' \Rightarrow \Delta'$ is a premiss of the active part of every rule which has $\star_s(\vec{B})$ principal on the right.”

lemma rightInvertible:

fixes $\Gamma \Delta :: \text{form multiset}$

assumes $R' \subseteq \text{scRules} \wedge R = \text{idRules} \cup R'$

and $(\Gamma \Rightarrow \star \Delta \oplus \text{Cpd } F \text{ } F_s, n) \in \text{derivable } R^*$

and $b: \forall r' \in R. \text{rightPrincipal } r' (\text{Cpd } F \text{ } F_s) \longrightarrow (\Gamma' \Rightarrow \star \Delta') \in \text{set } (\text{fst } r')$

shows $\exists m \leq n.$

$(\Gamma + \Gamma' \Rightarrow \star \Delta + \Delta', m) \in \text{derivable } R^*$

Proof. We prove the lemma by induction on the height n of the derivation of $\Gamma \Rightarrow \star_s(\vec{B}) \oplus \Delta$. If $n = 0$, then there exists some propositional variable P such that $P \in \Gamma$ and $P \in \Delta \oplus \star_s(\vec{A})$. We then have $P \in \Gamma + \Gamma'$ and $P \in \Delta + \Delta'$, and so $\Gamma + \Gamma' \Rightarrow \Delta + \Delta'$ is an axiom.

If $n > 0$, then we do case analysis on the last rule used in the derivation of $\Gamma \Rightarrow \star_s(\vec{B}) \oplus \Delta$. The rule was either a left rule or a right rule. If it was a right rule, and if it was a rule of which $\Gamma + \Gamma' \Rightarrow \Delta + \Delta'$ was a premiss, then we are done. Otherwise, it was an instance some other rule \hat{R} :

$$\frac{\Gamma''_1 \Rightarrow \Delta''_1 \quad \dots \quad \Gamma''_n \Rightarrow \Delta''_n}{\Gamma'' \Rightarrow \circ_t(\vec{D}), \Delta''} \hat{R}$$

We have that $\Gamma \equiv \Gamma''$, and $\Delta \oplus \star_s(\vec{B}) \equiv \Delta'' \oplus \circ_t(\vec{D})$. From this we have a Δ^\sim such that

1. $\Delta = \Delta^\sim \oplus \circ_t(\vec{D})$
2. $\Delta'' = \Delta^\sim \oplus \star_s(\vec{B})$

We have fixed formulae being added to the left and right contexts respectively when we apply the induction hypothesis. So, after rewriting the premisses of the instance of \hat{R} with this information, and applying the induction hypothesis, and then the instance of \hat{R} again, we get the derivation

$$\frac{\frac{\Gamma_1 \Rightarrow \Delta_1^\sim, \star_s(\vec{B})}{\Gamma''_1 + \Gamma' \Rightarrow \Delta_1^\sim + \Delta'} \quad \dots \quad \frac{\Gamma''_n \Rightarrow \Delta_n^\sim, \star_s(\vec{B})}{\Gamma''_n + \Gamma' \Rightarrow \Delta_n^\sim + \Delta'}}{\Gamma + \Gamma' \Rightarrow \Delta^\sim, \circ_t(\vec{D}), \Delta'} \hat{R}$$

Using the equation 1 we have the result.

If the last rule used was an instance of a left rule, say

$$\frac{\Gamma''_1 \Rightarrow \Delta''_1 \quad \dots \quad \Gamma''_n \Rightarrow \Delta''_n}{\Gamma'', \circ_t(\vec{D}) \Rightarrow \Delta''} \hat{R}$$

