Invertibility in Sequent Calculi

Peter Chapman
School of Computer Science, University of St Andrews
Email: pc@cs.st-andrews.ac.uk

Abstract. The invertibility of the rules of a sequent calculus is important for guiding proof search and can be used in some formalised proofs of Cut admissibility. We present sufficient conditions for when a rule is invertible with respect to a calculus. We illustrate the conditions with examples. It must be noted we give purely syntactic criteria; no guarantees are given as to the suitability of the rules.

1 Introduction

In this paper, we give an overview of some results about invertibility in sequent calculi. The framework is outlined in §2. The results are mainly concerned with multisuccedent calculi that have a single principal formula. We will use, as our running example throughout, the calculus $G_{3cp}$. In §4, we look at the formalisation of single-succedent calculi; in §5, the formalisation in Nominal Isabelle for first-order calculi is shown; in §6 the results for modal logic are examined. We return to multisuccedent calculi in §7 to look at manipulating rule sets.

2 Formalising the Framework

2.1 Formulae and Sequents

A formula is either a propositional variable, the constant $\bot$, or a connective applied to a list of formulae. We thus have a type variable indexing formulae, where the type variable will be a set of connectives. In the usual way, we index propositional variables by use of natural numbers. So, formulae are given by the datatype:

\[
\text{datatype } \text{form} = \text{At } \text{nat} \mid \text{Compound } \text{form list} \mid \text{ff}
\]

For $G_{3cp}$, we define the datatype $Gp$, and give the following abbreviations:

\[
\text{datatype } Gp = \text{con} \mid \text{dis} \mid \text{imp}
\]

\[
\text{type-synonym } Gp\text{-form} = Gp\text{ form}
\]
abbreviation con-form (infixl \( \&* \) 80) where
\( p \&* q \equiv \text{Compound con} \ [p,q] \)

abbreviation dis-form (infixl \( \lor* \) 80) where
\( p \lor* q \equiv \text{Compound dis} \ [p,q] \)

abbreviation imp-form (infixl \( \supset \) 80) where
\( p \supset q \equiv \text{Compound imp} \ [p,q] \)

A \textit{sequent} is a pair of multisets of formulae. Sequents are indexed by the connectives used to index the formulae. To add a single formula to a multiset of formulae, we use the symbol \( \oplus \), whereas to join two multisets, we use the symbol \( + \).

2.2 Rules and Rule Sets

A \textit{rule} is a list of sequents (called the premisses) paired with a sequent (called the conclusion). The two \textit{rule sets} used for multisuccedent calculi are the axioms, and the uniprincipal rules (i.e. rules having one principal formula). Both are defined as inductive sets. There are two clauses for axioms, corresponding to \( L\bot \) and normal axioms:

\textbf{inductive-set} \( Ax \) where
\begin{align*}
\text{id} & : ([], \llbracket \text{At} \ i \ \ddash \rrbracket \Rightarrow \ast \emptyset) \in Ax \\
\text{Lbot} & : ([], \llbracket \text{ff} \ i \ \ddash \rrbracket \Rightarrow \ast \emptyset) \in Ax
\end{align*}

The set of uniprincipal rules, on the other hand, must not have empty premisses, and must have a single, compound formula in its conclusion. The function \( \text{mset} \) takes a sequent, and returns the multiset obtained by adding the antecedent and the succedent together:

\textbf{inductive-set} \( \text{upRules} \) where
\begin{align*}
\text{I} & : \{ \text{mset} \ c \equiv \text{Compound R Fs} \ \ddash \rrbracket ; ps \neq [] \} \implies (ps,c) \in \text{upRules}
\end{align*}

For \( \text{G3cp} \), we have the following six rules, which we then show are a subset of the set of uniprincipal rules:

\textbf{inductive-set} \( \text{g3cp} \)

\textbf{where}
\begin{align*}
\text{conL} & : ([], \llbracket \text{A} \ \ddash \rrbracket + \llbracket \text{B} \ \ddash \rrbracket \Rightarrow \ast \emptyset), \llbracket \text{A \ \&* \ B} \ \ddash \rrbracket \Rightarrow \ast \emptyset) \in \text{g3cp} \\
\text{conR} & : ([0 \Rightarrow \ast \llbracket \text{A} \ \ddash \rrbracket, \emptyset \Rightarrow \ast \llbracket \text{B} \ \ddash \rrbracket], \emptyset \Rightarrow \ast \llbracket \text{A \ \&* \ B} \ \ddash \rrbracket) \in \text{g3cp} \\
\text{disL} & : ([], \llbracket \text{A} \ \ddash \rrbracket \Rightarrow \ast \emptyset, \llbracket \text{B} \ \ddash \rrbracket \Rightarrow \ast \emptyset), \llbracket \text{A \ \lor* \ B} \ \ddash \rrbracket \Rightarrow \ast \emptyset) \in \text{g3cp} \\
\text{disR} & : ([0 \Rightarrow \ast \llbracket \text{A} \ \ddash \rrbracket + \llbracket \text{B} \ \ddash \rrbracket], \emptyset \Rightarrow \ast \llbracket \text{A \ \lor* \ B} \ \ddash \rrbracket) \in \text{g3cp} \\
\text{impL} & : ([0 \Rightarrow \ast \llbracket \text{A} \ \ddash \rrbracket, \llbracket \text{B} \ \ddash \rrbracket \Rightarrow \ast \emptyset], \llbracket \text{A \ \supset \ B} \ \ddash \rrbracket \Rightarrow \ast \emptyset) \in \text{g3cp} \\
\text{impR} & : ([], \llbracket \text{A} \ \ddash \rrbracket \Rightarrow \ast \llbracket \text{B} \ \ddash \rrbracket, \emptyset \Rightarrow \ast \llbracket \text{A \ \supset \ B} \ \ddash \rrbracket) \in \text{g3cp}
\end{align*}

