Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 332 (2017) 57–73

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Formalized Meta-Theory of Sequent Calculi for Substructural Logics

Kaustuv Chaudhuri[a,1] Leonardo Lima[b,2] Giselle Reis[a,3]

[a] *Inria & LIX/École polytechnique, France*

[b] *Federal University of Paraíba, Brazil*

Abstract

When studying sequent calculi, proof theorists often have to prove properties about the systems, whether it is to show that they are "well-behaved", amenable to automated proof search, complete with respect to another system, consistent, among other reasons. These proofs usually involve many very similar cases, which leads to authors rarely writing them in full detail, only pointing to one or two more complicated cases. Moreover, the amount of details makes them more error-prone for humans. Computers, on the other hand, are very good at handling details and repetitiveness.
In this work we have formalized textbook proofs of the meta-theory of sequent calculi for linear logic in Abella. Using the infrastructure developed, the proofs can be easily adapted to other substructural logics. We implemented rules as clauses in an intuitive and straightforward way, similar to logic programming, using operations on multisets for the explicit contexts. Although the proofs are quite big, their writing took no more than a few weeks once the correct definitions were found. This is an evidence that machine-checked proofs of properties of sequent calculi can be obtained using a natural encoding on most proof assistants available nowadays.

Keywords: Sequent calculus, cut-elimination, formalized proof, linear logic, Abella

1 Introduction

Sequent calculus proof systems are perhaps the most standard technique used to formulate logics. New logics are nearly always proposed in terms of a sequent calculus. Such proposals are usually also accompanied by certain meta-theorems about the calculi. *Cut-elimination* is usually one of the first things to be established, as it usually entails the system's consistency and makes it suitable for automated proof search. Other meta-theorems include identity reduction, which shows internal completeness of the proof system; rule permutations and inversion lemmas to establish the polarities of connectives; and focusing theorems that establish the existence of

[1] kaustuv.chaudhuri@inria.fr

[2] leonardo.alfs@gmail.com

[3] giselle.reis@inria.fr

http://dx.doi.org/10.1016/j.entcs.2017.04.005

normal forms. Although this meta-theory is very important, the proofs are rarely spelled out in detail, let alone formally checked by a proof assistant. One big reason is that these proofs involve a number of cases which is sometimes exponential in the number of rules in the system, with many of them being very similar. A common approach in publications is to show one or two characteristic cases in detail and then to mention that the rest is "analogous" or "trivial".

Such informal proofs are risky. Girard himself underestimated the difficulty of cut-elimination in linear logic with exponentials. The terminating proof needed a much more involved inductive measure and was detailed later on in [4]. A proof of cut-elimination for full intuitionistic linear logic (FILL) was shown to have a mistake in [2], and the authors of the proof have later published a full corrected version [3]. A proof of cut-elimination for the sequent calculus GLS_V for the provability logic GL was the source of much controversy until this was resolved in [9] and formalized in [5] using Isabelle/HOL. Several sequent calculi proposed for bi-intuitionistic logic were "proved" to enjoy cut-elimination when, in fact, they did not. The mistake is analysed and fixed in [15]. More recently an error in the cut-elimination proof for modal logic nested systems was corrected in [13].

The repetitive and detail-intensive nature of these proofs makes them good candidates for computerization. However, it is rare to find such proofs formalized along the lines of their informal arguments. Indeed, formalization of these proofs requires the formalization of details that are generally left implicit in informal proofs. These include lemmas on sets and multisets which we take as standard (and invisible) background. The development of this infrastructure and explicit reasoning on context operations is what we believe makes proof theorists reluctant to formalize meta-theoretic proofs.

We have thus decided to put this "folk wisdom" to the test and formalize the meta-theory for several sequent calculi for various fragments of linear logic. As far as we know, this is the first formalization of its kind. We follow the usual textbook inductive proofs on the rank of the cut formula and/or proof heights, rewriting cuts to smaller cuts. We have proved cut-admissibility, invertibility of inference rules and generalized identity for several systems. Our results show that, with a good encoding of multisets and their properties, the formalization of particular meta-theorems can be completed quickly. Moreover, our formalizations use only elementary theorem proving techniques that can be explained to and carried out by undergraduate students. All that is required is a basic knowledge of proof theory and logic programming.

We have used the proof assistant Abella for this task. Our choice is motivated simply by our familiarity with the tool. As of now, the encoding does not use any exclusive feature of Abella and can be reproduced in any other proof assistant supporting induction (we have also an implementation of the multiset library and some of the meta-theorems with proofs in Coq).

The implementation can be found online at:

https://github.com/meta-logic/abella-reasoning.

The paper is organized as follows. We give a brief introduction of Abella in Section 2 and continue with the encoding in Section 3. We explain how multisets were implemented and show how they are used to specify sequent calculus rules. The cut-elimination proof contains many cases, one of which we explain in some detail. By following Section 3 closely, one should be able to generalize the approach to other sequent calculi. Other formalizations of sequent calculi and their meta-theory are discussed in Section 4.

2 Background: Relational Reasoning in Abella

We use the interactive proof assistant Abella [1] to formalize our different meta-theoretic proofs. The logic behind Abella is a conservative extension of intuitionistic first-order logic; the extensions that are relevant for this paper are:

- The pure simply typed λ-calculus as the term language, together with a primitive equality predicate on such terms that implements $\alpha\beta\eta$-equivalence with all uninterpreted constants treated as *constructors*. The logic is built atop this simply typed term language following the design of Church's simple theory of types. There is a type `prop` dedicated to formulas of the logic, and all logical connectives are implemented as constants of target type `prop`; for example, conjunction $\wedge$ has type $\texttt{prop} \to \texttt{prop} \to \texttt{prop}$, although we write it inline as $A \wedge B$ instead of as $\wedge\ A\ B$.
- Least and greatest fixed point definitions for predicates, *i.e.*, constants of target type `prop`. Such definitions come equipped with corresponding induction and co-induction rules for reasoning about assumptions and conclusions, respectively, and may additionally be *unfolded* to replace any instance of the predicate by its corresponding body.
- Support for extensional universal ($\forall$) quantification. Extensional variables, called *eigenvariables*, are allowed to be *instantiated* by arbitrary terms when reasoning about equations or during case-analysis. This can be highlighted by the formula $\forall x.\,(x = c) \supset p(x) \supset p(c)$ (for some constant c), which is provable because analyzing [4] $x = c$ has the effect of instantiating x with c, reducing the proof obligation to $p(c) \supset p(c)$. However, $\forall x.\, x \neq c$ is not provable [5] – for instance, it would be false in a model where c is the only element. Abella also has existential quantification ($\exists$) and an intensional quantification (∇) that mediates between the two; the latter of these is not relevant for this particular paper.