Then, we have $\Gamma = \Gamma'' \oplus \circ_t(\vec{D})$ and $\star_s(\vec{B}) \in \Delta''$. From the latter we have there is some Δ^\sim such that $\Delta'' = \Delta^\sim \oplus \star_s(\vec{B})$. Since the last rule used was left rule, we have that $\star_s(\vec{B})$ is not principal on the right, hence we have that $\star_s(\vec{B}) \in \Delta_i^\sim$. This is because $\star_s(\vec{B})$ must have been in the passive succedent of the rule. We then have the following derivation, where we can apply the induction hypothesis to each premiss:

$$\frac{\frac{\Gamma''_1 \Rightarrow \Delta_1^\sim, \star_s(\vec{B})}{\Gamma''_1 + \Gamma' \Rightarrow \Delta_1^\sim + \Delta'} \quad \dots \quad \frac{\Gamma''_n \Rightarrow \Delta_n^\sim, \star_s(\vec{B})}{\Gamma''_n + \Gamma' \Rightarrow \Delta_n^\sim + \Delta'}}{\Gamma'', \circ_t(\vec{D}), \Gamma' \Rightarrow \Delta + \Delta'} \hat{R}$$

Using $\Gamma = \Gamma'' \oplus \circ_t(\vec{D})$, we are done. \dashv

4.1.1 Examples

Consider the calculus **G3cp**. All of the right rules are invertible:

$$\frac{\Gamma \Rightarrow A, \Delta \quad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A \wedge B, \Delta} \quad \frac{\Gamma \Rightarrow A, B, \Delta}{\Gamma \Rightarrow A \vee B, \Delta}$$

$$\frac{\Gamma, A \Rightarrow B, \Delta}{\Gamma \Rightarrow A \supset B, \Delta}$$

However, when we consider a multisuccedent version of **G3ip**, we usually have the following rule for implication on the right (see, for instance (Troelstra & Schwichtenberg 2000)):

$$\frac{\Gamma, A \Rightarrow B}{\Gamma \Rightarrow A \supset B, \Delta}$$

Clearly, this is only invertible if $\Delta = \emptyset$, which is not true in general, and it only satisfies our lemma if $\Delta = \emptyset$.

4.2 Left Rules

Here, we get to appeal to symmetry with the multisuccedent right rule case.

Lemma 3 *The rule*

$$\frac{\Gamma, \star_s(\vec{B}) \Rightarrow \Delta}{\Gamma + \Gamma' \Rightarrow \Delta + \Delta'}$$

is strongly admissible if $\Gamma' \Rightarrow \Delta'$ is a premiss of the active part of every rule with $\star_s(\vec{B})$ principal on the left.

Proof. We prove the lemma by induction on the height n of the derivation of $\Gamma \oplus \star_s(\vec{B}) \Rightarrow \Delta$. If $n = 0$, then we have that $\Gamma \oplus \star_s(\vec{B}) \Rightarrow \Delta$ is an axiom, so there exists a propositional variable P such that $P \in \Gamma$ and $P \in \Delta$. This means that $\Gamma + \Gamma' \Rightarrow \Delta + \Delta'$ is also an axiom, as required. The rest of the proof is symmetrical to that of §4.1. \dashv

We have also formalised this result, with the statement as follows

lemma *leftInvertible:*

fixes $\Gamma \Delta :: \text{form multiset}$

assumes $R' \subseteq \text{scRules} \wedge R = \text{idRules} \cup R'$

and $(\Gamma \oplus \text{Cpd } F \text{ Fs} \Rightarrow \Delta, n) \in \text{derivable } R^*$

and $\forall r' \in R. \text{leftPrincipal } r' (\text{Cpd } F \text{ Fs}) \longrightarrow (\Gamma' \Rightarrow \Delta') \in \text{set } (\text{fst } r')$

shows $\exists m \leq n.$

$(\Gamma + \Gamma' \Rightarrow \Delta + \Delta', m) \in \text{derivable } R^*$

4.2.1 Examples

The rule for implication on the left for **G3ip** was not invertible (see §5.2), however the multisuccedent version of the calculus has the following form:

$$\frac{\Gamma, A \supset B \Rightarrow A, \Delta \quad \Gamma, B \Rightarrow \Delta}{\Gamma, A \supset B \Rightarrow \Delta}$$

For each premiss, the lemma applies. In the left case, we have that $\Gamma' = A \supset B$ and $\Delta' = A$, and in the right case we have that $\Gamma' = B$ and $\Delta' = \emptyset$.

5 Single succedent calculi

We have the restriction that the succedents contain only one formula. This means that if we try to apply the previous lemmata, we have that Δ' is empty.

