

¹ **A study of circular representations of**
² **infinite proofs for fixed-points logics,**
³ **their expressiveness and complexity**
⁴ **Ph. D. Thesis**

⁵ Rémi Nollet
under the direction of Christine Tasson and Alexis Saurin

⁶ February 16, 2021

1 Contents

2	1 Introduction	7
3	1.1 Generalities on least and greatest fixed points	7
4	1.1.1 Basic definitions	7
5	1.1.2 Proving their existence	7
6	1.1.3 Expressivity in logic	9
7	1.1.4 Expressivity in programs	11
8	1.1.5 Usage in logic	12
9	1.2 Least and greatest fixed points in proof theory	12
10	1.2.1 Proof theory	13
11	1.2.2 Finite proof systems for least and greatest fixed points	14
12	1.2.3 Infinite proof systems for least and greatest fixed points	15
13	1.2.4 Finite representations and circular proof systems for least and greatest fixed points	16
14	1.3 In this thesis	18
15	1.3.1 Fixed points in linear logic	18
16	1.3.2 Addressed questions, proposed answers	18
17	1.3.3 Outline of this thesis	21
19	2 Technical background	23
20	2.1 Proof theory for least and greatest fixed points	23
21	2.1.1 Usual proof theory and MALL	23
22	2.1.2 Finite proof trees: μ MALL	28
23	2.1.3 Infinite proof trees: μ MALL $^\infty$	30
24	2.1.4 Finite proof trees with back-edges: μ MALL $^\omega$	32
25	2.2 Complexity theory	41
26	2.2.1 Generalities on complexity and PSPACE	41
27	2.2.2 Some PSPACE-complete problems	44
28	2.3 Parity automata	45
29	3 PSPACE-completeness of the thread criterion	47
30	3.1 Deciding thread validity in PSPACE	48
31	3.2 PSPACE-Completeness	52
32	3.2.1 Outline of the PSPACE-Completeness Proof	52
33	3.2.2 Defining the Reduction	52
34	3.2.3 Main Theorem	54

Contents

1	3.3	Comments on our Approach and Discussion of Related Works	62
2	3.4	Conclusion	64
3	4	A polynomial sub-criterion	73
4	4.1	Labelling as validity	75
5	4.1.1	\mathcal{L} -proofs	75
6	4.1.2	Finite representations of circular \mathcal{L} -proofs.	76
7	4.1.3	Two alternative characterizations of μMALL^φ	79
8	4.2	On loops and threads	84
9	4.3	Conclusion of the chapter	87
10	5	Finitisation	89
11	5.1	On Brotherston-Simpson's conjecture: finitizing circular proofs	90
12	5.2	Relaxing the labelling of proofs	91
13	5.2.1	Extended finitization	95
14	5.3	Proofs of section 4.1.	98
15	5.4	Details and proofs for section 5.2	99
16	5.5	Details of finitization for π_∞	101
17	5.6	Conclusion	102
18	6	Conclusion	105
19	I	Annexes (temporaires ?)	117
20	.1	Definition of proofs	119
21	.1.1	Some mathematical tools	120
22	.1.2	Provability as an inductive property	121
23	.1.3	Proof trees for provability	123
24	.1.4	Proof trees with occurrences	125
25	.2	La vérité sur la formalisation des preuves	127
26	.2.1	Types de données	127
27	.2.2	Structures de preuves	130
28	.2.3	Validité d'une structure de preuve	134
29	.2.4	Autres notions	135
30	.3	Jones' characterization of complexity classes	135
31	.4	On Fischer-Ladner preorderning and subformula ordering	136
32	.5	Proof of PSPACE-completeness of $\text{BOOLE}_{\text{false}}$	138
33	.6	Assignment of priorities to formulas	142
34	.7	Vieilles remarques sur le background technique	143
35	.7.1	vieilles remarques sur le finitaire	144
36	.7.2	vieilles remarques sur le circulaire	144
37	.8	OCaml implementation of Jones reduction from BOOLE to BOOLE_0	150
38	.9	Commented bibliography	159
39	.9.1	On μMALL	159

Contents

1	.10 Notations	161
2	.11 A short reminder on complexity classes and completeness	161
3	.12 Open questions	163
4	.13 π_∞	164
5	.13.1 Size-change algorithm for the decision of the thread criterion . . .	165
6	.14 Checking finite representations vs. Circular pre-proofs	170
7	.15 Searching for circular proofs	172
8	.16 Quelques Remarques d'Orthographe et de Style	173
9	.16.1 Terminology	174
10	.16.2 Dialogues	175

Rémi: (???) signale les références internes manquantes, [???] signale les références externes manquantes.

11

¹ 1 Introduction

² 1.1 Generalities on least and greatest fixed points

³ 1.1.1 Basic definitions

- ⁴ The general subject of this thesis is the study of least and greatest fixed points in logic.
- ⁵ The basic notions of least and greatest fixed points are easily described in the setting of ordered sets.
- ⁷ If (E, \leq) is an order and $f: E \rightarrow E$ is a non-decreasing endofunction, an element $x \in E$ ⁸ is a *fixed point* of f when $f(x) = x$.
- ⁹ More than general fixed points, what interests us are *pre-* and *post-fixed points*. An ¹⁰ element $x \in E$ is a *pre-fixed point* of f when $f(x) \leq x$, and it is a *post-fixed point* of f ¹¹ when $x \leq f(x)$.
- ¹² Even more precisely, what we want to talk about are *least pre-fixed points* and *greatest ¹³ post-fixed points*. An element $x \in E$ is a *least pre-fixed point* of f when $f(x) \leq x$ and ¹⁴ $\forall y \in E, f(y) \leq y \Rightarrow x \leq y$. And x is a *greatest post-fixed point* of f when $x \leq f(x)$ and ¹⁵ $\forall y \in E, y \leq f(x) \Rightarrow y \leq x$. There are usual notations for that: the *least pre-fixed point* ¹⁶ of a non-decreasing function f is denoted, when it exists, by $\mu x f(x)$, and similarly its ¹⁷ greatest post-fixed point is denoted by $\nu x f(x)$.
- ¹⁸ Note that the least pre-fixed point of a non-decreasing function is always a fixed point, ¹⁹ and therefore it is its least fixed point.

²⁰ 1.1.2 Proving their existence

- ²¹ The main theorems on the existence of least and greatest fixed points are the following:

1 Introduction

¹ **Theorem 1.** Let (E, \leq) be an ordered set.

² 1. If

³ every well-ordered subset of E has a least upper bound (1.1)

⁴ then

⁵ every non-decreasing endofunction on E has a least pre-fixed point (1.2)

⁶ 2. Conversely, if

⁷ every non-decreasing endofunction on E has a least fixed point (1.3)

⁸ then

⁹ E has a minimum and every directed subset of E has a least upper bound (1.4)

¹⁰ in which we recall that a subset A of E is said to be directed when every finite subset of
¹¹ A has an upper bound in A .

¹² Proof elements and references.

¹³ • First remark that, as already mentionned above, a least pre-fixed point is always a
¹⁴ fixed point and, therefore, (1.2) is stronger than (1.3). Similarly, every well-ordered
¹⁵ subset of an order is either empty or directed. Hence (1.4) is stronger than (1.1).
¹⁶ That is why the two parts 1 and 2 of that theorem are indeed converse to each
¹⁷ other.

¹⁸ • The direction 1 seems to be a folklore theorem which is difficult to trace back to a
¹⁹ unique original author. Yet the first version of it seems to be that of Abian and
²⁰ Brown [1961], although it is very close to a similar theorem by Bourbaki [1949].
²¹ See [Lassez, Nguyen, and Sonenberg, 1982, Section 4] for a bibliographic study of
²² its origins. See Davey and Priestley [2002, Exercise 8.19, p. 198] for a quick proof
²³ using ordinal induction.

²⁴ • The direction 2 is more recent and has been proved by Markowsky [1976].

²⁵ To the reader interested by those questions, we recommend the book by Davey and
²⁶ Priestley [2002, in particular ch. 8, p. 175, and the bibliographic discussion p. 285], which
²⁷ contains more details and references about fixed-point theorems. \square

²⁸ That theorem characterizes, in a sense, the preorders on which it makes sense to study
²⁹ the least fixed points of non-decreasing endofunctions. And it says that in these preorders,

¹ those least fixed points are in fact least pre-fixed points. Those orders are called complete
² partial orders, or CPO.

³ Because of that theorem, we will commonly say “least fixed point” when talking about
⁴ least pre-fixed points, and similarly for greatest fixed points.

⁵ 1.1.3 Expressivity in logic

⁶ We will now motivate the will to add a connective to logic that has the behavior of
⁷ forming a least pre-fixed point by a first example, coming from temporal logic.

⁸ Let us consider a logic like LTL [Pnueli, 1977], in which the truth of a proposition A may
⁹ depend on an instant $t \in \mathbf{N}$. The boolean denotation of a formula A is a $\llbracket A \rrbracket : \mathbf{N} \rightarrow \{0, 1\}$
¹⁰ and if $t \in \mathbf{N}$, we denote by $\llbracket A \rrbracket_t \in \{0, 1\}$ the truth value of A at t . As an alternative,
¹¹ we may write $t \models A$ for $\llbracket A \rrbracket_t = 1$. We use one logical connective and two temporal
¹² connectives. For each of them, we give two equivalent definitions:

$$\begin{array}{lll} \text{“or”} & \llbracket A \vee B \rrbracket_t = \max\{\llbracket A \rrbracket_t, \llbracket B \rrbracket_t\} & t \models A \vee B \Leftrightarrow t \models A \text{ or } t \models B \\ \text{“next”} & \llbracket \bigcirc A \rrbracket_t = \llbracket A \rrbracket_{t+1} & t \models \bigcirc A \Leftrightarrow t+1 \models A \\ \text{“eventually”} & \llbracket \Diamond A \rrbracket_t = \max\{\llbracket A \rrbracket_s \mid s \geq t\} & t \models \Diamond A \Leftrightarrow \exists s \geq t, s \models A \end{array}$$

¹³ We abuse the notation \models by using $A \models B$ to denote the fact that $\forall t \in \mathbf{N}, \llbracket A \rrbracket_t \leq \llbracket B \rrbracket_t$,
¹⁴ that is, equivalently: $\forall t \in \mathbf{N}$, if $t \models A$ then $t \models B$. Now we say that

¹⁵ **Proposition 1.** *For every formulas A and B , the following are true:*

$$\begin{array}{ll} \text{16} \quad A \vee \bigcirc \Diamond A \models \Diamond A & (1.5) \\ & \frac{A \vee \bigcirc B \models B}{\Diamond A \models B} & (1.6) \end{array}$$

¹⁷ *Proof.*

¹⁸ 1. Proof of (1.5)

¹⁹ Assume that $t \in \mathbf{N}$ and $t \models A \vee \bigcirc \Diamond A$. There are two cases:

²⁰ 1.1. $t \models A$

²¹ In that case $t \models \Diamond A$.

1 Introduction

1.2. $t \models \bigcirc\Diamond A$

In that case $t + 1 \models \Diamond A$, that is $\exists s \geq t + 1, s \models A$, so $t \models \Diamond A$.

Hence, in any case, $t \models \Diamond A$.

2. Proof of (1.6)

Let us assume that

$$A \vee \bigcirc B \models B \quad (1.7)$$

and show that $\Diamond A \models B$.

2.1. We first prove the following lemma: $\forall u \in \mathbf{N}, \forall t \in \mathbf{N}, t + u \models A \Rightarrow t \models B$.

PROOF: By induction on u .

2.1.1. Case $u = 0$:

In that case we know that $t \models A$, hence $t \models A \vee \bigcirc B$. By assumption (1.7) we get $t \models B$.

2.1.2. Case $u = v + 1$:

In that case we know that $t + 1 + v \models A$. By induction hypothesis on v we know that $t + 1 \models B$, that is $t \models \bigcirc B$, hence $t \models A \vee \bigcirc B$. By assumption (1.7) we get $t \models B$.

2.2. From this, we immediately deduce the following:

$$\forall s \in \mathbf{N}, s \models A \Rightarrow \forall t \leq s, t \models B \quad (1.8)$$

2.3. We now prove that $\Diamond A \models B$.

Assume a $t \in \mathbf{N}$ and $t \models \Diamond A$, that is assume a $s \in \mathbf{N}, s \geq t$ and $s \models A$. It remains to show that $t \models B$. This is exactly given by (1.8) above.

22

□

23 This relates to our previous description of least/greatest pre-/post-fixed points in the
24 following way. If we consider \models as our order, we just proved that $\Diamond A$ is a least pre-fixed
25 point of $F: X \mapsto A \vee \bigcirc X$, because we proved that $F(\Diamond A) \leq \Diamond A$ and $\forall B, F(B) \leq B \Rightarrow$
26 $\Diamond A \leq B$, with \leq being \models .

27 That means that if we are allowed to use least pre-fixed points in the construction
28 of the formulas, we do not need \Diamond to be given as a primitive connective of the logic;
29 we could define it as $\Diamond A := \mu X(A \vee \bigcirc X)$. Dually, you can check that the “always”
30 operator, denoted by $\Box A$ and defined equivalently by $\llbracket \Box A \rrbracket_t = \min \{ \llbracket A \rrbracket_s \mid s \geq t \}$ or
31 $t \models \Box A \Leftrightarrow \forall s \geq t, s \models A$ could alternatively be defined as the greatest post-fixed point
32 $\Box A := \nu X(A \wedge \bigcirc A)$.

33 In other words, least pre-fixed points and greatest post-fixed points give you more
34 expressivity to define formulas. Such ideas are the basis of modal μ -calculus [Kozen,
35 1983].

¹ 1.1.4 Expressivity in programs

² Least pre-fixed points and greatest post-fixed points can also be used to model inductive
³ and coinductive datatypes in programming languages. We will try to show that on a
⁴ second example.

⁵ In this example, we will use an OCaml-like syntax, although we are not writing strictly
⁶ legit OCaml. We am trying to convey a general intuition, which probably apply *mutatis*
⁷ *mutandis* to any programming language in which one can define inductive algebraic
⁸ datatypes.

⁹ Let us consider the type of integer lists, which can be described as:

```
type int list = [] | ( :: ) of int * int list
```

¹⁰ And let us consider the following type t , parameterized over a type $'a$:

```
type 'a t = Nil | Cons of int * 'a
```

¹¹ Remark that the type t is conceptually simpler than **int list**, because it is not a
¹² recursive type. If you are familiar with algebraic datatypes, you may see that this type
¹³ could be written as

```
'a t = 1 + int * 'a
```

¹⁴ where we use 1 to denote the singleton type:

```
type 1 = ()
```

¹⁵ Now we can define two functions

```
inj : int list t -> int list
fold : ('a t -> 'a) -> int list -> 'a
```

¹⁶ as follows:

```
let inj = function
| Nil           -> []
| Cons (x, xs) -> x :: xs

let rec fold f = function
| []            -> f Nil
| x :: xs       -> f (Cons (x, fold f xs))
```

1

*

² In this example, for every two types α and β , let us say that $\alpha \leqslant \beta$ when the type $\alpha \rightarrow \beta$
³ is inhabited. Then if we take $F(\alpha)$ to be the type $\alpha \ t$, we have $F(\text{int list}) \leqslant \text{int list}$
⁴ because of `inj`. And each time we have a type α such that $F(\alpha) \leqslant \alpha$, we also have
⁵ `int list` $\leqslant \alpha$ thanks to `fold`. So it makes sense to say that `int list` is a least pre-fixed
⁶ point of `t`.

⁷ Another way of saying it is that `int list` = $\mu\alpha(1 + \text{int} * \alpha)$. And the general idea is
⁸ that inductive datatypes correspond to least pre-fixed points of functors. And, dually,
⁹ coinductive datatypes correspond to greatest post-fixed points of functors. For instance,
¹⁰ we could define a type of integer streams as `int stream` = $\nu\alpha(\text{int} * \alpha)$.

¹¹ *Remark 1.* Actually the previous example is not totally complete. That example characterises `int list` as the least pre-fixed point of `t`, but it happens that the singleton type
¹² `1` could fit this description as well. In fact, the description of least and greatest fixed
¹³ points in terms of orders or preorders does not give enough precision. To have a complete
¹⁴ characterisation of `int list` as a least fixed point, we would need to talk about the
¹⁵ computational behaviour of the functions, and we would need to shift from the setting
¹⁶ of orders and preorders to the setting of categories, which is out of the scope of this
¹⁷ introduction.
¹⁸

¹⁹ 1.1.5 Usage in logic

²⁰ There has been a lot of logics allowing the use of least and greatest fixed-point constructions in their formulas. de Bakker and de Roever [1972] define a logic with least
²¹ fixed points to prove properties of recursively defined programs. Aczel [1977] study the
²² extension of recursion theory with inductive definitions. Aho and Ullman [1979] study the
²³ relational calculus, which may be understood as first-order logic, and suggest extending
²⁴ it by adding a least fixed-point operator, in order to make it more expressive. Gurevich
²⁵ and Shelah [1986] study the expressive power of different extensions of first-order logic
²⁶ with fixed point induction. Dawar and Gurevich [2002] study the expressive power of
²⁷ fixed point logics.
²⁸

²⁹ 1.2 Least and greatest fixed points in proof theory

³⁰ Least and greatest fixed point of formulas may be seen as a way to formulate definitions
³¹ by induction, or by coinduction. We will study those least and greatest fixed points from

¹ the point of view of proof theory. It is to be noticed that, thanks to the proof-program correspondence, a lot of the analysis we make on proofs will also apply to programs.
² The advantage of proofs over programs for our study is that they provide a system
³ which makes things visible, decomposing things in simple elements: subformula property,
⁴ cut-elimination, formulas occurrences, ...
⁵

⁶ 1.2.1 Proof theory

⁷ We do here a short recall of a few elements that made the success of modern proof theory
⁸ and sequent calculus.

⁹ In usual sequent calculus, a proof is defined to be a finite proof tree.

¹⁰ The subformula property says that if you can prove a given conclusion then you can do
¹¹ it by using only subformulas of this conclusion. This is a fundamental property, saying,
¹² intuitively, that if I ask you a question (“Is this formula true ?”), you can answer it using
¹³ only the concepts that are already present in the question, you do not need to introduce
¹⁴ any new concept. You may still do it, because it may ease the task, but you do not need
¹⁵ it.

¹⁶ The cut rule is the rule that allows you to do some deductive reasoning. It is a generali-
¹⁷ sation of two logical principles, *modus ponens*, which says that from a proof of A and a
¹⁸ proof of $A \Rightarrow B$, you can build a proof of B , and the transitivity of implication, which
¹⁹ says that from a proof of $A \Rightarrow B$ and a proof of $B \Rightarrow C$ you can build a proof of $A \Rightarrow C$.
²⁰ One of the ideas that made sequent calculus so successful is that all inferences preserve
²¹ the subformula property, except for the cut rule. When following this discipline, the
²² subformula property amounts to saying that we can eliminate cuts from any proof.

²³ Globally, various logical settings have been introduced to reason about inductive and
²⁴ coinductive statements, both at the level of the logical languages modelling (co)induction
²⁵ (Martin Löf’s inductive predicates vs. fixed-point logics, that is μ -calculi) and at the level
²⁶ of the proof-theoretical framework considered (finite proofs with (co)induction à la Park
²⁷ [1969] vs. infinite proofs with fixed-point/inductive predicate unfoldings) [Brotherston,
²⁸ 2006, Brotherston and Simpson, 2007, 2011, Baelde and Miller, 2007, Baelde, 2009,
²⁹ 2012].

³⁰ Moreover, such proof systems have been considered over classical logic [Brotherston, 2006,
³¹ Brotherston and Simpson, 2011], intuitionistic logic [Clairambault, 2009], linear-time or
³² branching-time temporal logic [Kozen, 1983, Kaivola, 1995, Walukiewicz, 1993, 1995,
³³ Dax, Hofmann, and Lange, 2006, Doumane, 2017, Doumane, Baelde, Hirschi, and Saurin,
³⁴ 2016] or linear logic [Santocanale, 2002, Fortier and Santocanale, 2013, Baelde and Miller,
³⁵ 2007, Baelde, Doumane, and Saurin, 2016, Doumane, 2017].

$$\frac{\vdash \text{Gamma}, S \vdash S^\perp, F[S/X]}{\vdash \Gamma, \nu X F} (\nu_{\text{inv}})$$

Figure 1.1. Coinduction rule *à la* Park

- ¹ In all those proof systems, the treatment of inductive and coinductive reasoning brings
- ² some highly complex proof figures.

³ 1.2.2 Finite proof systems for least and greatest fixed points

- ⁴ The first systems designed to reason about fixed points of formulas were systems with
- ⁵ finite proofs, in which induction and coinduction principles are used in order to provide
- ⁶ a finite proof theory for reasoning on formulas with least or greatest fixed points [Kozen,
- ⁷ 1981, 1983, Baelde, 2012].
- ⁸ But finite proof systems for least and greatest fixed points have some drawbacks.
- ⁹ • To introduce a greatest fixed point or eliminate a least fixed point of formula, you
- ¹⁰ have to use a rule of induction or coinduction, and you have to provide an explicit
- ¹¹ invariant, which has to be a formula of the same system. This is a restriction
- ¹² because the language of formulas may not be expressive enough to express all the
- ¹³ invariants you may need to prove formulas that should intuitively be true.
- ¹⁴ • It breaks the subformula property.
- ¹⁵ • Here, in the finitary setting for least and greatest fixed points of formulas, the
- ¹⁶ failure of the subformula property can therefore be restated by saying that we
- ¹⁷ cannot eliminate all cuts. Nevertheless, it makes sense to define a procedure of “cut
- ¹⁸ elimination” for this setting. This procedure will not eliminate all cuts, but it will
- ¹⁹ simplify them and eliminate some of them and it is still a terminating procedure,
- ²⁰ which leaves the proof in a normal form in which the only remaining cuts are of
- ²¹ a very specific form, and are cuts that cannot be reduced anymore. The point is
- ²² that in this setting, besides the fact that we cannot completely eliminate cuts, this
- ²³ procedure of cut elimination turns out to be quite complex.
- ²⁴ For instance, in proof systems using (co)induction rules *à la* Park, the rules allowing to
- ²⁵ derive a coinductive property (or dually to use an inductive hypothesis) have a complex
- ²⁶ inference of the form of fig. 1.1 (when presented in the setting of fixed-point logic – here
- ²⁷ we follow the one-sided sequent tradition of MALL that we will adopt in the rest of the
- ²⁸ thesis).

1 Not only is it difficult to figure out intuitively what is the meaning of this inference,
 2 but it is also problematic for at least two additional and more technical reasons: (i) it
 3 is hiding a cut rule that *cannot* be eliminated, which is problematic for extending the
 4 Curry-Howard correspondence to fixed-points logics, and (ii) it breaks the subformula
 5 property, which is problematic for proof search: at each coinduction rule, one has to guess
 6 an invariant (in the same way as one has to guess an appropriate induction hypothesis in
 7 usual mathematical proofs) which is problematic for automation of proof search.

8 **1.2.3 Infinite proof systems for least and greatest fixed points**

9 Infinite proofs have been introduced to reason on (least and greatest) fixed points of
 10 formulas.

11 For all these reasons, infinite (non-wellfounded) proofs, which are infinite proofs satisfying
 12 the validity criteria, have been proposed, in recent years, as an alternative to induction
 13 and coinduction with explicit invariants [Brotherston, 2006, Brotherston and Simpson,
 14 2007, 2011]. By replacing the coinduction rule with simple fixed-point unfoldings and
 15 allowing for non-wellfounded branches, those proof systems address the problem of the
 16 subformula property for the cut-free systems. The cut-elimination dynamics for inductive-
 17 coinductive rules is also much simpler. In particular, Baelde, Doumane, and Saurin [2016],
 18 inspired notably by Dax, Hofmann, and Lange [2006], proposed a very successful system
 19 of infinite proofs to reason on least and greatest fixed points of formulas. Actually, this is
 20 for the propositional setting, but such ideas already existed to reason on inductive and
 21 coinductive predicates.

22 Infinite, non well-founded, proofs present the advantage over explicit induction or coinduc-
 23 tion to offer a framework in which it is possible to recover the good structural properties
 24 of sequent calculus, such as cut-elimination, subformula property and focusing, making
 25 them a more suitable tool to automated proof search. Indeed, cut-elimination and focusing
 26 have recently been extended to non well-founded proofs for μ MALL by Baelde, Doumane,
 27 and Saurin [2016], Doumane [2017].

28 Now the problem is that if we take this approach too naively, by simply allowing proof
 29 trees to be infinite, then two bad things happen:

- 30 1. the system becomes inconsistent, meaning that every formula becomes provable;
- 31 2. the cut-elimination procedure becomes a non-terminating, non-converging one.

32 The price to pay is that the consistency of the logical system is broken and that a validity
 33 criterion has to be added in order to ensure consistency.

$$\frac{\vdots \quad \vdots}{\frac{\vdash \mu XX, \Gamma^{(\mu)} \quad \vdash \nu XX, \Gamma^{(\nu)}}{\frac{\vdash \mu XX, \Gamma^{(\mu)} \quad \vdash \nu XX, \Gamma^{(\nu)}}{\vdash \Gamma}} \text{ (cut)}}$$

Figure 1.2

- ¹ More precisely, in those proof systems when considering all possible infinite, non-wellfounded derivations (*a. k. a.* preproofs), it is straightforward to derive any sequent Γ (see fig. 1.2).
- ⁴ Such preproofs are therefore unsound and one needs to impose a validity criterion to distinguish, among all preproofs, those which are logically valid proofs from the unsound ones.
- ⁷ A solution to that is to say that all these infinite proof trees are only preproofs, and that only some of these preproofs are valid proofs. This means that we need a criterion to distinguish valid (pre)proofs from invalid preproofs.
- ¹⁰ Therefore, in the setting of non-wellfounded proofs, a validity criterion is necessary to distinguish, among all infinite derivation trees (*a. k. a.* preproofs), those which are logically valid proofs.
- ¹³ This condition will actually reflect the inductive and coinductive nature of our two fixed-point connectives.
- ¹⁵ A standard approach [Brotherston, 2006, Brotherston and Simpson, 2007, 2011, Santocanale, 2002, Baelde, Doumane, and Saurin, 2016] is to consider a preproof to be valid if every infinite branch is supported by an infinitely progressing thread. This is called the thread criterion.
- ¹⁹ However, doing so, the logical correctness of circular proofs becomes a non-local property, much in the spirit of proof nets correctness criteria [Girard, 1987, Danos and Regnier, 1989].

²² **1.2.4 Finite representations and circular proof systems for least and greatest fixed points**

- ²⁴ The problem with infinite proofs, on the other hand, is mainly that they are infinite, which has two major drawbacks:

1 1. The first one is epistemic: we would like a proof to be a finite object, which I can
 2 communicate to you in finite time, and which you can check in finite time. The
 3 fact that a proof may be an infinite object means that I may not be able to give
 4 you a proof, but I will in fact give you the finite description of an infinite proof,
 5 formulated in the meta-theory.

6 2. The second one is practical: if we want our system to be used in an automated
 7 prover or in a proof assistant, we need those proofs to be finitely representable.
 8 It means that whatever system of representation you chose, you will not be able
 9 to represent all infinite proofs, because there is an uncountable number of infinite
 10 proofs and your system of finite representations will only be able to represent a
 11 countable number of them.

12 From that it may seem that going from finite to infinite proofs was a mistake. But infinite
 13 proofs give great insights on least and greatest fixed points of formulas, on their different
 14 proof systems and on the dynamic of cut-elimination in those systems, including the
 15 finitary ones. In particular they provide us with a new way to understand the finitary
 16 systems. Each finitary proof can be translated into an infinitary one. This means that
 17 finitary proofs may be seen as one particular way to represent some of those infinitary
 18 proofs. So now we may transform the question of designing a finitary proof system
 19 for least and greatest fixed points of formulas into the question of identifying suitable
 20 fragments of the infinitary system, which have some nice-behaved representations.

21 Among those non-wellfounded proofs, circular proofs, that have infinite but regular
 22 derivations trees, have attracted a lot of attention for retaining the simplicity of the
 23 inferences of non-wellfounded proof systems but being amenable to a simple finite
 24 representation making it possible to have an algorithmic treatment of those proof
 25 objects.

26 In this context, a very natural way of representing some infinite proofs is to use finite
 27 proof trees with back-edges. This means that instead of constructing explicitly an infinite
 28 branch, we are allowed to stop at some point and point out some previous step of the
 29 construction and say: from there, we start again at that point. Such a representation has
 30 a canonical unfolding into an infinite proof tree.

31 This system of representations allows us to represent some of the infinite preproofs. Those
 32 preproofs that can be represented by such a proof tree with back-edges are called circular
 33 preproofs. Those representations are called circular representations.

34 Despite the need for a validity condition, circular, *i. e.* non-wellfounded but regular proofs
 35 have received increasing interest in recent years with the simultaneous development of
 36 their applications and meta-theory: infinitary proof theory is now well-established in
 37 several proof-theoretical frameworks such as Martin Löf's inductive predicates, linear
 38 logic with fixed points, *etc.*

1 1.3 In this thesis

2 1.3.1 Fixed points in linear logic

3 This thesis focuses on circular proofs for MALL with fixed points. Least and greatest
4 fixed point were already well-established in linear logic: [Baelde and Miller, 2007, Baelde,
5 2012, Baelde, Doumane, and Saurin, 2016, Doumane, 2017]

6 This thesis is a contribution to several directions in the field of circular proofs:

- 7 1. the relationship between finite and circular proofs (at the level of provability and
8 at the level of proofs themselves) and
- 9 2. the certification of circular proofs, that is the production of fast and/or small pieces
10 of evidence to support validity of a circular preproof.

11 1.3.2 Addressed questions, proposed answers

12 **Proof-checking** Among all circular preproofs, some are valid proofs and some are not.
13 The thread criterion gives a non-ambiguous mathematical definition of whether a circular
14 representation represents a valid (pre)proof or an invalid preproof. The next interesting
15 question is whether there exist a method to tell whether the circular representation of
16 a preproof is valid or not. In other words: is the thread criterion on circular preproofs
17 decidable? Given a finite circular representation of a non-wellfounded preproof, can one
18 decide whether this preproof is valid with respect to the thread criterion?

19 The answer to that is yes: there is an algorithm which is able to tell the difference between
20 a valid circular representation of a preproof and an invalid one. In fact several such
21 algorithms are known.

22 The next question would be: how difficult is this problem? What is its computational
23 complexity? When we started to look at this problem, the state of the art was the
24 following: all known algorithms for this problem ran in exponential time and ran or
25 could be made to run in polynomial space. But no subexponential algorithm was known,
26 there was no lower bound on its complexity and the exact complexity of checking the
27 thread criterion was still unknown. Recall that $P \subseteq NP \subseteq PSPACE \subseteq EXP$. The first
28 contribution of this thesis is to prove that this problem is in fact PSPACE-complete.
29 This implies in particular that this problem is probably not in NP and that there is
30 probably no subexponential algorithm to solve it.

¹ Our proof is based on a deeper exploration of the connection between thread-validity
² and the size-change termination principle, which is usually used to ensure program
³ termination.

⁴ We work in particular by exploiting the connection between the usual thread-validity
⁵ and the size-change abstraction, that is usually used to ensure program termination.

⁶ Circular proofs have already proved useful in implementing efficient automatic provers,
⁷ e.g. the Cyclist prover [Gorogiannis and Rowe, 2014]. However, the complexity avoided
⁸ in the search, thanks to the fact that we need not to guess invariants, is counterbalanced
⁹ by the complexity of the validity criterion at the time of proof checking.

¹⁰ **A new validity criterion** Among all representations of valid circular proofs, a new
¹¹ fragment is described in chapter 4, based on a stronger validity criterion. This new
¹² criterion is based on a labelling of formulas and proofs, whose validity is purely local.

¹³ This allows this fragment to be easily handled, while being expressive enough to still
¹⁴ contain all circular embeddings of Baelde’s μ MALL finite proofs with (co)inductive
¹⁵ invariants: in particular deciding validity and computing a certifying labelling can be
¹⁶ done efficiently.

¹⁷ **Finitization** Comparing finite and infinite proofs is very natural. Informally, it amounts
¹⁸ to considering the relative strength of inductive reasoning versus infinite descent: while
¹⁹ infinite descent is a very old form of mathematical reasoning which appeared already
²⁰ in Euclid’s *Elements* and was systematically investigated by Fermat, making precise
²¹ its relationship with mathematical induction is still an open question for many proof
²² formalisms. Their equivalence is known as the Brotherston–Simpson conjecture. While it
²³ is fairly straightforward to check that infinite descent (circular proofs) prove at least as
²⁴ many statements as inductive reasoning, the converse is complex and remains largely
²⁵ open. A few years ago, Simpson [2017], on the one hand, and Berardi and Tatsuta
²⁶ [2017b,a], on the other hand, made progress on this question but only in the framework
²⁷ of Martin Löf’s inductive definitions, not in the setting of μ -calculi circular proofs in
²⁸ which invariant extraction is highly complex and known only for some fragments.

²⁹ We will show that the Brotherston–Simpson conjecture holds for the fragment we present:
³⁰ every labelled representation of a circular proof in the fragment is translated into a
³¹ standard finitary proof.

³² **Propositions of extensions** Finally we explore how to extend these results to a bigger
³³ fragment, by relaxing the labelling discipline while retaining (i) the ability to locally

1 Introduction

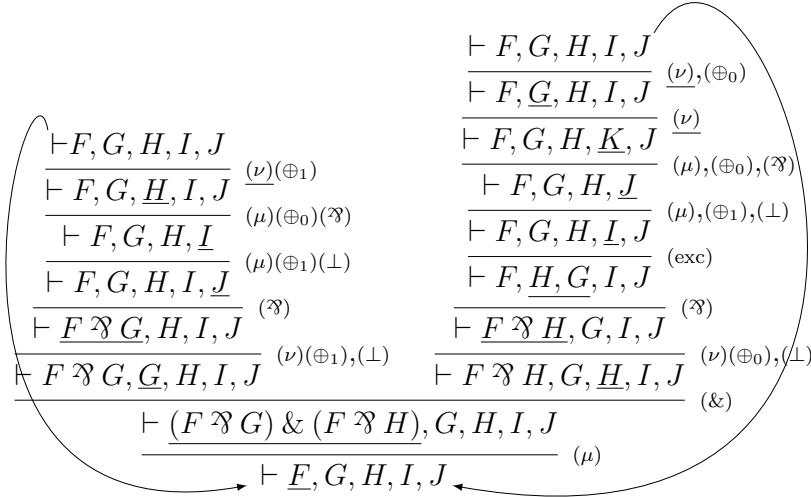


Figure 1.3. Proof π_∞

¹ certify the validity and (ii) to some extent, the ability to finitize circular proofs.

² **A complex example** We conclude this introduction by considering a typical example of a circular proof with a complex validating thread structure: while this infinite proof has a regular derivation tree, its branches and threads have a complex geometry. The circular (pre-)proof of Figure .2 derives the sequent $\vdash F, G, H, I, J$ where $F = \mu X.(X \otimes G) \& (X \otimes H)$, $G = \nu X.X \oplus \perp$, $H = \nu X.\perp \oplus X$, $I = \mu Z.((Z \otimes J) \oplus \perp)$, $J = \mu X.(K \otimes X) \oplus \perp$ and $K = \nu Y.\mu Z.((Z \otimes \mu X.(Y \otimes X) \oplus \perp) \oplus \perp)$.

⁸ This example of a circular derivation happens to be valid (it is a μ MALL $^\omega$ proof) but the description of its validating threads is quite complex. Indeed, each infinite branch β is validated by exactly one thread (see next section for detailed definitions) going through either G , H or K depending on the shape of the branch *at the limit* (infinite branches of this derivations can be described as ω -words on $A = \{l, r\}$ depending on whether the left or right back-edge is taken):
¹⁴ (i) if β *ultimately* follows always the left cycle ($A^* \cdot l^\omega$), the unfolding of H validates β ;
¹⁵ (ii) if β *ultimately* follows always the right cycle ($A^* \cdot r^\omega$), the unfolding of G validates β ;
¹⁶ (iii) if β *endlessly switches* between left and right cycles ($A^* \cdot (r^+ \cdot l^+)^\omega$), K validates β .
¹⁷ The description of the thread validating this proof is thus complex. This is reflected in the difficulty to provide a local way to validate this proof and in the lack of a general method for finitizing this into a μ MALL proof: to our knowledge, the usual finitization methods (working only for fragments of μ MALL circular proofs) do not apply here.

1.3.3 Outline of this thesis

² The subject of this thesis is the study of finite circular representations of infinite proofs
³ and preproofs.

⁴ It consists of 6 chapters:

- ⁵ • Chapter 1, this chapter, is an informal introduction to the subject of the thesis.
- ⁶ • Chapter 2 covers the technical background needed to develop the results of the
⁷ thesis.
- ⁸ • Chapters 3, 4 and 5 are the technical chapters, presenting the main results and
⁹ contributions of this thesis.
- ¹⁰ • Chapter 6 is the conclusion chapter.

¹¹ In Chapter 2 we recall the formulas and rules of linear logic with least and greatest fixed
¹² points, as well as the notions of preproofs and the thread validity criterion, and we recall
¹³ that the thread criterion is effectively decidable in PSPACE. The main section of the
¹⁴ first technical chapter is section 3.2, in which we show the PSPACE-completeness of the
¹⁵ thread criterion for μMALL^ω , in theorem 4. Section 3.3 is devoted to a discussion of our
¹⁶ approach and a comparison with related works. We conclude this chapter in section 3.4.

¹⁷ In Chapter 2, we provide the necessary background on infinitary and circular proof theory
¹⁸ of multiplicative additive linear logic with least and greatest fixed points (respectively
¹⁹ μMALL^∞ and μMALL^ω). Section 4.1 studies an approach to circular proofs based on
²⁰ labellings of greatest fixed points. We first motivate in section 4.1.1 such labellings as an
²¹ alternative way to express the validating threads. Then, in section 4.1.2 we introduce
²² finite representations of preproofs and use such labellings in order to locally certify
²³ their validity. Finally, in section 4.1.3, we turn to alternative characterizations of those
²⁴ circular proofs which can be labelled. The fragment of labellable proofs, while quite
²⁵ constrained (for instance, it does not include the example of Figure .2), is already enough
²⁶ to capture the circular proofs obtained by translation of μMALL proofs. In section 5.1,
²⁷ we address the converse: for any labelled derivation tree with back-edges, we provide
²⁸ a corresponding μMALL proof by generating a (co)inductive invariant based on an
²⁹ inspection of the labelling structure. Therefore, we answer the Brotherston–Simpson
³⁰ conjecture in a restricted fragment. In section 5.2, we introduce a more permissive
³¹ labelling strategy that allows to label more proofs (in particular by allowing to loop
³² not only on (ν) rules but on any rule) and that still ensures validity of the labellable
³³ derivations. For this relaxed labelling, we label the example of Figure .2 and show how to
³⁴ finitize it by adapting the method of section 5.1. Nevertheless, there is not yet a general
³⁵ method applicable to the complete extended labelling fragment. Relations between the

1 Introduction

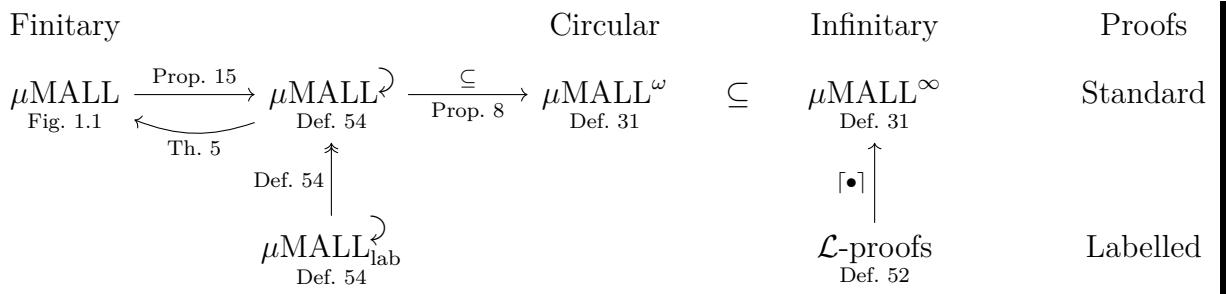


Figure 1.4. Relations between the different systems used in the second part of the thesis.

- ¹ various systems considered in this chapter are summarized in Figure 1.4.

²

*

³ **Statement of the contribution** On the question of how much time and space it takes
⁴ to check the **thread criterion** on a **circular representation** of an **infinite preproof**, it
⁵ was known how to do it in **PSPACE**, and we prove in this thesis that this problem is
⁶ **PSPACE-complete**, which means that we cannot do substantially better.

⁷ As we would like to be able to check our proofs in polynomial time, we provide a new
⁸ **validity criterion**, which is stronger than the **thread criterion** while accepting at least the
⁹ translations of **finitary proofs**, and which can be checked in quadratic time.

¹⁰ We also would like a proof system in which there is no **global criterion** to check, in
¹¹ which a proof is correct as soon as each inference used in it is correct. This is made
¹² possible. We provide such a proof system, obtained by adding some labelling to the
¹³ **circular representations** accepted by my new quadratic criterion.

¹⁴ Finally, this new proof system proves at least as much propositions than the **finitary**
¹⁵ **setting** and it is legit to ask how much more it does prove exactly. The answer is: No more.
¹⁶ This result may look disappointing but what it says is that every **circular representation**
¹⁷ of an **infinite preproof** that is valid for my quadratic criterion and every proof in my
¹⁸ labelled system can be turned into a **finitary proof** with the same conclusion. And we
¹⁹ provide an effective method to do it. In other words, we provide a method to **synthesize**
²⁰ **some induction and coinduction invariants**, **finitize** some circular proofs and partially
²¹ answer the **Brotherston-Simpson conjecture**.

¹ 2 Technical background

² 2.1 Proof theory for least and greatest fixed points

³ 2.1.1 Usual proof theory and MALL

⁴ Logic is generally built around two main concepts: formulas and proofs.

⁵ **Formulas** or *propositions*, model some statements that you may say, and which may,
⁶ intuitively, be true or false such as “The cat is black” or “Earth is flat”. But logic and
⁷ proof theory are more interested in understanding the nature of the logical connectives
⁸ and their dynamic than in what happens to be true in our world. That is why a formal
⁹ language of formulas is generally built out of some propositional variables and some
¹⁰ connectives. For instance a language of formulas for the classical logic LK may be defined
¹¹ by the following grammar:

$$A, B ::= X \mid \overline{X} \mid A \wedge B \mid A \vee B \mid \top \mid \perp$$

¹² where X ranges over a given set of propositional variables, which we denote by X, Y, Z, \dots ■

¹³ \wedge denotes conjunction, “and”, while \vee denotes disjunction, “or”. The constants \top and
¹⁴ \perp represent their respective neutral elements, that is respectively a true statement and
¹⁵ a false statement. The variables X, Y, Z, \dots represent some undetermined statements.
¹⁶ That means that, for instance, $(\overline{X} \vee Y) \wedge (\overline{Y} \vee Z)$ is a formula of LK, which you may
¹⁷ read as “not X or Y , and not Y or Z ”.

¹⁸ The main logic we will use to apply our methods in this thesis is the logic MALL,
¹⁹ composed of the Multiplicative and Additive fragments of Linear Logic. Linear logic
²⁰ was designed by Girard [1987] in a successful attempt to decompose the well-known
²¹ connectives of classical and intuitionistic logics into more elementary components. For
²² a detailed introduction to linear logic, see [Girard, 1987], [Girard, Taylor, and Lafont,
²³ 1989] or [Girard, 2011].

2 Technical background

- ₁ The formulas of MALL are defined by the following grammar:

Definition 1 (MALL formulas).

$$A, B ::= X \mid \bar{X} \mid A \otimes B \mid A \wp B \mid \mathbf{1} \mid \perp \mid A \oplus B \mid A \& B \mid \mathbf{0} \mid \top$$

- ₂ where X ranges over a given set of propositional variables.

- ₃ The set of all MALL formulas is denoted by Fml_{MALL} .

- ₄ \otimes and $\&$ are conjunctions of different natures and $\mathbf{1}$ and \top are their respective neutral elements. \wp and \oplus are disjunctions of different natures and \perp and $\mathbf{0}$ are their respective neutral elements.

- ₇ *Remark 2* (Precedence rules). The usage is that \otimes and \wp , the “multiplicative” connectives, have a higher precedence than \oplus and $\&$, the “additive” connectives. For instance $\bar{X} \wp \bar{Y} \& \bar{X}$ should be read as $(\bar{X} \wp \bar{Y}) \& (\bar{X} \wp \bar{Y})$.

- ₁₀ With such a syntax of formulas come a syntax for the positions of subformulas inside formulas. To that effect we use the following alphabet

- ₁₂ Let A_{Fml} be the following alphabet:

$$\mathcal{P}_{\text{MALL}} = \{\otimes_0, \otimes_1, \wp_0, \wp_1, \oplus_0, \oplus_1, \&_0, \&_1\}$$

- ₁₃ We denote by $\mathcal{P}_{\text{MALL}}^*$ the free monoid of finite words on $\mathcal{P}_{\text{MALL}}$. Those words are used to ₁₄ denote the position of a subformula in a formula.

- ₁₅ **Definition 2** (Positions of subformulas in a formula). The set of positions of subformulas of a given formula A is defined by induction on A :

$$\begin{aligned} \text{SubPos}(X) &= \{\epsilon\} & \text{SubPos}(\bar{X}) &= \{\epsilon\} & \text{SubPos}(\mathbf{1}) &= \{\epsilon\} & \text{SubPos}(\mathbf{0}) &= \{\epsilon\} \\ \text{SubPos}(\perp) &= \{\epsilon\} & \text{SubPos}(\top) &= \{\epsilon\} \\ \text{SubPos}(A \otimes B) &= \{\epsilon\} \cup \otimes_0 \cdot \text{SubPos}(A) \cup \otimes_1 \cdot \text{SubPos}(B) \\ \text{SubPos}(A \wp B) &= \{\epsilon\} \cup \wp_0 \cdot \text{SubPos}(A) \cup \wp_1 \cdot \text{SubPos}(B) \\ \text{SubPos}(A \oplus B) &= \{\epsilon\} \cup \oplus_0 \cdot \text{SubPos}(A) \cup \oplus_1 \cdot \text{SubPos}(B) \\ \text{SubPos}(A \& B) &= \{\epsilon\} \cup \&_0 \cdot \text{SubPos}(A) \cup \&_1 \cdot \text{SubPos}(B) \end{aligned}$$

¹ **Example 1.** The set of positions of subformulas of $X \otimes (\perp \oplus Y)$ is $\{\epsilon, \otimes_0, \otimes_1 \oplus_0, \otimes_1 \oplus_1\}$.

² Those formulas are equipped with an involutive negation, denoted by \cdot^\perp and defined
³ inductively as follows:

Definition 3.

$$\begin{array}{lllll} X^\perp = \overline{X} & \overline{X}^\perp = X & (A \otimes B)^\perp = A^\perp \wp B^\perp & (A \wp B)^\perp = A^\perp \otimes B^\perp & \mathbf{1}^\perp = \perp \\ \perp^\perp = \mathbf{1} & (A \oplus B)^\perp = A^\perp \& B^\perp & (A \& B)^\perp = A^\perp \oplus B^\perp & \mathbf{0}^\perp = \top & \top^\perp = \mathbf{0} \end{array}$$

⁴ **Proofs** are certificates used to attest the truth of a formula. In this thesis, proofs are
⁵ built in sequent calculus, following the usage of modern proof theory, initiated by Gentzen
⁶ [1935a,b, 1969].

⁷ In sequent calculus, a proof is a finite tree built out of some given deduction rules. We
⁸ recall the basics of that setting. We will exemplify it first on the particular case of MALL,
⁹ then on MALL extended with least and greatest fixed point in the system μ MALL. For
¹⁰ a more detailed introduction to sequent calculus, you may look at [Girard, Taylor, and
¹¹ Lafont, 1989] or [Girard, 1991].

¹² **Definition 4 (Sequent).** Given a set of formulas Fml, a *sequent* is defined to be a finite
¹³ list of formulas. If Γ is a sequent of size n , we use the notation $|\Gamma|$ to denote either n , the
¹⁴ size of the list, or the set $\{0, \dots, n - 1\}$, the set of indices of this list.¹

¹⁵ A sequent is denoted by the symbol \vdash followed by its formulas. A sequent should be
¹⁶ understood, intuitively, as the disjunction, in the \wp sense, of its formulas.

¹⁷ A proof is a tree made out of some logical inferences.