A comprehensive introduction to Abella, including a discussion of its features that are not used in this paper, may be found in the tutorial [1]. The proof theory of $\mathcal{G}$, the logic underlying Abella, is described in [7,8] and references therefrom.

Unlike many other proof assistants in popular use—such as Coq, Agda, Isabelle, etc.—Abella follows a *relational* approach rather than a *functional* approach to specifications. The equational theory on terms in Abella cannot be extended by

[4] More precisely, using the left-introduction rule for equality in the sequent calculus $\mathcal{G}$ [7,8].
[5] We define $s \neq t$ to be the formula $(s = t) \supset \bot$.

functional definitions, and hence the term language is just ordinary λ-terms built from variables, constants, λ-abstraction, and application. If we declare a type `nat` of natural numbers with two constants `z` : `nat` and `s` : `nat` $\rightarrow$ `nat`, then the definition of addition `plus` would be given in terms of a relation of type `nat` $\rightarrow$ `nat` $\rightarrow$ `nat` $\rightarrow$ `prop` that relates the first two arguments to their sum in the third argument. Concretely, this definition would be specified as follows:

```
Define plus : nat -> nat -> nat -> prop by
; plus z X X
; plus (s X) Y (s Z) := plus X Y Z.
```

This definition consists of two *definitional clauses* which are separated from each other by semi-colons, and each clause consists of a *head* and, optionally, a *body* separated by `:=`. Each clause is also implicitly universally ($\forall$) closed over its capitalized identifiers. The first clause above declares that for any `X`, the atom `plus z X X` is `true` (an omitted body in a clause is taken to stand for `true`). The second clause says that for every `X`, `Y`, and `Z`, the atom `plus (s X) Y (s Z)` is true if and only if `plus X Y Z` is true. This predicate is, moreover, given a least fixed point interpretation, which means that there are no other ways of deriving `plus s t u` (for any terms `s`, `t`, and `u`) besides using one of the two definitional clauses. Note that definitional clauses for a predicate do not need to have non-overlapping heads, nor is the body of a clause required to use only subterms of the terms at the head. Thus, iteratively unfolding a relation can be both non-deterministic and non-terminating.

To prove a theorem about such least fixed point definitions, we use the built in `induction` tactic that behaves identically for every definition. As an illustration, consider the following theorem:

```
Theorem plus_z_2 : forall X, plus X z X.
```

To prove this theorem, we need to proceed by induction on the structure of `X` (which is of type `nat`). However, as the only induction principles in Abella apply to least fixed point definitions, we need to reify the structure of `nat`s as such a definition:

```
Define is_nat : nat -> prop by
; is_nat z
; is_nat (s X) := is_nat X.
```

We can then state the theorem as follows:[6]

```
Theorem plus_z_2 : forall X, is_nat X -> plus X z X.
```

Note that the type signature of constants is not itself endowed with any induction principles because the signature is open-ended; it may always be extended with new constants of type `nat`, for instance. However, no such extension can falsify the theorem since the `is_nat` predicate is not extensible.

The proof begins by the tactic invocation `induction on 1`, which indicates induction on the first assumption `is_nat X`, called the *inductive argument*. Since there are two definitional clauses for `is_nat`, there will be two cases to consider. In the first case, we would obtain the equation `X = z` in order to match `is_nat X` against the clause *head* `is_nat z`; this in turn instantiates the (eigen)variable `X` to

[6] Concrete syntax for $\supset$, $\top$, $\bot$, $\wedge$, $\vee$, $\forall$, $\exists$, and ∇: `->`, `true`, `false`, `/\`, `\/`, `forall`, `exists`, and `nabla`.

`z`, leaving us with the obligation `plus z z z`, which is easily proved by the first clause of `plus`. In the second case, we would obtain `X = s X1` where `X1` is a new variable for which we know `is_nat X1`. The goal now is `plus (s X1) z (s X1)`, which we can unfold using the second clause of `plus` to reduce it to `plus X1 z X1`. Thus, we are left with the obligation of proving `plus X1 z X1` from the assumption `is_nat X1`.

To close this loop inductively, Abella reasons by induction on the *size* of the inductive argument, which in this case is `is_nat X`.[7] The initial invocation of the `induction` tactic had produced an *inductive hypothesis* `IH`:

```
IH : forall X, is_nat X * -> plus X z X
```

Here, `is_nat X *` stands for an instance of `is_nat` that is strictly smaller than the initial `is_nat X` in the goal. The goal is, in fact, rewritten to:

```
forall X, is_nat X @ -> plus X z X
```

where the annotation `@` indicates that its size is such that every `*`-annotated instance is strictly smaller. Unfolding the assumption `is_nat X @` reduces its size strictly, so that in the case of its second definitional clause we get a new assumption `is_nat X1 *` (where `X = s X1`). This can now be fed to the `IH` to obtain `plus X1 z X1`, which is what we needed to finish the proof.

Size annotations represent (strong) induction on linearly ordered sizes, but meta-theoretic proofs abound with inductions on more complex orderings, particularly lexicographic orderings. While the logic $\mathcal{G}$ underlying Abella has a general induction rule that can represent any (computable) well-ordering, the implementation of it using size annotations and circular inductive hypotheses in Abella need to be generalized further for lexicographic induction. This is achieved by means of *size levels* that are created by nested invocations of the `induction` tactic.