5.1 Right rules

Lemma 4 *The rule*

$$\frac{\Gamma \Rightarrow \star_s(\vec{B})}{\Gamma + \Gamma' \Rightarrow A}$$

is strongly admissible if $\Gamma' \Rightarrow A$ is a premiss of the active part of every rule which has $\star_s(\vec{B})$ principal on the right.

Proof. An immediate application of the lemma of §4.1. \dashv

5.1.1 Examples

Take the standard formulation of **G3ip** from (Troelstra & Schwichtenberg 2000). Then, consider the rules $R \supset$ and $R \wedge$. For $R \supset$:

$$\frac{\Gamma, A \Rightarrow B}{\Gamma \Rightarrow A \supset B}$$

we have the conditions satisfied, because $A \supset B$ is principal on the right only for this rule, with $\Gamma' = A$. Thus, the rule is invertible, as expected. Both premisses of $R \wedge$:

$$\frac{\Gamma \Rightarrow A \quad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B}$$

are derivable from the conclusion, and so the rule is invertible. By contrast, consider the rules for disjunction of the right:

$$\frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B} \quad \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B}$$

Since neither $\Gamma \Rightarrow B$ nor $\Gamma \Rightarrow A$ is a premiss of *every* rule which has $B \vee A$ principal on the right, then our lemma says nothing about the invertibility of either rule.

In the abstract, we said that the conditions were purely syntactic. If we changed the rule for right conjunction to

$$\frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \wedge B}$$

then this rule would be invertible, but the new calculus **G3ip'** would no longer admit Cut. For, consider when the rule Cut formula was a conjunction, and was principal on both sides:

$$\frac{\frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \wedge B} \quad \frac{\Gamma, A, B \Rightarrow C}{\Gamma, A \wedge B \Rightarrow C}}{\Gamma \Rightarrow C}$$

Then, unless we always have a derivation of $\Gamma \Rightarrow B$ for arbitrary B and Γ (i.e. the calculus is inconsistent), we cannot show the admissibility of Cut by the usual proof transformation:

$$\frac{\Gamma \Rightarrow B \quad \frac{\Gamma \Rightarrow A}{\Gamma, B \Rightarrow A} \quad \frac{\Gamma, A, B \Rightarrow C}{\Gamma, B \Rightarrow C}}{\Gamma \Rightarrow C}$$

5.2 Left Rules

Lemma 5 *The rule*

$$\frac{\Gamma, \star_s(\vec{B}) \Rightarrow A}{\Gamma + \Gamma' \Rightarrow A}$$

is strongly admissible if $\Gamma' \Rightarrow A$ is a premiss of the active part of every rule which has $\star_s(\vec{B})$ principal on the left.

Proof. A simple application of the Lemma 3, with the restriction to single formulae in succedents. \dashv

5.2.1 Examples

We have that most of the rules of **G3ip** and **G4ip** (Dyckhoff 1992) are shown to be invertible by this lemma. Left conjunction and left disjunction satisfy the conditions:

$$\frac{\Gamma, A \Rightarrow C \quad \Gamma, B \Rightarrow C}{\Gamma, A \vee B \Rightarrow C} \quad \frac{\Gamma, A, B \Rightarrow C}{\Gamma, A \wedge B \Rightarrow C}$$

For which rules is the lemma inapplicable? The left implication rule for **G3ip**, and the rule $L\supset$ for **G4ip**:

$$\frac{\Gamma, A \supset B \Rightarrow A \quad \Gamma, B \Rightarrow C}{\Gamma, A \supset B \Rightarrow C}$$

$$\frac{\Gamma, C, D \supset B \Rightarrow D \quad \Gamma \Rightarrow E}{\Gamma, (C \supset D) \supset B \Rightarrow E}$$

The right premisses are derivable from the conclusion, but the left premisses are not. The left premisses fail our conditions, owing to them having a different succedent to their respective conclusions.