¹⁸ **Definition 5 (Inference).** An *inference* consists of :

- ¹⁹ • A finite number of sequents, $\Gamma_0, \dots, \Gamma_{n-1}$, which are called the *premisses* of the
²⁰ inference
- ²¹ • A sequent Γ , which is called the *conclusion* of the inference

¹This small abuse of notation is nothing more than the usual set-theoretic convention of identifying an integer (or an ordinal) with the set of integers (or ordinals) that are smaller than it: $n = \{m \mid m < n\}$

2 Technical background

$$\begin{array}{c}
\frac{}{\vdash A, A^\perp} \text{(id)} \quad \frac{\vdash \Gamma, A \quad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta} \text{(cut)} \\
\\
\frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B} \text{(\otimes)} \quad \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \wp B} \text{(\wp)} \quad \frac{}{\vdash \mathbf{1}} \text{(\mathbf{1})} \quad \frac{\vdash \Gamma}{\vdash \Gamma, \perp} \text{(\perp)} \\
\\
\frac{\vdash \Gamma, A}{\vdash \Gamma, A \oplus B} \text{(\oplus_0)} \quad \frac{\vdash \Gamma, B}{\vdash \Gamma, A \oplus B} \text{(\oplus_1)} \quad \frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \& B} \text{(\&)} \quad \frac{}{\vdash \Gamma, \top} \text{(\top)}
\end{array}$$

Figure 2.1. MALL inference rules

- A partial function

$$\sigma: |\Gamma_0| + \dots + |\Gamma_{n-1}| \rightharpoonup |\Gamma| \times \mathcal{P}^*$$

where $|\Gamma_0| + \dots + |\Gamma_{n-1}|$ denotes the usual set-theoretic sum $\{0\} \times |\Gamma_0| \cup \dots \cup \{n-1\} \times |\Gamma_{n-1}|$. This function is called the *threading function*. It can equivalently be described by n partial functions

$$\sigma_0: |\Gamma_0| \rightharpoonup |\Gamma| \times \mathcal{P}^* \quad \dots \quad \sigma_{n-1}: |\Gamma_{n-1}| \rightharpoonup |\Gamma| \times \mathcal{P}^*$$

This inference is written

$$\frac{\Gamma_0 \quad \dots \quad \Gamma_{n-1}}{\Gamma}$$

- ¹ with the *threading function* σ generally left implicit.
- ² The inference rules of MALL are given on Figure 2.1.
- ³ For instance, the rule

$$\frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B} \text{(\otimes)}$$

- ⁴ should be understood, intuitively, as saying that for every lists of formulas Γ, Δ and
- ⁵ for every formulas A, B , whenever the sequents $\vdash \Gamma, A$ and $\vdash \Delta, B$ are true, so is
- ⁶ $\vdash \Gamma, \Delta, A \otimes B$.
- ⁷ This rule is in fact a short notation for something more precise and more general than
- ⁸ that.

Coming back to the rule (\otimes) above, what is implicit in it, as it is given above, is that in a (\otimes) inference, the function σ sends any position of formula in Γ or Δ in the premisses to the corresponding position in the conclusion and the empty path, sends the position of A in the first premiss on the position of $A \otimes B$ in the conclusion and the path \otimes_0 and sends the position of B in the second premiss on the position of $A \otimes B$ in the conclusion and the path \otimes_1 . On the other hand, the order of the formulas in the sequents is not imposed by the rule. For instance, this is a correct (\otimes) inference:

$$\frac{\vdash X \wp \bar{X}, X \quad \vdash X, Y, Z}{\vdash X \otimes Y, X \wp \bar{X}, X, Z} (\otimes)$$

with the implicit function

$$\begin{aligned}\sigma: \{0\} \times \{0, 1\} \cup \{1\} \times \{0, 1, 2\} &\rightharpoonup \{0, 1, 2, 3\} \times A_{\text{Fml}}^* \\ (0, 0) &\mapsto (1, \epsilon) \\ (0, 1) &\mapsto (0, \otimes_0) \\ (1, 0) &\mapsto (2, \epsilon) \\ (1, 1) &\mapsto (0, \otimes_1) \\ (1, 2) &\mapsto (3, \epsilon)\end{aligned}$$

¹ Here this function happens to be total. The possibility to be partial is used in the (cut) rule.

³ **Definition 6** (Proof tree). A *proof* for MALL is any finite proof tree built with these inference rules.

⁵ Here is an example:

Example 2.

$$\frac{\frac{\frac{\frac{\vdash \bar{X}, X}{\vdash \bar{X}, \bar{Y}, X} (\text{id}) \quad \frac{\vdash \bar{Y}, Y}{\vdash \bar{Y}, Y \oplus Z} (\oplus_0)}{\vdash \bar{X}, \bar{Y}, X \otimes (Y \oplus Z)} (\otimes)}{\vdash \bar{X} \wp \bar{Y}, X \otimes (Y \oplus Z)} (\wp)}{\vdash \bar{X} \wp \bar{Y} \& \bar{X} \wp \bar{Y}, X \otimes (Y \oplus Z)} (\&)}$$

⁶ One of the interests of the *threading functions* is that they can be composed.

2 Technical background

Definition 7 (composition of threading functions). If A, B, C are three sets and $\sigma: A \multimap B \times A_{\text{Fml}}^*$ and $\rho: B \multimap C \times A_{\text{Fml}}^*$ are two partial functions, we define their composite

$$\begin{aligned}\rho \circ \sigma: A &\multimap C \times A_{\text{Fml}}^* \\ a &\mapsto (c, v \cdot u) \quad \text{where } (b, u) = \sigma(a) \text{ and } (c, v) = \rho(b)\end{aligned}$$

- ¹ The interested reader may recognize the Kleisli category of the monad $_ \times A_{\text{Fml}}^*$ on Set,
- ² whose multiplication and unit are induced by the monoidal structure of A_{Fml}^* .

³ 2.1.2 Finite proof trees: μ MALL

- ⁴ In this section, we introduce the logic μ MALL [Baelde, 2012], its formulas and proofs,
- ⁵ which are finite sequent calculus proofs.

- ⁶ **μ MALL formulas** The grammar of formulas is obtained by extending the formulas of
- ⁷ MALL with two fixed-point connectives, μ and ν , denoting respectively least and greatest
- ⁸ fixed points of formulas.

- ⁹ Formulas of μ MALL are selected among a set of preformulas. Preformulas of μ MALL
- ¹⁰ are obtained by taking the usual formulas of MALL and adding two monadic second
- ¹¹ order binders, μ and ν :

Definition 8 (μ MALL preformulas).

$$A, B ::= X \mid A \otimes B \mid A \wp B \mid \mathbf{1} \mid \perp \mid A \oplus B \mid A \& B \mid \mathbf{0} \mid \top \mid \mu X A \mid \nu X A$$

- ¹² where X ranges over an infinite set of propositional variables.

- ¹³ The connectives μ and ν are binders and, as usual, preformulas are considered modulo
- ¹⁴ renaming of bound variables. For instance, $\nu X(X \otimes X)$ and $\nu Y(Y \otimes Y)$ denote the same
- ¹⁵ preformula.

- ¹⁶ **Definition 9** (μ MALL formulas). A formula is a closed preformula. We denote by
- ¹⁷ Fml the set of all formulas and we denote by \leq the usual subformula ordering between
- ¹⁸ formulas and preformulas.

- ¹⁹ **Definition 10** (μ MALL negation). An involutive negation \cdot^\perp is defined on every μ MALL
- ²⁰ preformula, inductively specified by:

$$\begin{array}{lll}(A \otimes B)^\perp = A^\perp \wp B^\perp & \mathbf{1}^\perp = \perp & X^\perp = X \\ (A \oplus B)^\perp = A^\perp \& B^\perp & \mathbf{0}^\perp = \top \\ & & (\mu X A)^\perp = \nu X A^\perp\end{array}$$

$$\frac{\vdash \Gamma, A[\mu X A[X]]}{\vdash \Gamma, \mu X A[X]} (\mu) \quad \frac{\vdash \Gamma, B \vdash B^\perp, A[B]}{\vdash \Gamma, \nu X A[X]} (\nu_{\text{inv}})$$

 Figure 2.2. μ MALL rules for μ and ν

$$\frac{\vdash \Gamma, A[\mu X A[X]]}{\vdash \Gamma, \mu X A[X]} (\mu) \quad \frac{\vdash \Gamma, B \vdash B^\perp, A[B]}{\vdash \Gamma, \nu X A[X]} (\nu_{\text{inv}})$$

 Figure 2.3. Threading functions for the (μ) and (ν_{inv}) rules of μ MALL

¹ **Example 3.** If A is any formula and $F = \nu X(\mu Y((A \otimes X) \wp Y))$ then $F^\perp = \mu X(\nu Y((A^\perp \wp X) \otimes Y))$.

³ **Remark 3.** It may be counterintuitive that $X^\perp = X$. Yet, in practice negation will only
⁴ be applied to formulas, which are closed preformulas. This simple hack allows us to avoid
⁵ the use of negative atoms \bar{X}, \bar{Y}, \dots . The fact that we have only positive atoms guarantees
⁶ in turn that bound variables can only appear in covariant position, thus avoiding the
⁷ need for a positivity condition when forming a fixed point formula.

⁸ In the presence of negative atoms, negation should be defined by:

$$X^\perp = \bar{X} \quad \bar{X}^\perp = X \\ (\mu X A[X])^\perp = \nu \bar{X} A[X]^\perp \quad (\nu X A[X])^\perp = \mu \bar{X} A[X]^\perp$$

⁹ which does not change its definition on closed formulas. For instance, in Example 3 we
¹⁰ would still have:

$$F^\perp = (\nu X(\mu Y((A \otimes X) \wp Y)))^\perp = \mu \bar{X}(\mu Y((A \otimes X) \wp Y))^\perp \\ = \mu \bar{X}(\nu \bar{Y}((A \otimes X) \wp Y)^\perp) = \mu \bar{X}(\nu \bar{Y}((A^\perp \wp \bar{X}) \otimes \bar{Y})) = \mu X(\nu Y((A^\perp \wp X) \otimes Y))$$

¹¹ **μ MALL inferences and proofs** The proofs for μ MALL are standard sequent calculus
¹² proofs, as described in Section 2.1.1. They are obtained by extending the inference
¹³ system for MALL, in Figure 2.1 with two rules. Those rules reflect the definitions of
¹⁴ least and greatest fixed points of non-decreasing function on ordered sets that we gave in
¹⁵ Section 1.1.1.

¹⁶ **Definition 11.** The set of rules of the sequent calculus μ MALL is the union of the rules
¹⁷ for MALL, given in Figure 2.1 and of the two rules given in Figures 2.2 and 2.3.

$$\frac{\vdash \Gamma, A[\mu X A[X]]}{\vdash \Gamma, \mu X A[X]}_{(\mu)} \quad \frac{\vdash \Gamma, A[\nu X A[X]]}{\vdash \Gamma, \nu X A[X]}_{(\nu)}$$

Figure 2.4. μMALL^∞ rules for μ and ν

$$\frac{\vdash \Gamma, A[\mu X A[X]]}{\vdash \Gamma, \mu X A[X]}_{(\mu)} \quad \frac{\vdash \Gamma, A[\nu X A[X]]}{\vdash \Gamma, \nu X A[X]}_{(\nu)}$$

Figure 2.5. Threading functions for the (μ) and (ν) rules of μMALL^∞

- ¹ *Remark 4.* As it was mentionned in the informal introduction, in Section 1.2.2, the (ν_{inv}) rule of μMALL sequent calculus breaks the subformula property. Indeed, the B and B^\perp that appears in the premisses of the rule, on Figure 2.2, do not appear in its conclusion.
- ² This means that anyone wanting to prove a ν formula by applying that rule has to find
- ³ an appropriate B , which will act as an induction or coinduction invariant.

⁶ 2.1.3 Infinite proof trees: μMALL^∞

- ⁷ μMALL^∞ [Baelde, Doumane, and Saurin, 2016, Doumane, 2017] is a non well-founded
- ⁸ proof system for an extension of MALL with least and greatest fixed points operators. It
- ⁹ was designed to fix the defects of the (ν_{inv}) rule of μMALL .

- ¹⁰ **Definition 12.** The formulas of μMALL^∞ are the same as the formulas of μMALL , in
- ¹¹ the previous section.

- ¹² **Inference rules for μMALL^∞ .** The proofs for μMALL^∞ will be defined as infinite, non
- ¹³ well-founded proof trees. They are built out of a set of inference rules, which is given in
- ¹⁴ the following definition.

- ¹⁵ **Definition 13 (μMALL^∞ inference rules).** The set of inference rules for μMALL^∞ is the
- ¹⁶ union of the rules for MALL, given in Figure 2.1 and of the two rules given in Figures 2.4
- ¹⁷ and 2.5.

¹ **Preproofs for μMALL^∞ .** Proofs for μMALL^∞ are selected among a set of preproofs,
² which are potentially infinite objects, defined by allowing ordinary proof trees (Definition 6)
³ to be infinite.

⁴ **Definition 14** (μMALL^∞ preproofs). A preproof for μMALL^∞ is any proof tree, finite
⁵ or infinite, built with the inferences for μMALL^∞ given in Definition 13.

⁶ **Example 4.** Let $F = \mu X \nu Y (X \wp Y)$ et $G = \nu Y \mu X (X \wp Y)$. The following are two
⁷ μMALL^∞ preproofs.

$$\begin{array}{c} \pi_1 \\ \vdash \nu XX, \mu X(X \wp G), \mu XX \quad \vdash \nu XX, \mu X(X \wp G), \mu XX \\ \hline \vdash \nu XX, \mu X(X \wp G), \mu XX \quad \vdash \nu XX, G, \mu XX \\ \hline \vdash \nu XX, \mu X(X \wp G), G, \mu XX \\ \hline \vdash \nu XX, \mu X(X \wp G) \wp G, \mu XX \\ \hline \vdash \nu XX, \mu X(X \wp G), \mu XX \end{array} \quad \begin{array}{c} \pi_1 \\ \vdash \nu XX, \mu X(X \wp G), \mu XX \quad \vdash \nu XX, G, \mu XX \\ \hline \vdash \nu XX, G, \mu XX \end{array} \quad \text{(2.1)}$$

$$\begin{array}{c} \pi_2 \\ \vdash \nu XX, \nu Y(F \wp Y), \mu XX \\ \hline \vdash \nu XX, F, \mu XX \\ \hline \vdash \nu XX, F, \mu XX \quad \vdash \nu XX, \nu Y(F \wp Y), \mu XX \\ \hline \vdash \nu XX, F, \nu Y(F \wp Y), \mu XX \\ \hline \vdash \nu XX, F \wp \nu Y(F \wp Y), \mu XX \\ \hline \vdash \nu XX, \nu Y(F \wp Y), \mu XX \end{array} \quad \begin{array}{c} \pi_2 \\ \vdash \nu XX, \nu Y(F \wp Y), \mu XX \quad \vdash \nu XX, \nu Y(F \wp Y), \mu XX \\ \hline \vdash \nu XX, \nu Y(F \wp Y), \mu XX \end{array} \quad \text{(2.2)}$$

¹⁰ **Remark 5** (Inconsistency of preproofs). Any μMALL sequent is the conclusion of a
¹¹ μMALL^∞ preproof. More precisely, for any sequent Γ , the following is a μMALL^∞
¹² preproof:

$$\frac{\vdots \quad \vdots}{\vdash \Gamma, \nu XX} \quad \frac{\vdash \mu XX}{\vdash \mu XX} \quad \frac{\vdash \Gamma, \nu XX \quad \vdash \mu XX}{\vdash \mu XX} \quad \frac{\vdash \Gamma, \nu XX \quad \vdash \mu XX}{\vdash \Gamma} \quad \text{(cut)}$$

2 Technical background

¹ **Proofs and validity for μMALL^∞** The validity criterion used to distinguish proofs
² among preproofs will be given in Definition 31 and can be stated as: “every infinite
³ branch must contain a valid thread”. To make this formal, we will first define how a
⁴ preproof induces two graphs and then define the “branches” and “threads” of a preproof
⁵ as infinite paths in these graphs.

⁶ **Definition 15** (thread of an infinite branch of a preproof). Given an infinite branch β
⁷ of a preproof π , we define the set of threads of β as follows. A thread in β is a sequence
⁸ $(s_n)_{n \in \mathbf{N}}$ of positions of formulas in π such that:

- ⁹ • each s_n belongs to a sequent of β
- ¹⁰ • $\forall n \in \mathbf{N}$, s_n is the immediate descendant of s_{n+1} in β , according to the threading
¹¹ functions of β .

¹² The following lemma is the key to the notion of a valid thread, which is defined right
¹³ after it. If s is a position of formula in a proof tree, we denote by $\text{fml}(s) \in \text{Fml}$ the
¹⁴ associated formula.

¹⁵ **Definition 16.** If $t = (s_n)_{n \in \mathbf{N}}$ is an infinite thread in a preproof, we define $\inf(t) =$
¹⁶ $\{A \in \text{Fml} \mid \forall n_0 \in \mathbf{N}, \exists n \geq n_0, s_n \text{ is principal and } \text{fml}(s_n) = A\}$ i.e. the set of formulas
¹⁷ that are infinitely often principal in t .

¹⁸ **Definition 17** (Valid thread). An infinite thread t is *valid* if $\inf(t)$ has a minimum, with
¹⁹ respect to the subformula ordering, and this minimum is a ν -formula.

²⁰ **Definition 18** (proofs). We say that an infinite branch b of a preproof ϖ is valid if there
²¹ is a valid infinite thread t on b .

²² A μMALL^∞ preproof ϖ is a proof if all its infinite branches are valid.

²³ 2.1.4 Finite proof trees with back-edges: μMALL^ω

²⁴ The aim of μMALL^ω is to have a system of finite proofs, as in μMALL , with only the rules
²⁵ of fixed point unfolding instead of a rule with an explicit invariant, as in μMALL^∞ .

²⁶ As well as in μMALL^∞ , proofs of μMALL^ω are selected among a set of preproofs.
²⁷ Preproofs of μMALL^ω are circular objects, defined by adding back-edges to ordinary
²⁸ proof trees.

¹ **Definition 19** (μMALL^ω formulas). The formulas of μMALL^ω are the same as the
² formulas of μMALL and μMALL^∞ (Definition 9).

³ **Definition 20** (Proof tree with open sequents). A *proof tree with open sequents* is a
⁴ proof tree in which it is not mandatory for a sequent to be the conclusion of a logical
⁵ inference. Those positions of sequents that are not the conclusion of a logical inference
⁶ are called *positions of open sequents*. The other positions are called *positions of closed*
⁷ *sequents*.

⁸ **Definition 21** (lower, closer to the root). Whenever v, v' are two vertices of a tree, we
⁹ say that v is *lower* than v' , or that v is *below* v' , or that v is *closer to the root* than v'
¹⁰ when v appears on the path from v' to the root.

¹¹ The following definition aims at defining some representation for the fragment of all
¹² μMALL^∞ preproofs that are regular, that is those that have only a finite number of
¹³ subtrees up to isomorphism.

¹⁴ **Definition 22** ($\Pi_0(\mu\text{MALL}^\omega)$: μMALL^ω b.e.-tree preproofs). A *μMALL^ω b.e.-tree pre-*
¹⁵ *proof* consists of a finite proof tree with open sequents π (Def. 20), composed using the
¹⁶ rules of μMALL^∞ given above in Def. 13, together with a function **back**, which associates
¹⁷ to each *position s of an open sequent* in π , a position **back**(s) of the same sequent in π ,
¹⁸ such that **back**(s) is strictly *below* s in π , i. e. between s and the root. We denote by
¹⁹ $\Pi_0(\mu\text{MALL}^\omega)$ the set of all μMALL^ω b.e.-tree preproofs.

²⁰ We will sometimes say simply preproof instead of b.e.-tree preproof, or circular preproof
²¹ representation.

²² **Example 5.** Let π be the following proof tree, with three *open sequents*, and let us
²³ denote by s_0, \dots, s_8 the positions of its sequents, as indicated:

$$\frac{\frac{s_4: \vdash \nu X(X \wp X), \mu XX \quad s_5: \vdash \nu XX, \nu X(X \wp X), \mu XX}{\frac{s_3: \vdash \nu X(X \wp X), \nu X(X \wp X), \mu XX}{\frac{s_2: \vdash \nu X(X \wp X) \wp \nu X(X \wp X), \mu XX}{\frac{s_1: \vdash \nu X(X \wp X), \mu XX}{s_0: \vdash \nu X(X \wp X)}}}}{(v)} \quad \frac{s_8: \vdash \nu XX}{\frac{s_7: \vdash \nu XX}{(v)}} \quad (\text{cut})$$

²⁴ then $(\pi, \{s_4 \mapsto s_1, s_6 \mapsto s_5, s_8 \mapsto s_7\})$ is a *μMALL^ω b.e.-tree preproof*, that we will more

2 Technical background

¹ simply denote by:

$$\begin{array}{c}
 \boxed{\vdash \nu X(X \wp X), \mu XX} \quad \frac{\vdash \nu XX, \nu X(X \wp X), \mu XX}{\vdash \nu XX, \nu X(X \wp X), \mu XX \xleftarrow{(\nu)} \text{(cut)}} \\
 \frac{\vdash \nu X(X \wp X), \nu X(X \wp X), \mu XX}{\vdash \nu X(X \wp X) \wp \nu X(X \wp X), \mu XX \xrightarrow{(\wp)} \text{(wp)}} \\
 \frac{\vdash \nu X(X \wp X) \wp \nu X(X \wp X), \mu XX}{\vdash \nu X(X \wp X), \mu XX \xrightarrow{(\nu)} \text{(wp)}} \\
 \frac{}{\vdash \nu X(X \wp X)} \xrightarrow{(\nu)} \text{(cut)}
 \end{array}$$

² The validity criterion that will be used to distinguish μMALL^ω proofs among preproofs
³ is the same as in μMALL^∞ . We simply have to adapt the formalism to be able to talk
⁴ about infinite branches and infinite threads of a finite circular representation. We will first
⁵ define how a preproof induces two graphs and then define the “branches” and “threads”
⁶ of a preproof as infinite paths in these graphs.

⁷ **Definition 23** (Graph). In the following definitions, a “*graph*” always means a directed
⁸ pseudograph, *i.e.* a directed graph which may have loops and in which there may be
⁹ several edges between any pair of vertices.

¹⁰ **Definition 24** (G_{branch} , branch graph of a preproof). Let (π, back) be a μMALL^ω
¹¹ b.e.-tree preproof. Its *branch graph* is the graph G_{branch} defined as follows. The vertices of
¹² G_{branch} are the positions of closed sequents in π . For each inference I with conclusion s
¹³ in π and for each premise s' of I , there is an edge in G_{branch} , from s to s' if s' is a *closed*
¹⁴ position of sequent in π , and from s to $\text{back}(s')$ if s' is an *open position of sequent* in π .

¹⁵ **Definition 25** (Infinite branch). If (π, back) is a b.e.-tree preproof and G_{branch} is its
¹⁶ branch graph, we call an *infinite branch* of this preproof any infinite path in G_{branch}
¹⁷ starting from the root of π .

¹⁸ To clarify the following definitions, remember that in every proof tree π , for every inference
¹⁹ I in π , every position of formula α in a premise of I has a unique immediate descendent
²⁰ in the conclusion of I , except if I is a cut and α is a cut formula, in which case α has no
²¹ immediate descendent.

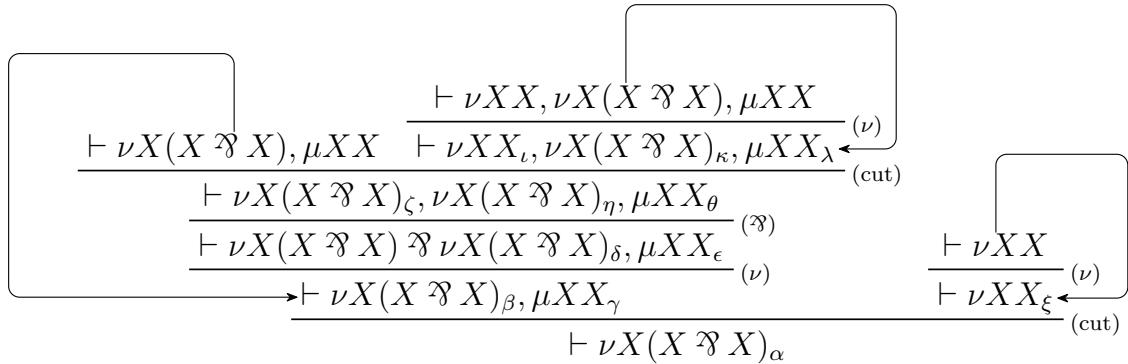
²² **Example 6.** The infinite branches of the preproof of Example 5 are $s_0(s_7)^\omega$, $s_0(s_1 s_2 s_3)^\omega$
²³ and all elements of $\{s_0(s_1 s_2 s_3)^k (s_5)^\omega \mid k \in \mathbf{N}\}$.

- ¹ Note that, in order to be totally rigorous, we should not only give the vertices of the
² paths but also the edges, *i.e.* when an inference has several premises, indicate explicitly
³ which one was chosen. These details are omitted here for concision; they will cause no
⁴ ambiguity on the validity of the preproof of Example 5.

⁵ **Definition 26** ($G_{\text{thread}}^{\text{out}}$, thread graph of a preproof). Let (π, \mathbf{back}) be a μMALL^ω b.e.-
⁶ tree preproof. Its thread graph is the graph $G_{\text{thread}}^{\text{out}}$ defined as follows. The vertices of
⁷ $G_{\text{thread}}^{\text{out}}$ are the positions of formulas in the closed sequents of π . For each inference I with
⁸ conclusion s in π , for each premise s' of I and for each position of formula β in s' which
⁹ has an immediate descendent α in s , there is an edge in $G_{\text{thread}}^{\text{out}}$, from α to β if s' is a
¹⁰ closed position of sequent in π , and from α to the position of the formula corresponding
¹¹ to β in $\mathbf{back}(s')$ if s' is an open position of sequent in π .

¹² **Definition 27** (thread). A *thread* in a b.e.-tree preproof is simply a path (finite or
¹³ infinite) in $G_{\text{thread}}^{\text{out}}$.

¹⁴ **Example 7.** Let us denote by $\{\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \eta, \theta, \iota, \kappa, \lambda, \xi\}$ the vertices of $G_{\text{thread}}^{\text{out}}$ for the
¹⁵ preproof shown on Example 5, as indicated here:



¹⁶ The maximal threads of this preproof, that is those that cannot be extended in any
¹⁷ direction, are $(\xi)^\omega, \gamma\epsilon\theta(\lambda)^\omega, (\iota)^\omega, \alpha(\beta\delta\zeta)^\omega$ and the elements of $\{\alpha(\beta\delta\zeta)^k\beta\delta\eta(\kappa)^\omega \mid k \in \mathbb{N}\}$.

¹⁸ Once again, in order to be totally rigorous, we should explicitly include the explicit choice
¹⁹ of a descendent relation, in cases where a position has several immediate ancestors.

²⁰ **Definition 28** ($\mathbf{U}: G_{\text{thread}}^{\text{out}} \rightarrow G_{\text{branch}}$). For any b.e.-tree preproof, there is an obvious
²¹ graph morphism from $G_{\text{thread}}^{\text{out}}$ to G_{branch} , associating to every position of a formula the
²² sequent position it belongs to. We denote this graph morphism by \mathbf{U} . If t is a path in
²³ $G_{\text{thread}}^{\text{out}}$ (*i.e.* an outer thread), we will also denote by $\mathbf{U}(t)$ the corresponding path in
²⁴ G_{branch} .

2 Technical background

¹ **Example 8.** The images, by the morphism of Definition 28, of the threads of Example 7
² are, with the notations of Example 5:

$$\begin{aligned}\mathbf{U}((\xi)^\omega) &= (s_7)^\omega & \mathbf{U}(\gamma\epsilon\theta(\lambda)^\omega) &= s_1s_2s_3(s_5)^\omega & \mathbf{U}((\iota)^\omega) &= (s_5)^\omega \\ \mathbf{U}(\alpha(\beta\delta\zeta)^\omega) &= s_0(s_1s_2s_3)^\omega & \forall k \in \mathbf{N}, \mathbf{U}(\alpha(\beta\delta\zeta)^k\beta\delta\eta(\kappa)^\omega) &= s_0(s_1s_2s_3)^{k+1}(s_5)^\omega\end{aligned}$$

³ The definition of a valid thread is then the same as in μMALL^∞ :

⁴ **Definition 29.** If $t = (s_n)_{n \in \mathbf{N}}$ is an infinite thread in a b.e.-tree preproof, we define
⁵ $\inf(t) = \{A \in \text{Fml} \mid \forall n_0 \in \mathbf{N}, \exists n \geq n_0, s_n \text{ is principal and } \text{fml}(s_n) = A\}$ i. e. the set of
⁶ formulas that are infinitely often principal in t .

⁷ **Definition 30** (Valid thread). An infinite thread t is *valid* if $\inf(t)$ has a minimum, with
⁸ respect to the subformula ordering, and this minimum is a ν -formula.

⁹ **Example 9.** Among the threads of Example 7:

- ¹⁰ • $(\xi)^\omega$ is valid: its smallest infinitely principal formula is νXX , which is principal at
¹¹ ξ ;
- ¹² • $(\iota)^\omega$ is valid: its smallest infinitely principal formula is νXX , which is principal at
¹³ ι ;
- ¹⁴ • $\alpha(\beta\delta\zeta)^\omega$ is valid: its smallest infinitely principal formula is $\nu X(X \wp X)$, which is
¹⁵ principal at β ;
- ¹⁶ • $\gamma\epsilon\theta(\lambda)^\omega$ is not valid: it has no principal formula;
- ¹⁷ • $\forall k \in \mathbf{N}, \alpha(\beta\delta\zeta)^k\beta\delta\eta(\kappa)^\omega$ is not valid: it has no principal formula after the last
¹⁸ position of β .

¹⁹ **Definition 31** (proofs). We say that an infinite branch b of a b.e.-tree preproof ϖ is
²⁰ valid if there is a valid infinite thread t of ϖ such that $\mathbf{U}(t)$ is a suffix of b .

²¹ A μMALL^ω b.e.-tree preproof ϖ is a *proof* if all its infinite branches are valid.

²² We denote by $\Pi(\mu\text{MALL}^\omega)$ the set of all μMALL^ω b.e.-tree proofs and we denote by
²³ $\overline{\Pi(\mu\text{MALL}^\omega)}$ its complement in $\Pi_0(\mu\text{MALL}^\omega)$, i. e. the set of all invalid b.e.-tree preproofs.

²⁴ **Example 10.** The preproof of Example 5 is a proof:

- ¹ • the branch $s_0(s_7)^\omega$ contains the valid thread $(\xi)^\omega$;
- ² • the branch $s_0(s_1s_2s_3)^\omega$ contains the valid thread $(\beta\delta\zeta)^\omega$;
- ³ • $\forall k \in \mathbf{N}$, the branch $s_0(s_1s_2s_3)^k(s_5)^\omega$ contains the valid thread $(\iota)^\omega$.

⁴ Link between circular representations and infinite preproofs

⁵ To every μMALL^ω b.e.-tree preproof ϖ is associated a canonical μMALL^∞ preproof
⁶ $\llbracket \varpi \rrbracket_\infty$. The finite circular preproof ϖ may then be seen as a finite representation of the
⁷ infinite preproof $\llbracket \varpi \rrbracket_\infty$.

⁸ Without going into too much details, we give an explanation of how to define the
⁹ transformation $\llbracket \cdot \rrbracket_\infty$. We first define a process F of expansion of a circular preproof.
¹⁰ Let ϖ be a circular preproof. We construct $F(\varpi)$ as follows. We say that a back-edge b
¹¹ is minimal in ϖ if the position of its target is minimal, meaning that no other back-edge
¹² has a target strictly closer to the root of ϖ . For every minimal back-edge b of ϖ , we
¹³ substitute, in place of the source of b , the whole subtree of ϖ rooted at the target of b ,
¹⁴ including its back-edges. This gives us $F(\varpi)$. Remark that the proof tree of ϖ is a strict
¹⁵ prefix of the proof tree of $F(\varpi)$ and that the greatest prefix of ϖ without any target of
¹⁶ back-edge is, again, strictly smaller than the greatest prefix of $F(\varpi)$ without any target
¹⁷ of back-edge. Said differently: the lowest target of back-edges in $F(\varpi)$ are strictly higher
¹⁸ than in ϖ . By iterating F on ϖ we then obtain a strictly increasing sequence of circular
¹⁹ preproofs, in which back-edges targets are higher and higher and in which the prefix of
²⁰ the proof tree which is free of all back-edge targets is increasing. $\llbracket \varpi \rrbracket_\infty$ is defined as the
²¹ limit of those prefixes: $\llbracket \varpi \rrbracket_\infty = \lim_{n \rightarrow \infty} F^n(\varpi)$, in a sense that can be made formal.

²² **Example 11.** Let us denote $A = \mu X \nu Y (X \otimes Y)$ and consider the following circular
²³ preproof:

$$\varpi = \boxed{\frac{\vdash A \quad \vdash \nu Y(A \otimes Y)}{\frac{\vdash A \otimes \nu Y(A \otimes Y)}{\frac{\vdash \nu Y(A \otimes Y) \xleftarrow{(\nu)}}{\xrightarrow{(\mu)} \vdash A}}^{(\otimes)}}$$

²⁴ then its first step of unfolding is

2 Technical background

$$\begin{array}{c}
\boxed{\frac{\vdash A \quad \vdash \nu Y(A \otimes Y)}{\vdash A \otimes \nu Y(A \otimes Y)}^{(\otimes)}} \\
\boxed{\frac{\vdash A \otimes \nu Y(A \otimes Y)}{\vdash \nu Y(A \otimes Y) \xleftarrow{(\mu)}}^{(\nu)}} \\
\frac{\vdash A \quad \vdash \nu Y(A \otimes Y)}{\vdash A \otimes \nu Y(A \otimes Y) \xrightarrow{(\otimes)} \vdash \nu Y(A \otimes Y) \xleftarrow{(\nu)}} \\
\frac{\vdash A \otimes \nu Y(A \otimes Y)}{\vdash \nu Y(A \otimes Y) \xleftarrow{(\mu)}}^{(\otimes)} \\
\frac{}{\vdash A}^{(\mu)}
\end{array}
\\
F(\varpi) =$$

¹ A second unfolding gives

$$\begin{array}{c}
\boxed{\frac{\vdash A \quad \vdash \nu Y(A \otimes Y)}{\vdash A \otimes \nu Y(A \otimes Y)}^{(\otimes)}} \\
\boxed{\frac{\vdash A \otimes \nu Y(A \otimes Y)}{\vdash \nu Y(A \otimes Y) \xleftarrow{(\mu)}}^{(\nu)}} \\
\frac{\vdash A \quad \vdash \nu Y(A \otimes Y)}{\vdash A \otimes \nu Y(A \otimes Y) \xrightarrow{(\otimes)} \vdash \nu Y(A \otimes Y) \xleftarrow{(\nu)}} \\
\frac{\vdash A \otimes \nu Y(A \otimes Y)}{\vdash \nu Y(A \otimes Y) \xleftarrow{(\mu)}}^{(\otimes)} \\
\frac{}{\vdash A}^{(\mu)}
\end{array}
\\
F^2(\varpi) =$$

² and, at the limit, we get the infinite preproof $\llbracket \varpi \rrbracket_\infty$ which is such that

$$\llbracket \varpi \rrbracket_\infty = \frac{\vdash \nu Y(A \otimes Y) \xleftarrow{(\mu)} \vdash A}{\vdash \nu Y(A \otimes Y) \xleftarrow{(\otimes)} \vdash \nu Y(A \otimes Y) \xleftarrow{(\nu)} \vdash A} \quad \text{with} \quad \pi = \frac{\vdash \llbracket \varpi \rrbracket_\infty \quad \vdash \nu Y(A \otimes Y)}{\vdash A \otimes \nu Y(A \otimes Y) \xrightarrow{(\otimes)} \vdash \nu Y(A \otimes Y) \xleftarrow{(\nu)} \vdash A}$$

- ³ The principal remark that can be made about this unfolding is that $F(\varpi)$, as a μ MALL $^\infty$ preproof, has the same branches as ϖ as a μ MALL $^\omega$ preproof. And each branch of $F(\varpi)$ has the same threads as the corresponding branch of ϖ . Hence, $F(\varpi)$ is valid as a

¹ μMALL^∞ preproof iff. ϖ is valid as a μMALL^ω preproof. Or: $F(\varpi)$ is a μMALL^∞ proof iff. ϖ is a μMALL^ω proof. This is no coincidence and that remark is the origin of our formulation of the thread criterion for finite, circular representations.

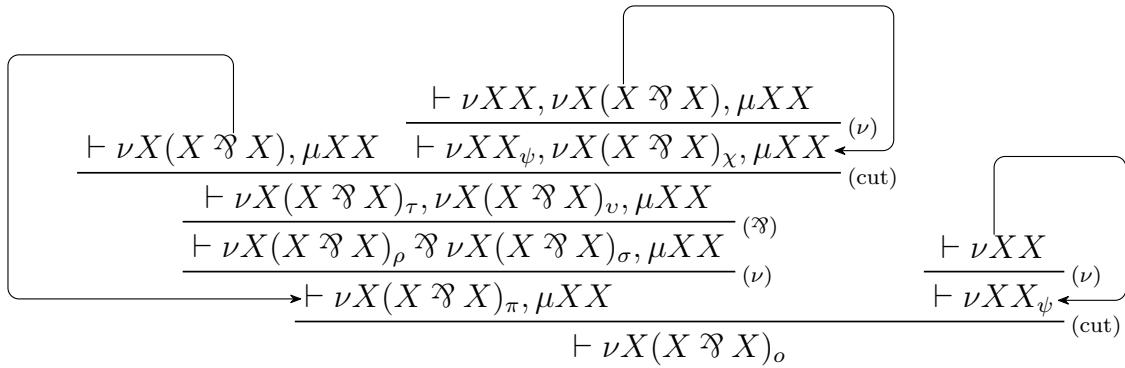
⁴ The second natural remark is that this induces an equivalence on circular preproofs: ϖ and ϖ' can be seen as representing the same infinite preproof when $F(\varpi) = F(\varpi')$. By ⁵ the previous remark, this equivalence relation is compatible with thread-validity.

⁷ **Inner threads**

⁸ **Definition 32** ($G_{\text{thread}}^{\text{in}}$, inner thread graph of a preproof). Let (π, \mathbf{back}) be a μMALL^ω
⁹ **b.e.-tree preproof**. Its inner thread graph is the graph $G_{\text{thread}}^{\text{in}}$ defined as follows. The
¹⁰ vertices of $G_{\text{thread}}^{\text{in}}$ are the positions of ν -subformulas in the **closed sequents** of π . For
¹¹ each inference I with conclusion s in π , for each premise s' of I , for each position of
¹² formula β_0 in s' which has an **immediate descendent** α_0 in s and for each position of
¹³ ν -subformula β in β_0 , whose **image** in α_0 is denoted α , there is an edge in $G_{\text{thread}}^{\text{in}}$, from α
¹⁴ to β if s' is a **closed position of sequent** in π , and from α to the position of the subformula
¹⁵ corresponding to β in $\mathbf{back}(s')$ if s' is an **open position of sequent** in π .

¹⁶ **Definition 33** (Inner thread). An **inner thread** in a b.e.-tree preproof is simply a path
¹⁷ (finite or infinite) in $G_{\text{thread}}^{\text{in}}$.

¹⁸ **Example 12.** Let us denote by $\{o, \pi, \rho, \sigma, \tau, v, \phi, \chi, \psi\}$ the vertices of $G_{\text{thread}}^{\text{in}}$ for the
¹⁹ preproof shown on Example 5, as indicated here:



²⁰ The maximal inner threads of this preproof are $(\psi)^\omega$, $(\psi)^\omega$, $o(\pi\rho\tau)^\omega$ and the elements of
²¹ $\{o(\pi\rho\tau)^k \pi\sigma v (\chi)^\omega \mid k \in \mathbf{N}\}$.

²² **Definition 34 (out: $G_{\text{thread}}^{\text{in}} \rightarrow G_{\text{thread}}^{\text{out}}$)**. For any b.e.-tree preproof, there is an obvious
²³ graph morphism from $G_{\text{thread}}^{\text{in}}$ to $G_{\text{thread}}^{\text{out}}$, associating to every position of subformula the

2 Technical background

- ¹ position of formula it belongs to. We denote this graph morphism by **out**. If t is a path
² in $G_{\text{thread}}^{\text{in}}$ (*i. e.* an **inner thread**), we will also denote by $\mathbf{out}(t)$ the corresponding path in
³ $G_{\text{thread}}^{\text{out}}$ (*i. e.* the correponding **thread**).

Example 13. The images, by the morphism of Definition 34, of the inner threads of Example 12 are, with the notations of Example 7:

$$\begin{aligned}\mathbf{out}((\psi)^\omega) &= (\mu)^\omega & \mathbf{out}((\psi)^\omega) &= (\iota)^\omega & \mathbf{out}(o(\pi\rho\tau)^\omega) &= \alpha(\beta\delta\zeta)^\omega \\ \forall k \in \mathbf{N}, \mathbf{out}(o(\pi\rho\tau)^k \pi\sigma v(\chi)^\omega) &= \alpha(\beta\delta\zeta)^k \beta\delta\eta(\kappa)^\omega\end{aligned}$$

- ⁴ **Definition 35** (Valid inner thread). An infinite inner thread $t = (s_n)_{n \in \mathbf{N}}$ is **valid** if
⁵ $\forall n_0 \in \mathbf{N}, \exists n \geq n_0, s_n$ is principal.

- ⁶ **Example 14.** Among the inner threads of Example 12:

- ⁷ • $(\psi)^\omega$ is valid: ψ is principal;
- ⁸ • $(\psi)^\omega$ is valid: ψ is principal;
- ⁹ • $o(\pi\rho\tau)^\omega$ is valid: π is principal;
- ¹⁰ • $\forall k \in \mathbf{N}, o(\pi\rho\tau)^k \pi\sigma v(\chi)^\omega$ is not valid: χ is not principal and it has no principal
¹¹ vertex after the last π .

- ¹² **Proposition 2** (Equivalence between the two definitions of valid infinite threads).

- ¹³ 1. *If t is a valid infinite inner thread then $\mathbf{out}(t)$ is a valid infinite thread.*
- ¹⁴ 2. *If u is a valid infinite thread then there is a unique valid infinite inner thread t such that $u = \mathbf{out}(t)$.*

- ¹⁶ *Proof.*

- ¹⁷ t **valid** \Rightarrow $\mathbf{out}(t)$ **valid** First remark that if A is a **formula** (*i. e.* closed) then the **images**
¹⁸ or **preimages** of any of its positions along any **descendent relation** are still positions
¹⁹ of A . Now, if $t = (s_n)_{n \in \mathbf{N}}$ is an **inner thread**, let us denote by $\mathbf{fml}(t) = \mathbf{fml}(s_0)$.
²⁰ Then $\forall n \in \mathbf{N}, \mathbf{fml}(s_n) = \mathbf{fml}(t)$. Because t is valid, this $\mathbf{fml}(t)$ is a ν -formula.
²¹ Each sequent position at which t is principal is also a position at which $\mathbf{fml}(t)$ is
²² principal in $\mathbf{out}(t)$, $\mathbf{fml}(t)$, hence $\mathbf{fml}(t)$ is infinitely principal in $\mathbf{out}(t)$. Finally,
²³ $\mathbf{fml}(t)$ is the smallest formula of $\mathbf{out}(t)$ because it is a subformula of every formula
²⁴ of $\mathbf{out}(t)$. Conclusion: $\mathbf{out}(t)$ is a valid infinite thread.

1 **Converse** if $t \in G_{\text{thread}}^{\text{out}}$ is valid, let $\nu X A$ be its validating formula, let $t = t_0 t_1 t_2 \dots$, let i_n
2 be the sequence of all i such that t_i is a principal position of $\nu X A$. If $i_n < i < i_{n+1}$,
3 we define u_i as the image of $t_{i_{n+1}}$ in t_i . Then $u = (u_i)_i$ is a valid inner thread such
4 that $\text{out}(u) = t$. It is easy to see that it is the only one, thanks to the following
5 lemma.

6 □

7 **Lemma 1.** *The positions of $\sigma X A[X]$ in $A[\sigma X A[X]]$ are exactly the positions of X in
8 $A[X]$.*

9 *Proof.* Otherwise, $\sigma X A[X]$ would be a subformula of $A[X]$, which is impossible. □

10 **Example 15.** The preproof of Example 5 is a proof:

- 11 • the branch $s_0(s_7)^\omega$ contains the valid inner thread $(\psi)^\omega$;
- 12 • the branch $s_0(s_1 s_2 s_3)^\omega$ contains the valid inner thread $(\pi\rho\tau)^\omega$;
- 13 • $\forall k \in \mathbf{N}$, the branch $s_0(s_1 s_2 s_3)^k(s_5)^\omega$ contains the valid inner thread $(\psi)^\omega$.

14 2.2 Complexity theory

15 2.2.1 Generalities on complexity and PSPACE

16 We give here a brief and somewhat informal recall of the essential notions of algorithmic
17 complexity that we will need in the thesis. For an in-depth perspective on that subject,
18 see, for instance, [Arora and Barak, 2009]. If you understand French, you may also read
19 the excellent book by Perifel [2014].

20 In particular we do not go here into the choice and definition of a precise model of
21 computation. All programs are considered deterministic. We assume that the inputs and
22 outputs of programs contain at least $\{0, 1\}^*$, the finite words on $\{0, 1\}$, and that there
23 is a pairing operation which allows to combine two entries x and y into a single one
24 (x, y) .

25 **Definition 36** (Notations). If f is a program and x an entry for this program, we denote
26 by $\|x\|$ the size of the entry x , we denote by $\text{time}(f, x)$ the execution time of f on x ,

2 Technical background

- ₁ which may be an integer or $+\infty$, and we denote by **space**(f, x) the memory space used
₂ by the execution of f on x , which may be an integer or $+\infty$.

₃ **Definition 37** (Problem, language). A *problem* or *language* is any subset of all possible
₄ program entries.

₅ **Definition 38.**

- ₆ • if $t: \mathbf{N} \rightarrow \mathbf{N}$ is a function, a language L is in $\text{DTIME}(t(n))$ if there is a program f
₇ such that

- ₈ – $\forall x \in L, f(x) = 1$
- ₉ – $\forall x \notin L, f(x) = 0$
- ₁₀ – $\exists \alpha > 0, \forall x, \mathbf{time}(f, x) \leq \alpha \cdot t(\|x\|)$

- ₁₁ • if $t: \mathbf{N} \rightarrow \mathbf{N}$ is a function, a language L is in $\text{DSPACE}(t(n))$ if there is a program
₁₂ f such that

- ₁₃ – $\forall x \in L, f(x) = 1$
- ₁₄ – $\forall x \notin L, f(x) = 0$
- ₁₅ – $\exists \alpha > 0, \forall x, \mathbf{space}(f, x) \leq \alpha \cdot t(\|x\|)$

₁₆ **Definition 39.**

- ₁₇ • **P** := $\bigcup_{k \in \mathbf{N}} \text{DTIME}(n^k)$
- ₁₈ • **EXP** := $\bigcup_{k \in \mathbf{N}} \text{DTIME}(2^{n^k})$
- ₁₉ • **PSPACE** := $\bigcup_{k \in \mathbf{N}} \text{DSPACE}(n^k)$
- ₂₀ • **NP** := $\{A \mid \exists p \text{ polynomial}, \exists B \in \mathbf{P}, \forall x, (x \in A \Leftrightarrow \exists y \in \{0, 1\}^{p(\|x\|)}, (x, y) \in B)\}$

Proposition 3.

$$\mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{PSPACE} \subseteq \mathbf{EXP}$$

¹ The strictness of each one of these inclusions is an open problem. Experts of the domain
² seem to believe that all these inclusions are in fact strict. We still know for sure that not
³ all of them can be equalities, as a consequence of Corollary 1 to Theorem 2 below.

⁴ **Definition 40.** A function $t: \mathbf{N} \rightarrow \mathbf{N}$ is *time-constructible* if there is a program f such
⁵ that

- ⁶ • $\forall n \in \mathbf{N}, f(1^n) = 1^{t(n)}$ (where 1^n is the word of length n made only of 1)
- ⁷ • $\exists \alpha > 0, \forall n \in \mathbf{N}, \text{time}(f, 1^n) \leq \alpha \cdot t(n)$

⁸ **Theorem 2** (Deterministic time hierarchy). *If $f, g: \mathbf{N} \rightarrow \mathbf{N}$ are two functions such that*

- ⁹ • $\forall n \in \mathbf{N}, f(n) > 0$
- ¹⁰ • g is *time-constructible*
- ¹¹ • $g(n) \gg f(n) \cdot \log(f(n))$

¹² then $\text{DTIME}(f(n)) \subsetneq \text{DTIME}(g(n))$.

Corollary 1.

$$\mathbf{P} \subsetneq \mathbf{EXP}$$

¹³ **Definition 41** (Polynomial-time many-one reduction). A *polynomial-time many-one*
¹⁴ *reduction* from a language B to a language A is a program f which runs in polynomial
¹⁵ time and such that $\forall x, x \in B \Leftrightarrow f(x) \in A$. If such a program exist, we say that B *reduces*
¹⁶ *to* A and we denote it by $B \leq A$.