Nested inductions are best explained by an example: consider this relational definition of the Ackermann function, where `ack X Y K` stands for $\mathtt{K} = A(\mathtt{X}, \mathtt{Y})$.

```
Define ack : nat -> nat -> nat -> prop by
; ack z X (s X)
; ack (s X) z K := ack X (s z) K
; ack (s X) (s Y) K := exists K1, ack (s X) Y K1 /\ ack X K1 K.
```

We may wish to show that this is a total relation, something that famously cannot be done with induction on natural numbers alone:

```
Theorem ack_total : forall X Y, is_nat X -> is_nat Y ->
  exists K, is_nat K /\ ack X Y K.
```

In this case, we want to induct using the lexicographic ordering of the sizes of `is_nat X` and `is_nat Y`, *i.e.*, the inductive hypothesis may be used if the size of `is_nat X` is strictly smaller, or it stays the same and that of `is_nat Y` is strictly smaller. In Abella we write this using the following invocation:

[7] Every instance of a least fixed point definition is, intuitively, equivalent to $\bot$ unless it can be shown to be true after unfolding it a finite number of times. Thus, *non-terminating* definitions with clauses such as `p X := p (s X)` would be interpreted as $\bot$. The size of such defined atoms is defined in such a way that it is larger than the number of times it needs to be unfolded to determine that it is true. The precise theory of these size annotations is out of scope for this paper but can be found in [6].

```
induction on 1. induction on 2.
```

This produces *two* inductive hypotheses and modifies the goal as follows:

```
IH1 : forall X Y, is_nat X * -> is_nat Y -> ...
IH2 : forall X Y, is_nat X @ -> is_nat Y ** -> ...
============================
 forall X Y, is_nat X @ -> is_nat Y @@ -> ...
```

where `...` in each case is `exists K, is_nat K /\ ack X Y K`. The hypothesis `IH1` is familiar from before: it just means that `is_nat X *` is strictly smaller than `is_nat X @`. The hypothesis `IH2`, on the other hand, has `is_nat Y **` which is strictly smaller than `is_nat Y @@`. This hypothesis also has an assumption `is_nat X @` which can only be supplied by the corresponding assumption—unmodified!—from the rewritten goal. Note that the `@` and `@@` annotations have no relation to each other except to denote that the latter was introduced while an induction on the former was in progress. Thus, `is_nat X @` would unfold to produce `*` annotations and `is_nat Y @@` would unfold to produce `**` annotations.

In the rest of this development, we will follow a certain style of specifications where typing predicates such as `is_nat` are not explicitly assumed in proofs but are rather produced by inversion on other predicates. Once again, an example illustrates it best: consider the `plus` relation again, but rewritten so that the following theorem holds of it:

```
Theorem plus_is : forall X Y Z, plus X Y Z ->
  is_nat X /\ is_nat Y /\ is_nat Z.
```

Writing it this way means that we never need to assume both `is_nat X` and `plus X Y Z`, for instance, since the former is derivable from the latter. Here is how we modify the definition of `plus` to guarantee `plus_is`:

```
Define plus : nat -> nat -> nat -> prop by
; plus z X X := is_nat X
; plus (s X) Y (s Z) := plus X Y Z.
```

The proof of `plus_is` is by straightforward induction on `plus X Y Z`. Note that we could have sprinkled more `is_nat` conjuncts in the bodies of the definitional clauses, but the above choice is sufficient. We will opt to alter the natural definitional clauses as minimally as possible to yield the necessary inversion lemmas.

3 Encoding an Object Language

In what follows we distinguish between *object logic*, the logic and proof systems for which we are formally establishing meta-theorems, and *meta logic*, which is the reasoning logic $\mathcal{G}$ that forms the basis of Abella.

3.1 Encoding Object Formulas

In this paper we will focus on propositional linear logics, both to simplify the presentation and to avoid a diversion into representations of object type systems. Formulas of linear logic are encoded as constants of target type `o`, which is a type reserved in Abella for a particular *specification language* based on higher-order

```
Type atom, natom    atm -> o.
Type tens, par      o -> o -> o.
Type one, bot       o.
Type wth, plus      o -> o -> o.
Type top, zero      o.

Define is_fm : o -> prop by
; is_fm (atom A)
; is_fm (natom A)
; is_fm (tens A B) := is_fm A /\ is_fm B
; is_fm one
; is_fm (par A B) := is_fm A /\ is_fm B
; is_fm bot
; is_fm (wth A B) := is_fm A /\ is_fm B
; is_fm top
; is_fm (plus A B) := is_fm A /\ is_fm B
; is_fm zero.
```

Fig. 1. Definitions of formulas

hereditary Harrop formulas. However, we will not be using the specification logic of Abella in this paper, so we reuse the `o` type to get access to the convenient syntax of lists that is built in for lists of os, using the type `olist`.[8]

The definition of linear logic formulas for a one-sided formulation of MALL is given in Figure 1. We define a new basic type `atm` of predicates; since type signatures are open-ended in Abella, our development will be parametric over the inhabitants of this type. From this type, atoms and negated atoms are built using `atom` and `natom` respectively. We keep formulas in negation-normal form in the one-sided formulation, so the only formally negated formulas are atoms. Together with these atoms, we define the predicate `is_fm` for inducting on the structure of formulas.

3.2 Multisets

The crucial ingredient in the representation of a one-sided sequent calculus for MALL is the definition of MALL contexts, which must satisfy the following desiderata.

(i) Given two contexts Γ and Δ, we must be able to tell when they are structurally identical, meaning that they contain the same elements with the same multiplicities.

(ii) Given contexts Γ and Δ and a formula A, we must be able to recognize when adding A to Γ results in a context that is structurally identical to Δ. This operation is required in order to implement inference rules as it is used to represent adding the principal formula in the conclusion of the rule, and the operands of the principal connective (if relevant) to the premises.

(iii) Generalizing this further, given three contexts Γ, Δ, and Θ, we must be able to say when adding all the elements of Δ to Γ results in a context that is structurally identical to Θ, *i.e.*, Θ is the *join* or the *multiset union* of Γ and Δ. This operation is not only required for implementing multiplicative rules such as $\otimes$, but also for defining the cut rule(s).