6 Extension to Rule Sets

We stated in §1 that the lemmata in (Dawson 2008) were logical consequences of our lemmata. Dawson is concerned with the admissibility of certain rules, rather than their strong admissibility. As is suggested by the names, strong admissibility implies admissibility. He is also investigating the invertibility of a set of rules, rather than the derivability of a given premiss of a rule. We require the following definition, of what if means for a set of defining rules to have the *unique conclusion property*:

$$\text{uniqueConc } R \equiv \forall r \in R. \forall t \in R. \text{snd } r = \text{snd } t \longrightarrow r = t$$

The lemma he proves is as follows

Lemma 6 *Let \mathcal{R} be a set of (active parts of) rules defining a sequent calculus. If each $r \in \mathcal{R}$ has a unique conclusion, (Ps, C) is a rule in the set of extensions of \mathcal{R} and C is derivable with respect to the extensions of \mathcal{R} , then so is every $p \in Ps$.*

Proof. Suppose that every rule has a unique conclusion, and further that (Ps, C) is a rule in the calculus and C is derivable with respect to the calculus. Let p be a premiss of this rule (i.e. $p \in Ps$). From the fact that every rule has a unique conclusion, we have that p is a premiss of every rule with conclusion C . Then, (depending on the particular calculus formation or form of C), we apply one of the lemmata from the previous sections, and so p is derivable. \dashv

What we actually prove is the stronger notion that the premiss is strongly admissible, not just admissible:

lemma invertibleRule:

assumes $R' \subseteq \text{scRules} \wedge R = \text{idRules} \cup R'$
and *uniqueConc* R'
and $(Ps, C) \in R^*$
and $(C, n) \in \text{derivable } R^*$
shows $\forall p \in \text{set } Ps. \exists m \leq n. (p, m) \in \text{derivable } R^*$

7 First-Order Calculi

The conditions under which we performed analysis in the previous sections were quite restrictive. In particular, we ruled out, in §2, first-order calculi, and modal logics, under the proviso of “no context dependent rules”. We seek now to relax this condition, in the first instance to permit our lemmata to be applicable to first-order calculi. We need to change our definition of formulae, so that it is similar to that in, for instance, (Chapman et al. 2008). An atomic formula is now a predicate applied to a list of variables, a (propositional) compound formula is defined as before, and first-order formulae bind a variable in a formula, with an identifying string:

nominal-datatype *form* = *At nat (var list)*
| *Cpd0 string (form-list)*
| *Cpd1 string (<<var>>form)*
and *form-list* = *FNil*
| *FCons form (form-list)*

Unfortunately, presently one cannot have nested types within a nominal datatype, hence the requirement to mutually define a list of formulae. We have a syntax abbreviation for first-order formulae using just one binder, ∇ , so for instance \forall and \exists would be represented as “All $\nabla[x].A$ ” and “Exists $\nabla[x].A$ ”.

We need to show weakening is strongly admissible in the presence of free and bound variables. The intuitive solution is to rename all of the variables in a derivation so that there are no clashes with any variables in the formulae with which we wish to weaken. This requires a substitution lemma to be strongly admissible. We first need some definitions. The first is found in (Rasga 2007):

Definition 4 (Freshness Proviso) *Suppose R is a rule with antecedent Γ , succedent Δ and some distinguished formula A . Such a rule is said to have a **freshness proviso** iff it has a side condition of the form*

$$y \notin FV(\Gamma), y \notin FV(\Delta), y \notin FV(A)$$

\dashv

In addition to the rule sets from the propositional cases, we also have two new rule sets. The first contains those rules which have a single, first-order formula in the conclusion of the active part. The second contains those rules which have a single, first-order formula in the conclusion of the active part and a freshness proviso on the variable which is bound. We call these **nprov** and **prov** rules respectively:

inductive-set *nprovRules* **where**
[[*mset* $c = \{\# F \nabla [x].A \#\}; ps \neq []$]]
 $\implies (ps, c) \in \text{nprovRules}$

inductive-set *provRules* **where**
[[*mset* $c = \{\# F \nabla [x].A \#\}; ps \neq []$;
 $x \# \text{set-of-prem } (ps - A)$]]
 $\implies (ps, c) \in \text{provRules}$

We use a notion from (Zamansky & Avron 2006) to give a general form for quantifiers. This was also used in (Ciabattoni & Terui 2006a):