Definition 42. A problem A is *PSPACE-complete* if A is in PSPACE and every PSPACE problem reduces to A . Equivalently, A is PSPACE-complete iff.

$$\forall B, B \in \text{PSPACE} \Leftrightarrow B \leq A$$

¹⁷ **Proposition 4.**

- ¹⁸ • A problem A is in PSPACE iff. its complement \overline{A} is in PSPACE.
- ¹⁹ • A problem A is PSPACE-complete iff. its complement \overline{A} is PSPACE-complete.

2 Technical background

1 *Proof.*

- 2 • Every $\text{DSPACE}(n^k)$ is closed under complement: if f recognizes A , \overline{A} is recognized
3 by $g(x) = 1 - f(x)$. Hence PSPACE is closed under complement.
- 4 • Suppose A is PSPACE -complete and B is PSPACE . We then show that B reduces to
5 \overline{A} . As B is PSPACE , so is \overline{B} . Hence there is a polynomial-time many-one reduction
6 f from \overline{B} to A . Then we show that f is also a reduction from B to \overline{A} . Indeed,
7 $\forall x, x \notin B \Leftrightarrow x \in \overline{B} \Leftrightarrow f(x) \in A$, and then $\forall x, x \in B \Leftrightarrow f(x) \notin A \Leftrightarrow f(x) \in \overline{A}$.

8

□

9 *Remark 6.* Although this will not be used in this thesis, we recall to the interested reader
10 that we also have $\text{PSPACE} = \text{NPSPACE} = \text{coNPSPACE}$ because of Savitch theorem.

11 2.2.2 Some PSPACE -complete problems

Definition 43 ($\text{BOOLE}_{\text{false}}$ and $\mathcal{B}_{\text{false}}$). A program in $\text{BOOLE}_{\text{false}}$ is a sequence of instructions $b = 1:I_1 \ 2:I_2 \ \dots \ m:I_m$ where an instruction can have one of the two following forms:

$$I ::= X := \neg X \mid \text{if } X \text{ then goto } \ell' \text{ else goto } \ell''$$

12 where X ranges over a finite set of variable names. The semantic is as expected, with all
13 variables being equal to `false` at the beginning of the program, and the program halting
14 when reaching instruction $m + 1$. Finally it is required of every program $b \in \text{BOOLE}_{\text{false}}$
15 that if b terminates then all variables have value *false* at the end of its execution.

We also denote the set of terminating programs as:

$$\mathcal{B}_{\text{false}} := \{b \in \text{BOOLE}_{\text{false}} \mid b \text{ terminates}\}$$

16 *Remark 7.* The constraint on the values of the variables at the end of the program
17 will be useful when reducing it, in Chapter 3, to the problem of validity of a μMALL^ω
18 b.e.-tree preproof. This preproof will encode the fact that the program b is terminating
19 by connecting the final state to the initial one, hence the necessity that its initial and
20 terminal states are the same.

21 **Lemma 2.** $\mathcal{B}_{\text{false}}$ is PSPACE -hard under LOGSPACE -reductions:

$$\text{PSPACE} \leqslant_L \mathcal{B}_{\text{false}}$$

¹ *Proof.* We reduce from the problem of termination for a more expressive language, which
² has been defined and proved PSPACE-complete by Jones in [Jones, 1997], under the
³ name of BOOLE. \square

⁴ 2.3 Parity automata

⁵ We recall here the basic definitions and property of parity automata. There are several
⁶ definitions of parity automata, all of which are equivalent. We chose a definition that
⁷ best suits our needs. For more informations on the subject of automata for infinite words,
⁸ see, for instance, [Grädel, Thomas, and Wilke, 2002] or [Perrin and Pin, 2004].

⁹ We denote by ω the set of natural integers, and we also denote by ω the first infinite
¹⁰ ordinal. We denote by $\omega + 1$ the set $\omega \cup \{\omega\}$, ordered by setting ω to be its maximum.
¹¹ The ordinal ω is considered even. All of that is consistent with usual set-theoretic
¹² conventions.

¹³ Given an alphabet A , we denote by A^ω the set of infinite words on A , that is the set of
¹⁴ sequences of elements of A , indexed by the integers.

¹⁵ **Definition 44** (Parity automaton). Given an alphabet A , a *parity automaton* on A
¹⁶ consists of

- ¹⁷ • a set Q of *states*;
- ¹⁸ • a subset $I \subseteq Q$ of *initial states*;
- ¹⁹ • a set $T \subseteq Q \times A \times (\omega + 1) \times Q$.

²⁰ Such a parity automaton is *finite* if A , Q and T are finite. In T , elements of $\omega + 1$ are
²¹ called *priorities*.

Definition 45. A *run*, or *path*, in a parity automaton \mathcal{A} is any infinite sequence

$$q_0 \xrightarrow{a_0/p_0} q_1 \xrightarrow{a_1/p_1} q_2 \xrightarrow{a_2/p_2} q_3 \dots$$

²² such that

- ²³ • $q_0 \in I$
- ²⁴ • $\forall n \in \omega, (q_n, a_n, p_n, q_{n+1}) \in T$

2 Technical background

- 1 If r is such a run, we denote by **label**(r) the infinite word $a_0a_1a_3\cdots \in A^\omega$.
- 2 **Definition 46.** Such a run r is *successful* in the parity automaton if there is a $p \in \omega + 1$ such that
 - 4 • p is odd (which implies $p \neq \omega$)
 - 5 • there are only finitely many $n \in \omega$ such that $p_n < p$
 - 6 • there are infinitely many $n \in \omega$ such that $p_n = p$
- 7 Equivalently : p is an odd priority and it is the smallest priority appering infinitely often in the run r .
- 9 **Definition 47** (Language of a parity automaton). The *language* of a parity automaton \mathcal{A} is the set $\mathcal{L}(\mathcal{A}) := \{\text{label}(p) \mid p \text{ is a successful run in } \mathcal{A}\}$.
- 11 And the main theorem that we will use is the following.
- 12 **Theorem 3.** *The problem of equality of languages for finite parity automata is decidable in polynomial space.*
- 14 *Proof.* We do not go into the details of this complex result. It relies on the fact that every parity automaton can be translated into an equivalent Büchi automaton with a polynomial increase of size, which is folklore, and on the fact that the problem of equality of languages for Büchi automata is decidable in polynomial space, which was proven by Sistla, Vardi, and Wolper [1987]. \square

¹ **3 PSPACE-completeness of the thread criterion**

²

³ As we explained in the introduction, the subject of this thesis is the study of finite
⁴ circular representations of infinite proofs and preproofs. In this context, the first question
⁵ arising is to distinguish, among circular representations of preproofs, those denoting valid
⁶ preproofs, *i. e.* proofs, from those denoting invalid preproofs.

⁷ It has already been shown by Doumane [2017] that this problem is decidable in PSPACE.
⁸ In the first section of this chapter, we recall the proof of this result, fixing a small omission
⁹ in Doumane’s proof at the same time.

¹⁰ The second section of this chapter is devoted to its main result: that the problem
¹¹ of deciding the validity of a circular representation of a μMALL^ω preproof is in fact
¹² PSPACE-complete. This result is established by a reduction from the problem of deciding
¹³ the termination of a boolean program.

Our proof takes a lot of inspiration from the proof of PSPACE-completeness of size-change termination by Lee, Jones and Ben Amram [Lee, Jones, and Ben-Amram, 2001]: in order to prove that deciding size-change termination is PSPACE-complete, they define a notion of boolean program and use the fact that the following set is complete in PSPACE:

$$\mathcal{B} = \{b \mid b \text{ is a boolean program and } b \text{ terminates.}\}$$

¹⁴ then they reduce \mathcal{B} to the problem of size-change termination. We adapt their method
¹⁵ by reducing \mathcal{B} to the problem of thread-validity in circular μMALL^ω preproof.

¹⁶ It would be very interesting to get a more precise understanding of the relation between
¹⁷ threads in circular proofs and size-change termination.

¹⁸ We show how our method adapts to other systems such as μLJ and μLK .

¹⁹ Rémi: référence à la section

3.1 Deciding thread validity in PSPACE

2 In this section, we recall that the problem of deciding whether the **circular representation**
 3 of a **preproof** is a valid **proof** is in PSPACE. Several algorithms can be used for deciding
 4 this problem in PSPACE. Here we reduce this problem to the problem of deciding equality
 5 of languages for **parity ω -automata**, which is known to be in PSPACE. See Section 2.3 of
 6 the technical background for more details on that. More precisely, given a **preproof** ϖ ,
 7 we define two **parity automata**: the language of the first one is the set of **infinite branches**
 8 of ϖ and the language of the second one is the set of **valid infinite branches** of ϖ .

9 We will immediately give two examples to show how the algorithm works.

10 Let $G := \nu Y \mu X (X \wp Y)$. The following preproof (3.1) is valid. The branches that
 11 ultimately always take the left back-edge are valid because of a thread going through
 12 $\nu X X$ and the branches that take infinitely often the right back-edge are valid because of
 13 a thread going through $\mu X (X \wp G)$ and G .

14

$$\begin{array}{c}
 \frac{\vdash \nu X X, \mu X (X \wp G), \mu X X}{\vdash \nu X X, \mu X (X \wp G), \mu X X}^{(\nu)} \quad \frac{\vdash \nu X X, \mu X (X \wp G), \mu X X}{\vdash \nu X X, G, \mu X X}^{(\nu)} \\
 \hline
 \frac{}{\vdash \nu X X, \mu X (X \wp G), G, \mu X X}^{(\wp)} \\
 \frac{\vdash \nu X X, \mu X (X \wp G), G, \mu X X}{\vdash \nu X X, \mu X (X \wp G) \wp G, \mu X X}^{(\wp)} \\
 \hline
 \vdash \nu X X, \mu X (X \wp G), \mu X X \leftarrow^{(\mu)}
 \end{array} \tag{3.1}$$

15 From this preproof, we build a first automaton, represented on Figure 3.1 p. 65, which
 16 recognizes the language of infinite branches of the preproof. It has one initial state and
 17 all paths are accepted. It recognizes the language $(abcd + abef)^\omega$.

And from the same preproof (3.1) we build a second automaton, represented on Figure 3.2,
 p. 66, which recognizes the language of valid infinite branches of the preproof (3.1). No
 priority indicated on an edge implicitly means ω , which is the highest non-accepting
 priority. There are four initial states, at the bottom of the automaton. Three edges have
 a priority $< \omega$

$$\nu X X \xrightarrow[1]{d} \nu X X \qquad G \xrightarrow[1]{f} \mu X (X \wp G) \qquad \mu X (X \wp G) \xrightarrow[2]{a} \mu X (X \wp G) \wp G$$

3.1 Deciding thread validity in PSPACE

It recognizes the language

$$\begin{aligned} & (abcd + abef)^*(abcd)^\omega + ((abcd)^*abef)^\omega \\ &= (abcd + abef)^\omega \end{aligned}$$

- ¹ Now let $F := \mu X \nu Y (X \wp Y)$. The following preproof (3.2), unlike the preproof (3.1), is
² not valid. The branches taking ultimately only the left back-edge are valid because of
³ a thread going through νXX , the branches taking ultimately only the right back-edge
⁴ are valid because of a thread going through $\nu Y(F \wp Y)$ but the branches which takes
⁵ infinitely often the left back-edge and infinitely often the right back-edge are not valid.

$$\begin{array}{c} \boxed{\vdash \nu XX, \nu Y(F \wp Y), \mu XX} \\ \hline \vdash \nu XX, F, \mu XX \quad (\mu) \\ \hline \boxed{\vdash \nu XX, F, \mu XX} \quad \vdash \nu XX, \nu Y(F \wp Y), \mu XX \quad (\nu) \\ \hline \vdash \nu XX, F, \nu Y(F \wp Y), \mu XX \quad (\text{cut}) \\ \hline \vdash \nu XX, F \wp \nu Y(F \wp Y), \mu XX \quad (\wp) \\ \hline \vdash \nu XX, \nu Y(F \wp Y), \mu XX \quad (\nu) \\ \hline \rightarrow \vdash \nu XX, \nu Y(F \wp Y), \mu XX \leftarrow \end{array} \quad (3.2)$$

- ⁶
- ⁷ The deduced automaton recognizing all infinite branches of preproof (3.2), is represented
⁸ on Figure 3.3, p. 67. It has one initial state. All paths are accepted. It recognizes the
⁹ language $(abcde + abf)^\omega$.

And the automaton of valid infinite branches of preproof (3.2) is represented on Figure 3.4,
 p. 68. It has 4 initial states. The only three transitions with priorities $< \omega$ are

$$\nu Y(F \wp Y) \xrightarrow[3]{a} F \wp \nu Y(F \wp Y) \quad \nu XX \xrightarrow[1]{d} \nu XX \quad F \xrightarrow[2]{e} \nu Y(F \wp Y)$$

It recognizes the language

$$\begin{aligned} & (abcde + abf)^*(abcde)^\omega + (abcde + abf)^*(abf)^\omega \\ &= (abcde + abf)^\omega \setminus ((abf)^*abcde(abcde)^*abf)^\omega \end{aligned}$$

- ¹⁰ We will now explain the procedure by which, in each case, those two automata were
¹¹ obtained.
- ¹² Let ϖ be a b.e.-tree preproof. Let G_{branch} be its branch graph, as defined in Definition 24.
¹³ Let $A := E_{\text{branch}}$ be the set of its edges. This will be the input alphabet of our automata.
- ¹⁴ The first ω -automaton is $\mathcal{A}_{\text{branch}} := (Q_{\text{branch}}, I_{\text{branch}}, T_{\text{branch}})$, where:

3 PSPACE-completeness of the thread criterion

- 1 • The set of states is $Q_{\text{branch}} := V_{\text{branch}}$, the set of vertices of G_{branch} , that is the set of closed positions of sequents in π .
- 2
- 3 • The set of initial states is the singleton $I := \{i_{\text{branch}}\}$, where i_{branch} is the position of the root of ϖ , that is the position of the conclusion sequent of ϖ .
- 4
- 5 • The set of transitions is

$$T_{\text{branch}} := \{ s \xrightarrow[1]{e} s' \mid e \text{ is an edge from } s \text{ to } s' \text{ in } G_{\text{branch}} \}$$

- 6 This amounts to saying that the accepted paths in $\mathcal{A}_{\text{branch}}$ are exactly the paths in G_{branch}
- 7 which start at the root of the proof tree. With that definition, the following lemma is
- 8 immediate:

9 **Lemma 3.** *The language $\mathcal{L}(\mathcal{A}_{\text{branch}})$ is the set of infinite branches of ϖ .*

- 10 For our second automaton, we need a priority assignment $\Omega: \text{Fml} \rightarrow \omega$. It will be used
- 11 to reflect the condition of validity of threads in the parity condition of our automata. We
- 12 need this priority assignment to have two main properties:

- 13 1. if A is a subformula of B then $\Omega(A) \leq \Omega(B)$;
- 14 2. $\forall A, \Omega(\mu X A)$ is even and $\Omega(\nu X A)$ is odd.

- 15 Remember that even priorities are rejecting and odd priorities are accepting (Definition 46).
- 16 Thus, those two properties reflect the condition of Definition 30.

Definition 48 ($\Omega: \text{Fml} \rightarrow \omega$). A function Ω is defined by induction, which associate a priority to every *preformula*:

$$\begin{aligned} \Omega(\nu X A) &:= \begin{cases} \Omega(A) & \text{if } \Omega(A) \text{ is odd} \\ \Omega(A) + 1 & \text{if } \Omega(A) \text{ is even} \end{cases} \\ \Omega(\mu X A) &:= \begin{cases} \Omega(A) & \text{if } \Omega(A) \text{ is even} \\ \Omega(A) + 1 & \text{if } \Omega(A) \text{ is odd} \end{cases} \\ \Omega(A \odot B) &:= \max\{\Omega(A), \Omega(B)\} && \text{for any binary connective } \odot \\ \Omega(\mathbf{c}) &:= 0 && \text{for any propositional constant } \mathbf{c} \\ \Omega(X) &:= 0 \end{aligned}$$

- 17 The following remarks are immediate:

¹ **Lemma 4.** For all formulas A and B :

- ² • $\Omega(\nu X A)$ is odd and $\Omega(\mu X A)$ is even.
- ³ • If A is a subformula of B then $\Omega(A) \leq \Omega(B)$.

⁴ Our second automaton is a **parity ω -automaton**, with priorities in $\omega + 1 = \omega \cup \{\omega\}$,
⁵ ω being even.¹ This second automaton is defined as $\mathcal{A}_{\text{thread}} = (Q_{\text{thread}}, I_{\text{thread}}, T_{\text{thread}})$,
⁶ where:

- ⁷ • the set of states is $Q_{\text{thread}} := V_{\text{thread}} + \{\perp_s \mid s \in V_{\text{branch}}\}$, i.e. the vertices of $G_{\text{thread}}^{\text{out}}$
⁸ plus one extra vertex for each vertex of G_{branch}
- ⁹ • If we keep the notation i_{branch} to denote the position of the endsequent of ϖ , the
¹⁰ set of initial states I_{thread} is the set of all positions of formulas in i_{branch} , plus the
¹¹ extra vertex $\perp_{i_{\text{branch}}}$.

¹² • the set of transitions is

$$\begin{aligned} T_{\text{thread}} := & \{ \perp_s \xrightarrow[\omega]{e} \perp_{s'} \mid e \text{ is an edge from } s \text{ to } s' \text{ in } G_{\text{branch}} \} \\ & \cup \{ \alpha \xrightarrow[\Omega(\alpha)]{\mathbf{U}(e)} \beta \mid e \text{ is an edge from } \alpha \text{ to } \beta \text{ in } G_{\text{thread}}^{\text{out}} \text{ and } \alpha \text{ is principal} \} \\ & \cup \{ \alpha \xrightarrow[\omega]{\mathbf{U}(e)} \beta \\ & \quad \mid e \text{ is an edge from } \alpha \text{ to } \beta \text{ in } G_{\text{thread}}^{\text{out}} \text{ and } \alpha \text{ is not principal} \} \\ & \cup \{ \perp_s \xrightarrow[\omega]{e} \alpha \\ & \quad \mid I \text{ is a (cut) inference in } \varpi, \\ & \quad s \text{ is the position of the conclusion sequent of } I, \\ & \quad s' \text{ is the position of a premise of } I, \\ & \quad e \text{ is an edge induced by } I \text{ in } G_{\text{branch}} \text{ from } s \text{ to } s' \\ & \quad \text{and } \alpha \text{ is the position of the corresponding cut-formula in } s' \} \end{aligned}$$

¹³ where $q \xrightarrow[i]{e} q'$ denote a transition from state $q \in Q_{\text{thread}}$ to state $q' \in Q_{\text{thread}}$ with
¹⁴ label $e \in A$ and priority $i \in \omega + 1$.

¹⁵ The acceptance condition is the one given in our definition of **parity automata** in
¹⁶ Definition 44: a run is accepted if the smallest priority appearing infinitely often is *odd*
¹⁷ (ω being even).

¹⁸ Once again, it should be clear from Definitions 17 and 18 that:

¹We use the usual set-theoretic convention that an ordinal is equal to the set of ordinals strictly below it: $\alpha = \{\beta \in \text{Ord} \mid \beta < \alpha\}$

3 PSPACE-completeness of the thread criterion

- ¹ **Lemma 5.** *The language $\mathcal{L}(\mathcal{A}_{\text{thread}})$ is the set of valid infinite branches of ϖ .*
- ² From these two lemmas it is immediate that
- ³ **Proposition 5.** *We have the inclusion $\mathcal{L}(\mathcal{A}_{\text{thread}}) \subseteq \mathcal{L}(\mathcal{A}_{\text{branch}})$ and the preproof ϖ is valid iff. this inclusion is an equality.*
- ⁵ Deciding this equality can be done in PSPACE (*c.f.* Theorem 3), and the constructions of these automata are obviously PSPACE, so:
- ⁷ **Proposition 6.** *The problem of deciding whether a μMALL^ω b.e.-tree preproof is valid is in PSPACE.*

⁹ 3.2 PSPACE-Completeness

¹⁰ 3.2.1 Outline of the PSPACE-Completeness Proof

- ¹¹ We now aim at proving that the problem of deciding the validity of a μMALL^ω b.e.-tree ¹² **preproof** is **PSPACE-complete**. As it is already known that this problem is in PSPACE, ¹³ it remains to prove that it is **PSPACE-hard**.

We follow the same methodology as Lee, Jones, and Ben-Amram [2001]: in order to prove that deciding size-change termination is PSPACE-complete, they define a notion of boolean program (see Definition 43) and use the fact that the following **problem** is PSPACE-complete:

$$\mathcal{B} = \{b \mid b \text{ is a boolean program and } b \text{ terminates.}\}$$

- ¹⁴ then they reduce \mathcal{B} to the decidability of size-change termination.
- ¹⁵ We try to adapt their method by reducing \mathcal{B} to $\Pi(\mu\text{MALL}^\omega)$.

¹⁶ 3.2.2 Defining the Reduction

- ¹⁷ We use the boolean programs that were defined in Definition 43. The following definition ¹⁸ will be used in the proof of Proposition 7:

¹ **Definition 49** (Call graph of a program). Assume a boolean program b with variables
² X_1, \dots, X_k and instructions $1 : I_1, \dots, m : I_m$. Define the call graph of b to be $G = (V, E)$
³ with

- ⁴ • $V = \{0, 1, \dots, m\}$
- ⁵ • $E = \{0 \xrightarrow{0} 1\}$
 $\cup \{\ell \xrightarrow{\ell} ((\ell + 1) \bmod (m + 1)) \mid I_\ell = \text{"X := not X"}\}$
 $\cup \{\ell \xrightarrow{\ell^+} \ell', \ell \xrightarrow{\ell^-} \ell'' \mid I_\ell = \text{"if X goto } \ell' \text{ else } \ell''\}$

⁶ The following definition is the main object of this chapter. It describes a transformation
⁷ that turns every boolean program b into a μMALL^ω b.e.-tree-preproof, with the property
⁸ that this preproof is thread-valid iff. the source program is non-terminating.

Definition 50 ($\llbracket \cdot \rrbracket : \text{BOOLE}_{\text{false}} \rightarrow \Pi_0(\mu\text{MALL}^\omega)$). For every boolean program $b \in \text{BOOLE}_{\text{false}}$, we define a preproof $\llbracket b \rrbracket \in \Pi_0(\mu\text{MALL}^\omega)$. Let X_1, \dots, X_k be the variables of b and $1 : I_1, \dots, m : I_m$ its instructions. We first give names to the formulas that will appear in $\llbracket b \rrbracket$: we define a unary operation $\dot{\iota}$, three formulas A, B, C , a family of unary operations $(\dot{\iota}_n)$ and two families of formulas $(D_n), (E_n)$:

$$\begin{aligned} A &= \dot{\iota}(\nu X \dot{\iota} X) & B &= \nu X (\perp \oplus X) & C &= \mu X (B \wp X) & E_n &= \dot{\iota}_n(\nu X \dot{\iota}_n X) \\ \dot{\iota} F &= \mu X (F \oplus (\perp \oplus (X \wp X))) & \dot{\iota}_n F &= \mu X (\perp \oplus (X \wp (\underbrace{F \wp \dots \wp F}_{n-1}))) \\ D_n &= \mu X (\underbrace{X \& \dots \& X}_n) \end{aligned}$$

⁹ We now define $\llbracket b \rrbracket$ to be the preproof

$$\frac{\vdash \underbrace{A^{2k}, B, C, D_2, D_m, E_m^m}_{\vdash A^{2k}, B, C, D_2, D_m, E_m^m} \quad \vdash \underbrace{A^{2k}, B, C, D_2, D_m, E_m^m}_{\vdash A^{2k}, B, C, D_2, D_m, E_m^m} \quad \vdash \underbrace{A^{2k}, B, C, D_2, D_m, E_m^m}_{\vdash A^{2k}, B, C, D_2, D_m, E_m^m} \quad \vdash \underbrace{A^{2k}, B, C, D_2, D_m, E_m^m}_{\vdash A^{2k}, B, C, D_2, D_m, E_m^m}}{(\text{ROOT}) \vdash A^{2k}, B, C, D_2, \underline{D_m}, E_m^m} \quad (3.3)$$

¹¹ where A^{2k} is an abbreviation for $\underbrace{A, \dots, A}_{2k}$ and E_m^m is an abbreviation for $\underbrace{E_m, \dots, E_m}_m$
¹² and the subtrees $\llbracket 0 : \rrbracket, \llbracket 1 : I_1 \rrbracket, \dots, \llbracket m : I_m \rrbracket$ will be defined below.

¹³ *Remark 8* (Short notation for long sequents). You just saw on Eq. (3.3) that, for any
¹⁴ formula A , we use A^n as an abbreviation for $\underbrace{A, \dots, A}_{n \text{ formulas}}$. Similarly, for any formulas A and
¹⁵ B , we may use $(A, B)^n$ as an abbreviation for $\underbrace{A, B, \dots, A, B}_{2n \text{ formulas}}$. We do so, for instance, on
¹⁶ Figure 3.6.

- ¹ The root of the preproof $\llbracket b \rrbracket$ is constructed by translating each pair $\ell : I_\ell$ of a label and an instruction into a finite segment of branch of preproof, as defined in Eq. (3.3), with each subderivation $\llbracket \ell : I_\ell \rrbracket$ defined in Fig. 3.6 and each subderivation $\llbracket \ell : \text{goto } \ell' \rrbracket$ in Fig. 3.5.
- ⁴ *Remark 9* (Implicit threading functions). Notice that in our description of the translation in the previous definition, the **threading functions** were left implicit. The only exception is in the definition of $\llbracket \ell : X_i := \text{not } X_i \rrbracket$, on Figure 3.6, in which we use arrows to express the exchange of the positions of two occurrences of A .
- ⁸ *Remark 10* (Infinite branches of $\llbracket b \rrbracket \simeq E^\omega$). The preproof $\llbracket b \rrbracket$ constructed from b by the reduction $\llbracket \cdot \rrbracket$ of Definition 50 is a finite tree with back-edges in which every finite branch ends with a back-edge to the root. This finite tree has exactly as many branches and consequently as many back-edges to the root, as the number **Card** E of edges in the call-graph of b (Definition 49). This in turn entails that the set of infinite branches of the preproof $\llbracket b \rrbracket$ is in one-to-one correspondence with the set E^ω of infinite words on E .
¹⁴ Note however that an infinite word $\bar{u} \in E^\omega$ has no reason *a priori* to be a path in G .
- ¹⁵ From now on, **we will refer directly to infinite branches of the preproof by words** $\bar{u} \in E^\omega$.

¹⁷ 3.2.3 Main Theorem

- ¹⁸ We now prove that $\Pi(\mu\text{MALL}^\omega)$ is PSPACE-complete.

Remark 11 (Thread groups). We need to be more precise about the occurrences of formulas in the conclusion sequent of preproof $\llbracket b \rrbracket$:

$$\underbrace{A, \dots, A}_{2k}, B, C, D_2, D_m, \underbrace{E_m, \dots, E_m}_m$$

Let us label the occurrences of A in this sequent as follows:

$$A_1^+, A_1^-, \dots, A_k^+, A_k^-, B, C, D_2, D_m, \underbrace{E_m, \dots, E_m}_m$$

so that we can talk precisely about them. It can be seen by examining the definition of $\llbracket \cdot \rrbracket$ (def. 50) that a valid thread in the preproof cannot pass through D_2 or D_m , which contain no ν , and that the remaining formulas are divided into $k + 2$ groups

$$\underbrace{A_1^+, A_1^-}_{}, \dots, \underbrace{A_k^+, A_k^-}_{}, \underbrace{B, C}_{}, \underbrace{E_m, \dots, E_m}_m$$

- ¹⁹ which cannot thread-interact with each other, in the sense that, for instance, no thread
²⁰ can contain a B and a E_m , or a A_ℓ^ϵ and a $A_{\ell'}^{\epsilon'}$ if $\ell \neq \ell'$.

¹ **Lemma 6.** An infinite branch $\bar{u} \in E^\omega$ in the preproof contains a validating thread

- ² • in the E_m group iff. no suffix of \bar{u} is a valid path in G .
- ³ • in the B, C group iff. 0 occurs only finitely in \bar{u} .

⁴ *Proof.* The proof goes by case on the instructions involved.

⁵ In order to prove the first part of the statement, that is that an infinite branch $\bar{u} \in E^\omega$ in
⁶ the preproof contains a validating thread in the E_m group iff. no suffix of \bar{u} is a valid path
⁷ in G , we reason by case on the instructions involved and remark that the E_m formulas
⁸ are touched only in the $\llbracket \ell : \text{goto } \ell' \rrbracket$ parts of the preproof.

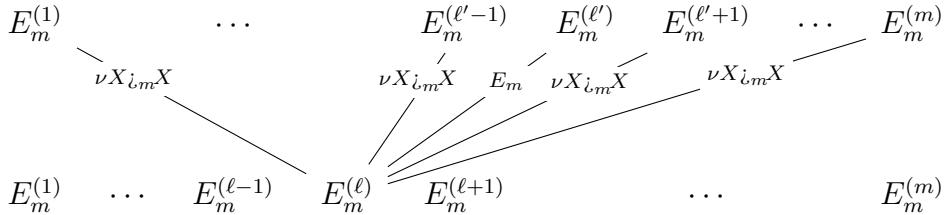
The E_m formulas are touched only in the $\llbracket \ell : \text{goto } \ell' \rrbracket$ parts of the preproof. Observe that
 in $\llbracket \ell : \text{goto } \ell' \rrbracket$ all E_m but one are erased, after which the remaining E_m recreates all of
 them. As a consequence, every infinite branch $\bar{u} \in E^\omega$ in the preproof has exactly one
 thread in the E_m group. Suppose a factor $e_1 e_2 \in E^2$ of \bar{u} and suppose their respective
 sources and targets in G to be named $\ell_1 \xrightarrow{e_1} \ell'_1$ and $\ell_2 \xrightarrow{e_2} \ell'_2$. The crucial observation is
 that the piece of the E_m thread delimited by e_1 has minimal formula equal to

$$\begin{cases} E_m \text{ (which is a } \mu\text{-formula)} & \text{if } \ell'_1 = \ell_2 \\ \nu X_{i_m} X & \text{if } \ell'_1 \neq \ell_2 \end{cases}$$

⁹ the formula $\nu X_{i_m} X$ being a subformula of E_m able to recreate E_m . As a result:

- ¹⁰ • if \bar{u} has a suffix which is a valid path in G then the principal formula of the E_m
¹¹ thread is E_m , hence this thread is a μ -thread, and there is no valid thread in the
¹² E_m group.
- ¹³ • otherwise, the principal formula of the E_m thread is $\nu X_{i_m} X$, and this thread is a
¹⁴ ν -thread, infinitely progressing, hence a validating thread.

This diagram sums up the behavior of the threads of the E_m group in $\llbracket \ell : \text{goto } \ell' \rrbracket$:



¹⁵ In order to prove the second part of the statement, that is that an infinite branch $\bar{u} \in E^\omega$ in
¹⁶ the preproof contains a validating thread in the B, C group iff. 0 occurs only finitely
¹⁷ in \bar{u} , we reason by case on the instructions involved.

3 PSPACE-completeness of the thread criterion

1 First note that B is a ν -formula and that it is a subformula of C , which is a μ -formula.
 2 Observe also that B can recreate B , but B cannot recreate C . Therefore a $\{B, C\}$ -thread,
 3 in order to be validating, must end with an infinite alternation $B \xrightarrow{(\nu)} (\perp \oplus B) \xrightarrow{(\oplus_1)} B \xrightarrow{(\nu)}$
 4 ... Let us now take a closer look at what happens to B and C in the different branches
 5 of the tree with back-edges p . Formulas B and C are touched only at the bottom of the
 6 $\llbracket \ell : I_\ell \rrbracket$ parts of the preproof $\llbracket b \rrbracket$, in the following way:

7 • when going through branch 0, B is erased and C forks into a new copy of B and a
 8 recreated C .

9 • When going through any other branch, two threads are maintained: one at B and
 10 one at C , and the thread at B progresses.

11 Therefore: if an infinite branch \bar{u} goes infinitely through 0, \bar{u} contains no infinite thread
 12 at B , only an infinite thread at C , which is a μ -thread, hence \bar{u} has no validating thread
 13 in the B/C part of the root sequent. If, on the contrary, \bar{u} goes only finitely many
 14 times through 0, it has then a thread at B , which is a ν -thread, and which is infinitely
 15 progressing, hence a validating thread.

These two diagrams sum up the behavior of the threads in the $\{B, C\}$ group in $\llbracket 0 : \cdot \rrbracket$ and in all other $\llbracket \ell : I'_\ell \rrbracket$ respectively:

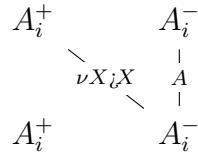


16

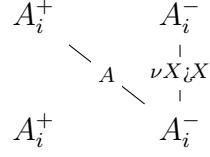
□

17 *Remark 12.* Because of lemma 6, the only infinite branches of $\llbracket b \rrbracket$ whose validity is not
 18 known in advance are the $\bar{u} \in E^\omega$ which are valid paths in G going infinitely many
 19 times through edge 0, and we know that these infinite branches may have validating
 20 threads only in one of the k groups $\{A_i^+, A_i^-\}_{1 \leq i \leq k}$. Such an infinite branch can always
 21 be factorized into $u_0 u_1 u_2 \dots$ where the u_n do not contain 0. As the edge 0 $\xrightarrow{0}$ 1, and because of the hypothesis that \bar{u} is a path in G , for $n \geq 1$
 22 every u_n has source and target 1 $\xrightarrow{u_n} 0$.
 23

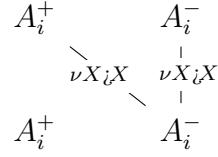
Lemma 7. Assume $1 \xrightarrow{u} \ell$, which does not contain the edge 0. If u is a prefix of the execution of b then the threads of $\{A_i^+, A_i^-\}$ in $0 \xrightarrow{0u} \ell$ are



if $\mathbf{X}_i = \text{false}$ at the end of u and

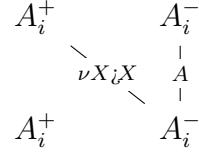


if $\mathbf{X}_i = \text{true}$ at the end of u ; and if u is not a prefix of the execution of b then there is an $i \in [1, m]$ such that the threads of $\{A_i^+, A_i^-\}$ in $0 \xrightarrow{0u}^+ \ell$ are

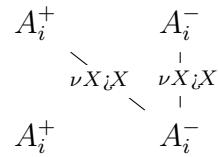


¹ Proof. The proof goes by induction on the length of u .

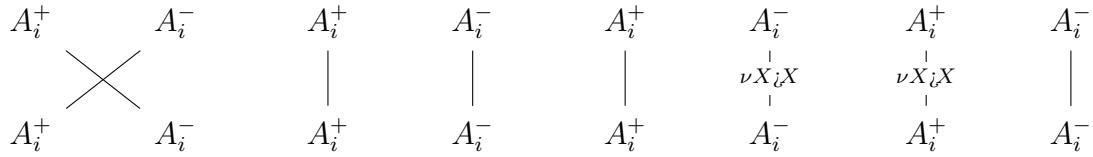
If u has length 0, $0u = 0$. It corresponds to having done 0 step of the execution of b , which implies that all variables have value *false*, and the threads of $\{A_i^+, A_i^-\}$ in p_0 are indeed



for all i . If u has length > 0 , it decomposes as $u = ve$ with $e \in E \setminus \{0\}$. There are then three cases : either ve is the beginning of the execution of b , or v is but ve is not, or v is already not the beginning of the execution of b . In the third case, by induction hypothesis, there is an i such that the threads of $\{A_i^+, A_i^-\}$ in $0v$ are

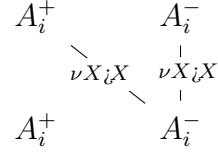


and, because $e \neq 0$, the threads of $\{A_i^+, A_i^-\}$ in e are of one of the four following forms:

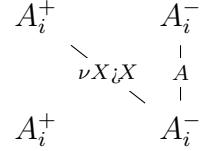


3 PSPACE-completeness of the thread criterion

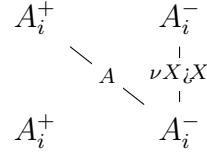
hence, by composition, the threads of $\{A_i^+, A_i^-\}$ in $0ve = 0u$ are still



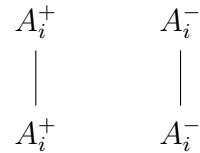
Otherwise v is a beginning of the execution of b . Then, by induction hypothesis, the threads of $\{A_i^+, A_i^-\}$ in $0 \xrightarrow{0v}^+ \ell$ are



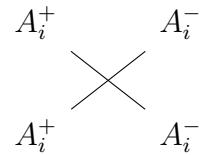
if $X_i = \text{false}$ at the end of v and



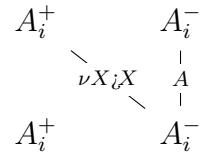
if $X_i = \text{true}$ at the end of v . The next instruction executed by b is either $I_\ell : X_i := \text{not } X_i$ or $I_\ell : \text{if } X_i \text{ goto } \ell' \text{ else } \ell''$. If the next instruction is $I_\ell : X_i := \text{not } X_i$ then e has to be $\ell \xrightarrow{\ell} ((\ell + 1) \bmod (m + 1))$, so $0u = 0ve$ is still a beginning of the execution of b , and then: for every $j \neq i$, the threads of $\{A_j^+, A_j^-\}$ in e are



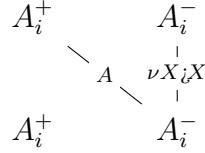
so the threads of $\{A_j^+, A_j^-\}$ in $0u$ have the same form as those in $0v$, while the value of X_j has not changed, hence the invariant is still respected for j . As for the threads in $\{A_i^+, A_i^-\}$, in e they are



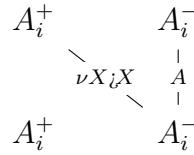
so if the threads of $\{A_i^+, A_i^-\}$ in $0v$ are



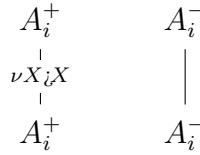
those in $0u$ are



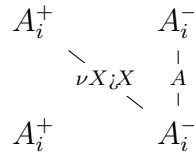
and *vice versa*. As the value of X_i is changed by this instruction, the invariant is still respected also for i . The last case we have to treat is when the next instruction executed by b after v is $I_\ell:\text{if } X_i \text{ goto } \ell' \text{ else } \ell''$. That means that v ends in vertex ℓ , from which there are two edges: $\ell \xrightarrow{\ell^+} \ell'$ and $\ell \xrightarrow{\ell^-} \ell''$. There are four cases, depending on the value of the variable X_i after v , and the choice of $e \in \{\ell^+, \ell^-\}$. If $X_i = \text{false}$ and $e = \ell^-$ then $0u = 0ve$ is still a prefix of the execution of b . The threads of $\{A_i^+, A_i^-\}$ in $0v$ where, by induction hypothesis:



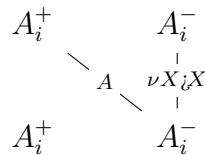
and those in $e = \ell^-$ are



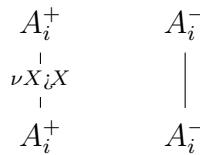
hence, by composition, the threads of $\{A_i^+, A_i^-\}$ in $0u$ are still



and the invariant is still respected. The situation is symmetric when $X_i = \text{true}$ and $e = \ell^+$. If $X_i = \text{true}$ and $e = \ell^-$ then $0u = 0ve$ is not a prefix of the execution of b . The threads of $\{A_i^+, A_i^-\}$ in $0v$ where, by induction hypothesis:



and those in $e = \ell^-$ are



3 PSPACE-completeness of the thread criterion

hence, by composition, the threads of $\{A_i^+, A_i^-\}$ in $0u$ are

$$\begin{array}{ccc} A_i^+ & & A_i^- \\ & \searrow_{\nu X_i X} & \swarrow_{\nu X_i X} \\ & & | \\ A_i^+ & & A_i^- \end{array}$$

- ${}_1$ (recall that $\nu X_i X$ is a subformula of A). The situation is symmetric when $X_i = \text{false}$ and
- ${}_2$ $e = l^+$. So in all of these four cases the invariant is respected.

${}_3$

□

- ${}_4$ **Proposition 7.** $\llbracket \cdot \rrbracket$ is a LOGSPACE reduction from $\overline{\Pi(\mu\text{MALL}^\omega)}$ to $\mathcal{B}_{\text{false}}$.

- ${}_5$ *Proof.* For the LOGSPACE character: the only data that need to be remembered while
- ${}_6$ constructing the preproof are integers like k, m, ℓ, ℓ' . Because $\ell, \ell' \leq m$ and the entry
- ${}_7$ has size $\Omega(k + m)$, this takes a space at most logarithmic in the size of the entry.

- ${}_8$ As for the fact that it is indeed a reduction: let us assume a $b \in \text{BOOLE}_{\text{false}}$ and prove
- ${}_9$ that $\llbracket b \rrbracket \notin \Pi(\mu\text{MALL}^\omega) \Leftrightarrow b \in \mathcal{B}_{\text{false}}$. Let $G = (V, E)$ be the call-graph of b , as defined in
- ${}_{10}$ Definition 49. Following remark 10, we denote by elements of E^ω the infinite branches of
- ${}_{11}$ $\llbracket b \rrbracket$. There are two cases: either $b \in \mathcal{B}_{\text{false}}$ and we have to prove that $p \notin \Pi(\mu\text{MALL}^\omega)$,
- ${}_{12}$ or $b \notin \mathcal{B}_{\text{false}}$ and we have to prove that $p \in \Pi(\mu\text{MALL}^\omega)$. First case: if $b \in \mathcal{B}_{\text{false}}$:
- ${}_{13}$ the execution of b induces a finite path $u = 1 \rightarrow^* 0$ in G . This finite path can be
- ${}_{14}$ completed into $v = 0 \xrightarrow{0} 1 \xrightarrow{u} 0$. Then v^ω is an invalid branch of $\llbracket p \rrbracket_\omega$. Here we use
- ${}_{15}$ the fact that when b terminates, every variable has value false . Second case: if $b \notin \mathcal{B}_{\text{false}}$:
- ${}_{16}$ let $\mathcal{P}_1 = \{vw_\infty \mid v \in E^*, w_\infty \in E^\omega \text{ and } w_\infty \text{ is a path in } G\}$ and $\mathcal{P}_2 = \{v_\infty \in \mathcal{P}_1 \mid$
- ${}_{17}$ 0 occurs infinitely in $v_\infty\}$. By construction, $\mathcal{P}_2 \subseteq \mathcal{P}_1 \subseteq E^\omega$. We will prove three facts:
- ${}_{18}$ that every branch $v_\infty \in E^\omega \setminus \mathcal{P}_1$ is thread-valid, that every branch $v_\infty \in \mathcal{P}_1 \setminus \mathcal{P}_2$ is
- ${}_{19}$ thread-valid and that every branch $v_\infty \in \mathcal{P}_2$ is thread-valid. These three facts, together
- ${}_{20}$ with the fact that $(E^\omega \setminus \mathcal{P}_1) \cup (\mathcal{P}_1 \setminus \mathcal{P}_2) \cup \mathcal{P}_2 = E^\omega$, are enough to conclude that every
- ${}_{21}$ branch $v_\infty \in E^\omega$ is thread-valid. The first fact, that every branch $v_\infty \in E^\omega \setminus \mathcal{P}_1$ is
- ${}_{22}$ thread-valid, is due to the thread going through the E_m . The second fact, that every
- ${}_{23}$ branch $v_\infty \in \mathcal{P}_1 \setminus \mathcal{P}_2$ is thread-valid, is due to the thread going through B . The third fact,
- ${}_{24}$ that every branch $v_\infty \in \mathcal{P}_2$ is thread-valid, is due to the fact that b is non-terminating
- ${}_{25}$ and that, because of that, one of the $2k$ threads going through the A is valid. □

Theorem 4. The problem $\Pi(\mu\text{MALL}^\omega)$ is PSPACE-hard:

$$\text{PSPACE} \leq \Pi(\mu\text{MALL}^\omega)$$

- ${}_{26}$ *Proof.* We reduce from $\mathcal{B}_{\text{false}}$, which is PSPACE-complete by Lemma 2. More precisely,
- ${}_{27}$ we reduce $\mathcal{B}_{\text{false}}$ to $\overline{\Pi(\mu\text{MALL}^\omega)}$, the complement of $\Pi(\mu\text{MALL}^\omega)$. This is enough because

¹ PSPACE is closed under complements, in the same way as all deterministic classes. The
² reduction $\llbracket \cdot \rrbracket : \text{BOOLE}_{\text{false}} \rightarrow \Pi_0(\mu\text{MALL}^\omega)$ is defined in Definition 50. It is a LOGSPACE
³ reduction, by Proposition 7, hence it is also a polynomial-time reduction. \square

⁴ *Remark 13.* In fact, since our construction do not use the (cut) rule, the cut-free fragment
⁵ of $\Pi(\mu\text{MALL}^\omega)$ is already PSPACE-hard.

⁶ **Corollary 2.** *The decidability of the thread criterion is also PSPACE-complete in μLJ ,
⁷ μLK , $\mu\text{LK}\bigcirc$ and $\mu\text{LK}\Box\Diamond$.*

⁸ *Proof.* It is true for μLJ because every preproof π in μMALL^ω can be translated to a
⁹ preproof π^* in μLJ , such that π^* is thread-valid iff. π is, by translating LL connectives
¹⁰ into LJ connectives and translating $\vdash \Gamma$ into $|\Gamma^\perp| \vdash \perp$.

¹¹ It is true for the other mentionned systems because μLJ is a fragment of them, therefore
¹² every μLJ preproof is already a preproof in each of them. \square

¹³ *Remark 14.* Note that the following adaptations from MALL to LK and LJ might be
¹⁴ simplified by replacing $F \vee F$ by F , $X \wedge X$ by X , $\perp \vee X$ by X and so on. A lot of the
¹⁵ complexity of these formulas is there to simulate structural rules in the linear world. When
¹⁶ we are in the classical world, these workaround may not be needed anymore. Anyway,
¹⁷ the translation we present here is simply to show that even without thinking about that,
¹⁸ a straightforward translation is possible, which gives the same PSPACE-completeness
¹⁹ result with LK and LJ and their extensions.

²⁰ **Generalisation to μLK , $\mu\text{LK}\bigcirc$ and $\mu\text{LK}\Box\Diamond$**

$$A = \dot{\iota}(\nu X \dot{\iota} X) \quad B = \nu X (\perp \vee X) \quad C = \mu X (B \vee X) \quad E_n = \dot{\iota}_n(\nu X \dot{\iota}_n X)$$

$$\dot{\iota}F = \mu X (F \vee (\perp \vee (X \vee X))) \quad \dot{\iota}_n F = \mu X (\perp \vee (X \vee (\underbrace{F \vee \dots \vee F}_{n-1})))$$

$$D_n = \mu X (\underbrace{X \wedge \dots \wedge X}_n)$$

²¹ We now define $\llbracket b \rrbracket$ to be the preproof

$$\frac{\vdots \llbracket 0 : \rrbracket \quad \vdots \llbracket 1 : I_1 \rrbracket \quad \dots \quad \vdots \llbracket m : I_m \rrbracket}{\vdash A^{2k}, B, C, D_2, D_m, E_m^m \quad \vdash A^{2k}, B, C, D_2, D_m, E_m^m \quad \vdash A^{2k}, B, C, D_2, D_m, E_m^m} \frac{}{(\text{ROOT}) \vdash A^{2k}, B, C, D_2, \underline{D_m}, E_m^m} \quad (3.4)$$

¹ **Generalisation to μ LJ**

$$A = \mathbf{i}(\mu X \mathbf{i} X) \quad B = \mu X (\top \wedge X) \quad C = \nu X (B \wedge X) \quad E_n = \mathbf{i}_n(\mu X \mathbf{i}_n X)$$

$$\mathbf{i} F = \nu X (F \wedge (\top \wedge (X \wedge X))) \quad \mathbf{i}_n F = \nu X (\top \wedge (X \wedge (\underbrace{F \wedge \cdots \wedge F}_{n-1})))$$

$$D_n = \nu X (\underbrace{X \vee \cdots \vee X}_n)$$

² We now define $\llbracket b \rrbracket$ to be the preproof

$$\frac{\vdots \llbracket 0 : \rrbracket \quad \vdots \llbracket 1 : I_1 \rrbracket \quad \dots \quad \vdots \llbracket m : I_m \rrbracket}{\begin{array}{c} A^{2k}, B, C, D_2, D_m, E_m^m \vdash \\ A^{2k}, B, C, D_2, D_m, E_m^m \vdash \\ \dots \\ A^{2k}, B, C, D_2, D_m, E_m^m \vdash \end{array} \frac{(A^{2k}, B, C, D_2, \underline{D_m}, E_m^m \vdash)}{(\text{ROOT}) A^{2k}, B, C, D_2, \underline{D_m}, E_m^m \vdash}}_{(\nu^L), (\vee^L)^{m-1}} \quad (3.5)$$

⁴ *Remark 15.* Our result extends to μ LJ, μ LK, μ LK \bigcirc and μ LK $\square\Diamond$, and we conjecture
⁵ that the method we illustrate here on μ MALL can apply as well to the guarded cases of
⁶ μ -calculi with modalities.