\textbf{lemma} \( \text{g3cp-upRules} \):
\textbf{shows} \( \text{g3cp} \subseteq \text{upRules} \)
\langle \text{proof} \rangle
We have thus given the active parts of the G3cp calculus. We now need to extend these active parts with passive parts.

Given a sequent \( C \), we extend it with another sequent \( S \) by adding the two antecedents and the two succedents. To extend an active part \((Ps, C)\) with a sequent \( S \), we extend every \( P \in Ps \) and \( C \) with \( S \):

\[
\text{overloading} \\
\text{extend} \equiv \text{extend} \\
\text{extendRule} \equiv \text{extendRule}
\]

begin

definition \text{extend}
\text{where} \text{extend forms seq} \equiv (\text{antec forms} + \text{antec seq}) \Rightarrow^* (\text{succ forms} + \text{succ seq})

definition \text{extendRule}
\text{where} \text{extendRule forms } R \equiv (\text{map (extend forms)} (\text{fst } R), \text{extend forms (snd } R))

end

Given a rule set \( \mathcal{R} \), the extension of \( \mathcal{R} \), called \( \mathcal{R}^* \), is then defined as another inductive set:

\[
\text{inductive-set} \ \text{extRules} :: 'a \text{ rule set} \Rightarrow 'a \text{ rule set} \ (-*)
\]
\text{for } R :: 'a \text{ rule set}
\text{where } I : r \in R \Rightarrow \text{extendRule seq } r \in R^*

The rules of G3cp all have unique conclusions. This is easily formalised:

\[
\text{overloading} \ \text{uniqueConclusion} \equiv \text{uniqueConclusion}
\]

begin

definition \text{uniqueConclusion} :: 'a \text{ rule set} \Rightarrow \text{bool}
\text{where} \text{uniqueConclusion } R \equiv \forall r1 \in R. \forall r2 \in R. (\text{snd } r1 = \text{snd } r2) \rightarrow (r1 = r2)

end

lemma g3cp-uc:
shows uniqueConclusion g3cp
(proof)

2.3 Principal Rules and Derivations

A formula \( A \) is left principal for an active part \( R \) iff the conclusion of \( R \) is of the form \( A \Rightarrow \emptyset \). The definition of right principal is then obvious. We have an inductive predicate to check these things:

\[
\text{inductive} \ \text{rightPrincipal} :: 'a \text{ rule } \Rightarrow 'a \text{ form } \Rightarrow \text{bool}
\]
\text{where}
\text{up: } C = (\emptyset \Rightarrow^* (\text{Compound } F Fs)) \Rightarrow
\text{rightPrincipal } (Ps, C) (\text{Compound } F Fs)
As an example, we show that if \( A \land B \) is principal for an active part in \( G_{3cp} \), then \( \emptyset \Rightarrow A \) is a premiss of that active part:

**lemma** principal-means-premiss:

**assumes**

- \( a: \text{rightPrincipal} \ r \ (A \land^* B) \)
- \( b: \ r \in G_{3cp} \)

**shows**

\( (\emptyset \Rightarrow^* A \upharpoonright) \in \text{set} \ (\text{fst} \ r) \)

**⟨proof⟩**

A sequent is *derivable* at height 0 if it is the conclusion of a rule with no premisses. If a rule has \( m \) premisses, and the maximum height of the derivation of any of the premisses is \( n \), then the conclusion will be derivable at height \( n + 1 \). We encode this as pairs of sequents and natural numbers. A sequent \( S \) is derivable at a height \( n \) in a rule system \( R \) iff \( (S, n) \) belongs to the inductive set \( \text{derivable} \ R \):

**inductive-set** derivable :: 'a rule set ⇒ 'a deriv set

**for**

- \( R :: 'a rule set \)
- \( \text{where} \)
- \( \text{base}: [([],C) \in R] \Rightarrow (C,0) \in \text{derivable} \ R \)
- \( \text{step}: [ r \in R ; (\text{fst} \ r) \neq [] ; \forall \ p \in \text{set} \ (\text{fst} \ r). \ \exists \ n \leq m. \ (p,n) \in \text{derivable} \ R ] \)
  \( \Rightarrow \ (\text{snd} \ r.m + 1) \in \text{derivable} \ R \)