Definition 5 (General Quantifiers) *An (n, k) -ary quantifier for $n > 0, k \geq 0$ is a generalised logical*

connective, which binds k variables and connects n formulae. \dashv

As an example, \wedge can be seen as a $(2, 0)$ -ary quantifier, as indeed can \vee and \supset . The usual first order \forall and \exists are $(1, 1)$ -ary quantifiers. The bounded universal ($\bar{\forall}$) and existential ($\bar{\exists}$) quantifiers given by

$$\bar{\forall}x.(p(x), q(x)) \equiv \forall x.(p(x) \supset q(x))$$

$$\bar{\exists}x.(p(x), q(x)) \equiv \exists x.(p(x) \wedge q(x))$$

are $(2, 1)$ -ary quantifiers. The rules for these quantifiers in an extension of **G3c** are a combination of the rules for \forall and \supset , for example:

$$\frac{\Gamma, [y/x]A \Rightarrow [y/x]B, \Delta}{\Gamma \Rightarrow \bar{\forall}x.(A, B), \Delta}$$

where y is fresh for Γ, Δ . We use similar notation to that described in §2 for such quantifiers: $\nabla_{m,k}\vec{x}.\vec{B}$ is an (m, k) -ary quantifier where \vec{x} is a k -tuple of variables, and \vec{B} is an m -tuple of meta-formulae.

Lemma 7 (Substitution lemma) *Given a calculus defined by a set of primitive rules \mathcal{R} which can contain freshness provisos, if y is a variable which is fresh for $\Gamma \Rightarrow \Delta$, then the rule*

$$\frac{\Gamma \Rightarrow \Delta}{[y/x]\Gamma \Rightarrow [y/x]\Delta}$$

is strongly admissible in the calculus.

Proof. A standard induction on the height of the derivation of an instance of $\Gamma \Rightarrow \Delta$. \dashv

We show here the formalised result which is the key step in the proof; if $y \# A$ and $y \# x$, then $F \nabla[x].A = F \nabla[y].([y/x]A)$:

lemma *formSubst:*
shows $y \# x \wedge y \# A \implies F \nabla[x].A = F \nabla[y].([y/x]A)$

We then have our required extension to the weakening result from §3:

Lemma 8 (Weakening - First Order) *If a calculus contains a general axiom $\Gamma \Rightarrow \Delta$ where there is some propositional variable P such that $P \in \Gamma$ and $P \in \Delta$, and there are no context dependent rules in the calculus other than freshness provisos, then weakening is depth-preserving admissible.*

Proof. A standard induction as in §3. We appeal to the Substitution Lemma when we the last rule used in a derivation was a rule with a freshness proviso, to ensure that the new formula introduced by the weakening is suitably fresh for the derivation. \dashv

In our setting, we want to be able to extend a rule with any sequent. The simple definition for the extension of a rule set from §2 will no longer suffice: we need to know that a sequent contains no variables free which are bound by a rule. Thus, we have the following definition of the extension of a rule set, again denoted by R^* for the set of active parts R :

inductive-set *extRules* :: rule set \Rightarrow rule set
for R :: rule set
where
id: $\llbracket r \in R ; r \in \text{idRules} \rrbracket \implies \text{extendRule } S \ r \in R^*$
sc: $\llbracket r \in R ; r \in \text{propRules} \rrbracket \implies \text{extendRule } S \ r \in R^*$
np: $\llbracket r \in R ; r \in \text{nprovRules} \rrbracket \implies \text{extendRule } S \ r \in R^*$
p: $\llbracket (ps, c) \in R ; (ps, c) \in \text{provRules} ;$
 $\quad \text{mset } c = \{\# F \nabla[x].A \#\} ; x \# \text{set-of-seq } S \rrbracket$
 $\implies \text{extendRule } S \ (ps, c) \in R^*$

where *set-of-seq* S is the set of formulae which appear in S . We then prove the following *safe extension lemma*, which is analagous to first-order weakening:

lemma *extend-for-any-seq:*

fixes S :: sequent

assumes

$$R1 \subseteq \text{propRules} \wedge R2 \subseteq \text{nprovRules} \wedge R3 \subseteq \text{provRules}$$

and $R = \text{idRules} \cup R1 \cup R2 \cup R3$

and $r \in R$

shows *extendRule* $S \ r \in R^*$

The interesting case is when the last rule used had a freshness proviso. The proof relies upon the existence of a variable which is fresh for both the new sequent, and the formula to which the proviso refers. We know such a variable exists because each formula has a finite support, and multisets, by definition, are finite², thus the support of a multiset is finite. We can always find a variable which is *not* in the support of a multiset, then, which is the definition of freshness.