There is a wider than expected design space here. A first attempt might be

[8] Abella has a monomorphic type system. A polymorphic extension is in progress and when that is available there will only be a single parametrically polymorphic type of lists.

```
Type is_o  o -> prop.

Define is_list : olist -> prop by
; is_list nil
; is_list (A :: L) := is_o A /\ is_list L.

% adj J A K : K is J with A inserted somewhere
Define adj : olist -> o -> olist -> prop by
; adj L A (A :: L) := is_o A /\ is_list L
; adj (B :: K) A (B :: L) := is_o B /\ adj K A L.

% merge J K L : J union K equals L.
Define merge : olist -> olist -> olist -> prop by
; merge nil nil nil
; merge J K L := exists A JJ LL, adj JJ A J /\ adj LL A L /\ merge JJ K LL
; merge J K L := exists A KK LL, adj KK A K /\ adj LL A L /\ merge J KK LL.

% perm J K : J and K have the same elements
Define perm : olist -> olist -> prop by
; perm nil nil
; perm K L := exists A KK LL, adj KK A K /\ adj LL A L /\ perm KK LL.
```

Fig. 2. Implementation of multisets.

to simply use `olist` as our representation of contexts, with addition of elements represented by list consing (`::`) and context joining with list append. This makes inductive reasoning on contexts rather straightforward, but, because linear contexts are structurally identical modulo exchange, it requires adding explicit exchange rules to the system, which complicates the meta-theory. An alternative that works is still to use `olist` as our representation, but to relax the notion of structural identity as follows: two lists are structurally identical if one is a permutation of the other. Thus, we need a predicate `perm : olist -> olist -> prop` to recognize list permutations.

To define the addition operation with this modified notion, we can continue to use list cons, but this will still require an explicit exchange rule. Instead, we define a generalized cons operation, called `adj`, that adds an element somewhere in an `olist`, not necessarily at the head. Note that this definition is still sensitive to the order of elements; for example, `adj [b, c] a [a, b, c]` holds, whereas `adj [b, c] a [a, c, b]` does not. Given this definition, it is a simple matter to define `perm` by induction: two lists are permutatively equal if they are produced by `adj`-ing the same elements. Finally, to define the join of `olist`s up to permutations, we simply iterate this process: an `olist` is the join, written `merge`, of two `olist`s if it is produced by `adj`-ing their elements.

The encoding of multisets we have just described is given in Figure 2. It takes `adj` as primitive, and builds `perm` and `merge` on top. We may conceivably have taken `perm` as primitive and defined the other operations in its terms, or some other combination, but we found our choice to be rather intuitive. Moreover, Abella's built in `search` tactic, which searches for simple proofs of bounded depth, is often able to automatically derive `perm` and `merge` instances.

The files `lib/merge.thm` and `lib/perm.thm` contain theorems about multisets that are used extensively on the transformations of sequent calculus proofs. These include simple properties, such as `merge`'s stability modulo permutation:

```
Theorem perm_merge_1 : forall J K L JJ,
```

$$\frac{}{\vdash a^{\perp}, a}\ \mathsf{init} \qquad \frac{\vdash \Gamma_1, A \qquad \vdash \Gamma_2, B}{\vdash \Gamma_1, \Gamma_2, A \otimes B}\ \otimes \qquad \frac{}{\vdash 1}\ 1 \qquad \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}\ \parr \qquad \frac{\vdash \Gamma}{\vdash \Gamma, \perp}\ \perp$$

$$\frac{\vdash \Gamma, A \qquad \vdash \Gamma, B}{\vdash \Gamma, A \,\&\, B}\ \& \qquad \frac{}{\vdash \Gamma, \top}\ \top \qquad \frac{\vdash \Gamma, A}{\vdash \Gamma, A \oplus B}\ \oplus_1 \qquad \frac{\vdash \Gamma, B}{\vdash \Gamma, A \oplus B}\ \oplus_2$$

Fig. 3. One-sided sequent calculus for MALL

```
Define mall : olist -> prop by
; mall L := exists A, adj (natom A :: nil) (atom A) L
; mall L := exists A B LL JJ KK J K,
    adj LL (tens A B) L /\ merge JJ KK LL /\
    adj JJ A J /\ mall J /\ adj KK B K /\ mall K
; mall (one :: nil)
; mall L := exists A B LL J K,
    adj LL (par A B) L /\ adj LL A J /\ adj J B K /\ mall K
; mall L := exists LL, adj LL bot L /\ mall LL
; mall L := exists A B LL J K,
    adj LL (wth A B) L /\ adj LL A J /\ mall J /\ adj LL B K /\ mall K
; mall L := exists LL, adj LL top L
; mall L := exists A B LL J, adj LL (plus A B) L /\ adj LL A J /\ mall J
; mall L := exists A B LL J, adj LL (plus A B) L /\ adj LL B J /\ mall J.
```

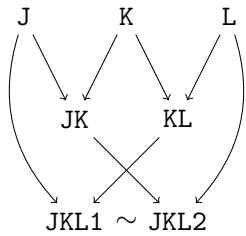
Fig. 4. Encoding of one-sided MALL

```
  merge J K L -> perm J JJ -> merge JJ K L.
```

We also require more complicated lemmas, such as the associativity of `merge`.

```
Theorem merge_assoc : forall J K L JK KL JKL1 JKL2,
  merge J K JK -> merge K L KL ->
  merge J KL JKL1 -> merge JK L JKL2 ->
  perm JKL1 JKL2.
```

This can be depicted more evocatively as follows, where the arrows define the first two arguments to `merge` and $\sim$ denotes `perm`.



Proving this theorem requires establishing that `perm` is an equivalence—specifically that it is transitive—which has a surprisingly unintuitive inductive proof. Such properties are usually taken for granted in informal proofs of cut-elimination. Nevertheless, our experience has been that every property of multisets needed to formalize cut-elimination is proved by straightforward induction.