In some instances, we do not care about the height of a derivation, rather that the root is derivable. For this, we have the additional definition of \( \text{derivable}' \), which is a set of sequents:

**inductive-set** derivable' :: 'a rule set ⇒ 'a sequent set

**for**

- \( R :: 'a rule set \)
- \( \text{where} \)
- \( \text{base}: [([],C) \in R] \Rightarrow C \in \text{derivable}' \ R \)
- \( \text{step}: [ r \in R ; (\text{fst} \ r) \neq [] ; \forall \ p \in \text{set} \ (\text{fst} \ r). \ p \in \text{derivable}' \ R ] \)
  \( \Rightarrow \ (\text{snd} \ r) \in \text{derivable}' \ R \)

It is desirable to switch between the two notions. Shifting from derivable at a height to derivable is simple: we delete the information about height. The converse is more complicated and involves an induction on the length of the premiss list:

**lemma** deriv-to-deriv:

**assumes** \( (C,n) \in \text{derivable} \ R \)

**shows** \( C \in \text{derivable}' \ R \)

**⟨proof⟩**

**lemma** deriv-to-deriv2:

**assumes** \( C \in \text{derivable}' \ R \)

**shows** \( \exists \ n. \ (C,n) \in \text{derivable} \ R \)

**⟨proof⟩**
3 Formalising the Results

A variety of “helper” lemmata are used in the proofs, but they are not shown. The proof tactics themselves are hidden in the following proof, except where they are interesting. Indeed, only the interesting parts of the proof are shown at all. The main result of this section is that a rule is invertible if the premisses appear as premisses of every rule with the same principal formula. The proof is interspersed with comments.

**lemma rightInvertible:**

**fixes** \( \Gamma \Delta :: 'a form multiset **assumes** rules: \( R' \subseteq \text{upRules} \land R = Ax \cup R' \) and \( a: (\Gamma \Rightarrow \Delta \oplus \text{Compound } F\ Fs,n) \in \text{derivable } R \) and \( b: \forall r' \in R. \text{rightPrincipal } r'(\text{Compound } F\ Fs) \rightarrow (\Gamma' \Rightarrow \Delta') \in \text{set } (\text{fst } r') \) shows \( \exists m \leq n. (\Gamma + \Gamma' \Rightarrow \Delta + \Delta',m) \in \text{derivable } R \)**

As an example, we show the left premiss of \( R \land \) in \textbf{G3cp} is derivable at a height not greater than that of the conclusion. The two results used in the proof (**principal-means-premiss** and **rightInvertible**) are those we have previously shown:

**lemma conRInvert:**

**assumes** \( (\Gamma \Rightarrow \Delta \oplus (A \land B),n) \in \text{derivable } (g3cp \cup Ax)* \) shows \( \exists m \leq n. (\Gamma \Rightarrow \Delta \oplus A,m) \in \text{derivable } (g3cp \cup Ax)* \)**

We can obviously show the equivalent proof for left rules, too:

**lemma leftInvertible:**

**fixes** \( \Gamma \Delta :: 'a form multiset **assumes** rules: \( R' \subseteq \text{upRules} \land R = Ax \cup R' \) and \( a: (\Gamma \Leftrightarrow \Delta \oplus \text{Compound } F\ Fs \Rightarrow \Delta,n) \in \text{derivable } R \) and \( b: \forall r' \in R. \text{leftPrincipal } r'(\text{Compound } F\ Fs) \rightarrow (\Gamma' \Rightarrow \Delta') \in \text{set } (\text{fst } r') \) shows \( \exists m \leq n. (\Gamma + \Gamma' \Rightarrow \Delta + \Delta',m) \in \text{derivable } R \)**

A rule is invertible iff every premiss is derivable at a height lower than that of the conclusion. A set of rules is invertible iff every rule is invertible. These definitions are easily formalised:

**overloading**

\( \text{invertible} \equiv \text{invertible} \)
\( \text{invertible-set} \equiv \text{invertible-set} \)

**begin**

**definition invertible**

where \( \text{invertible } r R \equiv \forall n S. (r \in R \land (\text{snd } (\text{extendRule } S r),n) \in \text{derivable } R*) \rightarrow (\forall p \in \text{set } (\text{fst } (\text{extendRule } S r)). \exists m \leq n. (p,m) \in \text{derivable } R*) \)

**definition invertible-set**
where invertible-set $R \equiv \forall (ps,c) \in R. \ invertible (ps,c) \ R$

end

A set of multisuccedent uniprincipal rules is invertible if each rule has a different conclusion. $G3cp$ has the unique conclusion property (as shown in §2.2). Thus, $G3cp$ is an invertible set of rules:

lemma unique-to-invertible:
assumes $R' \subseteq upRules \land R = Ax \cup R'$
and $uniqueConclusion R'$
shows invertible-set $R(\langle proof \rangle)$

lemma g3cp-invertible:
shows invertible-set $(Ax \cup g3cp)$
$\langle proof \rangle$

3.1 Conclusions

For uniprincipal multisuccedent calculi, the theoretical results have been formalised. Moreover, the running example demonstrates that it is straightforward to implement such calculi and reason about them. Indeed, it will be this class of calculi for which we will prove more results in §7.