⁷ Rémi: fusionner cette remarque avec ce qui est avant les traductions. La question
ouvert intéressante est celle des cas gardés.

⁸ Rémi: pour décrire ces logiques, citer les références données par Alexis et la thèse
d'Amina

⁹ *Remark 16.* There is a μ LJ defined by Clairambault [2009, 2010], which is a finitary
¹⁰ calculus in the spirit of μ MALL, with explicit invariants of induction and coinduction.
¹¹ The version we are considering here is an infinitary one, in which proofs are distinguished
¹² from invalid preproofs by a thread criterion, in the spirit of μ MALL $^\omega$.

¹³ Rémi: plutôt renommer ces trucs en ajoutant des ω

¹⁴ **3.3 Comments on our Approach and Discussion of
¹⁵ Related Works**

¹⁶ Our proof for the PSPACE-completeness of the thread criterion is an encoding and an
¹⁷ adaptation to our setting of the proof used by Lee, Jones and Ben Amram to prove

3.3 Comments on our Approach and Discussion of Related Works

1 that size-change termination is PSPACE-complete [Lee, Jones, and Ben-Amram, 2001].
 2 We reduce, as they do, from the problem of termination of boolean programs and the
 3 thread diagrams that we have used to describe the preproof generated by the reduction
 4 are very similar to the size-change graphs generated by their reduction; this is in fact
 5 what has guided the design of this preproof: formula A mimicks the X_i, \bar{X}_i part of their
 6 graphs and formulas B and C adapt the Z part of their graphs. We had to add the
 7 formulas D_2 and D_m in order to have branching rules in the preproof. One of the main
 8 novelties of our reduction, compared to the reduction of Lee, Jones and Ben Amram for
 9 size-change termination, lies in the E_m and $\llbracket \ell : \text{goto } \ell' \rrbracket$ part of the constructed preproof,
 10 which has no equivalent in the size-change graphs obtained by their reduction. This part
 11 of our construction allows us to construct a preproof which is a tree with back-edges,
 12 hence proving that the thread criterion is PSPACE-complete even when preproofs are
 13 represented by trees with back-edges. We could in fact drop the E_m and $\llbracket \ell : \text{goto } \ell' \rrbracket$
 14 part of the construction by constructing $\llbracket b \rrbracket$ as a rooted graph instead of a tree with
 15 back-edges. The constructions proofs are still correct — and shorter. The caveat is that it
 16 only proves the thread-criterion to be PSPACE-hard in graph-shaped preproofs and not
 17 in tree-with-back-edges-shaped preproofs. Furthermore, we could not have filled this gap
 18 by simply unfolding the graph into a tree with back-edges, for it could lead, as shown
 19 in the following example, to an exponential blow-up in size, which would prevent the
 20 reduction to be LOGSPACE, or even P. The following boolean program:

```

 1:if X then goto 2 else goto 2
 2:if X then goto 3 else goto 3
21          :
n:if X then goto n + 1 else goto n + 1
  
```

22 will be translated to a graph-shaped preproof of size $\Theta(n)$ but the unfolding of this
 23 preproof into a tree-with-back-edges-shaped preproof will have size $\Theta(2^n)$. Therefore we
 24 had to be clever in order to target trees with back-edges by *simulating* several vertices
 25 with a single one; this is accomplished by the E_m and $\llbracket \ell : \text{goto } \ell' \rrbracket$.

26 This improvement of the reduction of Lee, Jones and Ben Amram could in fact be adapted
 27 in the other direction, to show that size-change termination is already PSPACE-complete
 28 even when restricted to programs with only one function (in the terminology of [Lee,
 29 Jones, and Ben-Amram, 2001]), that is when the corresponding call graph / control flow
 30 graph has only one vertex.

31 If, as it is commonly believed, $\text{NP} \neq \text{PSPACE}$, our result implies that there is no way to
 32 add a polynomial quantity of information to a preproof so that its thread-validity can be
 33 checked in polynomial time. This can be seen as a problem, both for the complexity of
 34 proof search and proof verification. It suggests trying to find restrictions of the thread
 35 criterion which will be either decidable or certifiable in polynomial time, while keeping
 36 enough expressivity to validate interesting proofs. A first step in this direction has already
 37 been done in [Nollet, Saurin, and Tasson, 2018].

1 We recalled in section 3.1 that thread validity is decidable in PSPACE, and we did so by
2 reducing to the problem of language inclusion for ω -parity-automata. The original size-
3 change article [Lee, Jones, and Ben-Amram, 2001] gives two different methods to check
4 size-change termination, the first one is based on reducing to inclusions of ω -languages
5 defined by finite automata while the second one is a direct, graph-based approach. It is
6 in fact possible to use this more direct method to decide the thread criterion, and this
7 has already been done in [Dax, Hofmann, and Lange, 2006] by Dax, Hofmann and Lange,
8 who remark furthermore that this method leads to a more efficient implementation than
9 the automata-based one.

10 **3.4 Conclusion**

11 In the present chapter, we analyzed the complexity of deciding the validity of circular
12 proofs in μ MALL logic: while the problem was already known to be in PSPACE, we
13 established here its PSPACE-completeness. In doing so, we drew inspiration from the
14 PSPACE-completeness proof of SCT even though we defer at some crucial points on
15 order to build our reduction and carry our proof taking into account the specific forms of
16 circular proofs.

17 Our proof adapt straightforwardly to a number of other circular proof systems based on
18 sequent calculus such as intuitionistic or classical proof systems in addition to the linear
19 case on which we focused here.

20 While our result can be seen as negative one for circular proofs, it does not prevent
21 actual implementations to be tractable and usable on many situations as exemplified by
22 the Cyclist prover for instance. In such systems, validity checking does not seem to be
23 the bottleneck in circular proof construction as compared with the complexity that is
24 inherent to exploring and backtracking in the search tree [Brotherston, Gorogiannis, and
25 Petersen, 2012, Rowe and Brotherston, 2017, Tellez and Brotherston, 2017].

26 Our work suggests deep connections between thread-validity and SCT that we only
27 touched upon in the previous section. This confirms connections previously hinted by
28 other authors [Dax, Hofmann, and Lange, 2006, Hyvernaut, 2014, 2019, Lepigre and
29 Raffalli, 2019] that we plan to investigate further in the future.

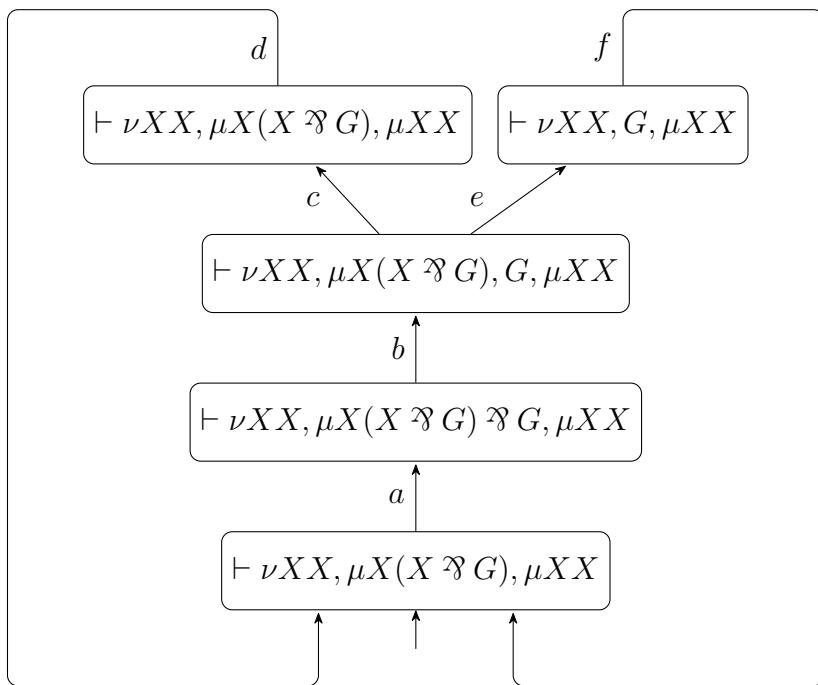


Figure 3.1. Automaton recognizing the branches of the preproof (3.1).

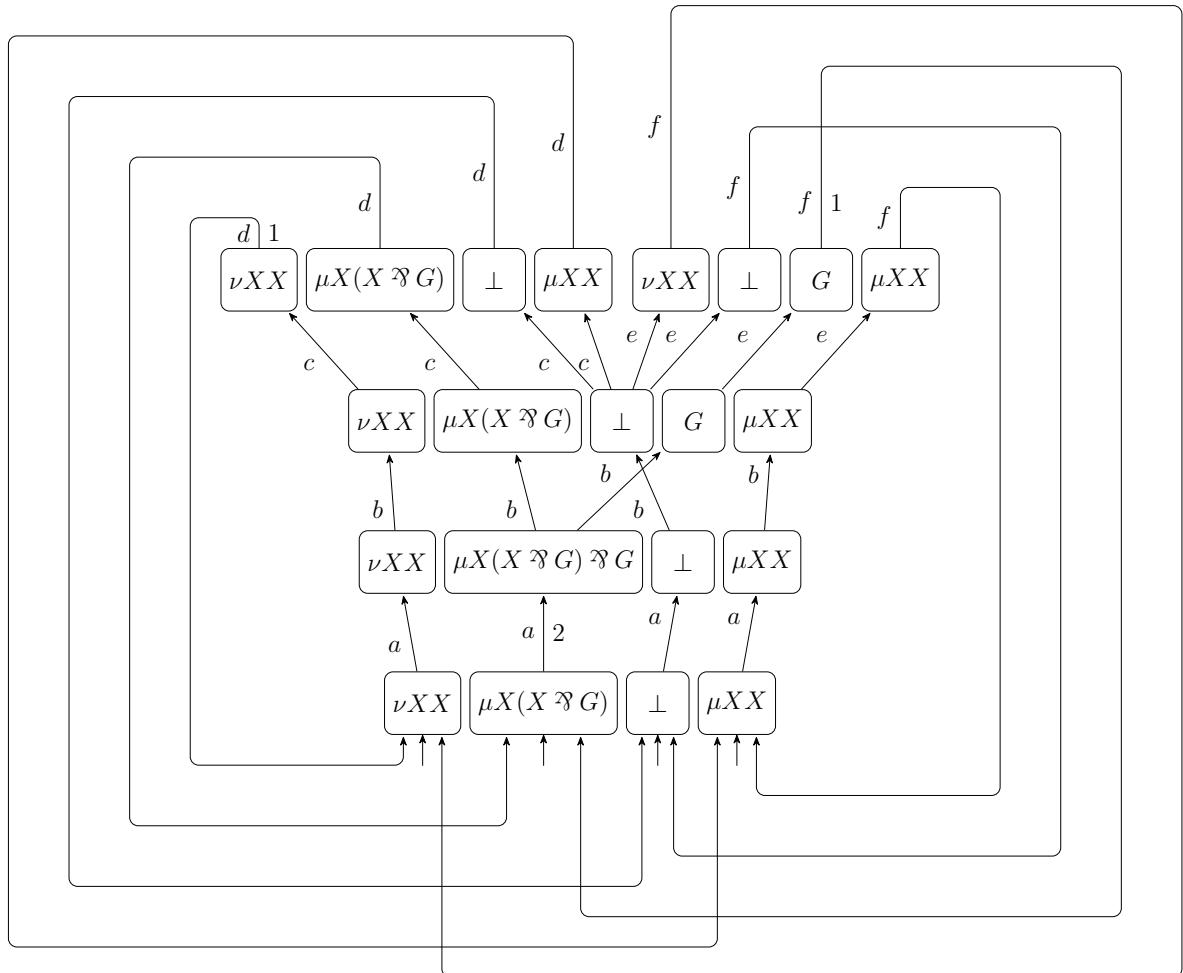


Figure 3.2. Automaton recognizing the valid branches of the preproof (3.1).

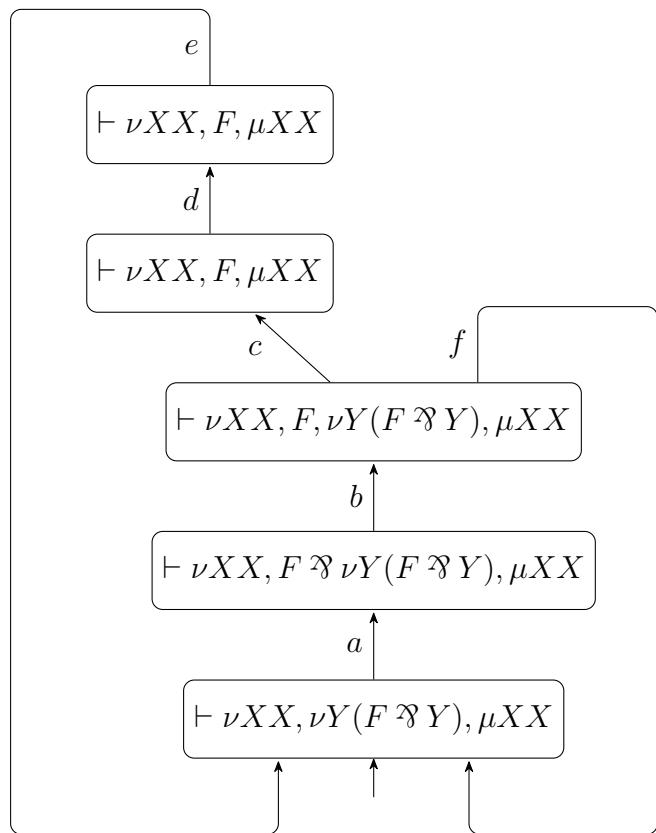


Figure 3.3. Automaton recognizing the branches of the preproof (3.2).

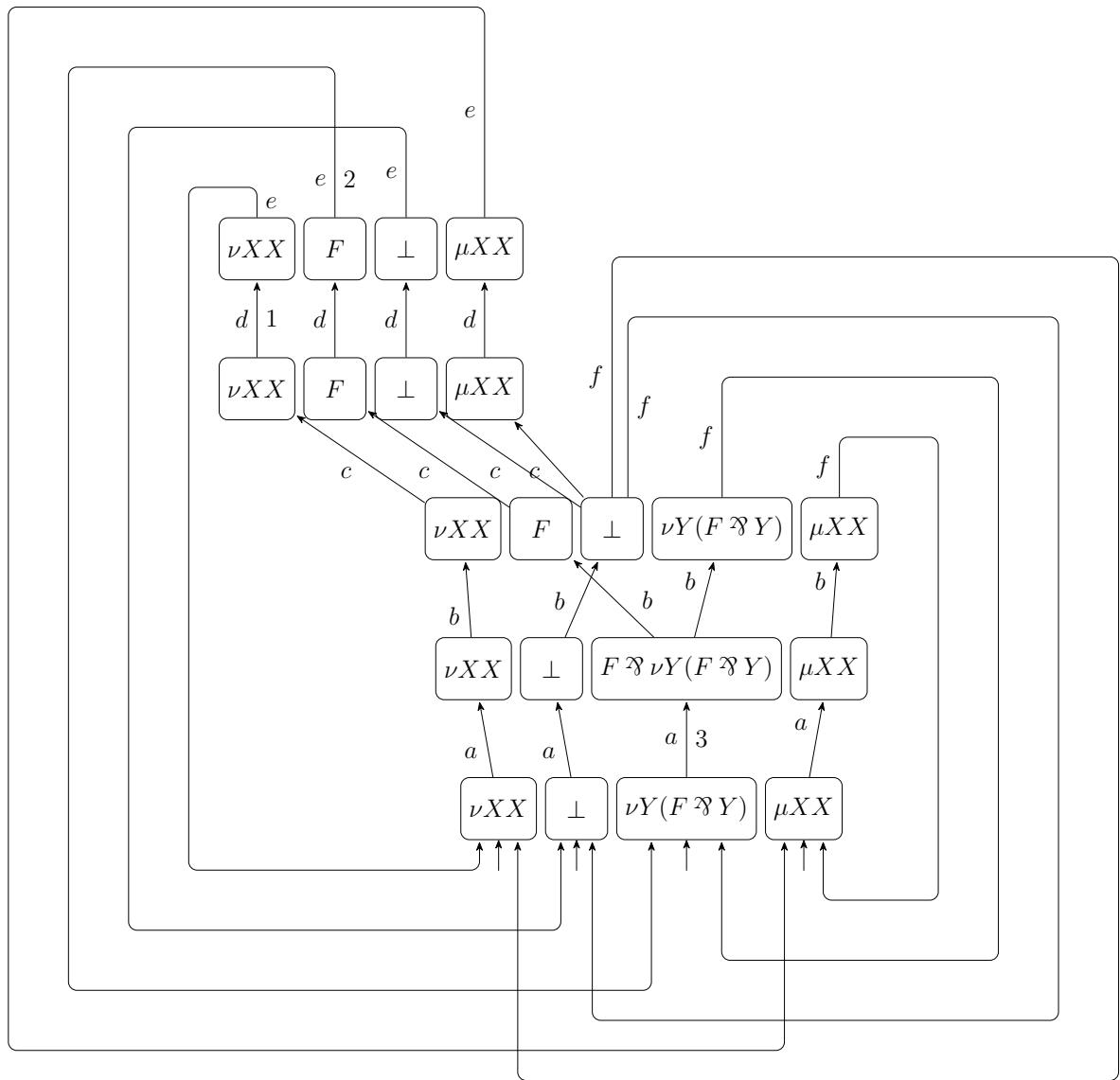


Figure 3.4. Automaton recognizing the valid branches of the preproof (3.2).

$$\begin{array}{c}
 \llbracket \ell : \text{goto } \ell' \rrbracket := \\
 \text{Back-edge to (ROOT)} \\
 \hline
 \frac{}{\vdash A, \dots, A, B, C, D_2, D_m, E_m, \dots, E_m} (\nu)^{m-1} \\
 \hline
 \frac{}{\vdash A, \dots, A, B, C, D_2, D_m, \underbrace{\nu X_{\dot{C}_m} X, \dots, \nu X_{\dot{C}_m} X}_{\ell'-1}, \underbrace{E_m, \nu X_{\dot{C}_m} X, \dots, \nu X_{\dot{C}_m} X}_{m-\ell'} } (\mu), (\oplus_1), (\wp)^{m-1} \\
 \hline
 \frac{}{\vdash \underbrace{A, \dots, A}_{2k}, B, C, D_2, D_m, \underbrace{E_m, \dots, E_m}_{\ell-1}, E_m, \underbrace{E_m, \dots, E_m}_{m-\ell}} ((\mu), (\oplus_0), (\perp))^{m-1}
 \end{array}$$

Figure 3.5. Back-edges of the preproof

$$\begin{array}{c}
 \vdots \llbracket 0 : \text{goto } 1 \rrbracket \\
 \hline
 \frac{}{\vdash (A, A)^k, B, C, D_2, D_m, E_m^m} (\nu)^k \\
 \hline
 \frac{}{\vdash (\nu X_{\dot{C}} X, A)^k, B, C, D_2, D_m, E_m^m} ((\mu), (\oplus_0))^k \\
 \llbracket 0 : \rrbracket := \frac{}{\vdash (A, A)^k, B, C, D_2, D_m, E_m^m} ((\mu), (\oplus_1), (\oplus_1), (\wp))^k \\
 \hline
 \frac{}{\vdash \underline{A}^k, B, C, D_2, D_m, E_m^m} ((\mu), (\oplus_1), (\oplus_0), (\perp))^k \\
 \hline
 \frac{}{\vdash (\underline{A}, A)^k, B, C, D_2, D_m, E_m^m} (\mu), (\wp) \\
 \hline
 \frac{}{\vdash A^{2k}, \underline{C}, D_2, D_m, E_m^m} (\nu), (\oplus_0), (\perp) \\
 \hline
 \vdots \llbracket \ell : \text{goto } (\ell + 1 \bmod m + 1) \rrbracket \\
 \hline
 \frac{}{\vdash A^{2(i-1)}, \underline{A}, \underline{A}, A^{2(k-i)}, B, C, D_2, D_m, E_m^m} (\nu), (\oplus_1) \\
 \hline
 \llbracket \ell : \text{X}_i := \text{not X}_i \rrbracket := \frac{}{\vdash A^{2(i-1)}, \underline{A}, \underline{A}, A^{2(k-i)}, \underline{B}, C, D_2, D_m, E_m^m} (\nu), (\oplus_1) \\
 \hline
 \llbracket \ell : \text{if X}_i \text{ then goto } \ell' \text{ else } \ell'' \rrbracket := \\
 \vdots \llbracket \ell : \text{goto } \ell' \rrbracket \qquad \qquad \vdots \llbracket \ell : \text{goto } \ell'' \rrbracket \\
 \hline
 \frac{\vdash A^{2(i-1)}, A, A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m}{\vdash A^{2(i-1)}, A, \nu X_{\dot{C}} X, A^{2(k-i)}, B, C, D_2, D_m, E_m^m} (\nu) \qquad \frac{\vdash A^{2(i-1)}, A, A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m}{\vdash A^{2(i-1)}, \nu X_{\dot{C}} X, A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m} (\nu) \\
 \hline
 \frac{\vdash A^{2(i-1)}, A, \underline{A}, A^{2(k-i)}, B, C, D_2, D_m, E_m^m}{\vdash A^{2(i-1)}, \underline{A}, \underline{A}, A^{2(k-i)}, B, C, D_2, D_m, E_m^m} (\mu), (\oplus_0) \qquad \frac{\vdash A^{2(i-1)}, \nu X_{\dot{C}} X, A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m}{\vdash A^{2(i-1)}, \underline{A}, A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m} (\mu), (\oplus_0) \\
 \hline
 \frac{\vdash A^{2k}, B, C, \underline{D}_2, D_m, E_m^m}{\vdash A^{2k}, \underline{B}, C, D_2, D_m, E_m^m} (\nu), (\oplus_1)
 \end{array}$$

 Figure 3.6. Premises p_ℓ of the preproof

$$\begin{array}{c}
 \vdots \llbracket 0:\text{goto } 1 \rrbracket \\
 \frac{\vdash (A, A)^k, B, C, D_2, D_m, E_m^m}{\vdash (\underline{\nu X} \dot{\cup} X, A)^k, B, C, D_2, D_m, E_m^m} (\nu)^k \\
 \frac{\vdash (\underline{A}, A)^k, B, C, D_2, D_m, E_m^m}{\vdash \underline{A}^k, B, C, D_2, D_m, E_m^m} ((\mu), (\vee_0), (\vee_1))^k \\
 \frac{\vdash (\underline{A}, A)^k, B, C, D_2, D_m, E_m^m}{\vdash (\underline{A}, A)^k, B, C, D_2, D_m, E_m^m} ((\mu), (\vee_1), (\vee_0), (\perp))^k \\
 \frac{\vdash A^{2k}, \underline{C}, D_2, D_m, E_m^m}{\vdash A^{2k}, \underline{B}, C, D_2, D_m, E_m^m} (\mu), (\vee) \\
 \frac{\vdash A^{2k}, \underline{B}, C, D_2, D_m, E_m^m}{\vdash A^{2k}, \underline{B}, C, D_2, D_m, E_m^m} (\nu), (\vee_0), (\perp) \\
 \\
 \vdots \llbracket \ell:\text{goto } (\ell + 1 \bmod m + 1) \rrbracket \\
 \frac{\vdash A^{2(i-1)}, \underline{A}, A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m}{\vdash A^{2(i-1)}, \underline{A}, A, A^{2(k-i)}, \underline{B}, C, D_2, D_m, E_m^m} (\nu), (\vee_1) \\
 \llbracket \ell:\text{X}_i := \text{not } \text{X}_i \rrbracket := \frac{\vdash A^{2(i-1)}, \underline{A}, A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m}{\vdash A^{2(i-1)}, \underline{A}, A, A^{2(k-i)}, \underline{B}, C, D_2, D_m, E_m^m} (\nu), (\vee_0) \\
 \llbracket \ell:\text{if } \text{X}_i \text{ then goto } \ell' \text{ else } \ell'' \rrbracket := \\
 \\
 \vdots \llbracket \ell:\text{goto } \ell' \rrbracket \quad \vdots \llbracket \ell:\text{goto } \ell'' \rrbracket \\
 \frac{\vdash A^{2(i-1)}, A, A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m}{\vdash A^{2(i-1)}, A, \underline{\nu X}(\dot{\cup} X), A^{2(k-i)}, B, C, D_2, D_m, E_m^m} (\nu) \quad \frac{\vdash A^{2(i-1)}, A, A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m}{\vdash A^{2(i-1)}, \underline{\nu X}(\dot{\cup} X), A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m} (\nu) \\
 \frac{\vdash A^{2(i-1)}, A, \underline{A}, A^{2(k-i)}, B, C, D_2, D_m, E_m^m}{\vdash A^{2(i-1)}, \underline{A}, A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m} (\mu), (\vee_0) \quad \frac{\vdash A^{2(i-1)}, \underline{A}, A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m}{\vdash A^{2(i-1)}, \underline{A}, A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m} (\mu), (\vee_0) \\
 \frac{\vdash A^{2k}, B, C, D_2, D_m, E_m^m}{\vdash A^{2k}, \underline{B}, C, D_2, D_m, E_m^m} (\nu), (\vee_1) \\
 \frac{\vdash A^{2k}, \underline{B}, C, D_2, D_m, E_m^m}{\vdash A^{2k}, \underline{B}, C, D_2, D_m, E_m^m} (\mu), (\wedge)
 \end{array}$$

 Figure 3.7. Premises p_ℓ of the preproof

$$\begin{array}{c}
 \llbracket \ell:\text{goto } \ell' \rrbracket := \\
 \text{Back-edge to (ROOT)} \\
 \frac{}{\vdash A, \dots, A, B, C, D_2, D_m, E_m, \dots, E_m} \\
 \frac{\vdash A, \dots, A, B, C, D_2, D_m, \underbrace{\underline{\nu X} \dot{\cup} \underline{X}, \dots, \underline{\nu X} \dot{\cup} \underline{X}}_{\ell'-1}, E_m, \underbrace{\underline{\nu X} \dot{\cup} \underline{X}, \dots, \underline{\nu X} \dot{\cup} \underline{X}}_{m-\ell'}}{\vdash A, \dots, A, B, C, D_2, D_m, E_m, \dots, E_m} (\nu)^{m-1} \\
 \frac{\vdash A, \dots, A, B, C, D_2, D_m, \underbrace{\underline{E}_m, \dots, \underline{E}_m}_{\ell-1}, E_m, \underbrace{\underline{E}_m, \dots, \underline{E}_m}_{m-\ell}}{\vdash \underbrace{A, \dots, A}_{2k}, B, C, D_2, D_m, \underbrace{\underline{E}_m, \dots, \underline{E}_m}_{\ell-1}, E_m, \underbrace{\underline{E}_m, \dots, \underline{E}_m}_{m-\ell}} ((\mu), (\vee_0), (\perp))^{m-1}
 \end{array}$$

Figure 3.8. Back-edges of the preproof

$$\begin{array}{c}
 \vdots \llbracket 0 : \text{goto } 1 \rrbracket \\
 \frac{(A, A)^k, B, C, D_2, D_m, E_m^m \vdash}{(\mu X \downarrow X, A)^k, B, C, D_2, D_m, E_m^m \vdash}^{(\mu^L)^k} \\
 \frac{\frac{(A, A)^k, B, C, D_2, D_m, E_m^m \vdash}{\frac{A^k, B, C, D_2, D_m, E_m^m \vdash}{\frac{(\underline{A}, A)^k, B, C, D_2, D_m, E_m^m \vdash}{\frac{A^{2k}, \underline{C}, D_2, D_m, E_m^m \vdash}{A^{2k}, \underline{B}, C, D_2, D_m, E_m^m \vdash}}^{(\nu^L), (\wedge^L)}}^{(\nu^L), (\wedge_0^L), (\wedge_1^L), (\wedge^L))^k}}{((\nu^L), (\wedge_1^L), (\wedge_1^L), (\wedge^L))^k} \\
 \llbracket 0 : \rrbracket := \\
 \vdots \llbracket \ell : \text{goto } (\ell + 1 \bmod m + 1) \rrbracket \\
 \frac{A^{2(i-1)}, \cancel{A}, \cancel{A}, A^{2(k-i)}, B, C, D_2, D_m, E_m^m \vdash}{A^{2(i-1)}, \cancel{A}, \cancel{A}, A^{2(k-i)}, \cancel{B}, C, D_2, D_m, E_m^m \vdash}^{(\mu^L), (\wedge_1^L)} \\
 \llbracket \ell : \text{X}_i := \text{not } \text{X}_i \rrbracket := \\
 \vdots \llbracket \ell : \text{if } \text{X}_i \text{ then goto } \ell' \text{ else } \ell'' \rrbracket := \\
 \vdots \llbracket \ell : \text{goto } \ell \rrbracket \quad \vdots \llbracket \ell : \text{goto } \ell'' \rrbracket \\
 \frac{A^{2(i-1)}, A, A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m \vdash}{A^{2(i-1)}, A, \mu X(\downarrow X), A^{2(k-i)}, B, C, D_2, D_m, E_m^m \vdash}^{(\mu^L)} \quad \frac{A^{2(i-1)}, A, A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m \vdash}{A^{2(i-1)}, \mu X(\downarrow X), A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m \vdash}^{(\mu^L)} \\
 \frac{A^{2(i-1)}, A, \cancel{A}, A^{2(k-i)}, B, C, D_2, D_m, E_m^m \vdash}{A^{2(i-1)}, \cancel{A}, A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m \vdash}^{(\nu^L), (\wedge_0^L)} \quad \frac{A^{2(i-1)}, \cancel{A}, A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m \vdash}{A^{2(i-1)}, \cancel{A}, A, A^{2(k-i)}, B, C, D_2, D_m, E_m^m \vdash}^{(\nu^L), (\wedge_1^L)} \\
 \frac{A^{2k}, B, C, \underline{D}_2, D_m, E_m^m \vdash}{A^{2k}, \underline{B}, C, D_2, D_m, E_m^m \vdash}^{(\mu^L), (\wedge_1^L)}
 \end{array}$$

 Figure 3.9. Premises p_ℓ of the preproof

$$\begin{array}{c}
 \llbracket \ell : \text{goto } \ell \rrbracket := \\
 \text{Back-edge to (ROOT)} \\
 \frac{}{A, \dots, A, B, C, D_2, D_m, E_m, \dots, E_m \vdash} \\
 \frac{}{A, \dots, A, B, C, D_2, D_m, \underbrace{\mu X \downarrow_m X, \dots, \mu X \downarrow_m X}_{\ell'-1}, E_m, \underbrace{\mu X \downarrow_m X, \dots, \mu X \downarrow_m X}_{m-\ell'} \vdash}^{(\mu^L)^{m-1}} \\
 \frac{}{A, \dots, A, B, C, D_2, D_m, \underbrace{E_m, \dots, E_m}_{\ell-1}, E_m, \underbrace{E_m, \dots, E_m}_{m-\ell} \vdash}^{(\nu^L), (\wedge_1^L), (\wedge^L)^{m-1}}
 \end{array}$$

Figure 3.10. Back-edges of the preproof

¹ 4 A polynomial sub-criterion

² We have shown in the previous chapter that deciding the validity of the circular representation of a preproof, with respect to the thread criterion, is a PSPACE-complete problem.

⁵ This implies in particular that there is probably no subexponential algorithm to check the validity of a circular representation. This also implies that there is probably no way to certify the validity of a circular preproof, so that it can be checked in polynomial time, without adding to it an exponential quantity of information.

⁹ We tackle both these problems by taking a different approach. Instead of trying to handle the existing criterion, we will look for a new, different criterion.

¹¹ The thread criterion has very good properties. In particular, Baelde, Doumane, and Saurin [2016] proved that it guarantees soundness with respect to boolean interpretation and full cut elimination. Therefore, we would like our new criterion to have the following properties:

¹⁵ • that any preproof valid for the new criterion is also valid for the thread criterion, so that it inherits its soundness properties,

¹⁷ • that this new criterion is decidable in reasonable time,

¹⁸ • that it is possible to add a reasonable amount of information to the circular representation of a preproof so that the validity of this certified preproof may be checked in linear time,

²¹ • that this new criterion is expressive enough.

²² This chapter provides such a criterion, which we called the **loop criterion**.

²³ There is an essential difference between the thread criterion and our loop criterion. In usual proof theory, a proof is a finite tree, made of logical inferences, and a proof is correct as soon as each one of its inferences is correct. This is not the case anymore with logics such as μMALL^ω , in which the soundness of each inference only ensure that the tree is a preproof, and a proof has to also pass the thread criterion, which is a global

4 A polynomial sub-criterion

1 criterion. The PSPACE-complete nature of the thread criterion forbid that it could have
2 a local definition. It is, and has to be, a *global* criterion, which can't be turned into a
3 local criterion. In contrast, our **loop criterion** gives rise to a proof system in which the
4 validity of a proof is a purely local property. More precisely, with our loop criterion comes
5 an enriched proof system, made of labelled proof trees, with two properties:

- 6 1. if the circular representation of a preproof is valid for our loop criterion, it is
7 possible to label it so as to obtain a proof in our labelled proof system,
8 2. in this labelled proof system, a proof is correct if and only if each one of its
9 individual inferences is correct.

10 This would not be possible with the thread criterion, or the labeling would probably
11 need to be at least exponential in the size of the proof.

12 There is another important difference between the usual thread criterion and our new
13 **loop criterion**. The thread criterion is really a criterion on the infinite preproof, not on
14 its representation. This means that if you have two different circular representations of
15 the same infinite preproof, either they are both valid or both invalid. In contrast, our
16 criterion really depends on the representation, and not only on the infinite preproof which
17 is represented. This means that among the circular representations of a given infinite
18 preproof, it may happen that some of them are valid for our loop criterion and some
19 other are not.

20 In this chapter we prove that:

- 21 • If a circular representation of an infinite preproof is valid for our loop criterion
22 then this preproof is valid for the thread criterion.
23 • Our loop criterion can be decided in quadratic time.
24 • Every circular representation which is valid for our loop criterion can be labelled so
25 as to be turned into a proof in our labelled proof system, in which the validity of
26 the proof only depends on the validity of each individual inference, and is therefore
27 checkable in linear time.
28 • There is a canonical translation of the finitary proofs in the style of Baelde [2012]
29 into circular representations of infinite proofs, which are valid for the thread criterion.
30 Those representations are also valid for our more restricted loop criterion.

¹ 4.1 Labelling as validity

² 4.1.1 \mathcal{L} -proofs

- ³ In this subsection, we briefly mention an alternative approach to ensure validity of
⁴ μMALL^∞ preproofs, aiming at motivating the tools used in the remainder of this chapter.
⁵ The idea is to witness thread progress by adding labels on some formulas.

⁶ **Definition 51** (Labelled formulas). Let \mathcal{L} be an infinite countable set of *atoms* and
⁷ call *labels* any finite list of atoms. Let $\mathcal{F}^{\mathcal{L}} := \{\sigma^L \mid \sigma \in \{\mu, \nu\}, L \in \text{list}(\mathcal{L})\}$. *Labelled*
⁸ *formulas*, or \mathcal{L} -formulas, are defined as μMALL formulas, by replacing $\mathcal{F} = \{\mu, \nu\}$ with
⁹ $\mathcal{F}^{\mathcal{L}}$ in the grammar of formulas, in Definition 8. Negation is lifted to labelled formulas, as
¹⁰ $(\mu^L X.A)^\perp = \nu^L X.A^\perp$. We write $\sigma X.A$ for $\sigma^\emptyset X.A$, and standard, unlabelled formulas can
¹¹ thus be seen as labelled formulas where every label is empty. We define a *label-erasing*
¹² function $\lceil \bullet \rceil$ that associates to every \mathcal{L} -formula A the μMALL -formula $\lceil A \rceil$ obtained by
¹³ erasing every label and satisfying $\lceil \sigma^L X.B \rceil = \sigma X.\lceil B \rceil$.

- ¹⁴ The standard μMALL^∞ proof system is adapted, to handle labels, by updating the (id)
¹⁵ and (ν) rules of Figures 2.1 and 2.4 as

$$\frac{\lceil A \rceil = \lceil B \rceil^\perp}{\vdash A, B} (\text{id}') \quad \frac{\vdash A[\nu^{L,a} X.A], \Gamma}{\vdash \nu^L X.A, \Gamma} (\nu_b(a))$$

- ¹⁶ where, in $(\nu_b(a))$, a must be a fresh label name, meaning that a does not appear free in
¹⁷ the conclusion sequent of $(\nu_b(a))$ (in particular, $a \notin L$).

- ¹⁸ Since we are in a one-sided framework, only labels on ν operators are relevant. Therefore,
¹⁹ from now on, formulas have non-empty labels only on ν and we require, for the cut
²⁰ inference, that all labels of cut formulas are empty. *\mathcal{L} -preproofs* are, as in Definition 14,
²¹ possibly infinite derivations using \mathcal{L} -formulas, and the validity condition is expressed in
²² terms of labels in the following definition.

- ²³ **Definition 52** (\mathcal{L} -proof). An *\mathcal{L} -proof* is an \mathcal{L} -preproof such that for every infinite
²⁴ branch $\gamma = (s_i)_{i \in \omega}$ (seen as a sequence of sequent occurrences), there exists a sequence
²⁵ $(\nu^{L_i} X.G_i)_{i \in \omega}$ and a strictly increasing function ϵ on natural numbers such that for every
²⁶ $i \in \omega$,

- ²⁷ 1. the formula $\nu^{L_i} X.G_i$ is principal in $s_{\epsilon(i)}$

4 A polynomial sub-criterion

₁ 2. $\lceil \nu^{L_i} X.G_i \rceil = \lceil \nu^{L_{i+1}} X.G_{i+1} \rceil$ and

₂ 3. $L_{i+1} = (L_i, a_i)$ for some $a_i \in \mathcal{L}$.

₃ Note that the label-erasing function $\lceil \bullet \rceil$ is easily lifted to sequents and to \mathcal{L} -preproofs.

₄ And if π is an \mathcal{L} -proof, then $\lceil \pi \rceil$ is a μMALL^∞ proof.

5 4.1.2 Finite representations of circular \mathcal{L} -proofs.

₆ We now turn our attention to finite representations of (circular) \mathcal{L} -proofs. Immediately a
₇ difficulty occurs in comparison to non-labelled proofs: whereas an infinite non-labelled
₈ proof may happen to be regular, a valid \mathcal{L} -proof cannot be circular, because along every
₉ infinite branch, the sets of labels will grow endlessly. To form circular proofs with labels,
₁₀ some atoms must be forgotten when going bottom-up.

₁₁ We introduce two more rules: $(\mathcal{Q}(a))$ and (L-Wk) . The first one allows to forget one atom,
₁₂ just before recreating it by means of a back-edge to an already encountered ν -rule. The
₁₃ other one allows to forget any atom that will not be used to validate the proof. It is used
₁₄ to synchronise the different labels in a sequent before travelling through a back-edge.

₁₅ • labelled back-edge: $\frac{}{\vdash \nu^{L,a} X.A, \Gamma} \mathcal{Q}(a)}$ with the constraint that it must be the
₁₆ source of a back-edge to the conclusion of a $\frac{\vdash A[\nu^{L,a} X.A], \Gamma}{\vdash \nu^L X.A, \Gamma} (\nu_b(a))$ below $(\mathcal{Q}(a))$.

₁₇ • labelled weakening: $\frac{\vdash \Gamma, B[\nu^L X.A], \Delta}{\vdash \Gamma, B[\nu^{L,a} X.A], \Delta} (\text{L-Wk})$

₁₈ **Definition 53** ($\mu\text{MALL}_{\text{lab}}^\circlearrowright$). $\mu\text{MALL}_{\text{lab}}^\circlearrowright$ denotes the finite derivations of \mathcal{L} -sequents built
₁₉ from the rules in Definition 13 by replacing (ν) with $(\nu_b(a))$, $(\mathcal{Q}(a))$, (L-Wk) , such that

₂₀ 1. the root sequent has empty labels and

₂₁ 2. for every two $(\nu_b(a))$ and $(\nu_b(b))$ occurring in the derivation, $a \neq b$.

₂₂ The label-erasing function $\lceil \bullet \rceil$ lifts to a translation from $\mu\text{MALL}_{\text{lab}}^\circlearrowright$ to μMALL^ω b.e.-tree

₂₃ preproofs. Every rule of the labelled $\mu\text{MALL}_{\text{lab}}^\circlearrowright$ proof is sent by $\lceil \bullet \rceil$ to a valid rule of
₂₄ unlabelled μMALL^ω , except for the (L-Wk) rule, which can safely be removed:

$$\frac{\vdash \Gamma, B[\nu^L X.A], \Delta}{\vdash \Gamma, B[\nu^{L,a} X.A], \Delta} \text{ (L-Wk)} \quad \text{becomes} \quad \frac{\vdash \lceil \Gamma \rceil, \lceil B \rceil[\nu X.[A]], \lceil \Delta \rceil}{\vdash \lceil \Gamma \rceil, \lceil B \rceil[\nu X.[A]], \lceil \Delta \rceil}$$

¹ Since $\mu\text{MALL}_{\text{lab}}^\curvearrowright$ proofs are finite, label-erasing give rise to μMALL^ω b.e.-tree preproofs:

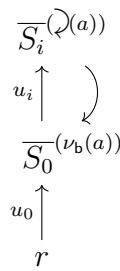
² **Definition 54** ($\mu\text{MALL}^\curvearrowright$). We denote by $\mu\text{MALL}^\curvearrowright$ the set of b.e.-tree preproofs that
³ are obtained from $\mu\text{MALL}_{\text{lab}}^\curvearrowright$ by label-erasing. This is a subset of all μMALL^ω b.e.-tree
⁴ preproofs.

⁵ **Proposition 8** ($\mu\text{MALL}^\curvearrowright \subseteq \mu\text{MALL}^\omega$). *Every preproof of μMALL^ω that is the image
⁶ of a proof in $\mu\text{MALL}_{\text{lab}}^\curvearrowright$ by label-erasing satisfies thread validity.*

⁷ We immediately give a proof sketch of this proposition; we then prove the two Lemmas 8
⁸ and 9 before giving a full proof of Proposition 8.

⁹ *Proof sketch of Proposition 8.* Consider a preproof $\lceil \pi \rceil$ in $\mu\text{MALL}^\curvearrowright$ which is the image
¹⁰ of an \mathcal{L} -proof π in $\mu\text{MALL}_{\text{lab}}^\curvearrowright$. We want to prove that every infinite branch b in $\lceil \pi \rceil$
¹¹ contains a **valid thread** (see Definition 17). Let b_0 be the corresponding infinite \mathcal{L} -branch
¹² in π . Notice that there is a sequent S_0 which is the lowest target of back-edge crossed
¹³ infinitely often by b_0 . Besides, S_0 is the conclusion of a $(\nu_b(a))$ rule, which unfolds some
¹⁴ $\nu^L X.A$.

¹⁵ We decompose b_0 , with root r ; S_0 conclusion of $(\nu_b(a))$ and $\nu^L X.A$ at position p_0 in S_0 ;
¹⁶ for any $i \geq 1$, S_i conclusion of a back-edge $(\mathcal{Q}(a))$ with $\nu^{L,a} X.A$ at position p_i in S_i . Then
¹⁷ we notice that $\mathfrak{T}(u_i)(p_0)$ is a thread $(S_0, p_0) \xrightarrow{*} (S_i, p_i)$ which is progressing, as its source
¹⁸ is the principal conclusion of the rule $(\nu_b(a))$. By gluing the $\mathfrak{T}(u_i)(p_0)$ and then erasing
¹⁹ labels, we get a valid thread of b in $\lceil \pi \rceil$.



4 A polynomial sub-criterion

- ¹ **Lemma 8.** Let b be an infinite branch in a b.e.-tree preproof, i.e. an infinite ascending
² path in its **branch graph**, starting from the root.
- ³ Then there is an occurrence of sequent in this b.e.-tree preproof, i.e. a vertex s in its
⁴ **branch graph**, which is the lowest one infinitely appearing on b .
- ⁵ Moreover, this occurrence of sequent (this vertex) is the target of a back-edge.
- ⁶ *Proof.* This is essentially a graph-theoretic property, which does not rely on the logical
⁷ content of the proof.
- ⁸ The crucial fact to notice is that, in general, in a tree, if S is a non empty, finite set of
⁹ vertices that is connected for the relation of comparability, i.e. if $\forall v, v' \in S, v \leq v'$ or $v' \leq$
¹⁰ v , then S has a minimum. This is proved by induction on the cardinal of S .
- ¹¹ Take then for S the set of vertices appearing infinitely on the branch b , and you get a
¹² vertex v , which is the desired vertex. In particular, when v is accessed in b from another
¹³ infinitely appearing vertex, it has to be via a back-edge. \square
- ¹⁴ **Lemma 9** (Follow-up of labels). If u is a path in the **branch graph** of a labelled circular
¹⁵ representation, if u does not cross the rule $(\nu_b(a))$, and if p is a position in the target
¹⁶ sequent of u (its top sequent) that is labelled with a , then $\mathbf{t}(u)(p)$ is defined and is a
¹⁷ position labelled with a in the source sequent of u (its bottom sequent).
- ¹⁸ *Proof.* This is quite straightforward, by induction on the length of u , and by looking at
¹⁹ the first (or the last) rule crossed by u . We use notably the fact that, when the induced
²⁰ thread $\mathfrak{T}(u)(p)$ is followed top-down, the label a cannot be erased because we do not
²¹ cross $(\text{Rec}(a))$ and the thread cannot reach a cut-formula because cut-formulas do not
²² contain labels. \square
- ²³ *Proof of Proposition 8.* Suppose π is a labelled circular representation.
- ²⁴ • Let $[\pi]$ be its erasure. $[\pi]$ is thus a circular representation of a μMALL^ω preproof.
 - ²⁵ • Suppose b an infinite branch of $[\pi]$, that is an infinite ascending path in the
²⁶ tree-with-back-edges $[\pi]$, starting from the root.
 - ²⁷ • Let b_0 be the corresponding infinite branch in π .
 - ²⁸ • Let S_0 be the occurrence of sequent in π which is the lowest back-edge target
²⁹ infinitely often crossed by b_0 , as given by Lemma 8. Being the target of some
³⁰ back-edge(s), S_0 is the conclusion of a $(\nu_b(a))$ rule, which unfolds some $\nu X.A$.

- 1 • This implies that b_0 is of the form $b_0 = r \xrightarrow{u_0}^* S_0 \xrightarrow{u_1}^* S_1 \xrightarrow{\text{be}} S_0 \xrightarrow{u_2}^* S_2 \xrightarrow{\text{be}} S_0 \dots$
 2 where r is the root of π and where the u_i s do not cross S_0 except at their sources.

- 3 • Let $p_0 = (0, \epsilon)$ be the position of the principal formula $\nu X.A$ in S_0 .
- 4 • Remark that, because of the existence of back-edges from every S_{i+1} to S_0 , all S_i s
 5 are identical sequents, except for the fact that a does not appear in S_0 whereas it
 6 appears at the only position p_0 in S_{i+1} .
- 7 • Now remark that for $i \geq 1$: $\mathfrak{T}(u_i)(p_0)$ is a ν -thread in u_i , its target is p_0 in S_i , which
 8 is labelled with a , in the occurrence of sequent just above S_0 , i.e. in the premise
 9 of $\nu_b(a)$, it goes through a position labelled with a , by Lemma 9, hence a position
 10 of $\nu X.A$ in the unfolding $A[\nu X.A]$, therefore, according to the definition of \mathfrak{T} , as
 11 described on Figure .1, p. 148, the source of $\mathfrak{T}(u_i)(p_0)$ is again the position p_0 of the
 12 main formula $\nu X.A$ in S_0 . To sum up: $\mathfrak{T}(u_i)(p_0)$ is a thread $(S_0, p_0) \xrightarrow{\mathfrak{T}(u_1)(p_1)}^* (S_1, p_0)$,
 13 and it is progressing, because its source is the principal conclusion of the rule
 14 $(\nu_b(a))$.

- 15 • By glueing the $\mathfrak{T}(u_i)(p_0)$ together, we get an infinite thread

$$(S_0, p_0) \xrightarrow{\mathfrak{T}(u_1)(p_0)}^* (S_1, p_0) \xrightarrow{\text{be}} (S_0, p_0) \xrightarrow{\mathfrak{T}(u_2)(p_0)}^* (S_2, p_0) \xrightarrow{\text{be}} (S_0, p_0) \dots$$

17 This thread is valid because every $\mathfrak{T}(u_i)(p_0)$ is progressing. And it is indeed a
 18 thread of $b_0 = r \xrightarrow{u_0}^* S_0 \xrightarrow{u_1}^* S_1 \xrightarrow{\text{be}} S_0 \xrightarrow{u_2}^* S_2 \xrightarrow{\text{be}} S_0 \dots$. Hence b_0 is valid, what was to
 19 be demonstrated.