3.3 One-Sided MALL

We have used the above encoding of multi-sets to define several one and two-sided sequent calculi for fragments of classical linear logic. Here we give an illustration of the one-sided multiplicative-additive fragment (MALL). Sequents in this fragment

```
Define dual : o -> o -> prop by
; dual (atom A) (natom A)
; dual (tens A B) (par AA BB) := dual A AA /\ dual B BB
; dual one bot
; dual (plus A B) (wth AA BB) := dual A AA /\ dual B BB
; dual zero top.
```

Fig. 5. An asymmetric duality predicate.

are of the form $\vdash \Gamma$, whose inference rules (sans cut) can be found in Fig. 3. The sequent judgement $\vdash \Gamma$ is encoded as the inductively defined atom `mall L`, where `L` represents Γ. The definition of `mall` is given in Fig. 4. Each definitional clause describes, precisely, one of the rules of the sequent calculus, where the head of the clause defines the conclusion of the inference rule, and the bodies the premises. The second definitional clause, for instance, first uses `adj` to remove the principal formula `tens A B` from `L`, yielding `LL`; this is then divided into `JJ` and `KK` using `merge`, after which each operand of the $\otimes$ is added to one of the components to build a corresponding `mall` premise.

Note that we do not have an explicit clause for exchange. Nevertheless, we can establish the following theorem by a straightforward induction.

```
Theorem mall_perm : forall K L, mall K -> perm K L -> mall L.
```

Note that the theorem itself says nothing about the sizes of `mall K` and `mall L`, even though it is the case that exchange is height-preserving admissible in the sequent system. The one-sided cut-admissibility theorem will therefore need to be set up in such a way that the size of the result of applying a permutation is not relevant for the inductive hypotheses.

In fact, we will set up the one-sided formulation in such a way that only the height of the derivation containing the positive variant—in the sense of focusing—of the cut formula is relevant. To this end, we define an asymmetric predicate `dual` that relates a positive formula with its dual, depicted in Fig. 5. For the negative formulas, which are the second arguments to `dual`, we will instead prove inversion lemmas by straightforward induction.

```
Theorem bot_inv : forall J L, mall L -> adj J bot L -> mall J.
Theorem par_inv : forall L JJ A B,
  mall L -> adj JJ (par A B) L ->
  exists KK LL, adj JJ A KK /\ adj KK B LL /\ mall LL.
Theorem wth_inv : forall L JJ A B,
  mall L -> adj JJ (wth A B) L ->
  exists KK LL, adj JJ A KK /\ mall KK /\ adj JJ B LL /\ mall LL.
```

The cut-admissibility theorem then uses our asymmetric `dual` predicate as follows:

```
Theorem cut : forall A B JJ J KK K LL,
  dual A B ->
  adj JJ A J -> mall J ->
  adj KK B K -> mall K ->
  merge JJ KK LL ->
  mall LL.
```

The proof proceeds by a nested induction on the first and third assumptions. This nesting encodes the following measure for appealing to the inductive hypotheses: either the rank decreases because of case analysis of `dual A B`, or the rank stays the same and the height of `mall J`, which stands for the derivation that contains

the positive half of the cut formula pair, decreases.

To illustrate the proof, here is the case where the final rule to be applied in the derivation of `mall J` is $\otimes$. Intuitively, we wish to implement the following reduction:

$$\dfrac{\dfrac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2\\ \vdash \Gamma_1, A & \vdash \Gamma_2, B\end{array}}{\vdash \Gamma_1, \Gamma_2, A \otimes B}\otimes \qquad \begin{array}{c}\mathcal{E}\\ \vdash \Gamma_3, A^\perp \parr B^\perp\end{array}}{\vdash \Gamma_1, \Gamma_2, \Gamma_3}\ \mathsf{cut} \quad \rightsquigarrow \quad \dfrac{\begin{array}{cc}\mathcal{D}_1 & \dfrac{\begin{array}{cc}\mathcal{D}_2 & \dfrac{\begin{array}{c}\mathcal{E}\\ \vdash \Gamma_3, A^\perp \parr B^\perp\end{array}}{\vdash \Gamma_3, A^\perp, B^\perp}\parr^{-1}\\ \vdash \Gamma_2, B\end{array}}{\vdash \Gamma_2, \Gamma_3, A^\perp}\ \mathsf{cut}\\ \vdash \Gamma_1, A\end{array}}{\vdash \Gamma_1, \Gamma_2, \Gamma_3}\ \mathsf{cut}$$

The cut is reduced to two cuts of lower rank, even though the right premise of the cuts can have larger sizes. Note the appeal to the inversion principle for $\parr$.

In the proof, this corresponds to the following proof state:

```
IH : forall A B JJ J KK K LL, dual A B * -> adj JJ A J -> mall J ->
       adj KK B K -> mall K -> merge JJ KK LL -> mall LL
H2 : adj JJ (tens A1 B1) J
H4 : adj KK (par AA BB) K
H5 : mall K
H6 : merge JJ KK LL
H7 : adj LL1 (tens A1 B1) J
H8 : merge JJ1 KK1 LL1
H9 : adj JJ1 A1 J1
H10 : mall J1 **
H11 : adj KK1 B1 K1
H12 : mall K1 **
H14 : perm JJ LL1
H15 : dual A1 AA *
H16 : dual B1 BB *
============================
 mall LL
```

Applying `par_inv` to `H4` and `H5` yields the new hypotheses:

```
H17 : adj KK AA KK2
H18 : adj KK2 BB LL2
H19 : mall LL2
```

The next step is to create the context $\Gamma_2, \Gamma_3, A^\perp$ which is the conclusion of the first cut on B. In the current proof state, this corresponds to merging `KK1` (Γ_2) and `KK2` ($\Gamma_3, A^\perp$). After merging the contexts, we can apply the inductive hypothesis `IH`, corresponding to the cut on B, which gives us the following new hypotheses:

```
H22 : merge KK1 KK2 L
H23 : mall L
```

Now we need to apply the cut on A, but to build the context of this cut we need to perform a few operations. First, we need to discern `AA` ($A^\perp$) from the context `L` ($\Gamma_2, \Gamma_3, A^\perp$). This is done via the `merge_unadj_2` theorem, which is part of the library of multisets.

```
Theorem merge_unadj_2 : forall J K L KK A,
  merge J K L -> adj KK A K -> exists LL, adj LL A L /\ merge J KK LL.
```