Intuitively, we want a premiss to be derivable from the conclusion of a rule if the freshness provisos are observed, and there are no new *specific* substitutions in the premiss. We want there to be only new *general* substitutions in the premiss, where the substituted variable can range over the entire domain for which it is defined. In other words, new substitutions such as $[y/x]$ are acceptable in a premiss, whereas $[t/x]$ is not, where t is some term. In *Isabelle*, we use the following definition of when a multiset contains a substitution:

constdefs *multSubst* :: form multiset \Rightarrow bool
multSubst $\Gamma \equiv$
 $(\exists A \in (\text{set-of } \Gamma). \exists x \ y \ B. [y,x]B = A \wedge y \neq x)$

We are now ready to extend the results from §4.1 and §4.2. We need only consider the cases where there is some variable binding, in other words the cases of (n, k) -ary connectives for which $k > 0$; the rest of the cases will be as before.

Lemma 9 (First-Order Right Rules) *The rule*

$$\frac{\Gamma \Rightarrow \nabla_{m,k}\vec{x}.\vec{B}, \Delta}{\Gamma + \Gamma' \Rightarrow \Delta + \Delta'}$$

is strongly admissible if

1. $\Gamma' \Rightarrow \Delta'$ is a premiss of the active part of every rule with $\nabla_{m,k}\vec{x}.\vec{B}$ principal on the right
2. Γ' and Δ' contain no term substitutions
3. All freshness provisos present in the (primitive) rules are observed

Proof. By induction on the height, n , of an instance of $\Gamma \Rightarrow \nabla_{m,k}\vec{x}.\vec{B} \oplus \Delta$. The proof is much the same as that in §4.1, except that condition 3 ensures that if the last rule used for a non-principal (m', k') -ary quantifier where $k' > 0$, then we can apply this rule after applying the induction hypothesis. Uses of the Substitution Lemma may be needed to rename variables to guarantee condition 3 holds. Condition 2 means that there are no new arbitrary terms in Γ' and Δ' . \dashv

This is formalised as follows:

lemma *rightInvert:*

fixes $\Gamma \ \Delta$:: form multiset

assumes

$$R1 \subseteq \text{propRules} \wedge R2 \subseteq \text{nprovRules} \wedge R3 \subseteq \text{provRules} \wedge$$

$$R = \text{idRules} \cup R1 \cup R2 \cup R3$$

and $(\Gamma \Rightarrow^* \Delta \oplus F \nabla[x].A, n) \in \text{derivable } R^*$

and $\forall r' \in R. \text{rightPrincipal } r' (F \nabla[x].A) \longrightarrow$

²the set upon which a multiset is based is finite. We can still have infinite copies of each formula in a multiset

$(\Gamma' \Rightarrow^* \Delta') \in \text{set } (\text{fst } r')$
and $\neg \text{multSubst } \Gamma' \wedge \neg \text{multSubst } \Delta'$
shows $\exists m \leq n. (\Gamma + \Gamma' \Rightarrow^* \Delta + \Delta', m) \in \text{derivable } R^*$

Lemma 10 (First-Order Left Rules) *The rule*

$$\frac{\Gamma, \nabla_{m,k} \vec{x}.(\vec{B}) \Rightarrow \Delta}{\Gamma + \Gamma' \Rightarrow \Delta + \Delta'}$$

is strongly admissible if

1. $\Gamma' \Rightarrow \Delta'$ is a premiss of the active part of every rule with $\nabla_{m,k} \vec{x}.(\vec{B})$ principal on the left
2. Γ' and Δ' contain no term substitutions
3. All freshness provisos present in the (primitive) rules are observed