4 Single Succedent Calculi

We must be careful when restricting sequents to single succedents. If we have sequents as a pair of multisets, where the second is restricted to having size at most 1, then how does one extend the active part of $L \supset \Gamma$ from $G3ip$? The left premiss will be $A \supset B \Rightarrow A$, and the extension will be $\Gamma \Rightarrow C$. The extend function must be able to correctly choose to discard the $C$.

Rather than taking this route, we instead restrict to single formulae in the succedents of sequents. This raises its own problems, since now how does one represent the empty succedent? We introduce a dummy formula $Em$, which will stand for the empty formula:

datatype 'a form = At nat |
| Compound 'a 'a form list |
| ff |
| Em |

When we come to extend a sequent, say $\Gamma \Rightarrow C$, with another sequent, say $\Gamma' \Rightarrow C'$, we only “overwrite” the succedent if $C$ is the empty formula:

overloading
extend \equiv extend
extendRule \equiv extendRule

begin
definition extend
  where extend forms seq ≡
    if (succ seq = Em)
    then (antec forms + antec seq) ⇒∗ (succ forms)
    else (antec forms + antec seq ⇒∗ succ seq)

definition extendRule
  where extendRule forms R ≡ (map (extend forms) (fst R), extend forms (snd R))

end

⟨proof⟩

Given this, it is possible to have right weakening, where we overwrite the empty formula if it appears as the succedent of the root of a derivation:

lemma dpWeakR:
  assumes (Γ ⇒∗ Em, n) ∈ derivable R∗
  and R′ ⊆ upRules
  and R = Ax ∪ R′
  shows (Γ ⇒∗ C, n) ∈ derivable R∗ — Proof omitted ⟨proof⟩

Of course, if C = Em, then the above lemma is trivial. The burden is on the user not to “use” the empty formula as a normal formula. An invertibility lemma can then be formalised:

lemma rightInvertible:
  assumes R′ ⊆ upRules ∧ R = Ax ∪ R′
  and (Γ ⇒∗ Compound F Fs, n) ∈ derivable R∗
  and ∀ r′ ∈ R. rightPrincipal r′ (Compound F Fs) −→ (Γ′ ⇒∗ E) ∈ set (fst r′)
  and E ≠ Em
  shows ∃ m ≤ n. (Γ + Γ′ ⇒∗ E, m) ∈ derivable R∗
  ⟨proof⟩

lemma leftInvertible:
  assumes R′ ⊆ upRules ∧ R = Ax ∪ R′
  and (Γ ⊕ Compound F Fs ⇒∗ δ, n) ∈ derivable R∗
  and ∀ r′ ∈ R. leftPrincipal r′ (Compound F Fs) −→ (Γ′ ⇒∗ Em) ∈ set (fst r′)
  shows ∃ m ≤ n. (Γ + Γ′ ⇒∗ δ, m) ∈ derivable R∗
  ⟨proof⟩

G3ip can be expressed in this formalism:

inductive-set g3ip
  where
    conL: ([ [ A j + B j ⇒∗ Em ] , [ A ∧∗ B j ⇒∗ Em ] ] , [ A i ] ) ∈ g3ip
    conR: ( [ [ A ⇒∗ B ] ] , [ A ∧∗ B ] ) ∈ g3ip
    disL: ( [ [ A j ] ⇒∗ Em ] , [ B j ⇒∗ Em ] ) ∈ g3ip
    disR1: ( [ [ A ⇒∗ A ] ] , [ A ⇒∗ (A ∧∗ B) ] ) ∈ g3ip
    disR2: ( [ [ A ⇒∗ B ] ] , [ A ⇒∗ (A ∨∗ B) ] ) ∈ g3ip
    impL: ( [ [ A ⊃ B ] ] , [ A j ] ) ∈ g3ip
    impR: ( [ [ A j ] ] , [ B j ⇒∗ Em ] ) ∈ g3ip
  ⟨proof⟩
As expected, $R \supset$ can be shown invertible:

\textbf{lemma} \textit{impRInvert}:
\textbf{assumes} $(\Gamma \Rightarrow (A \supset B), n) \in \text{derivable} \ (Ax \cup g3ip)^* \text{ and } B \neq \text{Em}$
\textbf{shows} $\exists \ m \leq n. \ (\Gamma \oplus A \Rightarrow B, m) \in \text{derivable} \ (Ax \cup g3ip)^*$

\section{First-Order Calculi}

To formalise first-order results we use the package \textit{Nominal Isabelle}. The details, for the most part, are the same as in §2. However, we lose one important feature: that of polymorphism.

Recall we defined formulae as being indexed by a type of connectives. We could then give abbreviations for these indexed formulae. Unfortunately this feature (indexing by types) is not yet supported in \textit{Nominal Isabelle}. Nested datatypes are also not supported. Thus, strings are used for the connectives (both propositional and first-order) and lists of formulae are simulated to nest via a mutually recursive definition:

\textbf{nominal-datatype} \textit{form} = \texttt{At nat var list}  \\
\hspace{1em} | \texttt{Cpd0 string form-list}  \\
\hspace{1em} | \texttt{Cpd1 string «var» form (- (\∇ [-].-))}  \\
\hspace{1em} | \texttt{ff}

\textbf{and} \textit{form-list} = \texttt{FNil}  \\
\hspace{1em} | \texttt{FCons form form-list}

Formulae are quantified over a single variable at a time. This is a restriction imposed by \textit{Nominal Isabelle}.