□

21 **Proposition 9.** μMALL proofs can be translated to $\mu\text{MALL}^\curvearrowright$.

22 *Proof.* The target of the usual translation $\mu\text{MALL} \rightarrow \mu\text{MALL}^\omega$ [Doumane, 2017] is
 23 included in $\mu\text{MALL}^\curvearrowright$. See key case of the translation on Figure 4.1. □

24 Observe that a proof in $\mu\text{MALL}^\curvearrowright$ is not, in general, the translation of a μMALL proof.

25 4.1.3 Two alternative characterizations of $\mu\text{MALL}^\curvearrowright$

26 In the two following sections, we give two characterizations of $\mu\text{MALL}^\curvearrowright$ through validating
 27 sets, in Definition 58, and through a threading criterion over back-edges, in Definition 59.

Figure 4.1. translation $\mu\text{MALL} \rightarrow \mu\text{MALL}_{\text{lab}}^{\circlearrowleft}$

$$\frac{\vdash A[B], B^\perp \vdash B, \Gamma}{\vdash \nu X.A, \Gamma} \nu_{\text{inv}} \equiv \frac{\frac{\overline{\vdash \nu^a X.A, B^\perp} \circlearrowleft(a)}{\vdash A[\nu^a X.A], A[B]^\perp} [A]}{\frac{\vdash A[\nu^a X.A], B^\perp \quad \vdash A[B], B^\perp}{\frac{\vdash A[\nu^a X.A], B^\perp}{\vdash \nu X.A, B^\perp} \nu_b(a)}} \text{cut} \quad \frac{\vdash \nu X.A, B^\perp}{\vdash B, \Gamma} \text{cut}$$

- ¹ **Definition 55.** Given a directed graph $G = (V, E)$ and a set $S \subseteq V$, the set of vertices from which S is accessible is denoted as $S\uparrow := \{v \in V \mid \exists s \in S, v \rightarrow^* s\}$. Similarly $S\downarrow$ is the set of vertices accessible from S .

Definition 56 (G_π). For a finite representation π of a μMALL^ω preproof, the graph G_π is s. t. (i) its *vertices* are all positions of ν -formulas in all occurrences of sequents in π , plus the vertex \perp :

$$V_\pi := \left\{ \begin{array}{l} (i) \text{ } v \text{ position of a sequent } \Gamma \text{ in } \pi \\ (ii) \text{ } i \text{ position of a formula } A \text{ in } \Gamma \\ (iii) \text{ } p \text{ position of a } \nu\text{-subformula in } A \end{array} \right\} \uplus \{\perp\};$$

- ⁴
⁵ and (ii) its *edges* go from a position in a formula to the position that comes from it in the
⁶ sequent just below, as induced by the threading function of Definition 96, or to the extra
⁷ vertex \perp if it is a cut formula. In case this is a conclusion formula, there is no outgoing
⁸ edge.

- ⁹ We illustrate the construction of the edges of the graph defined in definition 56 with the
¹⁰ the following examples in which we have indexed the apparent ν -formulas by numbers
¹¹ representing vertices of the graph:

$$\frac{\vdash \nu_1 X.X, \nu_2 X.X \vdash \mathbf{1} \oplus \nu_3 X.X}{\vdash \nu_4 X.X \otimes (\mathbf{1} \oplus \nu_5 X.X), \nu_6 X.X} \otimes$$

- ¹² induces edges $1 \rightarrow 4, 2 \rightarrow 6, 3 \rightarrow 5$,

$$\frac{\vdash \nu_1 X.X, (\mathbf{1} \oplus \nu_2 X.X), \nu_3 X.X}{\vdash \nu_4 X.X \wp (\mathbf{1} \oplus \nu_5 X.X), \nu_6 X.X} \wp$$

¹ induces edges $1 \rightarrow 4, 2 \rightarrow 5, 3 \rightarrow 6$ and

$$\frac{\vdash (\nu_4 Y.(\nu_5 X.(\nu_6 Y.X) \otimes X)) \otimes \nu_7 X.(\nu_8 Y.X) \otimes X, \nu_9 X.X}{\vdash \nu_1 X.(\nu_2 Y.X) \otimes X, \nu_3 X.X} \nu$$

² induces edges $4 \rightarrow 2, 6 \rightarrow 2, 8 \rightarrow 2, 5 \rightarrow 1, 7 \rightarrow 1, 9 \rightarrow 3$. Moreover, if the conclusion of
³ this last rule is the target of a back-edge whose source is $\vdash \nu_{10} X.(\nu_{11} Y.X) \otimes X, \nu_{12} X.X$
⁴ then this back-edge also induces edges $1 \rightarrow 10, 2 \rightarrow 11, 3 \rightarrow 12$.

⁵ In the case of a cut formula, the formula has no corresponding formula in the conclusion
⁶ sequent and in this case it induces an outgoing edge, pointing to the extra vertex \perp :

$$\frac{\vdash \nu_2 X.X \quad \vdash \mu X.X, \nu_3 X.X}{\vdash \nu_1 X.X} \text{cut}$$

⁷ induces edges $2 \rightarrow \perp, 3 \rightarrow 1$.

⁸ *Remark 17.* Note that a vertex of the above graph may therefore have

- ⁹ • many outgoing edges: in case it in a sequent which is the target of some back-edges;
- ¹⁰ • no outgoing edges: essentially the extra vertex \perp and the ν -formulas in the conclusion
¹¹ of the proof if it is not a target of back-edge;
- ¹² • many ingoing edges: see a ν -rule with $\nu X.X \otimes X$ or $\nu X.X \wp X$ as principal
¹³ conclusion;
- ¹⁴ • no ingoing edges: see the $\nu X.X$ in the $\mathbf{1} \oplus \nu X.X$ principal conclusion of a (\oplus_1) -rule.

¹⁵ **Definition 57** (G_r, S_r, T_r) . Let π be a finite representation of a μMALL^ω preproof
¹⁶ and (r) an occurrence of a (ν) -rule. We define the subgraph $G_r = (V_r, E_r)$ of G_π and
¹⁷ $S_r, T_r \subseteq V_r$ st:

- ¹⁸ – **vertices** V_r are the extra vertex \perp plus all positions that are in the conclusion of this
¹⁹ rule and in all above sequents, that is all sequents from which the conclusion of (r) can
²⁰ be reached, in the sense of Definition 55;
- ²¹ – **edges** E_r are all edges of G_π between those vertices minus the edges of G_π that are
²² induced by the back-edges of π targetting the conclusion of (r) , if there are some.
- ²³ – $S_r \subseteq V_r$ is the set of all positions of the principal formulas of the sources sequents of
²⁴ the back-edges targetting the conclusion of (r) ;
- ²⁵ – $T_r \subseteq V_r$ is the set of all positions of all subformulas of the conclusion of (r) except for
²⁶ the very position of its principal formula, plus the extra vertex \perp .

4 A polynomial sub-criterion

¹ **Definition 58.** Let (r) be an occurrence of a (ν) -rule in a preproof π of μMALL^ω . A ² *validating set* for (r) is a set $L \subseteq V_\pi$ such that $L = L\downarrow$ and $S_r \subseteq L \subseteq (V_r \setminus T_r)$.

³ **Proposition 10.** Let (r) be an occurrence of a (ν) -rule of a preproof π of μMALL^ω .

⁴ There exists a validating set for (r) iff T_r is not accessible from S_r in G_r iff $S_r\downarrow \subseteq$ ⁵ $V_r \setminus (T_r\uparrow)$.

⁶ In this case, $S_r\downarrow$ is the smallest validating set of (r) and $V_r \setminus (T_r\uparrow)$ is the biggest one.

⁷ *Proof.* It is based on the fact that the complement of a downward-closed set is upward-closed. We then get the inclusions : $S_r \subseteq S_r\downarrow \subseteq L\downarrow = L \subseteq V_r \setminus (T_r\uparrow) \subseteq V_r \setminus T_r$. \square

⁹ The following proposition gives an alternative criterion for μMALL^ω .

¹⁰ **Proposition 11.** A finite representation π of a μMALL^ω preproof is a representation of ¹¹ a $\mu\text{MALL}_{\text{lab}}^\omega$ proof iff. every occurrence of a ν -rule of π has a validating set.

Proof. Let us assume that every ν rule of π has a validating set. There is a finite number of ν rules in the representation; we choose a we label them with distinct variables a_1, \dots, a_n , in a way such that if the ν rule labelled by a_i is below the rule labelled by a_j in the representation then $i \leq j$. We denote by L_i a validating set for $\nu(a_i)$. We then do the following for each i , going from 1 to n : for each occurrence of ν -formula $\nu^V X.A$ that is at a position belonging to L_i , add the variable a_i to V , that is replace this occurrence of $\nu^V X.A$ with $\nu^{V,a_i} X.A$. By doing this it may happen that we break the validity of some rules of the representation: because L_i , although downward closed, is in general not upward closed, so we may end with a situation in which this

$$\frac{\vdash A, C[\nu^V X.D] \quad \vdash A, C[\nu^V X.D]}{\vdash A \& B, C[\nu^V X.D]} \&$$

becomes

$$\frac{\vdash A, C[\nu^{V,a} X.D] \quad \vdash B, C[\nu^V X.D]}{\vdash A \& B, C[\nu^{V,a} X.D]} \&$$

which is not anymore a valid rule. We then patch this by adding as many (L-Wk) rules as needed on the premises:

$$\frac{\vdash A, C[\nu^{V,a} X.D] \quad \vdash B, C[\nu^{V,a} X.D]}{\vdash A \& B, C[\nu^{V,a} X.D]} \xrightarrow{(\text{L-Wk})} \&$$

¹ Similarly it may happen that the source of a back-edge get a bigger labelling than the
² target of this back-edge; we patch this by adding (L-Wk) rules under the source sequent
³ of the back-edge. When this operation has been done for every i , from 1 to n , we obtain
⁴ a validly labelled proof of $\mu\text{MALL}_{\text{lab}}^\circlearrowleft$.

⁵ Conversely, let π_0 be a $\mu\text{MALL}_{\text{lab}}^\circlearrowleft$ representation such that $\pi = |\pi_0|$. Up to renaming, we
⁶ can assume that all (ν_b) rules of π_0 are labelled with distinct variables. For every (ν)
⁷ rule occurrence in π , consider the corresponding $(\nu_b(a))$ rule in π_0 and let L_a be the set
⁸ of all occurrences of ν -formulas in π_0 that carry the variable a in their labelling. The
⁹ constraints on the labelling of $\mu\text{MALL}_{\text{lab}}^\circlearrowleft$ proof precisely get L_a to be a validating set for
¹⁰ the considered occurrence of (ν_b) in π . \square

¹¹ **Proposition 12.** *Checking validity of a $\mu\text{MALL}_{\text{lab}}^\circlearrowleft$ preproof is decidable. Membership in
¹² $\mu\text{MALL}^\circlearrowleft$ can be decided in a time quadratic in the size of the (circular) preproof.*

¹³ *Proof.* The former is immediate. The latter reduces to checking accessibility in a graph
¹⁴ for each back-edge target, which can be done in quadratic time. \square

¹⁵ **Definition 59.** A finite representation of a μMALL^ω preproof finite representation is
¹⁶ *strongly valid* when:

- ¹⁷ (i) every back-edge targets the conclusion of a (ν) rule and
- ¹⁸ (ii) if an occurrence (r') of $\frac{\vdash A[\nu X.A], \Gamma}{\vdash \nu X.A, \Gamma}$ (ν) is the target of a back-edge, coming from
¹⁹ an occurrence (r) of $\overline{\vdash \nu X.A, \Gamma}^\circlearrowleft$ then every path t starting from the principal formula
²⁰ $\nu X.A$ of the conclusion of (r) , following the thread function (potentially through several
²¹ back-edges, but never on or below the occurrence (r') of (ν)), ends on the principal formula
²² $\nu X.A$ of the conclusion of (r') .

²³ **Proposition 13.** *A finite representation π of a μMALL^ω preproof is strongly valid iff.
²⁴ every ν -rule of π has a validating set iff. it is the representation of a $\mu\text{MALL}_{\text{lab}}^\circlearrowleft$ proof.*

²⁵ *Proof.* The second equivalence is Proposition 11, so we only need to check the first one:

²⁶ Let us assume that π has a validating set. Let us consider one occurrence $\frac{\vdash A[\nu X.A], \Gamma}{\vdash \nu X.A, \Gamma}$
²⁷ of a ν -rule in π and a path u in the subgraph above this ν -rule, going down, from the
²⁸ source of a back-edge targetting this ν -rule, to the ν -rule itself, ending by this ν -rule. u
²⁹ has then premise and conclusion equals to $\vdash \nu X.A, \Gamma$.

4 A polynomial sub-criterion

1 Let us denote by L a validating set of this (ν) -rule occurrence, and let us denote by t
2 the maximal thread going down in u starting from the main $\nu X.A$ in its premise. This
3 occurrence of $\nu X.A$ is in L , because L is a validating set. Then, because L is downward
4 closed, all vertices of t are in L . Therefore the lowest vertex of t , which is a position in
5 the $\vdash \nu X.A, \Gamma$ conclusion of the considered ν -rule, or \perp , is also in L . But in this last
6 sequent occurrence, the only position that is in L is the one of the main $\nu X.A$, which is
7 consequently the end point of t .

8 Conversely, let us consider an occurrence of a (ν) -rule in π , whose conclusion has the
9 form $\vdash \nu X.A, \Gamma$, and let us assume that it has no validating set. It is, by Proposition 10,
10 equivalent to say that there is a path t such that:

- 11 • t stays above the considered occurrence of (ν) -rule;
- 12 • t goes down from the source $\nu X.A, \Gamma$ of a back-edge targetting the (ν) -rule we
13 consider, to the conclusion $\nu X.A, \Gamma$ of this (ν) -rule;
- 14 • t starts from the main $\nu X.A$ of its premise;
- 15 • t ends either on a cut-formula or on a position that is not the principal $\nu X.A$.

16 u therefore violates strong validity, as defined in Definition 59. \square

17 **Corollary 3.** *The fragments defined in Definitions 54 and 59 coincide.*

18 4.2 On loops and threads

19 **Definition 60** ($\mu\text{MALL}^\varnothing$). The system and criteria of the previous section induce, by
20 erasing the labels and the inference rules taking care of labels and unfoldings of *back-edges*,
21 a fragment of μMALL^ω pre-proofs, denoted as $\mu\text{MALL}^\varnothing$.

22 **Lemma 10** (Properties of the tree with back-edges structure). *When considering the
23 ancestry order in the tree:*

- 24 1. *every upper-bounded pair is ordered*
- 25 2. *every non-empty set of vertices that is connected for the relation of comparability
26 has a minimum*
- 27 3. *two successive vertices on a path in the graph are comparable*

4. along an infinite path in the graph, the set of infinitely visited vertices has a minimum and this minimum is the target of a back-edge, hence a ν rule.

³ Proof sketch.

- 4 1. follows from the definition of a tree
 - 5 2. induction on the cardinal of this set
 - 6 3. follows from the imposed structure of back-edges
 - 7 4. immediate consequence of the three previous properties

□

9 Lemma 11 (Properties of paths in the labelled preproof).

- 10 1. when tracing a thread from the top (the end) of a path, the labels cannot disappear:
 11 if the starting formula (in the premise) is a $\nu^V X.A$ with $a \in V$ then the thread
 12 cannot end in a cut formula, it ends in the conclusion and all formulas along the
 13 thread contain the a label.

14 2. above $\nu_b(a)$, all occurrences of a are carried by occurrences of the same formula:
 15 they are all occurrences of the ν -formula that is the main formula of the conclusion
 16 of $\nu_b(a)$.

$\vdash \nu^V X.A, \Gamma$

- $a \in V$
 - $a \in W$ and this is the only occurrence of a in the conclusion

then this thread ends on $\nu^w X.A$ and all formulas along the thread contain $\nu X.A$ as a subformula.

23 Proof sketch.

- ²⁴ 1. induction on the length of the path, considering the last one.

4 A polynomial sub-criterion

- 1 2. induction on the height of the sequent in which a appears.
- 2 3. immediate consequence of the two previous properties.

3

□

4 **Proposition 14** (β). $\mu\text{MALL}^\beta \subseteq \mu\text{MALL}^\omega$. That is: the loop criterion implies the thread validity.

6 *Proof sketch.*

- 7 • take an arbitrary infinite branch, that is an infinite path in the graph
- 8 • look at it from the moment from which all visited vertices are infinitely visited
- 9 vertices
- 10 • take v_m to be the lowest of them: it is a $\nu_b(a)$, by Lemma 10
- 11 • cut the infinite path in parts delimited by the occurrences of v_m
- 12 • each of this part induces a thread from the main formula of $\nu_b(a)$ to itself, that
- 13 is a $\nu X.A$, and, along this thread, all formulas have $\nu X.A$ as a subformula, by
- 14 Lemma 11
- 15 • these thread parts can be joined as an infinite thread in which $\nu X.A$ is the smallest
- 16 formula and progress at each occurring of v_m , that is infinitely often. This thread
- 17 validates this branch.

18

□

19 **Proposition 15** (α). The target of the usual translation $\mu\text{MALL} \rightarrow \mu\text{MALL}^\omega$ is included

20 in μMALL^β .

Key of the translation.

$$\frac{\frac{\frac{\frac{\frac{\vdash \nu^a X.A, B^\perp}{\vdash \nu^a X.A, B^\perp} \beta(a)}{[A]} \quad \frac{\vdash A[\nu^a X.A], A[B]^\perp \quad \vdash A[B], B^\perp}{\vdash A[\nu^a X.A], B^\perp \quad \nu_b(a)} \text{cut}}{\vdash A[\nu^a X.A], B^\perp \quad \nu_b(a)} \text{cut}}{\vdash \nu^a X.A, \Gamma} \nu_{\text{inv}} \quad \equiv \quad \frac{\frac{\vdash \nu^\emptyset X.A, B^\perp}{\vdash \nu^\emptyset X.A, \Gamma} \text{cut}}{\vdash \nu^\emptyset X.A, \Gamma}$$

1

□

² 4.3 Conclusion of the chapter

³ This chapter introduced the loop criterion for circular representations of infinite preproofs
⁴ of μMALL^ω . This defines a fragment of the circular representations of μMALL^ω which
⁵ we called $\mu\text{MALL}^\circlearrowright$.

⁶ We also defined a new proof system called $\mu\text{MALL}_{\text{lab}}^\circlearrowright$. The proofs of $\mu\text{MALL}_{\text{lab}}^\circlearrowright$ are
⁷ labelings of circular representations of preproofs, valid for the loop criterion. While
⁸ circular representation of preproofs make use of a global validity criterion such as the
⁹ thread criterion or the loop criterion, the validity of a proof in $\mu\text{MALL}_{\text{lab}}^\circlearrowright$ is a purely
¹⁰ local property, which can be checked in linear time.

¹¹ We proved that the circular representation of preproof obtained by erasing the labels
¹² of a $\mu\text{MALL}_{\text{lab}}^\circlearrowright$ proof is valid for the loop criterion and, conversely, that any circular
¹³ representation that is valid for the loop criterion can be turned into a proof of $\mu\text{MALL}_{\text{lab}}^\circlearrowright$
¹⁴ by labelling some of its formulas.

¹⁵ We made that last property explicit by providing a procedure to check a circular represen-
¹⁶ tation with respect to the loop criterion and to turn it into a labelled proof of $\mu\text{MALL}_{\text{lab}}^\circlearrowright$
¹⁷ when it is valid. This algorithm runs in quadratic time.

¹ 5 Finitisation

² Remember that there was the finitary systems. Then infinitary systems were proposed as
³ an alternative. And there is a canonical translation from finitary proofs to infinitary proofs.
⁴ This implies in particular that any conclusion that is provable in the finitary system is
⁵ also provable in the infinitary system. The converse is known as the Brotherston-Simpson
⁶ conjecture. [Brotherston and Simpson, 2007] It is also called the problem of finitisation:
⁷ can we turn an infinitary proof into a finitary one, and how? It is known that for some
⁸ particular systems [???] this conjecture is false. But the question is still open in the case
⁹ of μMALL , μMALL^∞ and μMALL^ω .

¹⁰ Here we can split the question of finitisation into two questions:

- ¹¹ • If a conclusion is provable in μMALL^∞ , that is with an infinite proof, valid for the
¹² thread criterion, is it also provable by mean of a circular proof, that is in μMALL^ω ?
¹³ • If a conclusion is provable by a circular proof, valid for the thread criterion, that is
¹⁴ a proof in μMALL^ω , is it already provable in the finitary system μMALL ?

¹⁵ Both those questions are, as of today, open problems.

¹⁶ Now, in the previous chapter, we provided a new criterion, the loop criterion, which
¹⁷ defines a new logic $\mu\text{MALL}^\curvearrowright$, which has two properties:

- ¹⁸ • the canonical translation of any finitary proof is a circular representation which is
¹⁹ valid for the loop criterion, so any conclusion which is provable in μMALL is also
²⁰ provable in $\mu\text{MALL}^\curvearrowright$
²¹ • if the circular representation of a preproof is valid for the loop criterion, then it is
²² also valid for the thread criterion, so any conclusion that is provable in $\mu\text{MALL}^\curvearrowright$ is
²³ also provable in μMALL^ω .

²⁴ This allows us to split the problem of finitisation one more time:

- ²⁵ • If a conclusion is provable in μMALL^∞ , is it already provable in μMALL^ω ? (This
²⁶ is the same question as before.)

- 1 • If a conclusion is provable in μMALL^ω , is it already provable in $\mu\text{MALL}^\curvearrowleft$?
- 2 • If a conclusion is provable in $\mu\text{MALL}^\curvearrowleft$, is it already provable in μMALL ?
- 3 In this chapter, we answer positively this third question. We prove that any conclusion
4 provable in $\mu\text{MALL}^\curvearrowleft$ is already provable in μMALL . We do so by providing an explicit
5 method which takes as input a circular representation of preproof, valid for the loop
6 criterion, and output a standard, finitary μMALL proof.

7 **5.1 On Brotherston-Simpson's conjecture: finitizing 8 circular proofs**

- 9 The aim of this section is to prove a converse of Proposition 15: *Every provable sequent*
10 *of $\mu\text{MALL}^\curvearrowleft$ is provable in μMALL .*
- 11 This will be proved by defining a translation from every $\mu\text{MALL}^\curvearrowleft$ proof of a sequent $\vdash \Gamma$
12 containing no label variable into a μMALL proof of the same sequent.
- 13 Let us consider a $\mu\text{MALL}^\curvearrowleft$ proof π . Up to renaming of bound variables, we can assume
14 that all (ν_b) rules are labelled by distinct labels. For every two labels a and b occurring in
15 π , we say that $a \leq b$ whenever $(\nu_b(a))$ is under $(\nu_b(b))$. This order is well-founded because
16 finite.

17 **Definition 61.** For every rule $\frac{\vdash A[\nu^{V,a} X.A], \Gamma}{\vdash \nu^V X.A, \Gamma} (\nu_b(a))$ we define $\Gamma_{(a)}$ to be Γ .

18 We now define

- 19 1. for each atom a a sequent Γ_a formed of non-labelled formulas;
- 20 2. for each formula A (with labels) occurring in the proof, a formula $\llbracket A \rrbracket$ without
21 labels:

22 **Definition 62.** We define by mutual induction:

- 23 1. $\Gamma_a := \llbracket \Gamma_{(a)} \rrbracket$.

1 2. $H_\emptyset[F] := F$ and $H_{V,a}[F] := \otimes\Gamma_a^\perp \oplus H_V[F]$. (i. e. $H_V[F]$ is isomorphic to $(\bigoplus_{a \in V} \otimes\Gamma_a^\perp) \oplus F$.)

3 3. By induction on formula A , $\llbracket A \rrbracket$ is:

- 4 • $\llbracket \nu^V X.A \rrbracket := \nu X.H_V[\llbracket A \rrbracket]$
- 5 • it is homomorphic on other connectives: $\llbracket X \rrbracket := X$, $\llbracket \mathbf{1} \rrbracket := \mathbf{1}$, $\llbracket \mu X.A \rrbracket := \mu X.\llbracket A \rrbracket$, $\llbracket A \otimes B \rrbracket := \llbracket A \rrbracket \otimes \llbracket B \rrbracket$, etc.

7 4. $\llbracket \cdot \rrbracket$ is lifted from formulas to sequences of formulas, pointwise.

8 This is well-founded because, since any two distinct ν_b rules wear distinct variables,
 9 the only Γ_b that are needed in the computation of Γ_a are those with $b < a$. Note that
 10 $\llbracket A \rrbracket = A$ as soon as A has no label variable. We can now state and prove the finitization
 11 theorem:

12 **Theorem 5.** *Every provable sequent of μMALL^\swarrow is provable in μMALL .*

13 *Proof.* Let π be a $\mu\text{MALL}_{\text{lab}}^\swarrow$ proof and replace, everywhere, each formula A by $\llbracket A \rrbracket$. All
 14 rules in this (almost) new derivation are now valid instances of μMALL rules, except
 15 for (ν_b) , $(L\text{-Wk})$ and (Q) rules. Actually, images of these rules by sequent translation $\llbracket \cdot \rrbracket$
 16 are derivable in μMALL as shown in fig. 5.1 (a), (b) and (c) for (Q) , $(L\text{-Wk})$ and (ν_b) ,
 17 respectively.

18 Replacing each instance of a (ν_b) , $(L\text{-Wk})$ or (Q) rule in π by its derived version, we get a
 19 fully valid proof of μMALL . If the conclusion of the original μMALL^\swarrow proof was $\vdash \Gamma$ then
 20 what we get is a proof in μMALL of $\vdash \llbracket \Gamma \rrbracket$, i. e. the conclusion of the original μMALL^\swarrow
 21 proof, if Γ contains no label variable. \square

22 5.2 Relaxing the labelling of proofs

23 In this section, we discuss a possible extension of the labelling defined in section 3, in
 24 order to capture more proofs retaining (i) the ability to locally certify the validity and (ii)
 25 to some extent, the ability to finitize circular proofs. In order to motivate this extension,
 26 we shall consider a simpler example than the one in fig. .2 (π_∞).

$$\begin{array}{c}
 \frac{\frac{\frac{\frac{\frac{\vdash \llbracket A[\nu^V X.A] \rrbracket, \Gamma}{\vdash H_V[\llbracket A[\nu^V X.A] \rrbracket, \Gamma]^{|\mathcal{V}|}}^{(\oplus_1)}}{(\nu)} \quad \frac{\frac{\overline{\vdash \otimes \Gamma_a^\perp, \Gamma_a}^{(\otimes), (\text{id})}}{\vdash H_{V,a}[\llbracket A[\nu^{V,a} X.A] \rrbracket, \Gamma_a]}^{(\oplus_0)}}{(\nu)} \quad (a) \quad \frac{\overline{\vdash \otimes \Gamma_a^\perp, \Gamma_a}^{(\otimes), (\text{id})}}{\vdash \llbracket \nu^{V,a} X.A \rrbracket, \Gamma_a}^{(\nu)} \\
 \frac{\frac{\frac{\vdash \llbracket B[\nu^V X.A] \rrbracket, \Gamma}{\vdash H_V[\llbracket B[\nu^V X.A] \rrbracket, H_V[\llbracket A[\nu^V X.A] \rrbracket]}^{(\text{id})}}{\vdash H_{V,a}[\llbracket B[\nu^V X.A] \rrbracket, H_V[\llbracket A[\nu^V X.A] \rrbracket]}^{(\oplus_1)}}{(\mu)} \quad \frac{\frac{\vdash H_{V,a}[\llbracket A[\nu^V X.A] \rrbracket, [\nu^V X.A]^\perp]}{\vdash \llbracket \nu^{V,a} X.A \rrbracket, [\nu^V X.A]^\perp}^{(\nu_{\text{inv}}^0)}}{\frac{\frac{\vdash \llbracket B[\nu^{V,a} X.A] \rrbracket, [\llbracket B[\nu^V X.A] \rrbracket]^\perp}{\vdash \llbracket B[\nu^{V,a} X.A] \rrbracket, \Gamma}^{(\llbracket B \rrbracket)}}{\vdash \llbracket B[\nu^{V,a} X.A] \rrbracket, \Gamma}^{(\text{cut})}} \quad (b) \\
 \frac{\frac{\frac{\vdash \llbracket A[\nu^{V,a} X.A] \rrbracket, \Gamma_a}{\vdash H_V[\llbracket A[\nu^{V,a} X.A] \rrbracket, \Gamma_a]^{|\mathcal{V}|}}^{(\oplus_1)}}{\vdash H_V[\llbracket A[\nu^{V,a} X.A] \rrbracket, \mathfrak{F}\Gamma_a]^{(\mathfrak{F})}} \quad \frac{\frac{\vdash H_V[\llbracket A[\nu^{V,a} X.A] \rrbracket, H_V[\llbracket A[\nu^{V,a} X.A] \rrbracket]}{(\text{id})}}{\vdash H_V[\llbracket A[\nu^{V,a} X.A] \rrbracket, H_{V,a}[\llbracket A[\nu^{V,a} X.A] \rrbracket]}^{(\&)}}{(\mu)} \quad \frac{\vdash H_V[\llbracket A[\nu^{V,a} X.A] \rrbracket, [\nu^{V,a} X.A]^\perp]}{\vdash \llbracket \nu^V X.A \rrbracket, \Gamma_a}^{(\nu)} \quad (c)
 \end{array}$$

Figure 5.1. Derivability of (a) $\llbracket (\nu_f) \rrbracket$ rule ; (a) $\llbracket (\mathcal{Q}) \rrbracket$ rule ; (b) $\llbracket (L-Wk) \rrbracket$ rule and (c) $\llbracket (\nu_b) \rrbracket$ rule .

$\frac{\frac{\frac{D \vdash D}{(D \otimes L, L \vdash D \otimes T)} \stackrel{(id)}{\longrightarrow} \frac{(1)}{L, L \vdash T} (\mathcal{Q})}{\frac{D \otimes L, L \vdash D \otimes T}{L, L \vdash D \otimes T}} \stackrel{(\mathfrak{Y})(\otimes)}{\longrightarrow}$	$\frac{\frac{\frac{D \vdash D}{(D \otimes L^{a+}, L \vdash D \otimes T)} \stackrel{(id)}{\longrightarrow} \frac{(1)}{L^{a+}, L \vdash T} (\mathcal{Q}(a))}{\frac{D \otimes L^{a+}, L \vdash D \otimes T}{L^{a-}, L \vdash D \otimes T}} \stackrel{(\mathfrak{Y})(\otimes)}{\longrightarrow}$
$\frac{\frac{\frac{D \vdash D}{(D \otimes L, L \vdash D \otimes T)} \stackrel{(id)}{\longrightarrow} \frac{(1)}{L, L \vdash T} (\mathcal{Q})}{\frac{D \otimes L, L \vdash D \otimes T}{L, L \vdash D \otimes T}} \stackrel{(\mathfrak{Y})(\otimes)}{\longrightarrow}$	$\frac{\frac{\frac{D \vdash D}{(D \otimes L^{a+}, L \vdash D \otimes T)} \stackrel{(id)}{\longrightarrow} \frac{(1)}{L^{a+}, L \vdash T} (\mathcal{Q}(a))}{\frac{D \otimes L^{a+}, L \vdash D \otimes T}{L^{a-}, L \vdash D \otimes T}} \stackrel{(\mathfrak{Y})(\otimes)}{\longrightarrow}$

Figure 5.2. (a) Interleaving example; (b) Interleaving example labelled.

Corresponding sources and targets of back-edges are denoted by parenthesized numbers.

- ¹ Let D be an arbitrary formula. Lists of D can be represented as proofs of $L_0 := \mu X.1 \oplus (D \otimes X)$ and it is possible to encode in μMALL^ω the function taking two lists and computing the tree of all their possible interleaving, as a proof with conclusion¹ $L_0, L_0 \vdash T_0$, where $T_0 := \mu X.L_0 \oplus ((D \otimes X) \& (D \otimes X))$. By replacing L_0 and T_0 with $L := \mu X.D \otimes X$ and $T := \mu X.(D \otimes X) \& (D \otimes X)$, we get a example equally interesting and more readable, which we present in fig. 5.2. In this interleaving function, every recursive call leaves one of the two arguments untouched and makes the other one decrease. This guarantees that the tree of recursive calls is well-founded. Difficulties, however, arises from the fact that it is not necessarily always the same argument that will decrease.

- ¹⁰ More formally: every infinite branch in the preproof above has two interesting threads,
¹¹ going through the L formulas. In every branch going infinitely often to the left (resp.
¹² to the right), the thread going through the left L (resp. the right L) will be validating.
¹³ That preproof is thus a valid μMALL^ω proof. However, our previous labelling method
¹⁴ cannot be applied here for two reasons:

- 15 1. in our previous setting, labelled pre-proof have the property that one can know
16 which thread will validate a branch, just by knowing the lowest target of back-edge
17 that is visited infinitely often by the branch. This is not the case here, because the
18 two back-edges, while inducing different validating threads, have the same target;

- ¹⁹ 2. in our previous setting, back-edges must target (ν) rules, which is not the case here.

- Both difficulties have, in fact, the same origin, namely that in our previous setting the (ν) rule has two roles: being the target of a back-edge and ensuring thread progression. Both difficulties also have the same solution: dissociating these two roles. We therefore introduce, in def. 63, a new rule (Rec) , whose only effect is to allow its premise to be the target of a back-edge, and to introduce a new label. Since (Rec) is disentangled from greatest fixed point unfolding, the labelling must account for the progression of a thread. That is why every atomic label is now given in one of two modes: a passive mode $(a-)$

¹In the following, we write $A \multimap B$ for $\overline{A}^\perp \wp B$, and $\Gamma \vdash \Delta$ for $\vdash \Gamma^\perp, \Delta$; exchange rules are left implicit.

5 Finitisation

- ¹ and an active one ($a+$). Only an unfolding by a (ν) can turn a $-$ into a $+$.
- ² Let us now turn back to our introductory example: π_∞ . For that example, simply
³ separating the introduction of back-edges and the coinductive progress is not enough.
⁴ Indeed, since targets of back-edges do not require to unfold a ν , there is *a priori* no reason
⁵ to require that the sequents contains some ν -formula. While this is slightly hidden in the
⁶ merge example, π_∞ gives a clear example of that and suggests that the (Rec) inference
⁷ should have the ability to add labels *deeply* in the sequent, *i.e.* not only on the topmost
⁸ ν fixed-points, but also to greatest fixed points occurring under some other connectives.
⁹ The same remark applies to the back-edge rule since its conclusion sequents have the
¹⁰ same structure as those of (Rec) .

- ¹¹ Driven by these observations, we now define a new labelling of circular preproofs and
¹² prove its correctness with respect to thread-validity.

- ¹³ **Definition 63** (Extended labelling). Labelled formulas are built on the same grammar as
¹⁴ previously, except that labels are lists of *signed variables*, that is of pairs of a variable and
¹⁵ a symbol in $\{+, -\}$. Derivations are built with μ MALL inferences plus the following rules:
¹⁶
$$\frac{\vdash \nu^L X.A, \Gamma}{\vdash \nu^{L,a-} X.A, \Gamma} \text{ (L-Wk}(a-)) \quad \frac{\vdash \nu^{L,a-,L'} X.A, \Gamma}{\vdash \nu^{L,a+,L'} X.A, \Gamma} \text{ (L-Wk}(a+)) \quad \frac{\vdash A[\nu^{a_1+, \dots, a_n+} X.A], \Gamma}{\vdash \nu^{a_1-, \dots, a_n-} X.A, \Gamma} \text{ } (\nu) \quad \frac{\vdash \Gamma[\nu^{L,a-} X.A]}{\vdash \Gamma[\nu^L X.A]} \text{ } (Rec(a)) \quad \frac{}{\vdash \Gamma[\nu^{L,a+} X.A]} \text{ } (\bar{Q}(a))$$
- ¹⁷ and the constraints that:

- ¹⁸ • a cut-formula cannot contain a non-empty label;
- ¹⁹ • all (Rec) rules must wear distinct variables;
- ²⁰ • every $(Rec(a))$ rule must have at least one occurrence of “ $a-$ ” in its premise;

- ²¹ • each $\frac{}{\vdash \Gamma[\nu^{L,a+} X.A]} \text{ } (\bar{Q}(a))$ rule is connected to the premise of a $\frac{\vdash \Gamma[\nu^{L,a-} X.A]}{\vdash B[\nu^L X.A], \Gamma} \text{ } (Rec(a))$ via a back-edge. This implies in particular that this $(\bar{Q}(a))$ must be above this $(Rec(a))$ and that the premise of this $(Rec(a))$ must be the same sequent as the conclusion of this $(\bar{Q}(a))$ except for the change of sign of a , at every of its occurrences in the sequent.

- ²⁶ **Proposition 16** (Soundness of labelling). *If π is an extended labelled circular representation then $[\pi]$ is a circular representation of a valid μ MALL $^\omega$ proof.*

- ²⁸ *Proof.* See proof in appendix 5.4, p. 99. □

- ²⁹ We now label our two examples with this new system. We will show that, while it is
³⁰ quite straightforward for the interleaving, it requires to unfold one back-edge of π_∞ .

π_∞ is presented labelled according to the extended labelling of fig. 5.3. We make K apparent as a subformula of I and J respectively by decomposing:

$$I = I'[K] \quad J = J'[K] \quad J'[Y] := \mu X.((Y \wp X) \oplus \perp) \quad I'[Y] := \mu Z.((Z \wp J'[Y]) \oplus \perp).$$

¹ Then we first did one step of unfolding on the right back-edge, and we took advantage of
² the two new facilites of the extended labelling:

³ 1. we added three (Rec) rules, corresponding to the three ways for a branch of π_∞ to be

Shape of the branch	$A^* \cdot l^\omega$	$A^* \cdot r^\omega$	$l^* \cdot (r^+ \cdot l^+)^\omega$
Lowest (Rec) visited ∞ ly	b	a	c
Validating ν -formula	H	G	K

⁴ valid, as summarized in the following array.
⁵ 2. and so, we labelled the three formulas H , G and K at each corresponding (Rec) ,
⁶ using for K the ability to label several occurrences at a time, and to label deeply
⁷ ν -subformulas.

⁸ This indeed forms a correct labelling of π_∞ according to the extended labelling, hence
⁹ ensuring their thread-validity.

¹⁰ 5.2.1 Extended finitization

¹¹ As for the case of our previous labelling, we will rely on the labelled presentation of
¹² these proofs in order to finitize them. Observe already that the (Rec) rule, as introduced
¹³ in def. 63 is never really used in all its power because (i) in both examples above, no
¹⁴ ν -formula wears more than one variable and (ii) except for the labelling of K in π_∞ , (Rec)
¹⁵ is used only in the particular form $\frac{\vdash \nu^{a^-} X.A, \Gamma}{\vdash \nu X.A, \Gamma}$ ($Rec'(a)$) in which only one occurrence
¹⁶ of $\nu X.A$ is labelled and this occurrence is a formula of the sequent and not a strict
¹⁷ subformula.

¹⁸ We show now how to finitize any labelled representation which verify those two restrictions.
¹⁹ As this is the case of fig. 5.2, it gives a finitization for fig. 5.2. We will then show how to
²⁰ extend this method in an *ad hoc* way to finitize entirely π_∞ (fig. .2) from the labelling of
²¹ fig. 5.3.

As before, it is enough, in order to turn a labelled formula into an unlabelled one, to translate the ν connectives, leaving all other connectives untouched. For any unlabelled context Γ , we define the following unlabelled formulas:

$$\llbracket \nu^{\Gamma^-} X.A[X] \rrbracket_e := \nu X. \llbracket A \rrbracket_e [\otimes \Gamma^\perp \oplus X] \quad \llbracket \nu^{\Gamma^+} X.A[X] \rrbracket_e := \otimes \Gamma^\perp \oplus \llbracket \nu^{\Gamma^-} X.A[X] \rrbracket_e$$

²² so the following rules are derivable: (See full derivations on fig. 5.5, p. 98.)

$$\begin{array}{c}
 \frac{}{\vdash F, G, H, I'[K^{c+}], J'[K^{c+}] \quad (\mathcal{Q}(c))} \\
 \frac{}{\vdash F, G, \underline{H}, I_+, J_+ \quad (\nu)(\oplus_1)} \\
 \frac{}{\vdash F, G, H, \underline{I}_+ \quad (\mu)(\oplus_0)(\mathfrak{Y})} \\
 \frac{}{\vdash F, G, H, I_+, \underline{J}_- \quad (\mu)(\oplus_1)(\perp)} \\
 \frac{}{\vdash \underline{F} \mathfrak{Y} G, H, I_+, J_- \quad (\mathfrak{Y})} \\
 \frac{}{\vdash \underline{F} \mathfrak{Y} G, \underline{G}, H, I_+, J_- \quad (\nu)(\oplus_1)(\perp)} \\
 \frac{}{\vdash \underline{F} \mathfrak{Y} G, \underline{G}^{a-}, H, I_+, J_- \quad (\text{L-Wk}(a-))} \\
 \frac{}{\vdash \underline{F} \mathfrak{Y} X \& (\underline{F} \mathfrak{Y} H), G^{a-}, H, I_+, J_- \quad (\&) \quad (\mu)} \\
 \frac{}{\vdash \underline{F}, G^{a-}, H, I_+, J_- \quad (\text{Rec}(a))} \\
 \frac{}{\vdash F, \underline{G}, H, I_+, J_- \quad (\nu)(\oplus_0)} \\
 \frac{}{\vdash F, \underline{G}, H, I_+, J_- \quad (\nu)} \\
 \frac{}{\vdash F, G, H, \underline{K}^{c-}, J_- \quad (\mu)(\oplus_0)(\mathfrak{Y})} \\
 \frac{}{\vdash F, G, H, \underline{J}_- \quad (\mu)(\oplus_1)(\perp)} \\
 \frac{}{\vdash F, G, H, \underline{I}_-, J_- \quad (\mu)(\oplus_1)(\perp)} \\
 \frac{}{\vdash \underline{F} \mathfrak{Y} H, G, I_-, J_- \quad (\mathfrak{Y})} \\
 \frac{}{\vdash \underline{F} \mathfrak{Y} H, G, \underline{H}, I_-, J_- \quad (\nu)(\oplus_0)(\perp)} \\
 \frac{}{\vdash \underline{F} \mathfrak{Y} H, G, \underline{H}^{b-}, I_-, J_- \quad (\text{L-Wk}(b-))} \\
 \frac{}{\vdash \underline{F} \mathfrak{Y} X \& (\underline{F} \mathfrak{Y} H), G, H^{b-}, I_-, J_- \quad (\&) \quad (\mu)} \\
 \frac{}{\vdash \underline{F}, G, H^{b-}, I_-, J_- \quad (\text{Rec}(b))} \\
 \frac{}{\vdash F, G, \underline{H}, I_-, J_- \quad (\text{Rec}(c))} \\
 \frac{}{\vdash F, G, H, I'[K], J'[K] \quad (\text{Rec}(c))}
 \end{array}$$

Figure 5.3. Labelling of π_∞ . We use the following abbreviations: $I_- = I'[K^{c-}]$, $I_+ = I'[K^{c+}]$, $J_- = J'[K^{c-}]$ and $J_+ = J'[K^{c+}]$.

$$\begin{array}{c}
 \frac{}{\vdash F, G, H, \underline{L}^{c+}} (\mathcal{Q}(c)) \\
 \frac{}{\vdash F, G, \underline{H}, L^{c+}} (\nu)(\oplus_1) \\
 \frac{}{\vdash F, G, H, \underline{I}^{c+}} (\mu)(\oplus_0) \\
 \frac{}{\vdash F, G, H, I^{c+}, \underline{J}_-} (\mu)(\oplus_1)(\perp) \\
 \frac{}{\vdash F \wp G, H, I^{c+}, J_-} (\wp) \\
 \frac{}{\vdash F \wp G, \underline{G}, H, I^{c+}, J_-} (\nu)(\oplus_1)(\perp) \\
 \frac{}{\vdash F \wp G, \underline{G}^{a-}, H, I^{c+}, J_-} (\text{L-Wk}(a-)) \\
 \frac{}{\vdash (F \wp X) \& (F \wp H), G^{a-}, H, I^{c+}, J_-} (\&) \\
 \frac{}{\vdash \underline{F}, G^{a-}, H, I^{c+}, J_-} (\mu) \\
 \frac{}{\vdash F, \underline{G}, H, I^{c+}, J_-} (\text{Rec}(a)) \\
 \frac{}{\vdash F, \underline{G}, H, I^{c+}, J_-} (\nu)(\oplus_0) \\
 \frac{}{\vdash F, G, H, \underline{K}^{c-}, J_-} (\nu) \\
 \frac{}{\vdash F, G, H, J_-} (\mu)(\oplus_0)(\wp) \\
 \frac{}{\vdash F, G, H, \underline{I}_-, J_-} (\mu)(\oplus_1)(\perp) \\
 \frac{}{\vdash F, H, G, I_-, J_-} (\text{exc}) \\
 \frac{}{\vdash F \wp \underline{H}, G^{a-}, I^{c+}, J_-} (\wp) \\
 \frac{}{\vdash F \wp \underline{H}, G^{a-}, \underline{H}, I^{c+}, J_-} (\nu)(\oplus_0)(\perp) \\
 \frac{}{\vdash (F \wp X) \& (F \wp H), G^{a-}, H, I^{c+}, J_-} (\&) \\
 \frac{}{\vdash \underline{F}, G^{a-}, H, I^{c+}, J_-} (\mu) \\
 \frac{}{\vdash F, \underline{G}, H, I^{c+}, J_-} (\text{Rec}(b)) \\
 \frac{}{\vdash F, \underline{G}, H, I^{c+}, J_-} (\nu)(\oplus_0) \\
 \frac{}{\vdash F, G, H, \underline{K}^{c-}, J_-} (\nu) \\
 \frac{}{\vdash F, G, H, J_-} (\mu)(\oplus_0)(\wp) \\
 \frac{}{\vdash F, G, H, \underline{I}_-, J_-} (\mu)(\oplus_1)(\perp) \\
 \frac{}{\vdash F, H, G, I_-, J_-} (\text{exc}) \\
 \frac{}{\vdash F \wp \underline{H}, G, I_-, J_-} (\wp) \\
 \frac{}{\vdash F \wp \underline{H}, G, \underline{H}, I_-, J_-} (\nu)(\oplus_0)(\perp) \\
 \frac{}{\vdash F \wp \underline{H}, G, \underline{H}^{b-}, I_-, J_-} (\text{L-Wk}(b-)) \\
 \frac{}{\vdash (F \wp X) \& (F \wp H), G, H^{b-}, I_-, J_-} (\&) \\
 \frac{}{\vdash \underline{F}, G, H^{b-}, I_-, J_-} (\mu) \\
 \frac{}{\vdash F, \underline{G}, H^{b-}, I_-, J_-} (\text{Rec}(b)) \\
 \frac{}{\vdash F, \underline{G}, H^{b-}, I_-, J_-} (\text{Rec}(c)) \\
 \frac{}{\vdash F, G, H, I'[K], J'[K]} (\text{Rec}(c))
 \end{array}$$

- (a) Finitization of π_∞ . Brackets $[\bullet]_e$ should be put around every formula and rule name. They were omitted only for the sake of readability.