Proof. The proof is symmetrical to that of the previous lemma. \dashv

The formalisation is as follows:

lemma *leftInvert*:

fixes $\Gamma \Delta :: \text{form multiset}$

assumes

$R1 \subseteq \text{propRules} \wedge R2 \subseteq \text{nprovRules} \wedge R3 \subseteq \text{provRules} \wedge$
 $R = \text{idRules} \cup R1 \cup R2 \cup R3$

and $(\Gamma \oplus F \nabla [x].A \Rightarrow^* \Delta, n) \in \text{derivable } R^*$

and $\forall r' \in R. \text{leftPrincipal } r' (F \nabla [x].A) \longrightarrow$
 $(\Gamma' \Rightarrow^* \Delta') \in \text{set } (\text{fst } r')$

and $\neg \text{multSubst } \Gamma' \wedge \neg \text{multSubst } \Delta'$

shows $\exists m \leq n. (\Gamma + \Gamma' \Rightarrow^* \Delta + \Delta', m) \in \text{derivable } R^*$

7.1 Examples

We consider the four rules for (1,1)-ary quantifiers from **G3c**:

$$\frac{\Gamma, [t/x]A, \forall x.A \Rightarrow \Delta}{\Gamma, \forall x.A \Rightarrow \Delta} L\forall \qquad \frac{\Gamma \Rightarrow [y/x]A, \Delta}{\Gamma \Rightarrow \forall x.A, \Delta} R\forall$$

$$\frac{\Gamma, [y/x]A \Rightarrow \Delta}{\Gamma, \exists x.A \Rightarrow \Delta} L\exists \qquad \frac{\Gamma \Rightarrow [t/x]A, \exists x.A, \Delta}{\Gamma \Rightarrow \exists x.A, \Delta} R\exists$$

where y is fresh for the conclusions of $R\forall$ and $L\exists$. As is easily verifiable, $R\forall$ and $L\exists$ satisfy the conditions, and so are invertible. But what about $L\forall$ and $R\exists$? For both rules, Γ' or Δ' contain term substitutions. It could be argued that both premisses are derivable from the conclusion *at the same height* by an application of depth-preserving weakening, however, this suggests we know which term t to use in the weakened formula, which in general is not possible. We cannot even appeal to weakening for $R\exists$, however, when we consider the single succedent version of this rule³:

$$\frac{\Gamma \Rightarrow [t/x]A}{\Gamma \Rightarrow \exists x.A} R\exists$$

As a further example, consider the four rules for the bounded quantifiers $\bar{\forall}$ and $\bar{\exists}$, whose definitions were given above, and in (Zamansky & Avron 2006):

³note we must make appropriate restrictions upon Δ and Δ' to ensure the calculus is single succedent.

$$\frac{\Gamma, [t/x]A \Rightarrow \Delta \quad \Gamma, [t/x]B \Rightarrow \Delta}{\Gamma, \bar{\forall}x.(A, B) \Rightarrow \Delta} L\bar{\forall}$$

$$\frac{\Gamma, [y/x]A \Rightarrow [y/x]B, \Delta}{\Gamma \Rightarrow \bar{\forall}x.(A, B), \Delta} R\bar{\forall}$$

$$\frac{\Gamma, [y/x]A, [y/x]B \Rightarrow \Delta}{\Gamma, \bar{\exists}x.(A, B) \Rightarrow \Delta} L\bar{\exists}$$

$$\frac{\Gamma \Rightarrow [t/x]A, \Delta \quad \Gamma \Rightarrow [t/x]B, \Delta}{\Gamma \Rightarrow \bar{\exists}x.(A, B), \Delta} R\bar{\exists}$$

where y is fresh for the conclusions of $R\bar{\forall}$ and $L\bar{\exists}$. These two rules are also invertible, whereas $L\bar{\forall}$ and $R\bar{\exists}$ violate our conditions, and so we cannot conclude anything about their invertibility.

8 Conclusions and Further Work

The syntactic criteria we give for a rule to be invertible are simple. Moreover, they are general enough to be applicable in a large number of cases. We stated in §1 that we would like to be able to effectively prove Cut admissibility, and other such results, in *Isabelle*. The generic lemmata presented here will eliminate the need to prove invertibility results for specific calculi by direct methods. Such results usually account for a large portion of the formalisations, for instance in (Chapman 2008b) the proofs of invertibility are 323 lines of proof, in a 720 line file, and in (Chapman 2008a) (a formalisation of (Dyckhoff & Negri 2000)), they consist of 955 lines of proof in a 2100 line theory file, where the goal is to prove the admissibility of Contraction for **G4ip**. In both cases, the seemingly trivial lemmata account for roughly half of the total size of the file.