There are two new uniprincipal rule sets in addition to the propositional rule set: first-order rules without a freshness proviso and first-order rules with a freshness proviso. Freshness provisos are particularly easy to encode in \textit{Nominal Isabelle}. We also show that the rules with a freshness proviso form a subset of the first-order rules. The function \textit{set-of-prem} takes a list of premisses, and returns all the formulae in that list:

\textbf{inductive-set} \textit{provRules} \textbf{where}

\[ [ \text{mset} \ c = \set{ F \ \nabla \ [x].A \ \supset ; \ ps \neq \ [] ; \ x \ \nmid \text{ set-of-prem} (ps - A) } ] \]
\[ \implies (ps, c) \in \text{provRules} \]

\textbf{inductive-set} \textit{nprovRules} \textbf{where}

\[ [ \text{mset} \ c = \set{ F \ \nabla \ [x].A \ \supset ; \ ps \neq \ [] } ] \]
\[ \implies (ps, c) \in \text{nprovRules} \]

\textbf{lemma} \textit{nprovContain}:
\textbf{shows} \textit{provRules} $\subseteq$ \textit{nprovRules}

\langle\text{proof}\rangle
Substitution is defined in the usual way:

nominal-primrec

\( \text{subst-form} :: \text{var} \Rightarrow \text{var} \Rightarrow \text{form} \Rightarrow \text{form} \ (\cdot,\cdot) \)

and \( \text{subst-forms} :: \text{var} \Rightarrow \text{var} \Rightarrow \text{form-list} \Rightarrow \text{form-list} \ (\cdot,\cdot) \)

where

\[
[z, y] (At P \ xs) = At P ((z; y) \ xs) \\
x_n^{\#} (z, y) \mapsto [z, y] (F \ \nabla [x].A) = F \ \nabla [x].([z, y]\ A) \\
[z, y] (\text{Cpd0} \ F \ Fs) = \text{Cpd0} \ F \ ([z, y]\ Fs) \\
[z, y] ff = ff \\
[z, y] \text{FNil} = \text{FNil} \\
[z, y] (\text{FCons} \ f \ Fs) = \text{FCons} \ ([z, y] f) \ ([z, y] Fs)\ \text{(proof)}
\]

Substitution is extended to multisets in the obvious way.

To formalise the condition “no specific substitutions”, an inductive predicate is introduced. If some formula in the multiset \( \Gamma \) is a non-trivial substitution, then \( \text{multSubst} \ \Gamma \):

\[
\text{definition} \ \text{multSubst} :: \text{form} \ \text{multiset} \Rightarrow \text{bool} \ \text{where} \ \text{multSubst-def} \ \Gamma \equiv (\exists \ A \in (\text{set-mult} \ \Gamma) \ \exists \ x \ y. \ \{y, x\} B = A \ \land \ y \neq x)
\]

The notation \([z, y]\ xs\) stands for substitution of a variable in a variable list. The details are simple, and so are not shown.

Extending the rule sets with passive parts depends upon which kind of active part is being extended. The active parts with freshness contexts have additional constraints upon the multisets which are added:

\[
\text{inductive-set} \ \text{extRules} :: \text{rule set} \Rightarrow \text{rule set} \ \text{(\ast)}
\]

for \( \text{R} :: \text{rule set} \)

where

\[
id: \ [\ r \in \text{R} ; \ r \in \text{Ax} \ ] \Rightarrow \text{extendRule} \ S \ r \in \text{R}\ast \\
s: \ [\ r \in \text{R} ; \ r \in \text{upRules} \ ] \Rightarrow \text{extendRule} \ S \ r \in \text{R}\ast \\
np: \ [\ r \in \text{R} ; \ r \in \text{nprovRules} \ ] \Rightarrow \text{extendRule} \ S \ r \in \text{R}\ast \\
p: \ [\ (ps, c) \in \text{R} ; \ (ps, c) \in \text{provRules} ; \ \text{mset} \ c = \{ F \ \nabla [x].A \ \uparrow ; \ x \notin \text{set-of-seq} \ S \} \ ] \Rightarrow \text{extendRule} \ S \ (ps, c) \in \text{R}\ast
\]

The final clause says we can only use an \( S \) which is suitable fresh.

