

Formalising Proofs of Cut Admissibility

Peter Chapman

1 Introduction

In this document, we look at two methods of formalising a proof of Cut admissibility using *Isabelle*. The first uses **sets** of formulae for the contexts, and the second uses **multisets**. We have, where possible, hidden the particular representation of context behind some common notation. We begin with the multiset approach, and then consider the set approach. The general framework used for both was that proposed in [2] and extended in [1]. In particular, we have that our objects of study are *provable sequents*, augmented with a *level* parameter. As an example, we write $\Gamma \Rightarrow C \downarrow n$ to mean that $\Gamma \Rightarrow C$ is the root of a valid derivation of height n .

2 Multisets

In most texts on Proof Theory, multisets are the context of choice. As such, this is the most obvious starting point for a formalisation of a proof theoretic result. Unfortunately, the notation that *Isabelle* initially has for multisets is cumbersome. To augment a multiset (of formulae) with a formula, the notation is $\Gamma + \{\#A\#$. We defined an abbreviation for this, which is $\Gamma \oplus A$. This has the added benefit in that it forces us to adopt an ordering when writing antecedents: Γ must be a multiset, and A must be a formula. The operator \oplus associates to the left, so we are able to write, for instance, $\Gamma \oplus A \oplus B$, rather than $(\Gamma \oplus A) \oplus B$.

A lemma which was not in the *Isabelle* distribution, is the following

If $\Gamma \oplus A = \Gamma' \oplus B$, and $A \neq B$, then $A \in \Gamma'$.

We have proved this, as well as an extension of it, which is as follows

If $\Gamma \oplus A = \Gamma' \oplus B$, and $A \neq B$, then there is some Γ'' such that $\Gamma = \Gamma'' \oplus B$ and $\Gamma' = \Gamma'' \oplus A$.

Once this lemma is in place, the rest of the proof can proceed without much, if any, deviance from a proof that one would see in a textbook. Let us illustrate with an example. Suppose that the cut formula is $A \wedge B$, and further that it is not principal in the right premiss. Suppose also

that the right derivation is an instance of $L\wedge$ too, but on a different pair of formulae, say $D \wedge E$. Then, we have

$$\frac{\frac{\Gamma \Rightarrow A \downarrow n_1 \quad \Gamma \Rightarrow B \downarrow n_2}{\Gamma \Rightarrow A \wedge B \downarrow n_1 + n_2 + 1} \quad \Gamma \oplus A \wedge B \Rightarrow C \downarrow m}{\Gamma \Rightarrow C \downarrow n_1 + n_2 + m + 2} \text{Cut}$$

We can proceed by one of two ways here. We can either use inversion of the right sequent to give $\Gamma \oplus A \oplus B \Rightarrow C \downarrow m_1$, for some $m_1 \leq m$, or use inversion on the left sequent. We know, however, that since the right sequent is an instance of $L\wedge$, with principal formula $D \wedge E$, that there is some Γ' so that $\Gamma' \oplus D \wedge E = \Gamma \oplus A \wedge B$. We use the lemma above to then find a Γ'' with the two required properties. Now, we can rewrite the derivation as

$$\frac{\frac{\Gamma'' \oplus D \wedge E \Rightarrow A \downarrow n_1 \quad \Gamma'' \oplus D \wedge E \Rightarrow B \downarrow n_2}{\Gamma'' \oplus D \wedge E \Rightarrow A \wedge B \downarrow n_1 + n_2 + 1} \quad \Gamma'' \oplus A \wedge B \oplus D \wedge E \Rightarrow C \downarrow m}{\Gamma'' \oplus D \wedge E \Rightarrow C \downarrow n_1 + n_2 + m + 2} \text{Cut}$$

Then, we use inversion on the left premiss, to give $\Gamma'' \oplus D \oplus E \Rightarrow A \wedge B \downarrow n'$ for some $n' \leq n_1 + n_2 + 1$, and use the premiss of $L\wedge$ on the right to give $\Gamma'' \oplus A \wedge B \oplus D \oplus E \Rightarrow C \downarrow m - 1$. We then use the induction hypothesis to remove this cut, and then apply $L\wedge$:

$$\frac{\frac{\Gamma'' \oplus D \oplus E \Rightarrow A \wedge B \downarrow n' \quad \Gamma'' \oplus A \wedge B \oplus D \oplus E \Rightarrow C \downarrow m - 1}{\Gamma'' \oplus D \oplus E \Rightarrow C \downarrow} \text{IH}}{\Gamma \Rightarrow C \downarrow} L\wedge, \Gamma = \Gamma'' \oplus D \wedge E$$

If we had used the other available route, then we would have needed two cuts. These slight detours (via some Γ'') are needed, however they do not add much to the length of the proof. To prove context-sharing Cut admissibility, and also Contraction admissibility, which follows as a consequence, takes 990 lines.

Note that the example given above was slightly misleading; we would actually use inversion on the right premiss, and eliminate the two cuts (one on A , one on B), since then we do not need to know which rule was used on the right. The only case where the Cut formula is principal in the left premiss (i.e. was derived using a right rule) and we need to know which rule derived the right premiss is when the Cut formula is an implication. However, we also need to know the rule which derived the right premiss when using sets as contexts. The number of cases we have when using multisets for contexts are as follows, enumerated on the rule used to derive the left premiss

- Axiom : 10 cases (9 different ways to derive the right premiss, and when the right premiss is also an Axiom, we have two subcases where the propositional letter is the same for both premisses, or different)

- $L\perp$: 1 case
- $R\wedge$: 1 case
- RV_1 : 1 case
- RV_2 : 1 case
- $R\supset$: 10 cases
- $L\wedge$: 1 case
- $L\vee$: 1 case
- $L\supset$: 1 case

giving a total of 27 cases. To better illustrate the point made in the Axiom case, we have the subcase where the right premiss is also an Axiom. Suppose the left premiss was $\Gamma \Rightarrow P \downarrow 0$, where $P \in \Gamma$, then the right premiss is $\Gamma \oplus P \Rightarrow Q \downarrow 0$, where $Q \in \Gamma \oplus P$. Thus we consider two possibilities: $P = Q$ or $P \neq Q$. This disjunction gives us the extra case. The same is true when we consider $R\supset$ as the rule which derived the left premiss: there are two possibilities when we consider the right premiss being derived from $L\supset$.