Another obvious avenue of investigation is that of *necessary* conditions for invertibility. Such conditions are more difficult to come by: showing a sequent is not derivable at a given height is often achieved by a brute force search to find no valid derivations. However, this relies upon derivability being decidable. In general, one cannot assume this.

As stated in §2, the *Cpd* notation is clumsy for specifying the rules of a sequent calculus. Were we able to give conditions for when a general axiom to be admissible, i.e.

$$\overline{A \Rightarrow A}$$

for *any* A , then we could introduce polymorphism into the work. Rather than have such things as axioms, however, we would rather want them as derived rules, with premisses. If they were axioms (i.e. zero premiss rules with height 0), then the base case in the proofs would fail. For, consider the case where $\Gamma \Rightarrow \Delta \oplus \star_s(\vec{A})$ was derivable at height 0, and moreover came from an axiom with $\star_s(\vec{A})$ as the distinguished formula. In general, $\Gamma \Rightarrow \Delta$ will not be derivable, and so neither will $\Gamma + \Gamma' \Rightarrow \Delta + \Delta'$.

We submit that, with some work in the areas suggested, *Isabelle* can be made a more effective tool for formalising results in structural proof theory. Furthermore, we submit that the results in this paper are interesting in their own right.

References

- Chapman, P. (2008a), A formalisation of Contraction Admissibility for G4ip in Isabelle. University of St Andrews Computer Science Research Report.
- Chapman, P. (2008b), A Formalised Proof of Cut Admissibility for G3ip in Isabelle. University of St Andrews Computer Science Research Report, available at www.dcs.st-andrews.ac.uk/~pc.
- Chapman, P., McKinna, J. & Urban, C. (2008), Mechanising a Proof of Craig's Interpolation Theorem for Intuitionistic Logic in Nominal Isabelle, in 'AISC/MKM/Calculemus', Vol. 5144 of *Lecture Notes in Computer Science*, Springer, pp. 38–52.
- Ciabattoni, A. & Terui, K. (2006a), Modular cut-elimination: Finding proofs or counterexamples, in 'LPAR', pp. 135–149.
- Ciabattoni, A. & Terui, K. (2006b), 'Towards a semantic characterisation of cut-elimination', *Studia Logica*.
- Dawson, J. E. (2008), Isabelle files. available at <http://users.rsise.anu.edu.au/jeremy/isabelle/>.
- Dyckhoff, R. (1992), 'Contraction-free sequent calculi for intuitionistic logic', *Journal of Symbolic Logic*.
- Dyckhoff, R. & Negri, S. (2000), 'Admissibility of structural rules for contraction-free systems of intuitionistic logic', *J. Symb. Log.* **65**(4), 1499–1518.
- Negri, S. (2005), 'Proof analysis in modal logic', *Journal of Philosophical Logic* **34**, 507–544.
- Nipkow, T. (2002), Structured proofs in isar/hol, in 'TYPES', pp. 259–278.
- Nipkow, T., Paulson, L. & Wenzel, M. (2005), *A Proof Assistant for Higher-Order Logic*, number 2283 in 'Lecture Notes in Computer Science', Springer-Verlag.
- Rasga, J. (2007), 'Sufficient conditions for cut elimination with complexity analysis', *Ann. Pure Appl. Logic* **149**(1-3), 81–99.
- Tasson, C. & Urban, C. (2005), Nominal techniques in Isabelle/HOL, in 'Proceedings of the 20th International Conference on Automated Deduction (CADE 2005)', Vol. 3632 of *LNCS*, Springer-Verlag, pp. 38–53.
- Troelstra, A. S. & Schwichtenberg, H. (2000), *Basic Proof Theory*, number 43 in 'Cambridge Tracts in Computer Science', second edn, Cambridge University Press.
- Zamansky, A. & Avron, A. (2006), Canonical gentzen-type calculi with (n, k)-ary quantifiers, in 'IJCAR', pp. 251–265.