The only lemma which is unique to first-order calculi is the Substitution Lemma. We show the crucial step in the proof; namely that one can substitute a fresh variable into a formula and the resultant formula is unchanged. The proof is not particularly edifying and is omitted:

\[
\text{lemma} \ \text{formSubst}: \ \text{shows} \ y \notin x \ \land \ y \notin A \Rightarrow F \ \nabla [x].A = F \ \nabla [y].([y, x] A)\ \text{(proof)}
\]

Using the above lemma, we can change any sequent to an equivalent new sequent which does not contain certain variables. Therefore, we can extend with any sequent:

\[
\text{lemma} \ \text{extend-for-any-seq}: \\
\text{fixes} \ S :: \text{sequent} \\
\text{assumes} \ \text{rules} :: \text{R1} \subseteq \text{upRules} \ \land \ \text{R2} \subseteq \text{nprovRules} \ \land \ \text{R3} \subseteq \text{provRules}
\]
and rules2: $R = Ax \cup R1 \cup R2 \cup R3$
and rin: $r \in R$
shows extendRule $S \ r \in R*$
⟨proof⟩⟨proof⟩⟨proof⟩⟨proof⟩

We can then give the two inversion lemmata. The principal case (where the last inference had a freshness proviso) for the right inversion lemma is shown:

lemma rightInvert:
fixes $\Gamma \Delta :: form$ multiset
assumes rules: $R1 \subseteq upRules \land R2 \subseteq nprovRules \land R3 \subseteq provRules \land R = Ax \cup R1 \cup R2 \cup R3$
and a: $(\Gamma \Rightarrow* \Delta \oplus F \neg [x].A,n) \in \text{derivable } R*$
and b: $\forall \ r' \in R. \text{ rightPrincipal } r' (F \neg [x].A) \rightarrow (\Gamma' \Rightarrow* \Delta') \in \text{set } (fst \ r')$
and c: $\neg \text{ multSubst } \Gamma' \land \neg \text{ multSubst } \Delta'$
shows $\exists \ m \leq n. \ (\Gamma + \Gamma' \Rightarrow* \Delta + \Delta',m) \in \text{derivable } R*$

lemma leftInvert:
fixes $\Gamma \Delta :: form$ multiset
assumes rules: $R1 \subseteq upRules \land R2 \subseteq nprovRules \land R3 \subseteq provRules \land R = Ax \cup R1 \cup R2 \cup R3$
and a: $(\Gamma \oplus F \neg [x].A \Rightarrow* \Delta,n) \in \text{derivable } R*$
and b: $\forall \ r' \in R. \text{ leftPrincipal } r' (F \neg [x].A) \rightarrow (\Gamma' \Rightarrow* \Delta') \in \text{set } (fst \ r')$
and c: $\neg \text{ multSubst } \Gamma' \land \neg \text{ multSubst } \Delta'$
shows $\exists \ m \leq n. \ (\Gamma + \Gamma' \Rightarrow* \Delta + \Delta',m) \in \text{derivable } R*$

In both cases, the assumption labelled c captures the “no specific substitution” condition. Interestingly, it is never used throughout the proof. This highlights the difference between the object- and meta-level existential quantifiers.

Owing to the lack of indexing within datatypes, it is difficult to give an example demonstrating these results. It would be little effort to change the theory file to accommodate type variables when they are supported in Nominal Isabelle, at which time an example would be simple to write.

⟨proof⟩⟨proof⟩⟨proof⟩⟨proof⟩⟨proof⟩⟨proof⟩⟨proof⟩⟨proof⟩⟨proof⟩⟨proof⟩

6 Modal Calculi

Some new techniques are needed when formalising results about modal calculi. A set of modal operators must index formulae (and sequents and rules), there must be a method for modalising a multiset of formulae and we need to be able to handle implicit weakening rules.

The first of these is easy: instead of indexing formulae by a single type variable, we index on a pair of type variables, one which contains the propositional connectives, and one which contains the modal operators:

datatype ('a, 'b) form = At nat
| Compound ('a, 'b) form list
| Modal ('b, 'b) form list
| ff
**datatype-compat**

**form**

overloading

uniqueConclusion ≡ uniqueConclusion
modaliseMultiset ≡ modaliseMultiset

begin

definition uniqueConclusion :: ('a,'b) rule set ⇒ bool
  where uniqueConclusion R ≡ ∀ r1 ∈ R. ∀ r2 ∈ R. (snd r1 = snd r2) → (r1 = r2)

Modalising multisets is relatively straightforward. We use the notation \(! \cdot \Gamma\), where \(!\) is a modal operator and \(\Gamma\) is a multiset of formulae:

definition modaliseMultiset :: 'b ⇒ ('a,'b) form multiset ⇒ ('a,'b) form multiset
  where modaliseMultiset a Γ ≡ {# Modal a [p]. p ∈ # Γ #}

end

Similarly to §5, two new rule sets are created. The first are the normal modal rules:

inductive-set modRules2 where
  \[ ps \neq [] ; mset c = ? Modal M Ms \; \] ⇒ (ps,c) ∈ modRules2

The second are the modalised context rules. Taking a subset of the normal modal rules, we extend using a pair of modalised multisets for context. We create a new inductive rule set called p-e, for “prime extend”, which takes a set of modal active parts and a pair of modal operators (say \(!\) and \(\cdot\)), and returns the set of active parts extended with \(! \cdot \Gamma \Rightarrow \cdot \Delta\):

inductive-set p-e :: ('a,'b) rule set ⇒ 'b ⇒ 'b ⇒ ('a,'b) rule set
  for R :: ('a,'b) rule set and M N :: 'b
  where
  \[ (Ps, c) ∈ R ; R \subseteq modRules2 \] ⇒ extendRule (M·Γ ⇒∗ N·Δ) (Ps, c) ∈ p-e R M N