3 Sets

We have reused the same notation as multisets, just changed the abbreviation. So, we now have defined $\Gamma \oplus A$ to be $\Gamma \cup \{A\}$. Not surprisingly, this means that a lot of the proof can be simply copied. However, there are some differences. Most damaging is the duplication of the principal formula of a rule into the premisses. For instance, for multisets the rule $L\wedge$ would be

$$\frac{\Gamma \oplus A \oplus B \Rightarrow C \downarrow n}{\Gamma \oplus A \wedge B \Rightarrow C \downarrow n + 1}$$

for sets we have

$$\frac{\Gamma \oplus A \oplus B \Rightarrow C \downarrow n}{\Gamma \Rightarrow C \downarrow n + 1} A \wedge B \in \Gamma$$

What this means is that before, where we could just use inversion, we now have to know which rule was used if the cut formula is principal in the left premiss. For instance, consider the same proof transformation as in the previous section. We know that $A \wedge B$ is not principal in the right premiss, which means that if we use inversion, we have

$$\frac{\Gamma \oplus A \wedge B \oplus A \oplus B \Rightarrow C \downarrow m'}{\Gamma \oplus A \wedge B \Rightarrow C \downarrow m} \text{inv}, m' \leq m$$

We need to cut this extra $A \wedge B$, but this is not allowable by the induction hypothesis, because we *do not* know that $n + m' < n + m$. Thus, for the three cases where the left premiss is a right rule, we must know what rule was used in the right premiss. This means that we have a further 27 (9 more for each of $RV_1, RV_2, R\wedge$) cases when compared with using multisets for contexts.

Furthermore, the proof transformations are more complicated because of the duplication of the principal formula in left rules. We will show the transformation for $A \wedge B$ principal in both premisses, and omit the information about the height of the cut:

$$\frac{\frac{\Gamma \Rightarrow B}{\Gamma \oplus B \Rightarrow A} \quad w \quad \frac{\frac{\Gamma \Rightarrow A \wedge B}{\Gamma \oplus A \oplus B \Rightarrow A \wedge B} \quad w' \quad \Gamma \oplus A \wedge B \oplus A \oplus B \Rightarrow C}{\Gamma \oplus A \oplus B \Rightarrow C} \quad IH'}{\frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow C} \quad \frac{\Gamma \oplus B \Rightarrow C}{\Gamma \oplus B \Rightarrow C} \quad IH} \quad IH$$

where IH is an instance of the induction hypothesis based on *logical depth* of the formula, and IH' is an instance of the induction hypothesis based on the *height* of the derivations.

The increased number of cases, along with the increased complexity of some of the proof transformations, means that the proof script is longer, at 1177 lines. However, we do not need to prove Contraction admissibility; it is immediate for sets because $\Gamma \oplus A \oplus A = \Gamma \oplus A$.

4 Conclusions

We initially thought that sets would provide a simpler (i.e. shorter) proof of Cut admissibility. However, the drawbacks of using sets instead of multisets for contexts are two-fold. The first is that the duplication of the principal formula of a left rule into the premisses means we have to consider, in the cases where the Cut formula is principal in the left premiss, which rule was used to derive the right premiss. Secondly, this duplication means we *always* have to eliminate a Cut based on the height of the derivations, making the proof transformations more complicated. Sets can also “hide” details, such as contractions, which we would otherwise want to be explicit (these issues do not arise here, but elsewhere).

Multisets are thus more appealing. They are more prevalent in proof theory, and we have shown that they are just as easy to use as sets in a formalisation, albeit quite a straightforward formalisation. There is, of course, a third option for contexts, and that is as lists of formulae (the original choice made by Gentzen, see notes in [4], was *sequences* of formulae, hence the name *sequent calculus*. Sequences are essentially the same thing as lists, in this context). However, it is easy to create multisets from lists, so we can simply cast the lists as multisets, and proceed from there. If we attacked the problem directly, we would be required to prove a lot of extra lemmata about the exchange of formulae in a list, which would be inefficient.

Pfenning does not use multisets in [3], saying that they are “tedious”. He also uses contraction. We have thus moved away from this approach, instead embracing multisets as the most logical choice for our contexts.

References

- [1] P. Chapman. A formalised proof of cut admissibility. University of St Andrews Computer Science Research Report, available at www.dcs.st-andrews.ac.uk/~pc, 2008.
- [2] P. Chapman and J. McKinna. Mechanising a proof of Craig’s interpolation theorem for intuitionistic logic in Nominal Isabelle. University of St Andrews Computer Science Research Report, available at www.dcs.st-andrews.ac.uk/~pc, 2008.
- [3] F. Pfenning. Structural cut elimination i. intuitionistic and classical logic. *Information and Computation*, 2000.
- [4] A. S. Troelstra and H. Schwichtenberg. *Basic Proof Theory*. Number 43 in Cambridge Tracts in Computer Science. Cambridge University Press, second edition, 2000.