After applying this lemma, we will have a variable `LL3` (Γ_2, Γ_3) which we can thus merge with `JJ1` (Γ_1) to get the conclusion of the cut on A. The `IH` can now be applied to obtain the following new hypotheses.

```
H24 : adj LL3 AA L
H25 : merge KK1 KK LL3
H28 : merge JJ1 LL3 L1
H29 : mall L1
```

The case is nearly complete: we just need to show that `L1` is a permutation of `LL`, and then appeal to `mall_perm` on `H29`. Observe that they represent the same context $\Gamma_1, \Gamma_2, \Gamma_3$ but were constructed differently: `LL` is $(\Gamma_1, \Gamma_2), \Gamma_3$ while `L1` is $\Gamma_1, (\Gamma_2, \Gamma_3)$. We can first apply `merge_perm_1` to `H6` and `H14` to obtain:

```
H30 : merge LL1 KK LL
```

Finally, we can apply `merge_assoc` to `H8`, `H25`, `H26`, and `H30` to obtain the required:

```
H31 : perm L1 LL
```

3.4 The Exponential Case

While the MALL cut-elimination proof is long in details, it is not particularly difficult since there is always a single cut to eliminate. The picture gets considerably more complicated with the exponentials, since a single cut rule is no longer sufficient, or, to be more precise, the termination measure for eliminating cuts is much more complex. The main problem is with permuting cuts past contraction rules:

$$\dfrac{\dfrac{\dfrac{\mathcal{D}}{\vdash ?\Gamma_1, A}}{\vdash ?\Gamma_1, !A}\,! \qquad \dfrac{\dfrac{\mathcal{E}}{\vdash \Gamma_2, ?A^\perp, ?A^\perp}}{\vdash \Gamma_2, ?A^\perp}\,\mathsf{contr}}{\vdash ?\Gamma_1, \Gamma_2}\,\mathsf{cut} \quad \rightsquigarrow \quad \dfrac{\dfrac{\dfrac{\mathcal{D}}{\vdash ?\Gamma_1, A}}{\vdash ?\Gamma_1, !A}\,! \qquad \dfrac{\dfrac{\dfrac{\mathcal{D}}{\vdash ?\Gamma_1, A}}{\vdash ?\Gamma_1, !A}\,! \qquad \dfrac{\mathcal{E}}{\vdash \Gamma_2, ?A^\perp, ?A^\perp}}{\vdash ?\Gamma_1, \Gamma_2, ?A^\perp}\,\mathsf{cut}}{\vdash ?\Gamma_1, ?\Gamma_1, \Gamma_2}\,\mathsf{cut}^\dagger}{\vdash ?\Gamma_1, \Gamma_2}\,\mathsf{contr}^*$$

The instance of $\mathsf{cut}^\dagger$ is problematic, since neither premise is technically of strictly lower measure: the height and cut-rank is the same in the left-premise, and the right premise is the result of a cut that can be arbitrarily larger.

This problem can be solved in a number of ways, such as by including the number of contractions on the cut-formulas as part of the measure. However, to correctly formulate such a measure, we would need to incorporate multiset orderings, which is not currently supported by Abella's size annotations. We therefore use a different—but still standard—solution of moving to a dyadic sequent calculus with sequents of the form $\vdash \Gamma; \Delta$ where Γ is interpreted as a set— *i.e.*, admitting contraction and weakening—that accumulates the ?-formulas. This context is treated additively in binary rules and is allowed to be non-empty in axiomatic rules.

Importantly, with this separation of the context into *zones*, we have to increase the number of cut principles to account for occurrences of cut-formulas in both zones. Specifically, the dyadic formulation requires two cuts:

$$\dfrac{\vdash \Gamma; \Delta_1, A \qquad \vdash \Gamma; \Delta_2, A^\perp}{\vdash \Gamma; \Delta_1, \Delta_2}\,\mathsf{cut} \qquad \dfrac{\vdash \Gamma; A \qquad \vdash \Gamma, A^\perp; \Delta}{\vdash \Gamma; \Delta}\,\mathsf{ucut}$$

The conditions for appealing to the inductive hypothesis is now more complicated. An IH can be used if the cut-rank is smaller, or if the derivation with A is of lower height, but in the case where both stay the same we can reduce a cut to a ucut. The

issue with contractions above reappears as an issue with *dereliction* as follows:

$$\dfrac{\vdash \Gamma; A \quad \dfrac{\mathcal{E}}{\vdash \Gamma, A^{\perp}; \Delta, A^{\perp}}\,\mathsf{dl}}{\vdash \Gamma; \Delta}\,\mathsf{cut} \quad \rightsquigarrow \quad \dfrac{\vdash \Gamma; A \quad \dfrac{\mathcal{D} \qquad \mathcal{E}}{\vdash \Gamma, A^{\perp}; \Delta, A^{\perp}}\,\mathsf{ucut}}{\vdash \Gamma; \Delta}\,\mathsf{cut}$$

However, since a ucut is allowed to justify a cut, there is no termination issue.

Formalizing this proof requires a few modifications to the representation of MELL (multiplicative exponential linear logic) sequents, which are now given as a ternary predicate `mell : nat -> olist -> olist -> prop`. The first argument to `mell` is an explicit bound on the heights of derivations, which allows us to reason explicitly about the height instead of in terms of the implicit sizes of least fixed point definitions. This height is explicitly reduced by one in every recursive occurrence of the predicate in the bodies of its definitional clauses; for example, here is the clause corresponding to $\otimes$:

```
; mell (s X) QL L :=
    exists A B LL, adj LL (tens A B) L /\
    exists JJ KK, merge JJ KK LL /\
      (exists J, adj JJ A J /\ mell X QL J) /\
      (exists K, adj KK B K /\ mell X QL K)
```

To encode the ordering between the two cuts, we need to induct on an additional *weight* parameter to the cut theorem that determines the kind of cut. We encode it in Abella as follows:

```
Kind weight type.

Type heavy, light weight.

Define is_weight : weight -> prop by
; is_weight light
; is_weight heavy := is_weight light.
```

Note that `is_weight heavy` and `is_weight light` are both true, but the former requires strictly more unfolding operations to derive it. This is sufficient to order the two cuts, which we write as follows:

```
Theorem cut : forall A B X W,
  dual A B -> is_nat X -> is_weight W ->
     (W = light /\
      forall JJ J KK K QL Y LL,
        adj JJ A J -> mell X QL J ->
        adj KK B K -> mell Y QL K ->
        merge JJ KK LL ->
        exists Z, mell Z QL LL)
  \/ (W = heavy /\
      forall QL QQ K Y,
        mell X QL (A :: nil) ->
        adj QL B QQ -> mell Y QQ K ->
        exists Z, mell Z QL K).
```

The first disjunct represents cut, while the second is ucut. The proof then begins:

```
induction on 1. induction on 2. induction on 3.
```

which encode the required lexicographic measure. Observe that once the theorem is proved, each disjunct can be individually obtained by instantiating `W` with `light` and `heavy` respectively.