5 Finitisation

$$\begin{array}{c}
\begin{array}{c|c}
(a) \quad \frac{\vdash \nu X. \llbracket A \rrbracket_e[\Gamma^\perp \oplus X], \Delta}{\vdash \Gamma^\perp \oplus \nu X. \llbracket A \rrbracket_e[\Gamma^\perp \oplus X], \Delta}^{(\oplus_1)} & \frac{\vdash \llbracket A \rrbracket_e[\Gamma^\perp \oplus \nu X. \llbracket A \rrbracket_e[X]], \mu X. \llbracket A^\perp \rrbracket[X]}{\vdash \nu X. \llbracket A \rrbracket[X], \Delta}^{(\mu)[\llbracket A \rrbracket_e](\oplus_1)(\text{id})} \\
(b) \quad \frac{}{\vdash \llbracket \nu^{\Gamma^+} X. A \rrbracket_e, \Gamma}^{(\oplus_0)(\otimes^\dagger), (\text{id})} & (c) \quad \frac{}{\vdash \nu X. \llbracket A \rrbracket_e[\Gamma^\perp \oplus X], \Delta}^{(\nu_{\text{inv}})}
\end{array} \\
\hline
\frac{\vdash \llbracket A \rrbracket_e[\llbracket \nu^{\Gamma^+} X. A \rrbracket_e], \mu X. \llbracket A^\perp \rrbracket_e[X \& C]]^{(\mu)(\text{id})} \quad \frac{\vdash \llbracket \nu^{\Gamma^-} X. A \rrbracket_e, \mu X. \llbracket A^\perp \rrbracket_e[X \& C]}{\vdash \llbracket \nu^{\Gamma^-} X. A \rrbracket_e, (\mu X. \llbracket A^\perp \rrbracket_e[X \& C]) \& C}^{(\text{id})} \quad \frac{\vdash \llbracket \nu^{\Gamma^-} X. A \rrbracket_e, C}{\vdash \llbracket \nu^{\Gamma^-} X. A \rrbracket_e, C}^{(\mathfrak{N}^\dagger)} \quad \frac{\vdash \llbracket \nu^{\Gamma^-} X. A \rrbracket_e, (\mu X. \llbracket A^\perp \rrbracket_e[X \& C]) \& C}{\vdash \llbracket \nu^{\Gamma^-} X. A \rrbracket_e, C}^{(\&)}}{\vdash \llbracket A \rrbracket_e[\llbracket \nu^{\Gamma^+} X. A \rrbracket_e], (\mu X. \llbracket A^\perp \rrbracket_e[X \& C]) \& C}^{(\text{cut})} \quad \frac{}{\vdash \llbracket \nu^{\Gamma^+} X. A \rrbracket_e, \Gamma}^{(\oplus_0)(\otimes^\dagger), (\text{id})} \\
(d) & \vdash \nu X. \llbracket A \rrbracket_e, \Gamma^{(\nu_{\text{inv}})}
\end{array}$$

Figure 5.5. Derivability of a. $\llbracket_{(\text{L-Wk}(\Gamma+))} \llbracket A \rrbracket_e$ b. $\llbracket_{(\mathcal{Q}(\Gamma))} \llbracket A \rrbracket_e$ c. $\llbracket_{(\text{L-Wk}(\Gamma-))} \llbracket A \rrbracket_e$ & d. $\llbracket_{(\text{Rec}'(\Gamma))} \llbracket A \rrbracket_e$ with

$$\begin{array}{c}
\frac{C \not\models \exists^\Gamma \nu X. A, \Delta}{\vdash \llbracket \nu^{\Gamma^-} X. A \rrbracket_e, \Delta} \llbracket_{(\text{L-Wk}(\Gamma-))} \llbracket A \rrbracket_e \quad \frac{\vdash \llbracket \nu^{\Gamma^-} X. A \rrbracket_e, \Delta}{\vdash \llbracket \nu^{\Gamma^+} X. A \rrbracket_e, \Delta} \llbracket_{(\text{L-Wk}(\Gamma+))} \llbracket A \rrbracket_e \\
1 \quad \frac{\vdash \llbracket \nu^{\Gamma^-} X. A \rrbracket_e, \Gamma}{\vdash \llbracket \nu X. A \rrbracket_e, \Gamma} \llbracket_{(\text{Rec}'(\Gamma))} \llbracket A \rrbracket_e \quad \frac{}{\vdash \llbracket \nu^{\Gamma^+} X. A \rrbracket_e, \Gamma} \llbracket_{(\mathcal{Q}(\Gamma))} \llbracket A \rrbracket_e
\end{array}$$

2 Remark moreover that $\frac{\vdash \llbracket A[\nu^{\Gamma^+} X. A[X]] \rrbracket_e, \Delta}{\vdash \llbracket \nu^{\Gamma^-} X. A[X] \rrbracket_e, \Delta}^{(\nu)}$ is the usual (ν) rule.

- 3 These allow to translate any labelled proof verifying the constraints (i) and (ii) stated
4 at the beginning of sec. 5.2.1 into a μ MALL finitary proof, by choosing, for every label
5 variable, the context Γ corresponding to its (Rec) rule.

These works almost as well for finitizing π_∞ based on the labelling of fig. 5.3: it allows to expand everything concerning the variables a and b . It cannot however be applied as it is to expand the variable c , for which conditions (ii) is not verified. We can anyway finitize π_∞ , but at the cost of a somewhat *ad hoc* translation:

$$\begin{aligned}
\llbracket C \rrbracket_e &:= F \wp G \wp H & \llbracket K^{c-} \rrbracket_e &:= \nu Y. \mu_. ((C^\perp \oplus (I'[Y] \wp J'[Y])) \oplus \perp) \\
\llbracket I^{c+} \rrbracket_e &:= \llbracket I'_+ \rrbracket_e = \llbracket I'[K^{c+}] \rrbracket_e & &:= \mu_. ((C^\perp \oplus (I'[\llbracket K^{c-} \rrbracket_e] \wp J'[\llbracket K^{c-} \rrbracket_e])) \oplus \perp) \\
\llbracket L^{c+} \rrbracket_e &:= \llbracket I'[K^{c+}] \wp J'[K^{c+}] \rrbracket_e & &:= C^\perp \oplus (I'[\llbracket K^{c-} \rrbracket_e] \wp J'[\llbracket K^{c-} \rrbracket_e])
\end{aligned}$$

- 6 The analysis leading to this choice of formulas is detailed in appendix 5.5, p. 101. It allows
7 to make finitary the derivation of fig. 5.4a, by expanding every formula as explained
8 above, and by replacing every rule dealing with labels with an appropriate derivation,
9 while leaving untouched the structure of rules not dealing with labels.

10 5.3 Proofs of section 4.1.

11 **Proposition 17.** *The following inferences are derivable:*

₁ Alexis: and preserve validity criterion

$$\frac{A \perp B}{\vdash A, B} \text{ (id')} \quad \frac{\vdash A[\nu^V X.A], \Gamma}{\vdash \nu^V X.A, \Gamma} \text{ (\nu_f)}$$

₃ Rémi:

- Dérivables dans quel système ?
- Préservent quel critère ?
- Cette proposition est censée aller où et démontrer quoi ?

₄ Proof. Assuming that $A \perp B$, one has $\frac{\vdash [A], [A]^\perp}{\vdash A, B}$ ^(id) which shows derivability of ₅ (id') .

$$\frac{\vdash A[\nu^V X.A], \Gamma}{\frac{\vdash A[\nu^{V,a} X.A], \Gamma}{\vdash \nu^V X.A, \Gamma}} \text{ (L-Wk)} \quad \text{(\nu_b(a))} \quad \square$$

₇ 5.4 Details and proofs for section 5.2

₈ Remember that this proposition is about the extended labelling of def. 63:

₉ Proposition (16). If π is an extended labelled circular representation then $[\pi]$ is a ₁₀ circular representation of a valid μMALL^ω proof.

₁₁ Proof. First remark that lemma 9, as it is stated on p. 78, still holds for this extended ₁₂ labelling. The proof is the same as before, bearing in mind to replace every mention of ₁₃ $(\nu_b(a))$ with $(\text{Rec}(a))$. As for the previous labelling, the proof of this proposition crucially ₁₄ rely on it.

₁₅ Suppose π is a labelled circular representation. Let $[\pi]$ be its erasure. $[\pi]$ is thus a ₁₆ circular representation of a μMALL^ω preproof. Suppose b an infinite branch of $[\pi]$, that ₁₇ is an infinite ascending path in the tree-with-back-edges $[\pi]$, starting from the root. Let ₁₈ b_0 be the corresponding infinite branch in π . Let S_0 be the occurrence of sequent in π

5 Finitisation

- ¹ which is the lowest back-edge target infinitely often crossed by b_0 . Being the target of
² some back-edge(s), S_0 is the premise of a $(\text{Rec}(a))$ rule, for some variable a .
- ³ This implies that b_0 is of the form $b_0 = r \xrightarrow[u_0]{*} S_0 \xrightarrow[u_1]{*} S_1 \xrightarrow[\text{be}]{*} S_0 \xrightarrow[u_2]{*} S_2 \xrightarrow[\text{be}]{*} S_0 \cdots$ where r is
⁴ the root of π and where the u_i do not cross S_0 except at their sources.
- ⁵ Remark that the positions labelled by a are the same in all S_i , as there are back-edges
⁶ from every S_{i+1} to S_0 . The difference, however, is that these positions are labelled with
⁷ $a-$ in S_0 and with $a+$ in every S_{i+1} . Let P_0 be the set of those positions. P_0 is finite
⁸ and non empty. Now we would like, as in the proof of prop. 8, to construct an infinite
⁹ thread along b_0 . However, because P_0 may contain more than one element, we cannot
¹⁰ know by advance, for each S_i , which $p \in P_0$ will support an infinite thread. Thus, we
¹¹ will use König's lemma to show the existence of such a thread. Let T_0 be the tree whose
¹² vertices are the pairs (i, p) where $1 \leq i < \omega$ and $p \in P_0$, whose roots are the vertices of
¹³ the form $(1, p)$ and where, for $i > 1$, the father of (i, p) is² $(i - 1, t(u_i)(p))$. Here we have
¹⁴ to prove that $t(u_i)(p)$ is defined and that it belongs to P_0 for every i and $p \in P_0$. This is
¹⁵ ensured by lemma 9 thanks to the labels.
- ¹⁶ Remark that every edge in T_0 induces a progressing thread. Indeed, for $i \geq 1$ and $p \in P_0$:
- ¹⁷ • $\mathfrak{T}(u_i)(p)$ is a ν -thread in u_i ,
 - ¹⁸ • its target is p in S_i , which is labelled with $a+$
 - ¹⁹ • and its source is p in S_0 , which is labelled with $a-$.
- ²⁰ An examination of the rules that may compose u_i shows that the only way for that to be
²¹ true is that $\mathfrak{T}(u_i)(p)$ is progressing. Now T_0 is an infinite tree with a finite number of
²² roots and an arity bounded by $\text{Card}(P_0)$, hence, by König's lemma, it has an infinite
²³ branch $(1, p_1) \leftarrow (2, p_2) \leftarrow (3, p_3) \cdots$.
- ²⁴ This infinite branch induces in turn an infinite thread

$$\text{25} \quad (S_0, p_0) \xrightarrow[\mathfrak{T}(u_1)(p_1)]{*} (S_1, p_1) \xrightarrow[\text{be}]{} (S_0, p_1) \xrightarrow[\mathfrak{T}(u_2)(p_2)]{*} (S_2, p_2) \xrightarrow[\text{be}]{} (S_0, p_2) \cdots$$

- ²⁶ This thread is valid because every $\mathfrak{T}(u_i)(p_i)$ is progressing. And it is indeed a thread
²⁷ of $b_0 = r \xrightarrow[u_0]{*} S_0 \xrightarrow[u_1]{*} S_1 \xrightarrow[\text{be}]{*} S_0 \xrightarrow[u_2]{*} S_2 \xrightarrow[\text{be}]{*} S_0 \cdots$ Hence b_0 is valid, what was to be
²⁸ demonstrated. \square

²Recall that $t(u)$ and $\mathfrak{T}(u)$ are defined in defs. 96 and 97, p. 147.

¹ 5.5 Details of finitization for π_∞

² To finitize π_∞ we try to apply the same method as for the example (5.2) p. 93, by
³ expanding every labelled formula to a non-labelled one and expanding the rules that need
⁴ it to match these transform. This works perfectly for H and G , which appear respectively
⁵ as formulas of the premises (Rec(b)) and (Rec(a)). But the situation is more delicate for
⁶ K for which we have to face a double difficulty: in the premise of (Rec(c)), K is not a
⁷ formula of the sequent but a subformula, and it appears in two different formulas.

⁸ Let us try to transform this situation into one that would fit our method. First we would
⁹ like to have only one formula containing K instead of the two I and J . Unfortunately,
¹⁰ none of them can be unlabelled without breaking the labelling. Fortunately the solution
¹¹ to that is easy: I, J is simply equivalent to $L := I \wp J$.

¹² Now we would like $I \wp J$ to be a ν -formula that we could label. We already made use, in
¹³ the previous example, of the isomorphism $A[\nu X.B[A[X]]] \simeq \nu X.A[B[X]]$ (*)

¹⁴ to turn an almost- ν -formula into a real one. Let us apply that again.

¹⁵ The formula $L = I \wp J$ is equal to $L'[K]$ where $L'[Y] := I'[Y] \wp J'[Y]$, that is: $L =$
¹⁶ $L'[\nu Y.I'[Y]]$. In order to apply an isomorphism of the form (*) we would like $I'[Y]$ to be
¹⁷ of the form $M'[L'[Y]]$ for a given M' . This is unfortunately not the case as $I'[Y]$ is a
¹⁸ subformula of $L'[Y]$. However, a careful examination of the flow of I, J and K along the
¹⁹ loops of π_∞ makes apparent the fact that

$$\text{20} \quad I'[Y] = \mu Z.((Z \wp J'[Y]) \oplus \perp) \simeq \mu_.((I'[Y] \wp J'[Y]) \oplus \perp) = M'[L'[Y]]$$

²¹ where $M'[Y]$ is defined to be $\mu_.(Y \oplus \perp)$, in which we use the notation $\mu_..A$ to denote
²² a $\mu X.A$ with X not appearing free in A . This degenerate μ binder could be removed
²³ to simplify the formulas involved in the finitisation, but we keep it to stay as close as
²⁴ possible to the original structure of I , trying to preserve its head connective.

When we stick all that together we get $L = I \wp J \simeq L'[\nu Y.M'[L'[Y]]] \simeq \nu Y.L'[M'[Y]]$ which is a ν -formula that we know, when labelled, how to expand into an unlabelled formula. If we stopped here our analysis, we would then define:

$$C := F \wp G \wp H \quad L^{c-} := \nu Y.L'[M'[C^\perp \oplus Y]] \quad L^{c+} := C^\perp \oplus L^{c-}.$$

²⁵ However we will do yet a bit more work in order to get the structure of L^{c-} closer to L 's
²⁶ one.

²⁷ Indeed the isomorphism (*) can be used in the other direction:

$$\text{28} \quad \nu Y.L'[M'[C^\perp \oplus Y]] \simeq L'[\nu Y.M'[C^\perp \oplus L'[Y]]] = I'[\nu Y.M'[C^\perp \oplus L'[Y]]] \wp J'[\nu Y.M'[C^\perp \oplus L'[Y]]]. \blacksquare$$

This, finally, leads us to define: $C := F \wp G \wp H$ $K^{c-} := \nu Y. M'[C^\perp \oplus L'[Y]]$ which allows to expand $I'[K^{c-}]$ and $J'[K^{c-}]$. On the other hand, this is not sufficient to define an expansion of K^{c+} , and we still need an *ad hoc* treatment for formulas containing it:

$$\text{“}I'[K^{c+}]\text{”} := I^{c+} := M'[C^\perp \oplus L'[K^{c-}]] \quad \text{“}I'[K^{c+}] \wp J'[K^{c+}]\text{”} := L^{c+} := C^\perp \oplus L'[K^{c-}]$$

- ¹ With these expansions of labelled formulas into unlabelled formulas, we can finitize the derivation of fig. 5.3 into the very close derivation of fig. 5.4a, on which the rules dealing with labelling can be expanded into μ MALL derivations.

⁴ 5.6 Conclusion

⁵ **Summary of the contributions.** In this chapter, we contributed to the theory of circular proofs for μ MALL in two directions: (i) identifying fragments of circular proofs for which local conditions account for the validity of circular proof objects (in contrast to the global nature of thread conditions) and (ii) designing methods for translating circular proofs to finitary proofs (with explicit (co)induction rules). To do so, we introduced and studied several labelling systems, for circular proofs, or, more precisely, finite representation thereof, and made the following contributions:

¹² **(i)** First, we investigated how such labellings ensure validity of a labellable proof, turning a global and complex problem into a local and simpler one. Indeed, validity-checking is far from trivial in circular proof-theory for fixed-point logics, the best known bound for this problem being PSPACE. We provide two labellings, a simple and fairly restricted labelling discipline which forces back-edges to target (ν) -inferences and a more liberal one for which we only know that it ensures thread-validity.

¹⁸ **(ii)** Second, we provided evidence on the usability of such labellings as a helpful guide in the generation of (co)inductive invariants which are necessary to translate a circular proof in a finitary proof system with (co)induction rules à la Park. We provided a full finitization method in a fairly restricted labelling system which contains at least all the translations of μ MALL proofs. However, this fragment is too constrained to treat standard examples that we discuss in the chapter, and which contain most of the difficulties in finitizing circular proofs, namely: (i) interleaving of fixed-points and (ii) interleaving of back-edges resulting in various choices of a valid thread to support a branch.

²⁷ **Related and future works.** We discuss related works as well as perspectives for pursuing this work along the above-mentioned directions:

²⁹ **Labelling and local certification** is the basis of our approach. The idea of labelling μ -formulas to gather information on fixed-points unfoldings is naturally not new, already to

1 be found in fixed-point approximation methods (see [Dax, Hofmann, and Lange, 2006] for
 2 instance). The closest work in this direction is Stirling’s annotated proofs [Stirling, 2014]
 3 and the application Afshari and Leigh [Afshari and Leigh, 2017] made of such proofs
 4 in obtaining completeness for the modal μ -calculus. Our labelling system works quite
 5 differently since only fixed-point operators are labelled while, in Stirling’s annotated
 6 proofs, every formula is labelled and labels are transmitted to immediate subformulas
 7 with a label extension on greatest fixed-points. Despite their difference, the relationships
 8 of those systems should be investigated further (in particular the role of the annotation
 9 restriction rule of Stirling’s system, def. 4 of [Stirling, 2014]).

10 A less immediately connected topic is the connection between size-change termination
 11 (SCT) [Lee, Jones, and Ben-Amram, 2001] and thread validity in μ -calculi: connections
 12 between those fields are not yet well understood despite early investigations by Dax,
 13 Hofmann, and Lange [2006] for instance. More than a connection, this looks like an
 14 interplay: size-change termination is originally shown decidable by using Büchi automata
 15 and size-change graphs can be used to show validity of circular proofs [Dax, Hofmann,
 16 and Lange, 2006]. There seems to be connections with our labelling system too.

17 In addition to investigating more closely those connections, we have several directions
 18 for improving our labelled proof system. The first task is to lift the results of section 4.1
 19 to the extended labelling system. Indeed, for the more restricted fragment and given a
 20 circular proof presented as a graph with back-edges, we provided a method to effectively
 21 check that one can assign labels. It is therefore natural to expect extending these results
 22 to the relaxed framework. Another point we plan to investigate is whether every circular
 23 μ MALL proof can be labelled. Even though this can look paradoxical given the complexity
 24 of checking validity of circular proofs, one should keep in mind that it might well be the
 25 case that, in order to label a circular proof presented as a tree with back-edges, one has
 26 to unfold some of the back-edges, or possibly pick a different finite representation of the
 27 proof which may result in a space blow up. Related to this question is the connection
 28 of our labelling methods with size-change termination methods. Indeed, in designing
 29 the extended labelling, one gets closer to the kind of constructions one finds in SCT-
 30 based approaches: this should be investigated further since it may also be a key for our
 31 finitization objective. Note that the previous two directions would lead to a solution to
 32 the Brotherston-Simpson conjecture.

33 *Finitization of circular proofs* has been recently a very active topic with much research
 34 effort on solving Brotherston-Simpson’s conjecture. The following recent contributions
 35 were made in the setting of Martin-Löf’s inductive definitions: firstly, Berardi and Tatsuta
 36 proved [Berardi and Tatsuta, 2017b] that, in general, the equivalence is false by providing
 37 a counter-example inspired by the *Hydra* paradox. Secondly, Simpson [Simpson, 2017] on
 38 the one hand and Berardi and Tatsuta [Berardi and Tatsuta, 2017a] on the other hand
 39 provided a positive answer in the restricted frameworks when the proof system contains
 40 arithmetics. While Simpson used tools from reverse mathematics and internalized circular
 41 proofs in ACA_0 , a fragment of second-order arithmetic with a comprehension axiom on
 42 arithmetical statements, Tatsuta and Berardi proved an equivalent result by a direct proof

5 Finitisation

1 translation relying on an arithmetical version of the Ramsey and Podelsky-Rybalchenko
2 theorems. A very natural question for future work is to extend the still *ad hoc* finitization
3 method presented in the last section to the whole fragment of relaxed labelled proofs.
4 *Circular proof search* triggered interest compared to proof system with explicit inductive
5 invariants (lacking subformula property). This has actually been turned to practice by
6 Brotherston and collaborators [Brotherston, Gorogiannis, and Petersen, 2012]. We wish
7 to investigate the potential use of labellings in circular proof-search. Indeed, there are
8 several different labellings for a given finite derivation with back-edges where the labels
9 are weakened. Prop. 10 characterizes least and greatest validating sets: those extremal
10 validating sets correspond to different strategies in placing the labels, which have different
11 properties with respect to the ability to form back-edges or to validate the proof that
12 one may exploit in proof-search.

¹ 6 Conclusion

² We started this journey by explaining that the already existing finitary systems for least
³ and greatest fixed points of formulas, with induction and coinduction rules [??? Baelde],
⁴ needing explicit invariants were not satisfactory. We explained that the infinitary setting
⁵ designed by [??? Doumane et al.] was proposed as a solution to these issues. We then
⁶ complained about the fact that these infinite proof trees are infinite and explained that
⁷ this thesis is only concerned with the circular representations of infinite proofs. After
⁸ proving that the thread criterion is PSPACE-complete on these circular representations,
⁹ we argued for the search of a smaller, easier to check criterion, which would still be
¹⁰ expressive enough for practical use. We provided such a criterion, the loop criterion, and
¹¹ we finally reached the highest point of this work by showing how any circular preproof
¹² valid for our loop criterion can be turned into a finitary proof à la Baelde with explicit
¹³ induction and coinduction invariants.

¹⁴ I may seem that after all this work we finally reached our starting point.

¹ Bibliography

- ² Smbat Abian and Arthur B Brown. A theorem on partially ordered sets, with applications
³ to fixed point theorems. *Canadian Journal of Mathematics*, 13:78–82, 1961.
- ⁴ Peter Aczel. An introduction to inductive definitions. In *Studies in Logic and the
5 Foundations of Mathematics*, volume 90, pages 739–782. Elsevier, 1977.
- ⁶ Bahareh Afshari and Graham E. Leigh. Cut-free completeness for modal mu-calculus.
⁷ In *32nd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2017,
8 Reykjavik, Iceland, June 20-23, 2017*, pages 1–12. IEEE Computer Society, 2017. doi:
⁹ 10.1109/LICS.2017.8005088. URL <https://doi.org/10.1109/LICS.2017.8005088>.
- ¹⁰ Alfred V. Aho and Jeffrey D. Ullman. The universality of data retrieval languages. In
¹¹ Alfred V. Aho, Stephen N. Zilles, and Barry K. Rosen, editors, *Conference Record
12 of the Sixth Annual ACM Symposium on Principles of Programming Languages, San
Antonio, Texas, USA, January 1979*, pages 110–120. ACM Press, 1979. doi: 10.1145/
¹³ 567752.567763. URL <https://doi.org/10.1145/567752.567763>.
- ¹⁵ Sanjeev Arora and Boaz Barak. *Computational Complexity - A Modern Approach*. Cam-
bridge University Press, 2009. ISBN 978-0-521-42426-4. URL <http://www.cambridge.org/catalogue/catalogue.asp?isbn=9780521424264>.
- ¹⁸ David Baelde. On the proof theory of regular fixed points. In Martin Giese and
¹⁹ Arild Waaler, editors, *Automated Reasoning with Analytic Tableaux and Related Meth-
ods, 18th International Conference, TABLEAUX 2009, Oslo, Norway, July 6-10,
21 2009. Proceedings*, volume 5607 of *Lecture Notes in Computer Science*, pages 93–107.
²² Springer, 2009. doi: 10.1007/978-3-642-02716-1_8. URL https://doi.org/10.1007/978-3-642-02716-1_8.
- ²⁴ David Baelde. Least and greatest fixed points in linear logic. *ACM Trans. Comput.
Log.*, 13(1):2:1–2:44, 2012. doi: 10.1145/2071368.2071370. URL <https://doi.org/10.1145/2071368.2071370>.
- ²⁷ David Baelde and Dale Miller. Least and greatest fixed points in linear logic. In
²⁸ Nachum Dershowitz and Andrei Voronkov, editors, *Logic for Programming, Artificial
Intelligence, and Reasoning, 14th International Conference, LPAR 2007, Yerevan,*

Bibliography

- 1 Armenia, October 15-19, 2007, Proceedings, volume 4790 of *Lecture Notes in Computer*
2 *Science*, pages 92–106. Springer, 2007. doi: 10.1007/978-3-540-75560-9_9. URL
3 https://doi.org/10.1007/978-3-540-75560-9_9.
- 4 David Baelde, Andrew Gacek, Dale Miller, Gopalan Nadathur, and Alwen Tiu. The
5 bedwyr system for model checking over syntactic expressions. In Frank Pfenning, editor,
6 *Automated Deduction - CADE-21, 21st International Conference on Automated Deduc-*
7 *tion, Bremen, Germany, July 17-20, 2007, Proceedings*, volume 4603 of *Lecture Notes in*
8 *Computer Science*, pages 391–397. Springer, 2007. doi: 10.1007/978-3-540-73595-3\28.
9 URL https://doi.org/10.1007/978-3-540-73595-3_28.
- 10 David Baelde, Amina Doumane, and Alexis Saurin. Infinitary proof theory: the multi-
11 plicative additive case. In Jean-Marc Talbot and Laurent Regnier, editors, *25th EACSL*
12 *Annual Conference on Computer Science Logic, CSL 2016, August 29 - September*
13 *1, 2016, Marseille, France*, volume 62 of *LIPICS*, pages 42:1–42:17. Schloss Dagstuhl
14 - Leibniz-Zentrum fuer Informatik, 2016. doi: 10.4230/LIPIcs.CSL.2016.42. URL
15 <https://doi.org/10.4230/LIPIcs.CSL.2016.42>.
- 16 Stefano Berardi and Makoto Tatsuta. Equivalence of inductive definitions and cyclic
17 proofs under arithmetic. In *32nd Annual ACM/IEEE Symposium on Logic in Computer*
18 *Science, LICS 2017, Reykjavik, Iceland, June 20-23, 2017*, pages 1–12. IEEE Computer
19 Society, 2017a. doi: 10.1109/LICS.2017.8005114. URL <https://doi.org/10.1109/LICS.2017.8005114>.
- 21 Stefano Berardi and Makoto Tatsuta. Classical system of martin-löf’s inductive defi-
22 nitions is not equivalent to cyclic proof system. In Javier Esparza and Andrzej S.
23 Murawski, editors, *Foundations of Software Science and Computation Structures*
24 - 20th International Conference, FOSSACS 2017, Held as Part of the European
25 Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala,
26 Sweden, April 22-29, 2017, Proceedings, volume 10203 of *Lecture Notes in Com-*
27 *puter Science*, pages 301–317, 2017b. doi: 10.1007/978-3-662-54458-7_18. URL
28 https://doi.org/10.1007/978-3-662-54458-7_18.
- 29 Nicolas Bourbaki. Sur le theoreme de zorn. *Archiv der Mathematik*, 2(6):434–437, 1949.
- 30 James Brotherston. Cyclic proofs for first-order logic with inductive definitions. In
31 Bernhard Beckert, editor, *Automated Reasoning with Analytic Tableaux and Related*
32 *Methods, International Conference, TABLEAUX 2005, Koblenz, Germany, September*
33 *14-17, 2005, Proceedings*, volume 3702 of *Lecture Notes in Computer Science*, pages
34 78–92. Springer, 2005. doi: 10.1007/11554554_8. URL https://doi.org/10.1007/11554554_8.
- 36 James Brotherston. *Sequent calculus proof systems for inductive definitions*. PhD thesis,
37 University of Edinburgh. College of Science and Engineering. School of ..., 2006.

Bibliography

- 1 James Brotherston and Alex Simpson. Complete sequent calculi for induction and infinite
2 descent. In *22nd IEEE Symposium on Logic in Computer Science (LICS 2007), 10-12*
3 *July 2007, Wroclaw, Poland, Proceedings*, pages 51–62. IEEE Computer Society, 2007.
4 doi: 10.1109/LICS.2007.16. URL <https://doi.org/10.1109/LICS.2007.16>.
- 5 James Brotherston and Alex Simpson. Sequent calculi for induction and infinite descent.
6 *J. Log. Comput.*, 21(6):1177–1216, 2011. doi: 10.1093/logcom/exq052. URL <https://doi.org/10.1093/logcom/exq052>.
- 8 James Brotherston, Nikos Gorogiannis, and Rasmus Lerchedahl Petersen. A generic cyclic
9 theorem prover. In Ranjit Jhala and Atsushi Igarashi, editors, *Programming Languages*
10 *and Systems - 10th Asian Symposium, APLAS 2012, Kyoto, Japan, December 11-13,*
11 *2012. Proceedings*, volume 7705 of *Lecture Notes in Computer Science*, pages 350–
12 367. Springer, 2012. doi: 10.1007/978-3-642-35182-2_25. URL https://doi.org/10.1007/978-3-642-35182-2_25.
- 14 Pierre Clairambault. Least and greatest fixpoints in game semantics. In Luca
15 de Alfaro, editor, *Foundations of Software Science and Computational Structures,*
16 *12th International Conference, FOSSACS 2009, Held as Part of the Joint Euro-*
17 *pean Conferences on Theory and Practice of Software, ETAPS 2009, York, UK,*
18 *March 22-29, 2009. Proceedings*, volume 5504 of *Lecture Notes in Computer Sci-*
19 *ence*, pages 16–31. Springer, 2009. doi: 10.1007/978-3-642-00596-1_3. URL https://doi.org/10.1007/978-3-642-00596-1_3.
- 21 Pierre Clairambault. *Logique et Interaction : une Étude Sémantique de la Totalité. (Logic*
22 *and Interaction : a Semantic Study of Totality)*. PhD thesis, Paris Diderot University,
23 France, 2010. URL <https://tel.archives-ouvertes.fr/tel-00459307>.
- 24 Vincent Danos and Laurent Regnier. The structure of multiplicatives. *Arch. Math. Log.*,
25 28(3):181–203, 1989. doi: 10.1007/BF01622878. URL <https://doi.org/10.1007/BF01622878>.
- 27 Brian A. Davey and Hilary A. Priestley. *Introduction to Lattices and Order* (2. ed.).
28 Cambridge University Press, 2002. ISBN 978-0-521-78451-1.
- 29 Anuj Dawar and Yuri Gurevich. Fixed point logics. *Bull. Symb. Log.*, 8(1):65–88, 2002.
30 doi: 10.2178/bsl/1182353853. URL <https://doi.org/10.2178/bsl/1182353853>.
- 31 Christian Dax, Martin Hofmann, and Martin Lange. A proof system for the linear time μ -
32 calculus. In S. Arun-Kumar and Naveen Garg, editors, *FSTTCS 2006: Foundations of*
33 *Software Technology and Theoretical Computer Science, 26th International Conference,*
34 *Kolkata, India, December 13-15, 2006, Proceedings*, volume 4337 of *Lecture Notes in*
35 *Computer Science*, pages 273–284. Springer, 2006. doi: 10.1007/11944836_26. URL
36 https://doi.org/10.1007/11944836_26.

Bibliography

- 1 J. W. de Bakker and Willem P. de Roever. A calculus for recursive program schemes. In
2 Maurice Nivat, editor, *Automata, Languages and Programming, Colloquium, Paris,
3 France, July 3-7, 1972*, pages 167–196. North-Holland, Amsterdam, 1972.
- 4 Amina Doumane. *On the infinitary proof theory of logics with fixed points. (Théorie de
5 la démonstration infinitaire pour les logiques à points fixes)*. PhD thesis, Paris Diderot
6 University, France, 2017. URL <https://tel.archives-ouvertes.fr/tel-01676953>.
- 7 Amina Doumane, David Baelde, Lucca Hirschi, and Alexis Saurin. Towards completeness
8 via proof search in the linear time μ -calculus: The case of Büchi inclusions. In Martin
9 Grohe, Eric Koskinen, and Natarajan Shankar, editors, *Proceedings of the 31st Annual
10 ACM/IEEE Symposium on Logic in Computer Science, LICS ’16, New York, NY,
11 USA, July 5-8, 2016*, pages 377–386. ACM, 2016. doi: 10.1145/2933575.2933598. URL
12 <https://doi.org/10.1145/2933575.2933598>.
- 13 Lars-Henrik Eriksson. A finitary version of the calculus of partial inductive definitions. In
14 Lars-Henrik Eriksson, Lars Hallnäs, and Peter Schroeder-Heister, editors, *Extensions
15 of Logic Programming, Second International Workshop, ELP’91, Stockholm, Sweden,
16 January 27-29, 1991, Proceedings*, volume 596 of *Lecture Notes in Computer Science*,
17 pages 89–134. Springer, 1991. doi: 10.1007/BFb0013605. URL <https://doi.org/10.1007/BFb0013605>.
- 19 Seth Fogarty and Moshe Y. Vardi. Büchi complementation and size-change termination.
20 *Logical Methods in Computer Science*, 8(1), 2012. doi: 10.2168/LMCS-8(1:13)2012.
21 URL [https://doi.org/10.2168/LMCS-8\(1:13\)2012](https://doi.org/10.2168/LMCS-8(1:13)2012).
- 22 Jérôme Fortier and Luigi Santocanale. Cuts for circular proofs: semantics and cut-
23 elimination. In Simona Ronchi Della Rocca, editor, *Computer Science Logic 2013
24 (CSL 2013), CSL 2013, September 2-5, 2013, Torino, Italy*, volume 23 of *LIPICS*, pages
25 248–262. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2013. doi: 10.4230/
26 LIPICS.CSL.2013.248. URL <https://doi.org/10.4230/LIPICS.CSL.2013.248>.
- 27 Gerhard Gentzen. Untersuchungen über das logische schließen. i. *Mathematische
28 Zeitschrift*, 39(1):176–210, 1935a.
- 29 Gerhard Gentzen. Untersuchungen über das logische schließen. ii. *Mathematische
30 Zeitschrift*, 39(1):405–431, 1935b.
- 31 Gerhard Gentzen. Investigations into logical deduction. *The Collected Papers of Gerhard
32 Gentzen*, pages 68–131, 1969. URL <https://ci.nii.ac.jp/naid/10007157703/en/>.
- 33 Jean-Yves Girard. Linear logic. *Theor. Comput. Sci.*, 50:1–102, 1987. doi: 10.1016/
34 0304-3975(87)90045-4. URL [https://doi.org/10.1016/0304-3975\(87\)90045-4](https://doi.org/10.1016/0304-3975(87)90045-4).

- ¹ Jean-Yves Girard. Proof theory and logical complexity. *Annals of Pure and Applied Logic*, 53(4):197, 1991.
- ³ Jean-Yves Girard. *The Blind Spot: lectures on logic*. European Mathematical Society, 2011.
- ⁵ Jean-Yves Girard, Paul Taylor, and Yves Lafont. *Proofs and Types*. Cambridge University Press, New York, NY, USA, 1989. ISBN 0-521-37181-3.
- ⁷ Nikos Gorogiannis and Reuben Rowe. The cyclist theorem prover, 2014. URL <http://www.cyclist-prover.org/>.
- ⁹ Erich Grädel, Wolfgang Thomas, and Thomas Wilke, editors. *Automata, Logics, and Infinite Games: A Guide to Current Research [outcome of a Dagstuhl seminar, February 2001]*, volume 2500 of *Lecture Notes in Computer Science*, 2002. Springer. ISBN 3-540-00388-6. doi: 10.1007/3-540-36387-4. URL <https://doi.org/10.1007/3-540-36387-4>.
- ¹⁴ Yuri Gurevich and Saharon Shelah. Fixed-point extensions of first-order logic. *Ann. Pure Appl. Log.*, 32:265–280, 1986. doi: 10.1016/0168-0072(86)90055-2. URL [https://doi.org/10.1016/0168-0072\(86\)90055-2](https://doi.org/10.1016/0168-0072(86)90055-2).
- ¹⁷ Lars Hallnäs. Partial inductive definitions. *Theor. Comput. Sci.*, 87(1):115–142, 1991. doi: 10.1016/S0304-3975(06)80007-1. URL [https://doi.org/10.1016/S0304-3975\(06\)80007-1](https://doi.org/10.1016/S0304-3975(06)80007-1).
- ²⁰ Pierre Hyvernat. The size-change termination principle for constructor based languages. *Logical Methods in Computer Science*, 10(1), 2014. doi: 10.2168/LMCS-10(1:11)2014. URL [https://doi.org/10.2168/LMCS-10\(1:11\)2014](https://doi.org/10.2168/LMCS-10(1:11)2014).
- ²³ Pierre Hyvernat. The size-change principle for mixed inductive and coinductive types. *CoRR*, abs/1901.07820, 2019. URL <http://arxiv.org/abs/1901.07820>.
- ²⁵ Neil D. Jones. *Computability and complexity - from a programming perspective*. Foundations of computing series. MIT Press, 1997. ISBN 978-0-262-10064-9.
- ²⁷ Neil D. Jones. LOGSPACE and PTIME characterized by programming languages. *Theor. Comput. Sci.*, 228(1-2):151–174, 1999. doi: 10.1016/S0304-3975(98)00357-0. URL [https://doi.org/10.1016/S0304-3975\(98\)00357-0](https://doi.org/10.1016/S0304-3975(98)00357-0).
- ³⁰ Roope Kaivola. A simple decision method for the linear time mu-calculus. In *Structures in Concurrency Theory*, pages 190–204. Springer, 1995.
- ³² Dexter Kozen. On induction vs. $*$ -continuity. In Dexter Kozen, editor, *Logics of Programs*,

Bibliography

- ¹ *Workshop, Yorktown Heights, New York, USA, May 1981*, volume 131 of *Lecture Notes in Computer Science*, pages 167–176. Springer, 1981. doi: 10.1007/BFb0025782. URL <https://doi.org/10.1007/BFb0025782>.
- ⁴ Dexter Kozen. Results on the propositional mu-calculus. *Theor. Comput. Sci.*, 27: 333–354, 1983. doi: 10.1016/0304-3975(82)90125-6. URL [https://doi.org/10.1016/0304-3975\(82\)90125-6](https://doi.org/10.1016/0304-3975(82)90125-6).
- ⁷ Martin Lange. Size-change termination and satisfiability for linear-time temporal logics. In Cesare Tinelli and Viorica Sofronie-Stokkermans, editors, *Frontiers of Combining Systems, 8th International Symposium, FroCoS 2011, Saarbrücken, Germany, October 5-7, 2011. Proceedings*, volume 6989 of *Lecture Notes in Computer Science*, pages 28–39. Springer, 2011. doi: 10.1007/978-3-642-24364-6_3. URL https://doi.org/10.1007/978-3-642-24364-6_3.
- ¹³ Jean-Louis Lassez, V. L. Nguyen, and Liz Sonenberg. Fixed point theorems and semantics: A folk tale. *Inf. Process. Lett.*, 14(3):112–116, 1982. doi: 10.1016/0020-0190(82)90065-5. URL [https://doi.org/10.1016/0020-0190\(82\)90065-5](https://doi.org/10.1016/0020-0190(82)90065-5).
- ¹⁶ Chin Soon Lee, Neil D. Jones, and Amir M. Ben-Amram. The size-change principle for program termination. In Chris Hankin and Dave Schmidt, editors, *Conference Record of POPL 2001: The 28th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, London, UK, January 17-19, 2001*, pages 81–92. ACM, 2001. doi: 10.1145/360204.360210. URL <http://doi.acm.org/10.1145/360204.360210>.
- ²¹ Rodolphe Lepigre and Christophe Raffalli. Subtyping-based type-checking for system F with induction and coinduction. *CoRR*, abs/1604.01990, 2016. URL <http://arxiv.org/abs/1604.01990>.
- ²⁴ Rodolphe Lepigre and Christophe Raffalli. Practical subtyping for curry-style languages. *ACM Trans. Program. Lang. Syst.*, 41(1):5:1–5:58, 2019. doi: 10.1145/3285955. URL <https://doi.org/10.1145/3285955>.
- ²⁷ George Markowsky. Chain-complete posets and directed sets with applications. *Algebra universalis*, 6(1):53–68, 1976.
- ²⁹ Ralph Matthes. Monotone fixed-point types and strong normalization. In Georg Gottlob, Etienne Grandjean, and Katrin Seyr, editors, *Computer Science Logic, 12th International Workshop, CSL '98, Annual Conference of the EACSL, Brno, Czech Republic, August 24-28, 1998, Proceedings*, volume 1584 of *Lecture Notes in Computer Science*, pages 298–312. Springer, 1998. doi: 10.1007/10703163__20. URL https://doi.org/10.1007/10703163_20.
- ³⁵ Raymond McDowell and Dale Miller. Cut-elimination for a logic with definitions and

- ¹ induction. *Theor. Comput. Sci.*, 232(1-2):91–119, 2000. doi: 10.1016/S0304-3975(99)00171-1. URL [https://doi.org/10.1016/S0304-3975\(99\)00171-1](https://doi.org/10.1016/S0304-3975(99)00171-1).
- ³ N. P. Mendler. Inductive types and type constraints in the second-order lambda calculus.
⁴ *Ann. Pure Appl. Log.*, 51(1-2):159–172, 1991. doi: 10.1016/0168-0072(91)90069-X. URL
⁵ [https://doi.org/10.1016/0168-0072\(91\)90069-X](https://doi.org/10.1016/0168-0072(91)90069-X).
- ⁶ Dale Miller and Elaine Pimentel. A formal framework for specifying sequent calculus
⁷ proof systems. *Theor. Comput. Sci.*, 474:98–116, 2013. doi: 10.1016/j.tcs.2012.12.008.
⁸ URL <https://doi.org/10.1016/j.tcs.2012.12.008>.
- ⁹ Alberto Momigliano and Alwen Fernanto Tiu. Induction and co-induction in sequent
¹⁰ calculus. In Stefano Berardi, Mario Coppo, and Ferruccio Damiani, editors, *Types for
¹¹ Proofs and Programs, International Workshop, TYPES 2003, Torino, Italy, April 30
¹² - May 4, 2003, Revised Selected Papers*, volume 3085 of *Lecture Notes in Computer
¹³ Science*, pages 293–308. Springer, 2003. doi: 10.1007/978-3-540-24849-1__19. URL
¹⁴ https://doi.org/10.1007/978-3-540-24849-1_19.
- ¹⁵ Rémi Nollet, Alexis Saurin, and Christine Tasson. Local validity for circular proofs
¹⁶ in linear logic with fixed points. In Dan R. Ghica and Achim Jung, editors, *27th
¹⁷ EACSL Annual Conference on Computer Science Logic, CSL 2018, September 4-7,
¹⁸ 2018, Birmingham, UK*, volume 119 of *LIPICS*, pages 35:1–35:23. Schloss Dagstuhl
¹⁹ - Leibniz-Zentrum fuer Informatik, 2018. doi: 10.4230/LIPIcs.CSL.2018.35. URL
²⁰ <https://doi.org/10.4230/LIPIcs.CSL.2018.35>.
- ²¹ David Park. Fixpoint induction and proofs of program properties. *Machine intelligence*,
²² 5(59-78):5–3, 1969.
- ²³ Sylvain Perifel. *Complexité algorithmique*. Ellipses, 2014.
- ²⁴ Dominique Perrin and Jean-Éric Pin. *Infinite words: automata, semigroups, logic and
²⁵ games*, volume 141. Academic Press, 2004.
- ²⁶ Amir Pnueli. The temporal logic of programs. In *18th Annual Symposium on Foundations
²⁷ of Computer Science, Providence, Rhode Island, USA, 31 October - 1 November
²⁸ 1977*, pages 46–57. IEEE Computer Society, 1977. doi: 10.1109/SFCS.1977.32. URL
²⁹ <https://doi.org/10.1109/SFCS.1977.32>.
- ³⁰ Reuben N. S. Rowe and James Brotherston. Automatic cyclic termination proofs
³¹ for recursive procedures in separation logic. In Yves Bertot and Viktor Vafeiadis,
³² editors, *Proceedings of the 6th ACM SIGPLAN Conference on Certified Programs and
³³ Proofs, CPP 2017, Paris, France, January 16-17, 2017*, pages 53–65. ACM, 2017. doi:
³⁴ 10.1145/3018610.3018623. URL <https://doi.org/10.1145/3018610.3018623>.

Bibliography

- 1 Luigi Santocanale. A calculus of circular proofs and its categorical semantics. In
2 Mogens Nielsen and Uffe Engberg, editors, *Foundations of Software Science and*
3 *Computation Structures, 5th International Conference, FOSSACS 2002. Held as Part*
4 *of the Joint European Conferences on Theory and Practice of Software, ETAPS 2002*
5 *Grenoble, France, April 8-12, 2002, Proceedings*, volume 2303 of *Lecture Notes in*
6 *Computer Science*, pages 357–371. Springer, 2002. doi: 10.1007/3-540-45931-6_25.
7 URL https://doi.org/10.1007/3-540-45931-6_25.
- 8 Peter Schroeder-Heister. Rules of definitional reflection. In *Proceedings of the Eighth*
9 *Annual Symposium on Logic in Computer Science (LICS '93), Montreal, Canada, June*
10 *19-23, 1993*, pages 222–232. IEEE Computer Society, 1993. doi: 10.1109/LICS.1993.
11 287585. URL <https://doi.org/10.1109/LICS.1993.287585>.
- 12 Alex Simpson. Cyclic arithmetic is equivalent to peano arithmetic. In Javier Esparza
13 and Andrzej S. Murawski, editors, *Foundations of Software Science and Computation*
14 *Structures - 20th International Conference, FOSSACS 2017, Held as Part of the*
15 *European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala,*
16 *Sweden, April 22-29, 2017, Proceedings*, volume 10203 of *Lecture Notes in Computer*
17 *Science*, pages 283–300, 2017. doi: 10.1007/978-3-662-54458-7_17. URL https://doi.org/10.1007/978-3-662-54458-7_17.
- 19 A. Prasad Sistla, Moshe Y. Vardi, and Pierre Wolper. The complementation problem
20 for büchi automata with applications to temporal logic. *Theor. Comput. Sci.*, 49:
21 217–237, 1987. doi: 10.1016/0304-3975(87)90008-9. URL [https://doi.org/10.1016/0304-3975\(87\)90008-9](https://doi.org/10.1016/0304-3975(87)90008-9).
- 23 Colin Stirling. A tableau proof system with names for modal mu-calculus. In Andrei
24 Voronkov and Margarita V. Korovina, editors, *HOWARD-60: A Festschrift on the*
25 *Occasion of Howard Barringer's 60th Birthday*, volume 42 of *EPiC Series in Computing*,
26 pages 306–318. EasyChair, 2014. URL <http://www.easychair.org/publications/?page=1932281032>.
- 28 Gadi Tellez and James Brotherston. Automatically verifying temporal properties of
29 pointer programs with cyclic proof. In Leonardo de Moura, editor, *Automated Deduction*
30 - *CADE 26 - 26th International Conference on Automated Deduction, Gothenburg,*
31 *Sweden, August 6-11, 2017, Proceedings*, volume 10395 of *Lecture Notes in Computer*
32 *Science*, pages 491–508. Springer, 2017. doi: 10.1007/978-3-319-63046-5_30. URL
33 https://doi.org/10.1007/978-3-319-63046-5_30.
- 34 Alwen Tiu and Alberto Momigliano. Cut elimination for a logic with induction and
35 co-induction. *J. Appl. Log.*, 10(4):330–367, 2012. doi: 10.1016/j.jal.2012.07.007. URL
36 <https://doi.org/10.1016/j.jal.2012.07.007>.
- 37 Igor Walukiewicz. On completeness of the mu-calculus. In *Proceedings of the Eighth*

Bibliography

¹ Annual Symposium on Logic in Computer Science (LICS '93), Montreal, Canada, June
² 19-23, 1993, pages 136–146. IEEE Computer Society, 1993. doi: 10.1109/LICS.1993.
³ 287593. URL <https://doi.org/10.1109/LICS.1993.287593>.

⁴ Igor Walukiewicz. Completeness of kozen’s axiomatisation of the propositional mu-
⁵ calculus. In Proceedings, 10th Annual IEEE Symposium on Logic in Computer Science,
⁶ San Diego, California, USA, June 26-29, 1995, pages 14–24. IEEE Computer Society,
⁷ 1995. doi: 10.1109/LICS.1995.523240. URL <https://doi.org/10.1109/LICS.1995.523240>.

¹

Part I

²

Annexes (temporaires ?)

¹ .1 Definition of proofs

² In this section, we describe the formal constructs that we will use to give precise definitions
³ to the different proof systems that will be the objects of this thesis.

⁴ As it is the case for the thesis, we show those constructs on the particular example of the
⁵ logic MALL.

⁶ The logic MALL is usually defined by three things: its formulas, its negation and its
⁷ logical rules, all of which we recall now.

Definition 64 (MALL formulas). The set of formulas for MALL is denoted by Fml_{MALL} and is generated by the following grammar:

$$A, B ::= X \mid \overline{X} \mid A \otimes B \mid A \wp B \mid \mathbf{1} \mid \perp \mid A \oplus B \mid A \& B \mid \mathbf{0} \mid \top$$

⁸ where X ranges over a given set of propositional variables.