We need a method for extending the conclusion of a rule without extending the premisses. Again, this is simple:

overloading extendConc ≡ extendConc

begin

definition extendConc :: ('a,'b) sequent ⇒ ('a,'b) rule ⇒ ('a,'b) rule
  where extendConc S r ≡ (fst r, extend S (snd r))

end

The extension of a rule set is now more complicated; the inductive definition has four clauses, depending on the type of rule:

inductive-set ext :: ('a,'b) rule set ⇒ ('a,'b) rule set ⇒ 'b ⇒ 'b ⇒ ('a,'b) rule set
for $R \ R' : = \ (a, b)$ rule set and $M \ N : = \ 'b$

where

\begin{align*}
ax & : \ [ r \in R \mid r \in Ax ] \implies \text{extendRule seq } r \in \text{ext } R \ R' \ M \ N \\
up & : \ [ r \in R \mid r \in \text{upRules} ] \implies \text{extendRule seq } r \in \text{ext } R \ R' \ M \ N \\
mod1 & : \ [ r \in p-e \ R' \ M \ N \mid r \in R ] \implies \text{extendConc seq } r \in \text{ext } R \ R' \ M \ N \\
mod2 & : \ [ r \in R \mid r \in \text{modRules2} ] \implies \text{extendRule seq } r \in \text{ext } R \ R' \ M \ N
\end{align*}

Note the new rule set carries information about which set contains the modalised context rules and which modal operators which extend those prime parts.

We have two different inversion lemmata, depending on whether the rule was a modalised context rule, or some other kind of rule. We only show the former, since the latter is much the same as earlier proofs. The interesting cases are picked out:

**lemma rightInvert:**

*fixes* $\Gamma \Delta : = \ (a, b)$ form multiset

*assumes* rules: $R1 \subseteq \text{upRules} \land R2 \subseteq \text{modRules2} \land R3 \subseteq \text{modRules2} \land R = Ax \cup R1 \cup (p-e \ R2 \ M1 \ M2) \cup R3 \land R' = Ax \cup R1 \cup R2 \cup R3$

*and* $a: (\Gamma \implies^* \Delta \uplus \text{Modal } M \ M's, n) \in \text{derivable } (\text{ext } R \ R2 \ M1 \ M2)$

*and* $b: \forall r' \in R', \text{rightPrincipal } r' (\text{Modal } M \ M's) \ R' \rightarrow (\Gamma' \implies^* \Delta') \in \text{set } (\text{fst } r')$

*and* neq: $M2 \neq M$

*shows* $\exists m \leq n. (\Gamma + \Gamma' \implies^* \Delta + \Delta', m) \in \text{derivable } (\text{ext } R \ R2 \ M1 \ M2)$

We guarantee no other rule has the same modal operator in the succedent of a modalised context rule using the condition $M \neq M2$. Note this lemma only allows one kind of modalised context rule. In other words, it could not be applied to a calculus with the rules:

\[
\begin{align*}
\frac{! \cdot \Gamma \Rightarrow A \cdot \Delta \quad R1}{\Gamma', ! \cdot \Gamma \Rightarrow A, ! \cdot \Delta} \quad \frac{\bullet \cdot \Gamma \Rightarrow A, ! \cdot \Delta \quad R2}{\Gamma', \bullet \cdot \Gamma \Rightarrow \bullet A, ! \cdot \Delta, \Delta'}
\end{align*}
\]

since, if $([\emptyset \Rightarrow A], \emptyset \Rightarrow \bullet A) \in \mathcal{R}$, then $R1 \in \text{p-e } \mathcal{R} ! \bullet$, whereas $R2 \in \text{p-e } \mathcal{R} \bullet !$.

Similarly, we cannot have modalised context rules which have more than one modalised multiset in the antecedent or succedent of the active part. For instance:

\[
\begin{align*}
\frac{! \cdot \Gamma_1, \bullet \cdot \Gamma_2 \Rightarrow A, ! \cdot \Delta_1, \bullet \cdot \Delta_2 \quad R1'}{\Gamma_1', ! \cdot \Gamma_1 \Rightarrow A, ! \cdot \Delta_1, \bullet \cdot \Delta_2, \Delta'}
\end{align*}
\]

cannot belong to any p-e set. It would be a simple matter to extend the definition of p-e to take a set of modal operators, however this has not been done.