3.5 Two-Sided Calculi

We have also implemented the meta-theory of the two-sided sequent calculus for MALL. The big differences between the one-sided and two-sided formulations are that each connective has left and right introduction rules, and that the cut rules apply to formulas on either side of the sequent arrow rather than in terms of duality. Hence, we reason directly on `is_fm` instead of in terms of an asymmetric `dual` predicate, which in turn means that we do an additional nested induction instead of appealing to inversion lemmas. Cuts are now permuted upwards in both premise derivations until they become principal. While the proofs are now longer because of the larger number of inference rules, the ingredients remain largely the same. It is worth noting that the cut permutations proved in the two-sided system can be used to show strong normalization of a cut-elimination strategy for MALL, given an ordering of the cuts.

4 Related work

We are certainly not the first to formalize a cut-elimination proof in a proof assistant. We discuss here a few other projects on this direction and compare them with our approach. This list is far from exhaustive.

Closest to our approach (in the sense that sequents and multisets are encoded) we can cite [5] and [18]. In [5] the authors propose a generic method for formalizing sequent calculi in Isabelle/HOL, making all lemmas and theorems parametric on a set of rules. For the main cut-elimination theorem, weakening must be admissible. They have proved cut-elimination for the sequent calculus GLS_V for provability logic, although in practice they proved the admissibility of *multi-cut* instead of cut itself (the rules are shown to be equivalent for their system). The use of multi-cut is justified to avoid the complicated cases where the cut-formula is contracted, which is also our approach to exponentials.

A proof of cut-elimination for coalgebraic logics by Pattinson and Schröder was formalized in Coq in [18]. The formalization uncovered a few mistakes in the original proof which were discussed with Pattinson and Schröder and corrected. The author has implemented multisets as setoids in Coq with lists as the underlying type and permutation as the equivalence relation. Our treatment of multisets is largely similar. The author also chose to define a type for heterogeneous lists for lists of a fixed size as part of the encoding. As in [5], the proof is parametrized by a rule set.

To avoid dealing with explicit representations of contexts as multisets, a common approach is to find a different representation for sequent calculus rules which mention explicitly only the principal and auxiliary formulas. This is the path followed in [14], [17], [10] and [19]. In [14] the author annotates sequents of the calculus considered with proof terms, reducing cut-elimination to a type checking problem on those terms. Since the logical framework is intuitionistic, the structural rules of contraction and weakening are forced to be admissible for all such proof calculi. One of the obvious advantages of this approach is avoiding explicit representations of multisets; on the other hand, the adequacy of the term rewriting system to the

actual sequent calculus rules is only an informal argument that is not independently verified.

The method developed in [14] was used in [17] for formalizing a proof of completeness of focusing for intuitionistic logic. The author avoids having to show "tedious invertibility lemmas" by using a new proof of completeness that follows from cut-elimination and generalized identity. A number of meta-theoretical properties are proved in this formalization. It would be interesting to see if his proof of completeness of focusing could be formalized in Abella using our results. One commonality between our approach and that of [17] is the use of cut weights to set up a lexicographic measure. Another formal proof (in Coq) of completeness of focusing for several systems was developed in [10], using an algebraic interpretation of the logic which requires some assumptions on the sequent calculus, namely *harmony* (i.e., rules should come in "dual" pairs) and the admissibility of weakening and contraction. It is difficult to see how these ideas can be generalized to the substructural case.

Other linear logic encodings in various proof assistants can be found in [11,12,16]. The goal of those works however was to obtain proof search engines for linear logic, so there are no proofs of meta-theoretical properties of the encoded systems. In [11], the author implements linear logic in Isabelle and uses a calculus with exchange rules to avoid having to implement contexts modulo permutation. The same solution is used in [16] for implementing linear logic in Coq, although a later implementation by Cowley [9] uses permutation of contexts. In [12] linear logic is again implemented in Isabelle for proof search, but this time rules are encoded using multisets. On top of regular linear logic rules, the authors also add a set of "macro-rules" to the system for facilitating proof search.

5 Conclusion

We have shown an implementation of a "textbook" proof of cut-elimination, using the rewrite rules *à la* Gentzen, for various fragments of linear logic in the proof assistant Abella. This is the first formalization of cut-elimination for linear logic to the best of our knowledge. We have also implemented proofs of other meta-theoretical properties using the same techniques. It required the implementation and proofs of several lemmas about multisets, which we believe can be re-used for meta-theoretical proofs about other calculi. The encoding of sequent calculus rules is quite intuitive and similar to a logic program.

While formalizing this proof we have learned a few interesting things. First of all, it was good to realize that proof assistants are already usable enough to handle such proofs. We were skeptical about this at some points. In fact, we have started translating the Abella code to Coq. The multiset library is fully specified and we have some proofs for meta-theorems of MLL. Because Coq allows for fine programmatic control of proof search, nearly all the required lemmas about the representation of multisets are handled with single invocations of a simplification tactic tailor-made for reasoning about multi-sets (written using Ltac). On the other hand, Coq's induction

[9] https://github.com/acowley/LinearLogic

is more primitive than Abella's and requires making the induction measure explicit, which in turn complicates meta-theoretic proofs, particularly those that rely on lexicographic induction. Of course this might be caused by using an "Abella way of thinking" when implementing the proofs in Coq. We noticed that a familiarity with the proof assistant plays a big role when finding out the lemmas to prove and the proof strategy to follow. Since each proof assistant is unique, reproving something in another software is not so straightforward.