Definition 65 (MALL negation). Fml_{MALL} is equipped with an involutive negation, denoted by \cdot^\perp and inductively defined by:

$$\begin{array}{lllll} X^\perp = \overline{X} & \overline{X}^\perp = X & (A \otimes B)^\perp = A^\perp \wp B^\perp & (A \wp B)^\perp = A^\perp \otimes B^\perp & \mathbf{1}^\perp = \perp \\ \perp^\perp = \mathbf{1} & (A \oplus B)^\perp = A^\perp \& B^\perp & (A \& B)^\perp = A^\perp \oplus B^\perp & \mathbf{0}^\perp = \top & \top^\perp = \mathbf{0} \end{array}$$

Definition 66 (MALL rules (informal)).

$$\begin{array}{c} \frac{}{\vdash A, A^\perp} (\text{id}) \qquad \frac{\vdash \Gamma, A \quad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta} (\text{cut}) \\ \frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B} (\otimes) \qquad \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \wp B} (\wp) \qquad \frac{}{\vdash \mathbf{1}} (\mathbf{1}) \qquad \frac{\vdash \Gamma}{\vdash \Gamma, \perp} (\perp) \\ \frac{\vdash \Gamma, A}{\vdash \Gamma, A \oplus B} (\oplus_0) \qquad \frac{\vdash \Gamma, B}{\vdash \Gamma, A \oplus B} (\oplus_1) \qquad \frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \& B} (\&) \qquad \frac{}{\vdash \Gamma, \top} (\top) \end{array}$$

⁹ In the following subsections, we will show how to give a precise, rigorous meaning to
¹⁰ those rules, and how to define MALL proofs.

¹ **.1.1 Some mathematical tools**

- ² Before going into an explicit definition of proofs as mathematical objects, we recall some
³ basic mathematical tools that we will use.

⁴ **Multisets**

⁵ **Definition 67.** If X is a set, we set $\mathfrak{M}(X) := \mathbf{N}^X$, where \mathbf{N} is the set of natural integers.
⁶ The elements of $\mathfrak{M}(X)$ are called *multisets* from X . $\forall \Gamma \in \mathfrak{M}(X), \forall x \in X, \Gamma(x)$ is called
⁷ the *multiplicity* of x in Γ .

- ⁸ If $\Gamma, \Delta \in \mathfrak{M}(X)$, we define $\Gamma + \Delta$ to be the pointwise sum of Γ and Δ : $\forall x \in X, (\Gamma + \Delta)(x) =$
⁹ $\Gamma(x) + \Delta(x)$.

$\forall x \in X$, we define $[x] \in \mathfrak{M}(X)$ by

$$\forall y \in X, [x](y) = \begin{cases} 1 & \text{if } y = x \\ 0 & \text{if } y \neq x \end{cases}$$

- ¹⁰ More generally, $\forall x_0, \dots, x_{n-1} \in X$, we set $[x_0, \dots, x_{n-1}] := [x_0] + \dots + [x_{n-1}]$. In particular,
¹¹ $[]$ denotes the empty multiset.

¹² **Graphs**

¹³ We will use graphs all along this thesis as the basic structure to describe the shape of
¹⁴ formal proofs. As there are several notions of graphs, we state the following definition to
¹⁵ avoid ambiguities. These graphs that we are interested in are directed, may have loops
¹⁶ and may have several edges between two given vertices. These graphs are elsewhere called
¹⁷ directed pseudographs, or quivers.

¹⁸ **Definition 68** (Graph). A graph is a (V, E, s, t) where

¹⁹ • $V, E \in \text{Set}$

²⁰ • $s, t: E \rightarrow V$

²¹ The elements of V are called *vertices*, the elements of E are called *edges* and if $e \in E$
²² then $s(e)$ is called the *source* of e and $t(e)$ is called the *target* of e .

²³ When there is no ambiguity, s and t may be left out of the description of the graph.

¹ Trees are defined as a special case of graphs:

² **Definition 69.** A *tree* is a *graph* $T = (V, E)$ in which there is a vertex $r \in V$ such that
³ $\forall v \in V$, there is a unique path from r to v . Such a vertex is necessarily unique. This
⁴ vertex r is called the *root* of the tree.

⁵ **Signatures**

⁶ **Definition 70** (signature). A *signature* is a pair $S = (|S|, \alpha)$ where

⁷ • $|S| \in \text{Set}$

⁸ • $\alpha: |S| \rightarrow \text{Set}$

⁹ We simply write $a \in S$ to denote $a \in |S|$.

¹⁰ If S is a *signature*, we will often use the following construction, in which X can be any
¹¹ set or class:

$$\sum_{a \in S} X^{\alpha(a)} = \left\{ (a, (x_i)_{i \in \alpha(a)}) \mid a \in S \wedge \forall i \in \alpha(a), x_i \in X \right\}$$

¹² When we do, we may also use the following notation:

¹³ **Definition 71.** If S is a *signature*, if $y = (a, (x_i)_{i \in \alpha(a)}) \in \sum_{a \in S} X^{\alpha(a)}$ and if $b \in \alpha(a)$
¹⁴ then $y \cdot b := x_b$.

¹⁵ **.1.2 Provability as an inductive property**

¹⁶ The simplest way to give a rigorous meaning to the rules of Definition 66 is to see them
¹⁷ as an inductive definition of a set of sequents.

¹⁸ **Definition 72** (Multiset sequents). We define $\text{Seq}_{\text{MALL}} := \mathfrak{M}(\text{Fml}_{\text{MALL}})$. The elements
¹⁹ of Seq_{MALL} are called *sequents*.

²⁰ The rules of MALL are formalized as a function

Definition 73. We define $F_{\text{MALL}}: \mathfrak{P}(\text{Seq}_{\text{MALL}}) \rightarrow \mathfrak{P}(\text{Seq}_{\text{MALL}})$ by

$$\begin{aligned} \forall E \subseteq \text{Seq}_{\text{MALL}}, F_{\text{MALL}}(E) := \\ \{[A, A^\perp] \mid A \in \text{Fml}_{\text{MALL}}\} \\ \cup \{\Gamma + \Delta \mid A \in \text{Fml}_{\text{MALL}} \wedge \Gamma, \Delta \in \mathfrak{M}(\text{Fml}_{\text{MALL}}) \wedge \Gamma + [A] \in E \wedge \Delta + [A^\perp] \in E\} \\ \cup \{\Gamma + \Delta + [A \otimes B] \\ \mid A, B \in \text{Fml}_{\text{MALL}} \wedge \Gamma, \Delta \in \mathfrak{M}(\text{Fml}_{\text{MALL}}) \wedge \Gamma + [A] \in E \wedge \Delta + [B] \in E\} \\ \cup \{\Gamma + [A \wp B] \mid A, B \in \text{Fml}_{\text{MALL}} \wedge \Gamma \in \mathfrak{M}(\text{Fml}_{\text{MALL}}) \wedge \Gamma + [A, B] \in E\} \\ \cup \{[1]\} \\ \cup \{\Gamma + [\perp] \mid \Gamma \in \mathfrak{M}(\text{Fml}_{\text{MALL}}) \wedge \Gamma \in E\} \\ \cup \{\Gamma + [A \oplus B] \mid A, B \in \text{Fml}_{\text{MALL}} \wedge \Gamma \in \mathfrak{M}(\text{Fml}_{\text{MALL}}) \wedge \Gamma + [A] \in E\} \\ \cup \{\Gamma + [A \oplus B] \mid A, B \in \text{Fml}_{\text{MALL}} \wedge \Gamma \in \mathfrak{M}(\text{Fml}_{\text{MALL}}) \wedge \Gamma + [B] \in E\} \\ \cup \{\Gamma + [A \& B] \mid A, B \in \text{Fml}_{\text{MALL}} \wedge \Gamma \in \mathfrak{M}(\text{Fml}_{\text{MALL}}) \wedge \Gamma + [A] \in E \wedge \Gamma + [B] \in E\} \\ \cup \{\Gamma + [\top] \mid \Gamma \in \mathfrak{M}(\text{Fml}_{\text{MALL}})\} \end{aligned}$$

- ¹ Now we could use Knaster-Tarski's theorem to define the set of provable sequents, but
- ² its demonstration is so simple that we can inline it:

Definition 74. The set of *provable sequents* of MALL is

$$\vdash_{\text{MALL}} := \bigcap \{E \subseteq \text{Seq}_{\text{MALL}} \mid F_{\text{MALL}}(E) \subseteq E\}$$

³ **Proposition 18.**

- ⁴ • $F_{\text{MALL}}(\vdash_{\text{MALL}}) \subseteq \vdash_{\text{MALL}}$
- ⁵ • $\forall E \subseteq \text{Seq}_{\text{MALL}}, \text{ if } F_{\text{MALL}}(E) \subseteq E \text{ then } \vdash_{\text{MALL}} \subseteq E$

Proof. The crucial observation is that F_{MALL} is non decreasing with respect to the inclusion relation:

$$\forall E_1, E_2 \subseteq \text{Seq}_{\text{MALL}}, \text{ if } E_1 \subseteq E_2 \text{ then } F_{\text{MALL}}(E_1) \subseteq F_{\text{MALL}}(E_2)$$

- ⁶ That should be obvious from the definition of F_{MALL} . We now denote $\mathcal{E} := \{E \subseteq \text{Seq}_{\text{MALL}} \mid F_{\text{MALL}}(E) \subseteq E\}$.
- ⁷ We want to prove that

1 •

2

□

3 .1.3 Proof trees for provability

4 We define a signature adapted to the set of rules of the logic:

Definition 75. $\text{sigS}_{\text{MALL}} = (|\text{sigS}_{\text{MALL}}|, \alpha)$ with

$$|\text{sigS}_{\text{MALL}}| = \{\text{id}, \text{cut}, \otimes, \wp, \mathbf{1}, \perp, \oplus_0, \oplus_1, \&, \top\}$$

$$\alpha(\text{id}) = \{\mathbf{c}\} \quad \alpha(\text{cut}) = \{0, 1, \mathbf{c}\} \quad \alpha(\otimes) = \{0, 1, \mathbf{c}\} \quad \alpha(\wp) = \{0, \mathbf{c}\} \quad \alpha(\mathbf{1}) = \{\mathbf{c}\}$$

$$\alpha(\perp) = \{0, \mathbf{c}\} \quad \alpha(\oplus_0) = \{0, \mathbf{c}\} \quad \alpha(\oplus_1) = \{1, \mathbf{c}\} \quad \alpha(\&) = \{0, 1, \mathbf{c}\} \quad \alpha(\top) = \{\mathbf{c}\}$$

5 *Remark 18.* The symbol \mathbf{c} , which stands for “conclusion”, belongs to $\alpha(a)$ for every
6 $a \in \text{sigS}_{\text{MALL}}$. This essential fact will be used in Definition 78.

Definition 76 (Multiset rule). A *logical rule* is an element of

$$\sum_{a \in \text{sigS}_{\text{MALL}}} \text{Seq}_{\text{MALL}}^{\alpha(a)}$$

7 We can now give a precise meaning to the rules presented on Definition 66:

Definition 77 (MALL rules, with multiset sequents). We define the set of *logical rules* of MALL

$$\text{Rules}_{\text{MALL}} \subseteq \sum_{a \in \text{sigS}_{\text{MALL}}} \text{Seq}_{\text{MALL}}^{\alpha(a)}$$

as follows:

$$\begin{aligned}
\text{Rules}_{\text{MALL}} := & \left\{ \text{id}\{\mathbf{c} \mapsto [A, A^\perp]\} \mid A \in \text{Fml}_{\text{MALL}} \right\} \\
& \cup \left\{ \text{cut}\{0 \mapsto \Gamma + [A], 1 \mapsto \Delta + [A^\perp], \mathbf{c} \mapsto \Gamma + \Delta\} \right. \\
& \quad \left. \mid A \in \text{Fml}_{\text{MALL}} \wedge \Gamma, \Delta \in \mathfrak{M}(\text{Fml}_{\text{MALL}}) \right\} \\
& \cup \left\{ \otimes\{0 \mapsto \Gamma + [A], 1 \mapsto \Delta + [B], \mathbf{c} \mapsto \Gamma + \Delta + [A \otimes B]\} \right. \\
& \quad \left. \mid A, B \in \text{Fml}_{\text{MALL}} \wedge \Gamma, \Delta \in \mathfrak{M}(\text{Fml}_{\text{MALL}}) \right\} \\
& \cup \left\{ \wp\{0 \mapsto \Gamma + [A, B], \mathbf{c} \mapsto \Gamma + [A \wp B]\} \mid A, B \in \text{Fml}_{\text{MALL}} \wedge \Gamma \in \mathfrak{M}(\text{Fml}_{\text{MALL}}) \right\} \\
& \cup \left\{ \mathbf{1}\{\mathbf{c} \mapsto [1]\} \right\} \\
& \cup \left\{ \perp\{0 \mapsto \Gamma, \mathbf{c} \mapsto \Gamma + [\perp]\} \mid \Gamma \in \mathfrak{M}(\text{Fml}_{\text{MALL}}) \right\} \\
& \cup \left\{ \oplus_0\{0 \mapsto \Gamma + [A], \mathbf{c} \mapsto \Gamma + [A \oplus B]\} \mid A, B \in \text{Fml}_{\text{MALL}} \wedge \Gamma \in \mathfrak{M}(\text{Fml}_{\text{MALL}}) \right\} \\
& \cup \left\{ \oplus_1\{1 \mapsto \Gamma + [B], \mathbf{c} \mapsto \Gamma + [A \oplus B]\} \mid A, B \in \text{Fml}_{\text{MALL}} \wedge \Gamma \in \mathfrak{M}(\text{Fml}_{\text{MALL}}) \right\} \\
& \cup \left\{ \&\{0 \mapsto \Gamma + [A], 1 \mapsto \Gamma + [B], \mathbf{c} \mapsto \Gamma + [A \& B]\} \right. \\
& \quad \left. \mid A, B \in \text{Fml}_{\text{MALL}} \wedge \Gamma \in \mathfrak{M}(\text{Fml}_{\text{MALL}}) \right\} \\
& \cup \left\{ \top\{\mathbf{c} \mapsto \Gamma + [\top]\} \mid \Gamma \in \mathfrak{M}(\text{Fml}_{\text{MALL}}) \right\}
\end{aligned}$$

- ¹ Recall that, as mentioned in Remark 18, $\forall a \in \text{sigS}_{\text{MALL}}$, the symbol \mathbf{c} belongs to $\alpha(a)$.
- ² This justifies the following definition:

- ³ **Definition 78** (Proof structure). A *proof structure* is a $(\text{Spos}, \text{Sval}, \text{Inf})$ with

⁴ 1. $\text{Spos} \in \text{Set}$

⁵ 2. $\text{Sval}: \text{Spos} \rightarrow \text{Seq}_{\text{MALL}}$

⁶ 3. $\text{Inf} \subseteq \sum_{a \in \text{sigS}_{\text{MALL}}} \text{Spos}^{\alpha(a)}$ such that the function $\begin{array}{c} \text{Inf} \rightarrow \text{Spos} \\ I \mapsto I \cdot \mathbf{c} \end{array}$ is injective.

- ⁷ The elements of Spos are called *positions of sequents*. The elements of Inf are called
- ⁸ *inferences*. If $I \in \text{Inf}$, the position of sequent $I \cdot \mathbf{c} \in \text{Spos}$ is called the *conclusion* of the
- ⁹ inference I . The condition in point 3. thus asks that every position of sequent is the
- ¹⁰ conclusion of at most one inference.

- ¹¹ **Definition 79** (Graph associated to a proof structure). If $\pi = (\text{Spos}, \text{Sval}, \text{Inf})$ is a *proof structure* and $I \in \text{Inf}$ is an inference of π , we define $\text{Sgraph}(\pi)$ to be the *graph* with

- ¹ • $V = \text{Spos}$
- ² • $E = \{(I, b) \mid I \in \text{Inf}, I = (a, (p_b)_{b \in \alpha(a)}), b \in \alpha(a), b \neq \mathbf{c}\}$
- ³ • $s(I, b) = I \cdot \mathbf{c}$
- ⁴ • $t(I, b) = I \cdot b$

Definition 80 (Rule associated to an inference). If $\pi = (\text{Spos}, \text{Sval}, \text{Inf})$ is a **proof structure** and $I = (a, (p_b)_{b \in \alpha(b)}) \in \text{Inf}$ is an inference of π , we define

$$\begin{aligned} \text{Ival}(I) &\in \sum_{a \in \text{sigS}_{\text{MALL}}} \text{Seq}_{\text{MALL}}^{\alpha(a)} \\ \text{Ival}(I) &:= (a, (\text{Sval}(p_i))_{b \in \alpha(a)}) \end{aligned}$$

⁵ **Definition 81** (Proof). A **proof** is a **proof structure** $\pi = (\text{Spos}, \text{Inf}, \text{Sval})$ such that

- ⁶ • Each **position of sequent** is the **conclusion** of an **inference**. Equivalently: the function $\text{Inf} \rightarrow \text{Spos}$ $I \mapsto I \cdot \mathbf{c}$ is bijective.
- ⁸ • $\forall I \in \text{Inf}, \text{Ival}(I) \in \text{Rules}_{\text{MALL}}$.
- ⁹ • **Sgraph**(π) is a finite tree.

¹⁰ .1.4 Proof trees with occurrences

¹¹ We define an other signature. This signature will be used to link together not the positions of sequents but the positions of formulas.

Definition 82. $\text{sigF}_{\text{MALL}} = (|\text{sigF}_{\text{MALL}}|, \alpha)$ with

$$\begin{aligned} |\text{sigF}_{\text{MALL}}| &= \{\text{id}, \text{cut}, \otimes, \wp, \mathbf{1}, \perp, \oplus_0, \oplus_1, \&, \top\} \cup \{\text{aux}_n \mid n \in \{0, 1, 2\}\} \\ \alpha(\text{id}) &= \{\overline{0}, \overline{1}\} \quad \alpha(\text{cut}) = \{0, 1\} \quad \alpha(\otimes) = \{0, 1, \mathbf{p}\} \quad \alpha(\wp) = \{0, 1, \mathbf{p}\} \\ \alpha(\mathbf{1}) &= \{\mathbf{p}\} \quad \alpha(\perp) = \{\mathbf{p}\} \quad \alpha(\oplus_0) = \{0, \mathbf{p}\} \quad \alpha(\oplus_1) = \{1, \mathbf{p}\} \quad \alpha(\&) = \{0, 1, \mathbf{p}\} \\ \alpha(\top) &= \{\mathbf{p}\} \quad \alpha(\text{aux}_n) = \{m \in \mathbf{N} \mid 0 \leq m < n\} \cup \{\mathbf{a}\} \end{aligned}$$

¹ From now on, we will use a notion of sequent which is different of the first, simple one
² given in Definition 72:

³ **Definition 83** (Sequent). From now on, a *sequent* is a family of formulas, that is a
⁴ $\Gamma = (|\Gamma|, \text{fml})$ with

- ⁵ • $|\Gamma| \in \text{Set}$
- ⁶ • $\text{fml}: |\Gamma| \rightarrow \text{Fml}_{\text{MALL}}$

⁷ This enriched notion of sequent allows us to give a more precise meaning to logical
⁸ rules:

⁹ **Definition 84** (Logical rule). From now on, a *logical rule* is a

- ¹⁰ • $\in \sum_{a \in \text{sigS}_{\text{MALL}}} \text{Set}^{\alpha(a)}$

¹¹ **Definition 85** (MALL rules).

Definition 86 (MALL proof structure). A proof structure is a

$$(\text{Spos}, \text{Inf}, \text{Fpos}, \text{Links}, \text{Fval}, \text{Lval}, \mathcal{U}_0, \mathcal{U}_1, \mathcal{U}_2)$$

¹² with

- ¹³ • $\text{Spos}, \text{Fpos}, \text{Links} \in \text{Set}$
- ¹⁴ • $\text{Inf} \subseteq \sum_{a \in \text{sigS}} \text{Spos}^{\alpha(a)}$ such that $\begin{array}{c} \text{Inf} \rightarrow \text{Spos} \\ I \mapsto I \cdot c \end{array}$ is injective
- ¹⁵ • $\text{Fval}: \text{Fpos} \rightarrow \text{Fml}$
- ¹⁶ • $\text{Lval}: \text{Links} \rightarrow \prod_{a \in \text{sigF}_{\text{MALL}}} \text{Fpos}^{\alpha(a)}$
- ¹⁷ • $\mathcal{U}_0: \text{Fpos} \rightarrow \text{Spos}$
- ¹⁸ • $\mathcal{U}_1: \text{Links} \rightarrow \text{Inf}$
- ¹⁹ • $\forall \ell \in \text{Links}, \forall b \in \alpha(\text{Lval}(\ell)), \mathcal{U}_2(\ell, b) \in \alpha(\mathcal{U}_1(\ell))$ such that $\mathcal{U}_0(\text{Lval}(\ell) \cdot b) = \mathcal{U}_1(\ell) \cdot \mathcal{U}_2(\ell, b)$

²⁰ **Definition 87** (MALL proof).

¹ .2 La vérité sur la formalisation des preuves

² .2.1 Types de données

³ Dictionnaires

⁴ **Definition 88.** Un dictionnaire est une paire $d = (|d|, f)$ où $|d|$ est un ensemble et f est
⁵ une fonction de domaine $|d|$.

⁶ C'est une structure non typée qui permet de structurer des données.

⁷ Si $d = (|d|, f)$ est un dictionnaire et $x \in |d|$, la valeur $f(x)$, associée à x dans d , a
⁸ tendance à être notée $d \cdot x$.

⁹ Signatures

¹⁰ **Definition 89.** Une signature est un dictionnaire à valeurs dans Set. Autrement dit,
¹¹ c'est une paire $\sigma = (|\sigma|, \alpha)$ où $|\sigma|$ est un ensemble et $\forall a \in |\sigma|, \alpha(a) \in \text{Set}$.

¹² Types algébriques

La forme générale d'un type de donnée algébrique c'est :

$$T = \sum_{a \in A} \prod_{b \in B(a)} C_a(b)$$

avec

$$A \in \text{Set} \quad B \in \text{Set}^A \quad C \in \prod_{a \in A} \text{Set}^{B(a)}$$

¹³ Un $t \in T$ est alors de la forme $t = (a, f)$ avec $a \in A$ et $\forall b \in B(a), f(b) \in C_a(b)$.

¹⁴ Remarquer que t se comporte presque comme $(B(a), f)$, qui est un dictionnaire. À cause
¹⁵ de ça, si $b \in B(a)$, $f(b)$ est noté $t \cdot b$.

¹⁶ Le couple (A, B) est une signature. Et en pratique, elle préexiste au type algébrique. On
¹⁷ a donc une signature σ et un type algébrique

$$T = \sum_{a \in |\sigma|} \prod_{b \in \alpha(a)} C_a(b)$$

- ¹ Du coup, si $t = (a, f) \in T$, on note $\text{tag}(t) := a \in |\sigma|$ et $\forall b \in \alpha(\text{tag}(t))$, on note
- ² $t \cdot b := f(b) \in C_a(b)$.
- ³ Un cas particulier courant est celui où C est constant. Dans ce cas

$$T = \sum_{a \in |\sigma|} \prod_{b \in \alpha(a)} C = \sum_{a \in |\sigma|} C^{\alpha(a)}$$

- ⁴ et si $t = (a, f) \in T$, $\text{tag}(t) = a \in |\sigma|$ et $\forall b \in \alpha(\text{tag}(t))$, $t \cdot b = f(b) \in C$.

⁵ Graphes simples

- ⁶ Pour décrire la forme des arbres de preuve, on utilise des graphes (carquois). Parce que
- ⁷ c'est une interface simple et que les gens connaissent et comprennent. Parce que ça rend
- ⁸ immédiate la définition des chemins. Par opposition aux graphes opérades / foncteurs
- ⁹ polynomiaux, avec un ensemble de noeuds, *etc.*
- ¹⁰ En revanche ça n'est plus vrai pour relier les occurrences de formules. Par exemple à
- ¹¹ cause de la coupure, qui n'a pas de conclusion.

¹² Graphes à opérations

- ¹³ Pour structurer un ensemble V de sommets, de positions, on peut utiliser un ensemble B
- ¹⁴ de liens, d'opérations, relié à V par une famille de liens binaires :

$$V \xleftarrow{s} E \xrightarrow{p} B$$

- ¹⁵ C'est comme un foncteur polynomial, mais version cyclique : pas de conclusion à droite,
- ¹⁶ tout est à gauche, y compris les conclusions des inférences.
- ¹⁷ Comme pour les foncteurs polynomiaux, au lieu de fournir explicitement E et p , on peut
- ¹⁸ les décrire via une unique fonction

$$p^{-1}: B \rightarrow \text{Set}$$

¹ À la fois E et p peuvent alors être reconstruits de la manière suivante :

$$\begin{aligned} E &:= \sum_{b \in B} p^{-1}(b) \\ \forall (b, A) \in E, p(b, A) &:= b \end{aligned}$$

² Et dans ce cas, la fonction $s: E \rightarrow V$ a le type suivant :

$$\begin{aligned} s: \sum_{b \in B} p^{-1}(b) &\rightarrow V \\ \forall b \in B, s_b: p^{-1}(b) &\rightarrow V \end{aligned}$$

³ Il est donc possible de décrire simultanément E , p et s à l'aide d'une unique fonction

$$f: B \rightarrow \sum_{A \in \text{Set}} V^A$$

⁴ à partir de laquelle on les reconstruit comme suit :

$$\begin{aligned} \forall b \in B, p^{-1}(b) &:= \text{tag}(f(b)) \\ E &:= \sum_{b \in B} \text{tag}(f(b)) \\ \forall b \in B, \forall a \in \text{tag}(f(b)), p(b, a) &:= b \\ \forall b \in B, \forall a \in \text{tag}(f(b)), s(b, a) &:= f(b) \cdot a \end{aligned}$$

⁵ En pratique, les arités A associées aux points de B sont paramétrées par une signature
⁶ σ , et on a

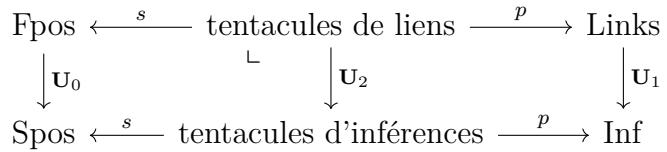
$$f: B \rightarrow \sum_{a \in |\sigma|} V^{\alpha(a)}$$

¹ qui permet encore de reconstruire E , p et s comme suit :

$$\begin{aligned}\forall b \in B, p^{-1}(b) &:= \alpha(\text{tag}(f(b))) \\ E &:= \sum_{b \in B} \alpha(\text{tag}(f(b))) \\ \forall b \in B, \forall c \in \alpha(\text{tag}(f(b))), p(b, c) &:= b \\ \forall b \in B, \forall c \in \alpha(\text{tag}(f(b))), s(b, c) &:= f(b) \cdot c\end{aligned}$$

² .2.2 Structures de preuves

³ Une structure de preuve est représentée par le diagramme suivant :



⁴ dans lequel :

⁵ • Spos = positions de séquents

⁶ • Fpos = positions de formules

⁷ • Inf = inférences

⁸ • Links = liens

⁹ Les ensembles de tentacules et les fonctions s et p sont décrites implicitement, comme
¹⁰ expliqué plus haut, par

$$\begin{aligned}\text{Ival: } \text{Inf} &\rightarrow \sum_{a \in |\text{sigS}|} \text{Spos}^{\alpha(a)} \\ \text{Lval: } \text{Links} &\rightarrow \sum_{a \in |\text{sigF}|} \text{Fpos}^{\alpha(a)}\end{aligned}$$

¹¹ *Remark 19.* Comme Ival et Lval n'ont aucune structure à part ça, on s'autorise à noter

- ¹ • $\text{tag}(I)$ pour $\text{tag}(\text{Ival}(I))$ si $I \in \text{Inf}$
- ² • $I \cdot a$ pour $\text{Ival}(I) \cdot a$ si en outre $a \in \alpha(\text{tag}(I))$
- ³ • $\text{tag}(L)$ pour $\text{tag}(\text{Lval}(L))$ si $L \in \text{Links}$
- ⁴ • $L \cdot a$ pour $\text{Lval}(L) \cdot a$ si en outre $a \in \alpha(\text{tag}(L))$

⁵ et, du coup :

$$\begin{aligned}\text{tentacules d'inférences} &:= \sum_{I \in \text{Inf}} \alpha(\text{tag}(I)) \\ \text{tentacules de liens} &:= \sum_{L \in \text{Links}} \alpha(\text{tag}(L))\end{aligned}$$

⁶ À chaque fois, p est la première projection et s est \cdot :

$$\begin{aligned}\forall I \in \text{Inf}, \forall a \in \alpha(\text{tag}(I)), p(I, a) &= I \\ \forall I \in \text{Inf}, \forall a \in \alpha(\text{tag}(I)), s(I, a) &= I \cdot a \\ \forall L \in \text{Links}, \forall a \in \alpha(\text{tag}(L)), p(L, a) &= L \\ \forall L \in \text{Links}, \forall a \in \alpha(\text{tag}(L)), s(L, a) &= L \cdot a\end{aligned}$$

⁷ **U₂ doit faire commuter le diagramme**

⁸ Les foncteurs d'oubli **U** doivent vérifier :

$$\begin{aligned}\forall L \in \text{Links}, \forall a \in \alpha(\text{tag}(L)), \quad \mathbf{U}_1(p(L, a)) &= p(\mathbf{U}_2(L, a)) \\ \mathbf{U}_1(L) &= p(\mathbf{U}_2(L, a))\end{aligned}$$

⁹ Donc **U₂**(L, a) est un (I, b) avec $I \in \text{Inf}$, $b \in \alpha(\text{tag}(I))$ et $I = \mathbf{U}_1(L)$.

¹⁰ Donc **U₂**(L, a) est un $(\mathbf{U}_1(L), b)$ avec $b \in \alpha(\text{tag}(\mathbf{U}_1(L)))$.

¹¹ D'autre part :

$$\begin{aligned}\forall L \in \text{Links}, \forall a \in \alpha(\text{tag}(L)), \quad & \mathbf{U}_0(s(L, a)) = s(\mathbf{U}_2(L, a)) \\ & \mathbf{U}_0(L \cdot a) = s(\mathbf{U}_2(L, a))\end{aligned}$$

- ¹ Donc $\mathbf{U}_2(L, a)$ est un (I, b) avec $I \in \text{Inf}$, $b \in \alpha(\text{tag}(I))$ et $I \cdot b = \mathbf{U}_0(L \cdot a)$.
- ² Donc, au total, $\mathbf{U}_2(L, a)$ est un $(\mathbf{U}_1(L), b)$ avec $b \in \alpha(\text{tag}(\mathbf{U}_1(L)))$ et $\mathbf{U}_1(L) \cdot b = \mathbf{U}_0(L \cdot a)$.
- ⁴ Il suffit donc de définir ce b comme un $\mathbf{u}_2(L, a) \in \alpha(\text{tag}(\mathbf{U}_1(L)))$ tel que $\mathbf{U}_1(L) \cdot \mathbf{u}_2(L, a) = \mathbf{U}_0(L \cdot a)$, de sorte que $\mathbf{U}_2(L, a) := (\mathbf{U}_1(L), \mathbf{u}_2(L, a))$.
- ⁶ Dit autrement, le fait que \mathbf{U}_2 soit de la forme

$$\begin{aligned}\mathbf{U}_2: \sum_{L \in \text{Links}} \alpha(\text{tag}(L)) &\longrightarrow \sum_{I \in \text{Inf}} \alpha(\text{tag}(I)) \\ (L, a) &\longmapsto (\mathbf{U}_1(L), \mathbf{u}_L(a))\end{aligned}$$

⁷ avec

$$\forall L \in \text{Links}, \quad \mathbf{u}_L: \alpha(\text{tag}(L)) \longrightarrow \alpha(\text{tag}(\mathbf{U}_1(L)))$$

⁸ garantit la commutation du carré

$$\begin{array}{ccc} \text{tentacules de liens} & \xrightarrow{p} & \text{Links} \\ \downarrow \mathbf{U}_2 & & \downarrow \mathbf{U}_1 \\ \text{tentacules d'inférences} & \xrightarrow{p} & \text{Inf} \end{array}$$

⁹ tandis que la contrainte

$$\mathbf{U}_1(L) \cdot \mathbf{u}_L(a) = \mathbf{U}_0(L \cdot a)$$

¹⁰ assure la commutation du carré

$$\begin{array}{ccc}
 \text{Fpos} & \xleftarrow{s} & \text{tentacules de liens} \\
 \downarrow \mathbf{U}_0 & \lrcorner & \downarrow \mathbf{U}_2 \\
 \text{Spos} & \xleftarrow{s} & \text{tentacules d'inférences}
 \end{array}$$

¹ **Chaque séquent est conclusion d'au plus une inférence**

² Encore une chose. Chaque inférence a une conclusion, chaque position de séquent est la
³ conclusion d'au plus une règle. Ou encore : la fonction

$$\begin{aligned}
 \text{Inf} &\longrightarrow \text{Spos} \\
 I &\longmapsto \text{Ival}(I) \cdot \mathbf{c}
 \end{aligned}$$

⁴ est injective. Une conséquence est que la fonction Ival est elle-même injective. À cause
⁵ de ça, on se permet de supposer que $\text{Inf} \subseteq \sum_{a \in |\text{sigS}|} \text{Spos}^{\alpha(a)}$ et que Ival est simplement
⁶ l'inclusion. Cela est compatible avec les conventions de la remarque 19.

⁷ **Dans une inférence, chaque position de formule est attachée à exactement une
⁸ extrémité d'un lien**

⁹ Cette contrainte correspond au fait que le carré de gauche est un pullback. La bonne
¹⁰ manière de le voir est de considérer, pour $(I, a) \in \sum_{I \in \text{Inf}} \alpha(\text{tag}(I))$ fixé, la fonction

$$\begin{aligned}
 \sum_{L \in \mathbf{U}_1^{-1}(I)} \mathbf{u}_L^{-1}(a) &\longrightarrow \mathbf{U}_0^{-1}(I \cdot a) \\
 (L, b) &\longmapsto L \cdot b
 \end{aligned}$$

¹¹ et de demander à ce qu'elle soit bijective.

¹² Cette fonction est plus claire si on comprend que

¹³ • $(I, a) \in \sum_{I \in \text{Inf}} \alpha(\text{tag}(I))$ est le choix d'une inférence et d'une extrémité de cette
¹⁴ inférence, c'est-à-dire une de ses prémisses ou bien sa conclusion

- 1 • $\sum_{L \in \mathbf{U}_1^{-1}(I)} \mathbf{u}_L^{-1}(a)$ est l'ensemble des extrémités de liens de cette inférence attachés à
- 2 une formule de cette extrémité de l'inférence
- 3 • $\mathbf{U}_0^{-1}(I \cdot a)$ est l'ensemble des positions de formules du séquent associé à (I, a) .

4 .2.3 Validité d'une structure de preuve

5 L'astuce est : on n'explique pas comment assembler des règles, à la place on explique
 6 comment décomposer un arbre en ses inférences.

7 *Remark 20.* J'ai fait un truc génial : j'ai défini les formes de liens, c'est-à-dire la signature
 8 $\text{sigF}_{\text{MALL}}$, de telle sorte que dans une inférence valide, chaque occurrence de formule,
 9 dans chaque occurrence de séquent impliqué, est une unique extrémité d'un unique lien
 10 de l'inférence.

11 Dis autrement : une règle = un ensemble de liens !!

12 Donc une règle =

- 13 • un tag $a \in |\text{sigS}_{\text{MALL}}|$
- 14 • un multiensemble de liens, où chaque lien consiste en :
- 15 – un tag $b \in |\text{sigF}_{\text{MALL}}|$
- 16 – une fonction $\alpha(b) \rightarrow \alpha(a) \times \text{Fml}$

17 Maintenant il faut définir quand est-ce qu'une inférence correspond à une règle. Étant
 18 donnée une inférence $I \in \text{Inf}$, on peut définir

- 19 • son tag $\text{tag}(I) \in |\text{sigS}_{\text{MALL}}|$
- 20 •

₁ .2.4 Autres notions

₂ .3 Jones' characterization of complexity classes

₃ This is a summing up of some work by Jones [1997, 1999].

₄ Its main result is that P is identical to the set of problems solvable by `cons`-free programs
₅ with recursion, that is by recursive read-only programs.

₆ The question for our interest is to characterize functions that do not return a boolean but
₇ construct a data structure. The point would be to say that, given a class of complexity
₈ \mathcal{C} , that is a $\mathcal{C} \subseteq \mathfrak{P}(\mathbf{Sexp})$, that is a $\mathcal{C} \subseteq \mathfrak{F}(\mathbf{Sexp}, \mathbf{Bool})$, a function $f : \mathbf{Sexp} \rightarrow \mathbf{Sexp}$
₉ is in \mathcal{C} if $\forall g : \mathbf{Sexp} \rightarrow \mathbf{Bool}, g \in \mathcal{C} \Rightarrow g \circ f \in \mathcal{C}$.

₁₀ The precise reduction from `BOOLE` to `BOOLE0` is implemented and analysed in Appendix .8.
₁₁

₁₂ **Method to reduce an ACG to a single vertex** Suppose given a size-change ACG \mathcal{G}
₁₃ where all vertices $\{v_1, \dots, v_m\}$ have the same set of variables $\{x_1, \dots, x_n\}$. Then define a
₁₄ new ACG \mathcal{H} with a single vertex v and variables $\{x_1, \dots, x_n, v_1, \dots, v_m\}$ and for each
₁₅ size-change graph $G : v_i \rightarrow v_j \in \mathcal{G}$, a size-change graph $H : v \rightarrow v \in \mathcal{H}$ defined by:

₁₆ $\langle 1 \rangle 1.$ the restriction of H to $\{x_1, \dots, x_n\}$ is equal to G .

₁₇ $\langle 1 \rangle 2.$ A preserving, non progressing arrow $v_i \xrightarrow{\geq} v_j$.

₁₈ $\langle 1 \rangle 3.$ For each $k \neq j$, a progressing arrow $v_i \xrightarrow{>} v_k$.

₁₉ **Proposition 19.** *The ACG \mathcal{H} thus defined is terminating iff. \mathcal{G} is.*

₂₀ *Proof.* There is, by construction, a bijection between size-change graphs in \mathcal{G} and in \mathcal{H} .

₂₁ Therefore, every multipath in \mathcal{G} is identified to a multipath in \mathcal{H} .

₂₂ $\langle 1 \rangle 1.$ ASSUME: p an infinite multipath in \mathcal{H} .

₂₃ $\langle 2 \rangle 1.$ CASE: p has a suffix q which is an infinite multipath in \mathcal{G}

₂₄ PROVE: p is terminating iff. q is.

₂₅ $\langle 2 \rangle 2.$ CASE: p has no suffix which is an infinite multipath in \mathcal{G}

₂₆ PROVE: p is terminating.

- ¹ *Remark 21.* Step ⟨1⟩3 of the reduction could be done symmetrically by putting instead,
² for each $l \neq i$, a progressing arrow $v_l \xrightarrow{>} v_j$. The proposition 19 and its proof would still
³ be valid.

⁴ .4 On Fischer-Ladner preordering and subformula ordering

⁵ Rémi: Chez Amina l'argument est essentiellement un argument de connexité, voire de connexité forte. Ça rappelle que dans un arbre, toute partie connexe pour la comparabilité a un min. Ici la connexité primitive, intuitive, est celle qui relie une formule à sa sous-formule de Fischer-Ladner immédiate. Effectivement, la connexité d'une partie ne suffit pas pour que le min soit une formule de point fixe. Prendre par exemple une formule sans point fixe et un chemin jusqu'à une sous-formule minimale. Pour que le min soit une formule de point fixe, on a besoin de la connexité forte.

⁶

Rémi: C'est ici qu'on développe la théorie de Fischer-Ladner et le fait que les diagrammes de threads peuvent être composés. Main result should be:

1. if (A_0, B, A_1) is an edge of a path diagram then $A_0 \xrightarrow{>^*_{\text{FL}}} B \xleftarrow{<^*_{\text{FL}}} A_1$
2. if $B_1 \xleftarrow{<^*_{\text{FL}}} A \xrightarrow{>^*_{\text{FL}}} B_2$ then either $B_1 \xleftarrow{<^*_{\text{FL}}} B_2$ or $B_1 \xrightarrow{>^*_{\text{FL}}} B_2$
3. diagram of a path composition is the composition of the path diagrams

⁷

⁸ Rémi: L'interface de cette partie ne devrait pas mentionner Fischer-Ladner.

- ⁹ The main lemma we want to prove is the following:

¹⁰ **Lemma 12.** *Let $t = (s_n)_{n \in \mathbb{N}}$ be an infinite thread in a preproof.*

¹¹ *If $\inf(t) \neq \emptyset$, i. e. if t encounters infinitely often principal formulas, then it contains a
¹² smallest infinitely principal formula, and this formula is a fixed point formula : $\exists \sigma \in$
¹³ $\{\mu, \nu\}, \exists C, \sigma XC \in \inf(t)$ and $\forall A \in \inf(t), \sigma XC \leqslant A$. As a minimum, this formula is
¹⁴ unique.*

¹⁵ Recall that “formula” means *closed* preformula, and that \leqslant is the usual, syntactical,
¹⁶ subformula ordering between formulas.

Definition 90 (Fischer-Ladner reduction). First define the reduction $\rightarrow_{\sigma}^{\text{FL}}$ by:

$$\forall A, \forall \sigma' \in \{\mu, \nu\} : \sigma' X A[X] \xrightarrow{\sigma}^{\text{FL}} A[\sigma' X A[X]]$$

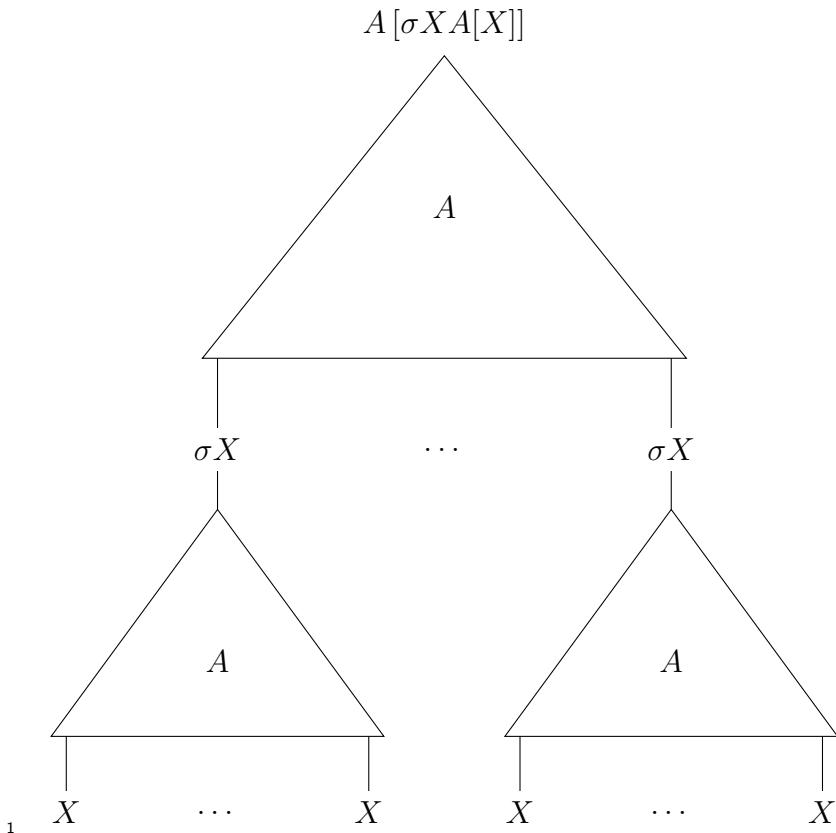
- ¹ Then simply define \rightarrow_{FL} to be $> \cup \rightarrow_{\sigma}^{\text{FL}}$. We denote by $\rightarrow_{\text{FL}}^*$ the preorder generated by \rightarrow_{FL} , *i. e.* its reflexive, transitive closure.

³ **Lemma 13.** *If $B \leqslant A[\sigma X A[X]]$ then either $B \leqslant \sigma X A[X]$ or $B \geqslant \sigma X A[X]$.*

⁴ *Proof.* Some terminology: if T is the syntactic tree of a preformula A , if p is a path in T , from the root of T to a node n in T , and if $T|_n$, subtree of T rooted in n , is the syntactic tree of a preformula C , we simply say that $T|_n$ is the subtree of A starting at p and that ⁷ p is a position of C in A . If p and q are two such paths, we denote by $p \sqsubseteq q$ the fact that ⁸ p is a prefix of q .

⁹ Let p_1, \dots, p_n be the positions of $\sigma X A[X]$ in A or, equivalently, the positions of X in $A[X]$. Let b be a position of B in $A[\sigma X A[X]]$.

¹¹ If $\exists i$ such that $p_i \sqsubseteq b$ or $b \sqsubseteq p_i$ then, respectively, $B \leqslant \sigma X A[X]$ or $\sigma X A[X] \leqslant B$.
¹² Otherwise the subtree of $A[\sigma X A[X]]$ starting at b is identical to the subtree of $A[X]$ starting at the same position. That means that b is also a position of B in $A[X]$, and in ¹³ this case $B \leqslant \sigma X A[X]$. \square
¹⁴



² **Lemma 14.** If $n \geq 0$ and $A_0 \rightarrow_{\text{FL}} A_1 \rightarrow_{\text{FL}} \dots \rightarrow_{\text{FL}} A_n$ then $\{A_0, \dots, A_n\}$ has a
³ minimum.

⁴ *Proof.* By induction on n , by examining $A_0 \rightarrow_{\text{FL}} A_1$ and using lemma 13. □

⁵ **Definition 91.** We note $A \leq_{\text{FL}}^* B$ if there is $n \geq 0$ and formulas A_1, \dots, A_n such that
⁶ $A \rightarrow_{\text{FL}} A_1 \rightarrow_{\text{FL}} \dots \rightarrow_{\text{FL}} A_n = B$ and $\forall i, A \leq A_i$.

⁷ Rémi: Remark that \leq_{FL}^* implies \leq and that \geq_{FL}^* is equivalent to \geq . ■

⁸ **Lemma 15.** If $A \geq_{\text{FL}}^* B \leq C$ then either $A \leq C$ or $A \geq C$.

¹⁰ .5 Proof of PSPACE-completeness of $\text{BOOLE}_{\text{false}}$

¹¹ **Lemma 16.** $\text{PSPACE} \leq_L (\text{BOOLE}_{\text{false}}, \mathcal{B}_{\text{false}})$

Rémi
 En fait on pourrait similairement définir $A \geq_{\text{FL}}^* B$, parce que ce qui nous intéresse vraiment d'exprimer c'est $A \geq_{\text{FL}}^* B \leq_{\text{FL}}^* C$, c'est-à-dire un chemin de Fischer-Ladner, dont on a identifié le minimum donné par le lemme 14.

¹ We prove this by reduction from a more general form of programs:

Definition 92 (BOOLE (from p. 387 of [Jones, 1997] and def. 17 of [Lee, Jones, and Ben-Amram, 2001])). A program $b \in \text{BOOLE}$ is a sequence of instructions $b = 1:I_1\ 2:I_2\ \dots\ m:I_m$ where the form of instructions is given by

$$\begin{aligned} I &::= X := E \mid I_1; I_2 \mid \text{goto } \ell \mid \text{if } E \text{ then } I_1 \text{ else } I_2 \\ E &::= X \mid \text{true} \mid \text{false} \mid E_1 \vee E_2 \mid E_1 \wedge E_2 \mid \neg E \mid E_1 \Rightarrow E_2 \mid E_1 \Leftrightarrow E_2 \\ X &::= X_0 \mid X_1 \mid \dots \end{aligned}$$

² The semantic is as expected, with all variables being equal to `false` at the beginning of
³ the program, and the program halting when reaching instruction $m + 1$.

The language BOOLE_0 is the fragment of BOOLE obtained by keeping only two forms of instructions :

$$I ::= X := \neg X \mid \text{if } X \text{ then goto } \ell \text{ else goto } \ell'$$

⁴ *Proof of lemma 16.* We show two things:

⁵ 1. a program in BOOLE can be transformed into an equivalent program in BOOLE
⁶ in which, in case of termination, all variables have value *false* at the end of the
⁷ execution;

⁸ 2. a program in BOOLE can be transformed into an equivalent program in BOOLE_0 .

⁹ The first transformation simply consists in adding, at the end of the program, an
¹⁰ instruction `X := false` for each variable `X` occurring in the program.

¹¹ The second transformation consists in coding every instruction of BOOLE into a sequence
¹² of instructions of BOOLE_0 with the same semantic. To deal with the assignments we add
¹³ one new variable to the program for each expression appearing in the original program.
¹⁴ In doing that we have to insert new labels between the original labels.