As an example, classical modal logic can be formalised. The (modal) rules for this calculus are then given in two sets, the latter of which will be extended with $\Box \cdot \Gamma \Rightarrow \Diamond \cdot \Delta$:

**inductive-set** $g3\text{mod2}$

*where*
We then show the strong admissibility of the rule:

\[
\Gamma \Rightarrow \Box A, \Delta \\
T \Rightarrow A, \Delta
\]

**Lemma invertBoxR:**

**Assumes** \( R = Ax \cup g3up \cup (p-e \ g3mod1 \ Box) \cup g3mod2 \)**

**And** \( (\Gamma \Rightarrow \Box \Delta, n) \in \text{derivable} (\text{ext } R \ g3mod1 \ Box) \)**

**Shows** \( \exists m \leq n. (\Gamma \Rightarrow \Box A, m) \in \text{derivable} (\text{ext } R \ g3mod1 \ Box) \)**

where principal is the result which fulfills the principal formula conditions given in the inversion lemma, and \( g3 \) is a result about rule sets.

### 7 Manipulating Rule Sets

The removal of superfluous and redundant rules [1] will not be harmful to invertibility: removing rules means that the conditions of earlier sections are more likely to be fulfilled. Here, we formalise the results that the removal of such rules from a calculus \( \mathcal{L} \) will create a new calculus \( \mathcal{L}' \) which is equivalent. In other words, if a sequent is derivable in \( \mathcal{L} \), then it is derivable in \( \mathcal{L}' \). The results formalised in this section are for uniprincipal multisuccedent calculi.

When dealing with lists of premisses, a rule \( R \) with premisses \( P \) will be redundant given a rule \( R' \) with premisses \( P' \) if there exists some \( p \) such that \( P = p\#P' \). There are other ways in which a rule could be redundant; say if \( P = Q\@P' \), or if \( P = P'\@Q \), and so on. The order of the premisses is not really important, since the formalisation operates on the finite set based upon the list. The more general “append” lemma could be proved from the lemma we give; we prove the inductive step case in the proof of such an append lemma. This is a height preserving transformation. Some of the proof is shown:

**Lemma removeRedundant:**

**Assumes** \( r1 = (p\#ps, c) \land r1 \in \text{upRules} \)

**And** \( r2 = (ps, c) \land r2 \in \text{upRules} \)

**And** \( R1 \subseteq \text{upRules} \land R = Ax \cup R1 \)

**And** \( (T,n) \in \text{derivable} (R \cup \{r1\} \cup \{r2\})^* \)

**Shows** \( \exists m \leq n. (T,m) \in \text{derivable} (R \cup \{r2\})^* \)
Recall that to remove superfluous rules, we must know that Cut is admissible in the original calculus [1]. Again, we add the two distinguished premisses at the head of the premiss list; general results about permutation of lists will achieve a more general result. Since one uses Cut in the proof, this will in general not be height-preserving:

**lemma** removeSuperfluous:
assumes \( r_1 = (\emptyset \Rightarrow \ast \{A\}) \# ((\{A\} \Rightarrow \ast \emptyset) \# ps), c) \land r_1 \in upRules \)
and \( R_1 \subseteq upRules \land R = Ax \cup R_1 \)
and \( \langle T,n \rangle \in \text{derivable} (R \cup \{r_1\})^\ast \)
and \( CA; \forall \Gamma \Delta A. ((\Gamma \Rightarrow \ast \Delta \oplus A) \in \text{derivable}^' R^\ast) \longrightarrow \)
\( (\Gamma \oplus A \Rightarrow \ast \Delta) \in \text{derivable}^' R^\ast \) \( \longrightarrow \)
\( (\Gamma \Rightarrow \ast \Delta) \in \text{derivable}^' R^\ast \)
shows \( T \in \text{derivable}^' R^\ast \langle \text{proof} \rangle \)

**Combinable rules** can also be removed. We encapsulate the combinable criterion by saying that if \((p\#P, T)\) and \((q\#P, T)\) are rules in a calculus, then we get an equivalent calculus by replacing these two rules by \((\text{extend } p \ q) \# P, T)\). Since the extend function is commutative, the order of \(p\) and \(q\) in the new rule is not important. This transformation is height preserving:

**lemma** removeCombinable:
assumes \( a: r_1 = (p \# ps, c) \land r_1 \in upRules \)
and \( b: r_2 = (q \# ps, c) \land r_2 \in upRules \)
and \( c: r_3 = (\text{extend } p \ q \# ps, c) \land r_3 \in upRules \)
and \( d: R_1 \subseteq upRules \land R = Ax \cup R_1 \)
and \( \langle T,n \rangle \in \text{derivable} (R \cup \{r_1\} \cup \{r_2\})^\ast \)
shows \( \langle T,n \rangle \in \text{derivable} (R \cup \{r_3\})^\ast \langle \text{proof} \rangle \)

8 Conclusions

Only a portion of the formalisation was shown; a variety of intermediate lemmata were not made explicit. This was necessary, for the Isabelle theory files run to almost 8000 lines. However, these files do not have to be replicated for each new calculus. It takes very little effort to define a new calculus. Furthermore, proving invertibility is now a quick process; less than 25 lines of proof in most cases.

**theory** SequentInvertibility
**imports** MultiSequents SingleSuccedent NominalSequents ModalSequents SRCTransforms
**begin**

**end**

References

1. A. Avron and I. Lev. Canonical propositional Gentzen-type systems. In Automated Reasoning, First International Joint Conference, IJCAR 2001, Siena, Italy, June 18-