This being said, and despite the fact that we successfully finished several such proofs, we must admit that the amount of boilerplate in the proofs shows us that this approach is not yet ready for general purpose use. The trade-off between having a formalized proof and the time taken to formalize it is still too big for the average proof theorist. We believe this to be a general problem with proof assistants—not just with Abella—given the related work we have found and our experience in porting the code to Coq. Modularity techniques in proof assistants are already a great help (indeed we have one implementation of multisets which is used by all encodings), but there is still a considerable gap between the kinds of informal meta-theoretic proofs one finds in the average proof theory paper and the formalizations. We are investigating better ways to deal with the tedious and repetitive parts of proofs.

References

[1] Baelde, D., K. Chaudhuri, A. Gacek, D. Miller, G. Nadathur, A. Tiu and Y. Wang, *Abella: A system for reasoning about relational specifications*, Journal of Formalized Reasoning **7** (2014).
URL http://jfr.unibo.it/article/download/4650/4137

[2] Bierman, G., *A note on full intuitionistic linear logic*, Annals of Pure and Applied Logic **79** (1996), pp. 281 – 287.
URL http://www.sciencedirect.com/science/article/pii/0168007296000048

[3] Braüner, T. and V. de Paiva, *Cut-elimination for full intuitionistic linear logic*, Technical Report BRICS-RS-96-10, BRICS, Aarhus, Danemark (1996), also available as Technical Report 395, Computer Laboratory, University of Cambridge.

[4] Danos, V., "Une Application de la Logique Linéaire a l'Etude des Processus de Normalisation (principalement du λ-calcul)," Ph.D. thesis, Université Paris (1990).

[5] Dawson, J. E. and R. Goré, *Generic methods for formalising sequent calculi applied to provability logic*, in: *Logic for Programming, Artificial Intelligence, and Reasoning - 17th International Conference, LPAR-17, Yogyakarta, Indonesia, October 10-15, 2010. Proceedings*, 2010, pp. 263–277.
URL http://dx.doi.org/10.1007/978-3-642-16242-8_19

[6] Gacek, A., "A Framework for Specifying, Prototyping, and Reasoning about Computational Systems," Ph.D. thesis, University of Minnesota (2009).

[7] Gacek, A., D. Miller and G. Nadathur, *Nominal abstraction*, Information and Computation **209** (2011), pp. 48–73.

[8] Gacek, A., D. Miller and G. Nadathur, *A two-level logic approach to reasoning about computations*, Journal of Automated Reasoning **49** (2012), pp. 241–273.
URL http://arxiv.org/abs/0911.2993

[9] Goré, R. and R. Ramanayake, *Valentini's cut-elimination for provability logic resolved*, The Review of Symbolic Logic **5** (2012), pp. 212–238.
URL http://journals.cambridge.org/article_S1755020311000323

[10] Graham-Lengrand, S., "Polarities & Focussing: a journey from Realisability to Automated Reasoning," Habilitation thesis, Université Paris-Sud (2014).
URL http://hal.archives-ouvertes.fr/tel-01094980

[11] Groote, P., *Linear logic with isabelle: Pruning the proof search tree*, in: P. Baumgartner, R. Hähnle and J. Possega, editors, *Theorem Proving with Analytic Tableaux and Related Methods: 4th International Workshop, TABLEAUX* (1995), pp. 263–277.
URL http://dx.doi.org/10.1007/3-540-59338-1_41

[12] Kalvala, S. and V. D. Paiva, *Mechanizing linear logic in isabelle*, in: *In 10th International Congress of Logic, Philosophy and Methodology of Science*, 1995.

[13] Marin, S. and L. Straßburger, *Label-free modular systems for classical and intuitionistic modal logics*, in: *Advances in Modal Logic 10, invited and contributed papers from the tenth conference on "Advances in Modal Logic," held in Groningen, The Netherlands, August 5-8, 2014*, 2014, pp. 387–406.
URL http://www.aiml.net/volumes/volume10/Marin-Strassburger.pdf

[14] Pfenning, F., *Structural cut elimination*, in: *Proceedings of the 10th Annual IEEE Symposium on Logic in Computer Science*, LICS '95 (1995), pp. 156–.
URL http://dl.acm.org/citation.cfm?id=788017.788741

[15] Pinto, L. and T. Uustalu, *Proof search and counter-model construction for bi-intuitionistic propositional logic with labelled sequents*, in: M. Giese and A. Waaler, editors, *Automated Reasoning with Analytic Tableaux and Related Methods: 18th International Conference, TABLEAUX 2009, Oslo, Norway, July 6-10, 2009. Proceedings* (2009), pp. 295–309.
URL http://dx.doi.org/10.1007/978-3-642-02716-1_22

[16] Power, J. and C. Webster, *Working with linear logic in coq*, in: *12th International Conference on Theorem Proving in Higher Order Logics*, 1999, pp. 1–16.

[17] Simmons, R. J., *Structural focalization*, ACM Transactions on Computational Logic **15** (2014), pp. 21:1–21:33.
URL http://doi.acm.org/10.1145/2629678

[18] Tews, H., *Formalizing cut elimination of coalgebraic logics in coq*, in: D. Galmiche and D. Larchey-Wendling, editors, *Automated Reasoning with Analytic Tableaux and Related Methods: 22nd International Conference, TABLEAUX 2013, Nancy, France, September 16-19, 2013, Proceedings* (2013), pp. 257–272.
URL http://dx.doi.org/10.1007/978-3-642-40537-2_22

[19] Urban, C. and B. Zhu, *Revisiting cut-elimination: One difficult proof is really a proof*, in: A. Voronkov, editor, *Rewriting Techniques and Applications: 19th International Conference, RTA 2008 Hagenberg, Austria, July 15-17, 2008 Proceedings* (2008), pp. 409–424.
URL http://dx.doi.org/10.1007/978-3-540-70590-1_28