¹⁵ Some examples:

¹⁶ `X := true`

¹⁷ becomes

¹⁸ 1: if `X` then goto 3 else goto 2
¹⁹ 2: `X := not X`

₁ and

₂ X := false

₃ becomes

₄ 1: if X then goto 2 else goto 3

₅ 2: X := not X

₆ X := Y

₇ becomes intuitively

₈ if Y then X := true else X := false

₉ that is

₁₀ 1: if Y then goto 2 else goto 3

₁₁ 2: if X then goto 5 else goto 4

₁₂ 3: if X then goto 4 else goto 5

₁₃ 4: X := not X

₁₄ X := Y and Z

₁₅ becomes intuitively

₁₆ if Y then X := Z else X := false

₁₇ which gives

₁₈ 1: if Y then goto 2 else goto 4 // X := Y and Z

₁₉ 2: if Z then goto 3 else goto 4 // X := Z

₂₀ 3: if X then goto 6 else goto 5 // X := true

₂₁ 4: if X then goto 5 else goto 6 // X := false

₂₂ 5: X := not X

₂₃ X := Y or Z

₁ becomes intuitively

₂ if Y then X := true else X := Z

₃ which gives

```

4 1: if Y then goto 3 else goto 2 // X := Y or Z
5 2: if Z then goto 3 else goto 4 // X := Z
6 3: if X then goto 6 else goto 5 // X := true
7 4: if X then goto 5 else goto 6 // X := false
8 5: X := not X

```

₉ X := (A or B) and C

₁₀ becomes

```

11 [X := (A or B) and C]: if A then [X := C] else [X := B and C]
12 [X := B and C]: if B then [X := C] else [X := false]
13 [X := C]: if C then [X := true] else [X := false]
14 [X := true]: if X then [end] else [X := not X]
15 [X := false]: if X then [X := not X] else [end]
16 [X := not X]: X := not X
17 [end]:

```

₁₈ that is

```

19 1: if A then goto 3 else goto 2 // X := (A or B) and C
20 2: if B then goto 3 else goto 5 // X := B and C
21 3: if C then goto 4 else goto 5 // X := C
22 4: if X then goto 7 else goto 6 // X := true
23 5: if X then goto 6 else goto 7 // X := false
24 6: X := not X

```

₂₅ This last transformation is not very satisfactory because it makes new expressions appear
₂₆ which are not subexpressions of the original expression. Here is an idea to counter that.
₂₇ Instead of reducing

₂₈ X := (A or B) and C

₁ to

₂ if A then X := C else X := B and C

₃ we translate

₄ if (A or B) and C then c1 else c2

₅ into

₆ if A or B then (if C then c1 else c2) else c2

₇ which becomes in turn

₈ if A then (if C then c1 else c2) else (if B then (if C then c1 else c2) else c2)■

₉ so, that we get

₁₀ 1: if A then goto 3 else goto 2 // if (A or B) and C then X := true else X := false
₁₁ 2: if B then goto 3 else goto 5 // if B then (if C then X := true else X := false)
₁₂ 3: if C then goto 4 else goto 5 // if C then X := true else X := false
₁₃ 4: if X then goto 7 else goto 6 // X := true
₁₄ 5: if X then goto 6 else goto 7 // X := false
₁₅ 6: X := not X

₁₆ So we get the same result, but in a more satisfactory way.

₁₇

□

₁₈ .6 Assignment of priorities to formulas

₁₉ In the section, we show how to define a function $\Omega: \text{Fml} \rightarrow \omega$ such that:

₂₀ 1. if A is subformula of B then $\Omega(A) \leq \Omega(B)$

₂₁ 2. $\forall A, \Omega(\mu X A)$ is even and $\Omega(\nu X A)$ is odd

We consider ω as $2 \cdot \omega$. It means that priorities are pairs of a natural integer and a boolean, ordered lexicographically:

$$(0, \text{false}) < (0, \text{true}) < (1, \text{false}) < (1, \text{true}) < \dots$$

¹ and equipped with the following ceiling functions:

Definition 93.

$$\begin{array}{ll} \lceil(n, \text{false})\rceil^{\text{false}} = (n, \text{false}) & \lceil(n, \text{false})\rceil^{\text{true}} = (n, \text{true}) \\ \lceil(n, \text{true})\rceil^{\text{false}} = (n + 1, \text{false}) & \lceil(n, \text{true})\rceil^{\text{true}} = (n, \text{true}) \end{array}$$

Definition 94 (Acceptance of a priority).

$$\text{A priority } (n, b) \text{ is } \begin{cases} \text{accepting} & \text{if } b = \text{true} \\ \text{rejecting} & \text{if } b = \text{false} \end{cases}$$

Definition 95 ($\Omega: \text{Fml} \rightarrow 2 \cdot \omega$). A function Ω is defined by induction, which associate a priority to every *preformula*:

$$\begin{array}{ll} \Omega(\nu X A) = \lceil\Omega(A)\rceil^{\text{true}} & \\ \Omega(\mu X A) = \lceil\Omega(A)\rceil^{\text{false}} & \\ \Omega(A \odot B) = \max\{\Omega(A), \Omega(B)\} & \text{for any binary connective } \odot \\ \Omega(\mathbf{c}) = (0, \text{false}) & \text{for any propositional constant } \mathbf{c} \\ \Omega(X) = (0, \text{false}) & \end{array}$$

² The following remarks are immediate:

³ **Lemma 17.** *For all formulas A and B:*

⁴ • $\Omega(\nu X A)$ is accepting and $\Omega(\mu X A)$ is rejecting.

⁵ • If A is a subformula of B then $\Omega(A) \leq \Omega(B)$.

⁶ **.7 Vieilles remarques sur le background technique**

⁷ Rémi: threads internes liés à la vision mu-calcul et aux preuves à la Stirling

1 Rémi: remarque pour le fait que les threads internes pourraient être définis sans problème sur les preuves infinies. Peut être essayer de l'écrire de manière suffisamment modulaire et encapsulée pour qu'il soit déplaçable.

2 Rémi: définir l'unfolding d'une représentation circulaire en une prépreuve infinie. Parler de l'équivalence induite sur les repr. Qu'elle est décidable. Que deux repr equiv ont la même validité.

3 Rémi: mentionner les inclusions entre prouvabilités des trois logiques. Et la traduction de la règle finitaire en une repr circulaire.

4 .7.1 vieilles remarques sur le finitaire

5 Rémi: Background sur μ MALL finitaire. Aller voir la littérature.

6 Rémi: distinguer ce qui parle de plus petits et plus grands points fixes et ce qui parle de points fixes génériques ? Brotherston et Simpson utilisent des systèmes à la Martin-Lof vs. les gens qui font du mu-calcul, ce qui contient muMALL, et un peu Santocanale, par exemple dans son papier avec Fortier. Dale est passé des systèmes de def inductives à la ML tels que SchHei et Holnas vers des systèmes à base de mu-calcul.

7 Rémi: En quoi est-ce que tous ces travaux apportent à ma thèse ? Et qu'est-ce que je veux en raconter ? Reprendre ça du point de vue de *ma* thèse, des problématiques de *ma* thèse.

8 Rémi: Il y doit y avoir des travaux plus récents, Brotherston, Simpson, Tatsuta, systèmes circulaires, finitisation.

9 .7.2 vieilles remarques sur le circulaire

10 Rémi: Définir “non-wellfounded and circular proof systems”. Aller voir la littérature.

Rémi: Avoir une référence précise pour une formalisation précise des arbres de preuves qui soit compatible avec mon utilisation formelle, en particulier avec l'existenece de séquents ouverts. La bonne manière est probablement de faire remarquer que n'importe quel système peut être étendu avec une règle genre Daimon, "open sequent" pour obtenire ce que je veux.

¹

Rémi: Un argument de plus pour parler des objets finis est le fait que dans cette formalisation il est très naturel de considérer la question de quand deux représentations circulaires sont équivalentes parce qu'elles représentent intuitivement le même arbre de preuve infini. D'où le fait d'être prêt à répondre à ça voire d'y répondre par avance. D'où le fait d'avoir les arbres infinis qui sont *la* bonne manière de définir cette équivalence (se souvenir des essais sur les formules modulo déroulage).

²

³ Sequents and preproofs

Rémi: Idée fondamentale de mon approche : Je vais parler d'objets infinitaires en travaillant uniquement dans un monde fini. Je vais refléter des notions infinies dans ce cadre fini.

⁴

Rémi: C'est d'ailleurs une bonne manière de montrer le problème avec le critère de threads, qui force l'utilisation de notions infinies. D'où le fait de chercher un critère qui fait seulement appel à des notions finies. Et de chercher à relier ce système de preuve à un système purement finitaire.

⁵

Rémi: Mes notations ne sont pas celles de la littérature. C'est gênant parce que les lecteurs qui vont comparer ce que je fais avec les autres, où aller vérifier des résultats que je cite vont me haïr pour avoir changer toutes les notations. Première chose à faire : signaler la différence de vocabulaire avec le reste de la littérature, en la citant. Deuxième chose : justifier ce choix, par exemple avec une remarque qui dit que comme dans la suite ces représentations finies sont les seules qu'on utilisera, on se permet de les appeler prépreuves circulaires.

⁶

Rémi: La bonne manière de mentionner que je ne parle pas de cut-elim c'est de dire que le périmètre auquel je m'intéresse est celui des représentations finies, parce que c'est ça qui m'intéresse, parce que *etc*. Or les représentations finies circulaires ne sont pas closes par cut-elim / ne sont pas un cadre satisfaisant / suffisant pour étudier la (dynamique de la) cut-elim.

⁷

1 Rémi: L'annotation des sommets des graphes telle que faite ici par des lettres grecques dans les séquents n'est pas très lisible. Dans la version pour écran couleur, mettre de la couleur. Trouver une solution pour la version papier.

1

2 Rémi: Le fait de nommer des sommets μ ou ν peut-il être gênant ? Peut-on, dans le doute, trouver quelque chose qui évite ce problème ?

2

3 Rémi: Ajouter des exemples plus simples ! Par exemple avec une preuve de $\nu X(X \otimes X)$. Notamment pour avoir pour chaque définition un exemple simple qui illustre correctement cette notion et pas trop davantage. Et il n'y a pas de problème à ce qu'éventuellement une définition soit illustrée par plusieurs exemples, au contraire. Utiliser mon exemple pour ce qu'il illustre. Par exemple pour la distinction entre non bien fondé, circulaire, représentation finie.

3

Ici l'arbre de preuve de l'exemple que j'utilise partout :

$$\begin{array}{c}
 \frac{\vdash \nu XX, \nu X(X \wp X), \mu XX \quad \frac{\vdash \nu XX, \nu X(X \wp X), \mu XX}{\vdash \nu X(X \wp X), \nu X(X \wp X), \mu XX} (\nu)}{\vdash \nu X(X \wp X), \nu X(X \wp X), \mu XX} (\text{cut}) \\
 \frac{\vdash \nu X(X \wp X) \wp \nu X(X \wp X), \mu XX \quad \frac{\vdash \nu XX \quad \frac{\vdash \nu XX}{\vdash \nu X(X \wp X)}}{\vdash \nu X(X \wp X), \mu XX} (\nu)}{\vdash \nu X(X \wp X)} (\wp)
 \end{array}$$

4 Rémi: Donner d'autres exemples. Des exemples qui montrent les problèmes de soundnes des prépreuves sans critère. Des exemples avec des modalités. Avec des *streams*.

4

5 Rémi: Faire remarquer que tout séquent est conclusion d'une prépreuve, et que ce problème de soundness est la raison pour laquelle on a besoin d'un critère de correction, donc de la sous-section qui vient tout de suite, et qui n'a de sens qu'après cette discussion sur la soundness.

5

6 Rémi: Parler de l'équivalence des représentations. Quand deux représentations sont-elles équivalentes ? Peut-on le décider facilement ?

6

¹ **Proofs**

² Rémi: Signaler qu'on veut distinguer les preuves parmi les prépreuves. Que cette section a pour but de définir ça. En somme Expliciter l'intention du paragraphe.

³ The validity criterion used to distinguish proofs among preproofs will be given in Definition 31 and can be stated as: “every infinite branch must contain a valid thread”. Note that:

⁶ •

⁷ Rémi: Écrire quelque part, proprement, la définition formelle, rigoureuse de ces graphes. Telle qu'elle est écrite on pourrait croire qu'un graphe est une fonction $V \times V \rightarrow \mathbf{N}$ alors que ce que je veux dire c'est une fonction $V \times V \rightarrow \text{Set}$. Quel lien entre cette vision et les équivalences $\text{Set}/X \simeq \text{Set}^X$? Et donner un exemple qui justifie le choix de cette définition plutôt que l'autre, qui montre en quoi la version non nommée serait insuffisante.

⁸ • If (π, back) is a **preproof**, we say that a position of a sequent in π is “**closed**” when it is not an **open sequent** i. e. it is the conclusion of some inference in π .

¹⁰ Rémi: Faire rentrer les deux définitions suivantes dans le cadre formel de cette partie.

¹¹ **Definition 96.** Every rule r of μMALL^∞ comes with a *threading function* $t(r)$ (see Figure .1) mapping each position of a subformula in a premise to a position of a subformula in the conclusion, except for cut-formulas, by relating the subformula positions of a premise formula F with the corresponding (subformula) positions of the conclusion F' , F being the FL-subformula associated to F' by inference r ; note that in the case of the unfolding of fixed point $F' = \nu X.G$ into $F = G[\nu X.G/X]$ every position of $\nu X.G$ in F is associated to the root position of F' and every position of a subformula in (a copy of) G in F is associated to the corresponding subformula position in G in F' . More formally, if s_1 is the conclusion and s_2 a premise of the same position of rule r , then r induces a partial function $t(r): \text{Pos}(s_2) \rightharpoonup \text{Pos}(s_1)$, where $\text{Pos}(A_0, \dots, A_{n-1}) = \{(k, p) \mid 0 \leq k < n \text{ and } p \text{ is a position of a subformula in } A_k\}$.

²² Rémi: La figure suivante n'est plus en phase avec la description des règles donnée en figure 13 : pas le même nombre de règles, pas le même agencement des règles, par la même notation des points fixes, pas la même règle d'échange, etc. Régler ça. Faire une remarque sur le fait qu'il n'y a rien à donner pour les règles sans prémisses.

$$\begin{array}{c}
\frac{}{\vdash F_1, \Gamma} (\oplus_1) \quad \frac{}{\vdash F_2, \Gamma} (\oplus_2) \quad \frac{\vdash \Gamma, F \quad \vdash F^\perp, \Delta}{\vdash \Gamma, \Delta} (\text{Cut}) \\
\frac{}{\vdash \Gamma} (\perp) \quad \frac{\vdash F, \Gamma \quad \vdash G, \Gamma}{\vdash F \& G, \Gamma} (\&) \quad \frac{\vdash F, \Gamma \quad \vdash G, \Delta}{\vdash F \otimes G, \Gamma, \Delta} (\otimes) \\
\frac{}{\vdash F, G, \Gamma} (\wp) \quad \frac{}{\vdash F \wp G, \Gamma} (\wp) \quad \frac{\vdash \Gamma, F, G, \Delta}{\vdash \Gamma, G, F, \Delta} (\times) \\
\frac{}{\vdash F[\mu X.F/X], \Gamma} (\mu) \quad \frac{\vdash \Gamma, F, G, \Delta}{\vdash \Gamma, G, F, \Delta} (\times) \\
\frac{}{\vdash G[\nu X.G/X], \Gamma} (\nu) \quad \frac{}{\vdash \mu X.F, \Gamma} (\mu)
\end{array}$$

Figure .1. Threading function

- 1 By composing these partial maps we define $\mathbf{t}(u)$ for any path u , mapping positions of
2 subformulas in the top sequent of u to positions of subformulas in its bottom sequent.

3 **Definition 97** ($\mathfrak{T}(u)(p)$). If u is a finite path in a μMALL^∞ preproof and p a position
4 of subformula in its top sequent then there is a unique thread in u , going from $\mathbf{t}(u)(p)$
5 up to p . This thread is constructed by following the threading relation and is denoted as
6 $\mathfrak{T}(u)(p)$.

7 **Definition 98** (G_{branch} , branch graph of a preproof). Let π be a μMALL^∞ preproof. Its
8 *branch graph* is the tree G_{branch} defined as follows. The vertices of G_{branch} are the positions
9 of *sequents* in π . For each inference I with conclusion s in π and for each premise s' of I ,
10 there is an edge in G_{branch} , from s to s' .

11 **Example 16.**

12 **Definition 99** (Infinite branch). If π is a *preproof* and G_{branch} is its branch graph, we
13 call an *infinite branch* of this preproof any infinite path in G_{branch} starting from the root
14 of G_{branch} .

15 **Example 17.**

16 **Definition 100** ($G_{\text{thread}}^{\text{out}}$, thread graph of a preproof). Let π be a μMALL^∞ preproof.
17 Its thread graph is the graph $G_{\text{thread}}^{\text{out}}$ defined as follows. The vertices of $G_{\text{thread}}^{\text{out}}$ are the
18 positions of formulas in the sequents of π . For each inference I with conclusion s in π ,
19 for each premise s' of I and for each position of formula β in s' which has an *immediate
20 descendant* α in s , there is an edge in $G_{\text{thread}}^{\text{out}}$, from α to β .

21 **Example 18.**

22 **Example 19.**

23 **Example 20.**

- ¹ *Remark 22.* Even when t is an infinite thread, $\mathbf{U}(t)$ may not be an infinite branch because
² it may not start at the root of the preproof. However, if t is an infinite thread, then $\mathbf{U}(t)$
³ is a suffix of an infinite branch.

- ⁴ **Example 21** (valid and invalid preproofs).

- ⁵ **Example 22.** The infinite branches of the preproof of Example 5 are $s_0(s_7)^\omega$, $s_0(s_1s_2s_3)^\omega$
⁶ and all elements of $\{s_0(s_1s_2s_3)^k(s_5)^\omega \mid k \in \mathbf{N}\}$.

- ⁷ Note that, in order to be totally rigorous, we should

- ⁸ 1.

Rémi: Donne un exemple où ne pas faire la chose suivante serait problématique
⁹ :

- ¹⁰ not only give the vertices of the paths but also the edges, *i.e.* when an inference
¹¹ has several premises, indicate explicitly which one was chosen;

- ¹² 2. include the implicit (exc) rules.

- ¹³ These details are omitted here for concision; they will cause no ambiguity on the validity
¹⁴ of the preproof of Example 5.

Example 23. An example of why we need more information than simply the sequence
of sequent positions:

$$\frac{\vdash X, \overline{X} \quad \vdash X, \overline{X}}{\rightarrow \vdash X, \overline{X} \leftarrow} \text{(cut)}$$

- ¹⁵ The branch graph of this circular representation has one vertex and two loops, which we
¹⁶ want to distinguish *a priori*.

Rémi: Définir ce qu'est une formule ou une position (de formule ou de sous-formule)
principale. Remarquer en particulier que si une position de sous-formule dans un
séquent est la formule principale du séquent alors c'est en fait une position de for-
mule du séquent, pas une sous-formule stricte.

¹⁷

Rémi: Vérifier qu'on a fait dans l'ordre suivant :

- MALL
- μ et ν
- de même on peut étendre LJ et LK en μ LJ et μ LK

1

2 .8 OCaml implementation of Jones reduction from BOOLE 3 to BOOLE₀

```
open! Base
open Boole_types

let module_name = Caml.__MODULE__

module Iterm_repr = struct
  (* Intermediate representation, well-suited to internal transformations. *)

  let module_name = module_name ^ ".Iterm_repr"

  module Var : sig
    type t = int
    val of_boole : Boole.var -> t
    val to_boole0 : t -> Boole_const.var
    val dummy : t

    type stock = int
    val create : vars:stock -> stock * t
  end = struct
    (* let module_name = module_name ^ ".Var" *)

    type t = int
    let of_boole x = x
    let to_boole0 x = x
    let dummy = 0

    type stock = int
    let create ~vars:n = (n + 1, n)
  end
```

```

module Label = struct
  let module_name = module_name ^ ".Label"

  type t = int list
end

module Expr = struct
  let module_name = module_name ^ ".Expr"

  type t =
    | Var of Var.t
    | True
    | False
    | Or of t * t
    | And of t * t
    | Not of t
    | Implies of t * t
    | Equiv of t * t

  let rec of_boole : Boole.expr -> t =
    let open! Boole in
    function
    | Var x -> Var (Var.of_boole x)
    | True -> True
    | False -> False
    | Or (e1, e2) -> Or (of_boole e1, of_boole e2)
    | And (e1, e2) -> And (of_boole e1, of_boole e2)
    | Not e -> Not (of_boole e)
    | Implies (e1, e2) -> Implies (of_boole e1, of_boole e2)
    | Equiv (e1, e2) -> Equiv (of_boole e1, of_boole e2)

  let name_of_var_exn expr =
    let fun_name = module_name ^ ".name_of_var_exn" in
    match expr with
    | Var x ->
      x
    | True | False | Or (_, _) | And (_, _) | Not _ | Implies (_, _) |
      Equiv (_, _) ->
      failwith fun_name

  let assign_const_to_boole0_exn x exp =
    let fun_name = module_name ^ ".assign_const" in
    let open Boole_const in
    match exp with

```

```

| True ->
  Assign_true x
| False ->
  Assign_false x
| Var _ | Or (_, _) | And (_, _) | Not _ | Implies (_, _) |
  Equiv (_, _) ->
    failwith fun_name

let rec nb_vars : t -> int =
function
| Var x -> x + 1
| True | False -> 0
| Or (exp1, exp2) | And (exp1, exp2) | Implies (exp1, exp2) |
  Equiv (exp1, exp2) -> max (nb_vars exp1) (nb_vars exp2)
| Not exp -> nb_vars exp
end

module Instr = struct
let module_name = module_name ^ ".Instr"

type t =
| Assign of Var.t * Expr.t
| Seq of t * t
| Goto of Label.t
| If of Expr.t * t * t

let rec of_boole : Boole.instr -> t =
let open! Boole in
function
| Assign (x, e) -> Assign (Var.of_boole x, Expr.of_boole e)
| Seq (i1, i2) -> Seq (of_boole i1, of_boole i2)
| Goto l -> Goto [l]
| If (e, i1, i2) -> If (Expr.of_boole e, of_boole i1, of_boole i2)

let label_of_goto_exn instr =
let fun_name = module_name ^ ".label_of_goto_exn" in
match instr with
| Goto lab ->
  lab
| Assign (_, _) | Seq (_, _) | If (_, _, _) ->
  failwith fun_name

let rec nb_vars : t -> int =
function

```

```

| Assign (x, exp) ->
  max (x + 1) (Expr.nb_vars exp)
| Seq (exp1, exp2) ->
  max (nb_vars exp1) (nb_vars exp2)
| Goto _ ->
  0
| If (exp, ins1, ins2) ->
  max (Expr.nb_vars exp) (max (nb_vars ins1) (nb_vars ins2))
end

module Prog = struct
  let module_name = module_name ^ ".Prog"

  type t =
  | Instr of Instr.t
  | Seq of t list

  let rec of_boole_list (prog : Boole.prog) : t list =
    match prog with
    | [] -> []
    | i :: prog -> Instr (Instr.of_boole i) :: of_boole_list prog

  let of_boole (prog : Boole.prog) : t =
    Seq (of_boole_list prog)

  let rec nb_vars : t -> int =
    function
    | Instr ins ->
      Instr.nb_vars ins
    | Seq seq ->
      List.fold_right seq ~f:(fun pr n -> max (nb_vars pr) n) ~init:0
end

module To_Boole_const_exn = struct
  (** Translates to Boole_const a program in intermediate representation, which
  has already been transformed into a Boole_const format. *)
  let module_name = module_name ^ ".To_Boole_const_exn"

  let rec nb_instrs : Prog.t -> int =
    let open Prog in
    function
    | Instr _ ->
      1

```

```

| Seq seq ->
  List.fold_right seq
    ~f:(fun prog acc -> nb_instrs prog + acc)
    ~init:0

let rec label (prog : Prog.t) (lab : Label.t) : Boole_const.label =
  let fun_name = module_name ^ ".label" in
  let open Prog in
  match prog, lab with
  | (Instr _ | Seq _), [] -> 0
  | Seq seq, n :: lab -> list_label seq n lab
  | Instr _, _ :: _ -> failwith fun_name

and list_label seq n lab =
  match seq, n with
  | prog :: _, 0 -> label prog lab
  | prog :: seq, n -> nb_instrs prog + list_label seq (n - 1) lab
  | [], _ -> 0

let instr (prog : Prog.t) (ins : Instr.t) : Boole_const.instr =
  let fun_name = module_name ^ ".instr" in
  let open Boole_const in
  let open Instr in
  match ins with
  | Assign (x, v) ->
    Expr.assign_const_to_boole0_exn (Var.to_boole0 x) v
  | If (b, i1, i2) ->
    let x = Expr.name_of_var_exn b in
    let l1 = Instr.label_of_goto_exn i1 in
    let l2 = Instr.label_of_goto_exn i2 in
    If_goto (Var.to_boole0 x, label prog l1, label prog l2)
  | Seq (_, _) | Goto _ ->
    failwith fun_name

let prog (pr : Prog.t) : Boole_const.prog =
  let open Prog in
  let rec flatten : Prog.t -> Boole_const.prog = function
    | Instr ins -> [instr pr ins]
    | Seq seq -> List.concat_map seq ~f:flatten in
  flatten pr
end

module Translation = struct
  let if_goto (x : Var.t) (l1 : Label.t) (l2 : Label.t) : Prog.t =

```

```

let open Prog in
let open Instr in
let open Expr in
Instr (If (Var x, Goto 11, Goto 12))
(* constant time *)

let goto (lab : Label.t) : Prog.t =
  if_goto Var.dummy lab lab
(* constant time *)

let assign_const (x : Var.t) (c : bool) : Prog.t =
  let open Prog in
  let open Instr in
  let open Expr in
  match c with
  | true -> Instr (Assign (x, True))
  | false -> Instr (Assign (x, False))
(* constant time *)

let rec assign (x : Var.t) (exp : Expr.t)
  ~(pos : int list) ~(vars : Var.stock)
  : Var.stock * Prog.t =
  let open Prog in
  let open Instr in
  let open Expr in
  match exp with
  | Var y ->
    let seq =
      [if_goto y (List.rev (1 :: pos)) (List.rev (3 :: pos));
       assign_const x true;
       goto (List.rev (4 :: pos));
       assign_const x false] in
    (vars, Seq seq)
  | True | False as const ->
    (vars, Instr (Assign (x, const)))
  | Or (exp1, exp2) ->
    let vars, x1 = Var.create ~vars in
    let vars, x2 = Var.create ~vars in
    let vars, ass_x1_0 = assign x1 exp1 ~pos:(0 :: pos) ~vars in
    let vars, ass_x2_1 = assign x2 exp2 ~pos:(1 :: pos) ~vars in
    let seq =
      [ass_x1_0;
       ass_x2_1;
       if_goto x1 (List.rev (4 :: pos)) (List.rev (3 :: pos))];
```

```

        if_goto x2 (List.rev (4 :: pos)) (List.rev (6 :: pos));
        assign_const x true;
        goto (List.rev (7 :: pos));
        assign_const x false] in
    (vars, Seq seq)
| And (exp1, exp2) ->
    let vars, x1 = Var.create ~vars in
    let vars, x2 = Var.create ~vars in
    let vars, ass_x1_0 = assign x1 exp1 ~pos:(0 :: pos) ~vars in
    let vars, ass_x2_1 = assign x2 exp2 ~pos:(1 :: pos) ~vars in
    let seq =
        [ass_x1_0;
         ass_x2_1;
         if_goto x1 (List.rev (3 :: pos)) (List.rev (6 :: pos));
         if_goto x2 (List.rev (4 :: pos)) (List.rev (6 :: pos));
         assign_const x true;
         goto (List.rev (7 :: pos));
         assign_const x false] in
    (vars, Seq seq)
| Implies (exp1, exp2) ->
    let vars, x1 = Var.create ~vars in
    let vars, x2 = Var.create ~vars in
    let vars, ass_x1_0 = assign x1 exp1 ~pos:(0 :: pos) ~vars in
    let vars, ass_x2_1 = assign x2 exp2 ~pos:(1 :: pos) ~vars in
    let seq =
        [ass_x1_0;
         ass_x2_1;
         if_goto x1 (List.rev (3 :: pos)) (List.rev (4 :: pos));
         if_goto x2 (List.rev (4 :: pos)) (List.rev (6 :: pos));
         assign_const x true;
         goto (List.rev (7 :: pos));
         assign_const x false] in
    (vars, Seq seq)
| Equiv (exp1, exp2) ->
    let vars, x1 = Var.create ~vars in
    let vars, x2 = Var.create ~vars in
    let vars, ass_x1_0 = assign x1 exp1 ~pos:(0 :: pos) ~vars in
    let vars, ass_x2_1 = assign x2 exp2 ~pos:(1 :: pos) ~vars in
    let seq =
        [ass_x1_0;
         ass_x2_1;
         if_goto x1 (List.rev (3 :: pos)) (List.rev (4 :: pos));
         if_goto x2 (List.rev (5 :: pos)) (List.rev (7 :: pos));
         if_goto x2 (List.rev (7 :: pos)) (List.rev (5 :: pos));

```

```

        assign_const x true;
        goto (List.rev (8 :: pos));
        assign_const x false] in
    (vars, Seq seq)
| Not exp ->
    let vars, ass_x_0 = assign x exp ~pos:(0 :: pos) ~vars in
    let seq =
        [ass_x_0;
         if_goto x (List.rev (4 :: pos)) (List.rev (2 :: pos));
         assign_const x true;
         goto (List.rev (5 :: pos));
         assign_const x false] in
    (vars, Seq seq)
(* the [List.revs] run in linear time
   all other non-recursive calls run in constant or linear time
   the function [assign] runs in quadratic time *)

let rec instr (ins : Instr.t) ~(pos : int list) ~(vars : Var.stock)
    : Var.stock * Prog.t =
let open Expr in
let open Instr in
let open! Prog in
match ins with
| Assign (x, exp) ->
    assign x exp ~pos ~vars
| Seq (ins1, ins2) ->
    let vars, pr1 = instr ins1 ~pos:(0 :: pos) ~vars in
    let vars, pr2 = instr ins2 ~pos:(1 :: pos) ~vars in
    (vars, Seq [pr1; pr2])
| Goto lab ->
    (vars, goto lab)
| If (exp, ins1, ins2) ->
    let vars, x = Var.create ~vars in
    let vars, ass_x_exp_0 = assign x exp ~pos:(0 :: pos) ~vars in
    let if_x_goto_1 =
        Instr (If (Var x,
                    Goto (List.rev (2 :: pos)),
                    Goto (List.rev (4 :: pos)))) in
    let vars, pr1_2 = instr ins1 ~pos:(2 :: pos) ~vars in
    let goto_end_3 = goto (List.rev (5 :: pos)) in
    let vars, pr2_4 = instr ins2 ~pos:(4 :: pos) ~vars in
    let res : Prog.t =
        Seq [ass_x_exp_0;
              if_x_goto_1;

```

```

        pr1_2;
        goto_end_3;
        pr2_4] in
    (vars, res)
(* calls to [List.rev]s run in linear time
calls to [assign] run in quadratic time
all other non-recursive calls run in constant or linear time
the function [instr] runs in cubic time *)

let rec prog_rec (pr : Prog.t) ~(pos : int list) ~(vars : Var.stock)
  : Var.stock * Prog.t =
  let open Prog in
  match pr with
  | Instr ins ->
    instr ins ~pos ~vars
  | Seq seq ->
    let vars, seq =
      List.fold_map seq
        ~init:vars
        ~f:(fun i vars pr -> prog_rec pr ~pos:(i :: pos) ~vars)
    in
    (vars, Seq seq)
(* each call to [instr] runs in cubic time and the number of such calls
is less than the size of the argument [pr]
the calls to [List.fold_map] run in linear time
so [prog_rec] runs in time  $O(n^4)$  *)
let prog (pr : Prog.t) : Prog.t =
  let _vars, res = prog_rec pr ~pos:[] ~vars:(Prog.nb_vars pr) in
  res
(* is only a call to [prog_rec]
[prog] runs in time  $O(n^4)$  *)
end
end

```

¹ **Complexité de cette traduction** The translation consists in three parts:

- ² 1. The first part is the translation to the intermediate representation. It is implemented in module `Interm_repr` by functions `Var.of_boole`, `Expr.of_boole`, `Instr.of_boole` and `Prog.of_boole`. They only copy and paste the data structure, so this operation runs in linear time.

1 2. The second part is the internal translation. It is performed by the functions of
2 module `Interm_repr.Translation`.

3 It is where the essential work happens and it is essentially a map and it is linear.

4 3. The third part is the translation to the datatype of BOOLE0 programs. It is
5 essentially a map but each computation of a label is linear. Therefore the whole
6 translation is quadratic.

7 *Remark 23.* We could be more precise but we are only interested in polytime

8 *Remark 24.* we could optimise the code, for instance by registering the translations of
9 goto labels into a map or a hashtable. but we are only interested in polytime

Rémi: À faire pour rendre ça plus limpide :

- remplacer la monade d'état par de vraies références
- remplacer les arbres par des offsets comme suggéré par Alexis
- enlever du code tout ce qui n'est pas strictement nécessaire

10

11 .9 Commented bibliography

12 .9.1 On μ MALL

13 • [Doumane, 2017, p. 54, Section 2.4.1 “Finitary proof system”] Décrit les règles
14 d'introduction finitaires des points fixes. Décrit la fonctorialité. Désigne Baelde
15 [2012] comme référence.

16 • [Baelde, 2012] Introduit μ MALL. Utilise une technique à la Girard (candidats
17 de réductibilité ?) pour montrer l'élimination des coupures. Extrait de son intro
18 ci-dessous. C'est l'article principal de sa thèse, qui prouve la cut-elim de muMALL.

19 “The logic μ MALL was initially designed as an elementary system for studying
20 the focusing of logics supporting (co)inductive definitions [Momigliano and Tiu,
21 2003]; leaving aside the simpler underlying propositional layer (MALL instead of
22 LJ), fixed points are actually more expressive than this notion of definition since
23 they can express mutually recursive definitions. But μ MALL is also relatively close
24 to type theoretical systems involving fixed points [Matthes, 1998, Mendler, 1991].

The main difference is that our logic is a first-order one, although the extension to second-order would be straightforward and the two fundamental results would extend smoothly. Inductive and coinductive definitions have also been approached by means of cyclic proof systems [Brotherston, 2005, Santocanale, 2002]. These systems are conceptually appealing, but generally weaker in a cut-free setting; some of our earlier work [Baelde, 2009] addresses this issue in more details. There is a dense cloud of work related to μ MALL. Our logic and its focusing have been used to revisit the foundations of the system Bedwyr [Baelde, Gacek, Miller, Nadathur, and Tiu, 2007], a proof search approach to model checking. A related work [Baelde, 2009] carried out in μ MALL establishes a completeness result for inclusions of finite automata leading to an extension of cyclic proofs. The treatment of fixed points in μ MALL, as presented in this paper, can be used in full linear logic (μ LL) and intuitionistic logic (μ LJ). μ LL has been used to encode and reason about various sequent calculi [Miller and Pimentel, 2013]. μ LJ has been given a game semantics [Clairambault, 2009].”

- Momigliano and Tiu [2003] [Tiu = Thesard de Dale] introduced a logic with λ -terms, induction and co-induction, which carefully adds principles of induction and co-induction to a first-order intuitionistic logic based on a proof-theoretic notion of definitions. This proof-theoretic (rather than set-theoretic) notion of definition follows on work (among others) by Hallnäs [1991], Eriksson [1991], Schroeder-Heister [1993], McDowell and Miller [2000]. This logic is defined in sequent calculus. Their rules of induction and coinduction implicitly incorporate a cut, and they prove cut-elimination for their system.
- There is also [Tiu and Momigliano, 2012], which is the journal version of the previous one, and in which they provide a direct cut-elimination procedure in the presence of general inductive and co-inductive definitions based on reducibility-candidate technique.
- [Hallnäs, 1991] Inductive definitions of datatypes. Partial inductive definitions, and then an object with such a definition may or may not be totally defined. Analog phenomenon as with the definitions of partial recursive functions, which may happen to be total recursive functions. Mention a related joint work with Schroeder-Heister and another one with Eriksson, which are not those cited by Baelde [2012]. Every partial inductive definition defines a particular sequent calculus used to infer whether an object belongs to the defined set. These partial inductive definitions and their associated calculi are in general infinite.
- Eriksson [1991] provide a way to encode the (partial) inductive definitions of Hallnäs [1991] in a finitary way, so that it can be manipulated by programs. Their system of finitary representations can only represent countably many partial inductive definitions and derivations while there are uncountably many of both kinds, hence their system cannot represent every definition or derivation.

- ¹ • Schroeder-Heister [1993] starts from the principle of “definitional reflection” defined by Hallnäs [1991].
- ²
- ³ • McDowell and Miller [2000] Thesard de Dale.
- ⁴ • Matthes [1998]
- ⁵ • Mendler [1991]. De quoi ça parle ?
- ⁶ • [Brotherston, 2005] Il y probablement un peu plus de références de lui intéressantes aujourd’hui.
- ⁷
- ⁸ • [Santocanale 2001] = [Santocanale, 2002]. Probablement une publi et un rapport technique. De quoi ça parle ?
- ⁹
- ¹⁰ • [Baelde, 2009]. De quoi ça parle ?
- ¹¹ • [Baelde and Miller, 2007]. De quoi ça parle ? Quoi par rapport à la thèse de David ?
- ¹²
- ¹³ • [Baelde, Gacek, Miller, Nadathur, and Tiu, 2007]. De quoi ça parle ?
- ¹⁴ • [Miller and Pimentel 2010] = [Miller and Pimentel, 2013].
- ¹⁵ • [Clairambault, 2009]. De quoi ça parle ? Quoi par rapport à sa thèse ?

¹⁶ .10 Notations

- ¹⁷ • If A is a set then $\mathfrak{P}(A)$ denotes the powerset of A , that is the set of all subsets of A .
- ¹⁸

¹⁹ .11 A short reminder on complexity classes and completeness

²¹ Rémi: Déplacer en annexe.

²² **Definition 101** (Problem). A problem consists of three sets $\Omega \supseteq I \supseteq P$:

1. The set Ω is the universe, the analytic matter, what programs can take as input. It could be, for instance, $\{0, 1\}^*$, as in a computer, or \mathcal{A}^* with \mathcal{A} a finite alphabet as is usual in automata theory and in the study of Turing machines, or s-expressions $\mathbf{S} = \{\text{nil}\} + \underset{\mu}{\mathbf{S}} \times \mathbf{S}$ as used in LISP languages, and advocated by Jones [Jones, 1997] for the formal study of complexity.
6. The set I is the set of well-formed instances, which will effectively be given as inputs of programs. It could be, for instance, the set of all correct encodings of undirected finite graphs.
9. The set P is a subset of I : the set of all well-formed instances which should be “accepted”, whatever that means. It could be, for instance, the set of all correct encodings of all *3-colorable* undirected finite graphs.

12 **Definition 102** (Recognition). A program π recognizes, or accepts, a problem $\Omega \supseteq I \supseteq P$ if:

14. 1. π “accepts” the elements of P ,
 15. 2. π “rejects” the elements of $I \setminus P$
 16. 3. and π can do anything on $\Omega \setminus I$. In particular, π may perfectly neither “accept” nor “reject” the elements of $\Omega \setminus I$.
- 18 And it is *a priori* meaningless to ask how a program π would behave when given as input an element outside Ω .

20 **Definition 103** (Reduction). A reduction $(\Omega, I, P) \leq_{\mathcal{F}} (\Omega', I', P')$ is a program $f: \Omega \rightarrow \Omega'$ such that:

22. 1. $f(P) \subseteq P'$,
23. 2. $f(I \setminus P) \subseteq I' \setminus P'$
24. 3. f can do anything on $\Omega \setminus I$
25. 4. $f \in \mathcal{F}(I)$

26 *Remark 25.* The two first conditions can be equivalently stated as:

27. 1. $f(I) \subseteq I'$

¹ 2. $\forall x \in I, f(x) \in P' \Leftrightarrow x \in P$

² *Remark 26.* An example to illustrate the fourth condition: setting $\mathcal{F} = \text{ptime}$ means that
³ f is asked to run in ptime *on* I . We *really* do not care about the behavior of f outside I .

⁴ Because, in each case, we do not care about what happens in $\Omega \setminus I$, we generally omit
⁵ Ω in the definition of the problem, and we only define f on I in the definition of a
⁶ reduction.

⁷ .12 Open questions

- ⁸ • quelle est la différence d'expressivité entre l'image de μMALL et μMALL^\supset ? Com-
⁹ ment l'exhiber, l'expliciter ? (On peut déjà mentionner l'imbrication des boucles.)
- ¹⁰ • peut-on étendre la procédure de finitisation à un fragment plus large, qui contienne
¹¹ les lunettes ?
- ¹² • Qu'entend-on exactement par « finitiser » ? C'est obtenir une preuve finie « équiv-
¹³ alente » à la preuve infinie. Que signifie « équivalente » ?
 - ¹⁴ – Avoir la même conclusion n'est pas assez.
 - ¹⁵ – Équivalence équationnelle ? Pour quelle théorie équationnelle ?
 - ¹⁶ – Équivalence contextuelle ? N'est pas toujours résistant aux extensions du
¹⁷ système. Et nécessite de parler de la réduction.
 - ¹⁸ – Égalité des interprétations dans une certaine sémantique ? Une telle égalité
¹⁹ doit avoir des conséquences concrètes, sans quoi on court le risque qu'elle soit
²⁰ trop ad hoc.
 - ²¹ – Égalité des preuves obtenues par normalisation ? Est-ce que la procédure est
²² confluente ?
- ²³ • si on finitise puis qu'on déroule, ou l'inverse, qu'obtient-on ?

²⁴ Rémi: Lister, classifier et trouver des notations pour les systèmes impliqués.

Figure .2

$$\begin{array}{c}
 \star \\
 \frac{}{\vdash F, G, H, I, J} \\
 \frac{\star}{\vdash F, G, \underline{H}, I, J} \quad (\nu)(\oplus_1) \\
 \frac{}{\vdash F, G, H, \underline{I}, J} \quad (\mu)(\oplus_0)(\wp) \\
 \frac{}{\vdash F, G, H, \underline{I}} \quad (\mu)(\oplus_0)(\perp) \\
 \frac{}{\vdash F, G, H, I, \underline{J}} \quad (\mu)(\oplus_1)(\perp) \\
 \frac{}{\vdash F \wp G, H, I, J} \quad (\wp) \\
 \frac{}{\vdash F \wp G, \underline{G}, H, I, J} \quad (\nu)(\oplus_1), (\perp) \\
 \frac{}{\vdash F \wp G, H, I, J} \quad (\nu)(\oplus_1) \\
 \frac{}{\vdash F, G, H, I, J} \quad (\nu), (\oplus_0) \\
 \frac{}{\vdash F, G, H, \underline{K}, J} \quad (\nu) \\
 \frac{}{\vdash F, G, H, J} \quad (\mu), (\oplus_0), (\wp) \\
 \frac{}{\vdash F, G, H, \underline{J}} \quad (\mu), (\oplus_1), (\perp) \\
 \frac{}{\vdash F, H, G, I, J} \quad (\mu), (\oplus_1), (\perp) \\
 \frac{}{\vdash F \wp H, G, I, J} \quad (\wp) \\
 \frac{}{\vdash F \wp H, G, \underline{H}, I, J} \quad (\nu)(\oplus_0), (\perp) \\
 \frac{}{\vdash F \wp H, G, H, I, J} \quad (\wp) \\
 \frac{\vdash (F \wp G) \& (F \wp H), G, H, I, J}{\star \vdash F, G, H, I, J} \quad (\mu)
 \end{array}$$

.13 π_∞

² In this section, we investigate a pathological example of a circular proof in μ MALL that
³ arguably cannot be presented with an equivalent finite representation that can be labelled
⁴ with the loop criterion.

⁵ Let us consider the following formulas:

- ⁶ • $F = \mu X.(X \wp G) \& (X \wp H);$
- ⁷ • $G = \nu X.X \oplus \perp;$
- ⁸ • $H = \nu X.\perp \oplus X;$
- ⁹ • $K = \nu Y.\mu Z.((Z \wp \mu X.(Y \wp X) \oplus \perp) \oplus \perp);$
- ¹⁰ • $I = \mu Z.((Z \wp \mu X.(K \wp X) \oplus \perp) \oplus \perp);$
- ¹¹ • $J = \mu X.(K \wp X) \oplus \perp.$

¹² And the following proof: on figure .2

¹³ Each infinite branch is validated by a thread going through either G, H or K :

- ¹⁴ • if the branch ultimately goes always to the left cycle ($u \ddot{u} l^\omega$), then the validating thread goes through H ;
- ¹⁵

- 1 • if the branch ultimately goes always to the right cycle ($u \circ r^\omega$), then the validating
2 thread goes through G ;
- 3 • if the branch ever switch between left and right ($l^* \cdot (r^+ \cdot l^+)^{\omega}$), then the validating
4 thread goes through K

5 .13.1 Size-change algorithm for the decision of the thread criterion

6 **Definition 104.** We call *size-change graph* any function $f : E \rightarrow \mathbf{B} \times E$ where E is a
7 finite set and $\mathbf{B} = \{\text{tt}, \text{ff}\}$ is the set of booleans.

8 Size-change graphs can be composed with :
$$\frac{f(x) = (b_1, y) \quad g(y) = (b_2, z)}{(g \circ f)(x) = (b_1 \vee b_2, z)}$$

9 Rémi: apprendre (un fragment suffisant minimal de) tikz et présenter les tuiles sous forme de dessins.

10 For every target $\vdash \Gamma$ of back-edge(s) we consider the finite set $\text{Pos}(\Gamma)$ of positions of ν
11 formula in Γ and we define a set T of size-change graphs on the set $\text{Pos}(\Gamma)$ by following,
12 on each possible path from a source of back-edge to its target all ν formulas. Then we
13 close this set under composition.

14 We exemplify this on the glasses: there is only one target of back-edges: the conclusion
15 sequent; there are 6 occurrences of ν -formula in the conclusion: the G and H in F, G ,
16 H , the K in I and the K in J . Therefore we will consider size-change graphs of arity 6.
17 There are two back-edges targetting this sequent and no nested loop. Therefore we will
18 consider a set of two size-change graphs. Those size-change graphs are constructed by
19 following the ν -formulas top down.

We denote by $E = \{G_F, H_F, G, H, K_I, K_J\}$ the set of occurrences of ν -formula in the conclusion. The size-change graphs are:

$$\begin{aligned} \text{left: } E &\rightarrow \mathbf{B} \times E \\ G_F &\mapsto (\text{ff}, G_F) \\ H_F &\mapsto (\text{ff}, H_F) \\ G &\mapsto (\text{ff}, G_F) \\ H &\mapsto (\text{tt}, H) \\ K_I &\mapsto (\text{ff}, K_I) \\ K_J &\mapsto (\text{ff}, K_I) \end{aligned}$$

$$\begin{aligned}
right: E &\rightarrow \mathbf{B} \times E \\
G_F &\mapsto (\text{ff}, G_F) \\
H_F &\mapsto (\text{ff}, H_F) \\
G &\mapsto (\text{tt}, G) \\
H &\mapsto (\text{ff}, H_F) \\
K_I &\mapsto (\text{tt}, K_J) \\
K_J &\mapsto (\text{ff}, K_J)
\end{aligned}$$

- ¹ **Definition 105.** If T is a set of size-change graphs on the same domain, we denote by
² T^+ the closure of T under composition.
- ³ **Definition 106.** We say that a set T of size-change graphs on the same domain is *valid* if
⁴ every idempotent size-change graph $f \in T^+$ contains a mapping of the form $x \mapsto (\text{tt}, x)$.
- ⁵ **Definition 107.** We say that a μMALL^ω preproof is *size-change-valid* if all its back-edge
⁶ targets have valid sets of size-change graphs.
- ⁷ **Proposition 20.** *The representation of a μMALL^ω preproof is thread-valid iff. it is
⁸ size-change-valid.*
- ⁹ *Proof.* (\Leftarrow) Let us assume that a μMALL^ω preproof π is *not* thread-valid.
¹⁰ (1) to every infinite branch of π we can associate a word of size-change graphs such that
¹¹ the two have the same threads.
¹² (2) π has then an infinite branch / infinite word of size-change graphs with no valid
¹³ thread and where the number of threads is maximal
¹⁴ (3) from this we get the same where no infinite thread (of infinite word of SC graphs)
¹⁵ ever progresses
¹⁶ (4) by a pigeon-hole-principle argument we get a periodic word
¹⁷ (5) by iterating it we get a never-progressing idempotent period, thus breaking size-change
¹⁸ validity.
¹⁹ (\Rightarrow) Conversely, any invalid size-change graph in the transitive closure of the generated
²⁰ size-change graphs induces a periodic invalid branch. \square

À définir en
dehors de la
preuve.

¹ **Proposition 21.** *To every set of size-change graphs on the same set — that is to every size-change graph — we can associate a rewriting system on a \mathbf{N}^k which is terminating iff. the size-change graph is valid.*

⁴ *Proof.* This is SC folklore. See Ben-Amram. □

⁵ This sheds some new light on the finitenesse of the thread criterion for circular proofs.
⁶ Indeed the thread criterion, as it is formulated, imposes to check an infinity of infinite
⁷ branches and to ensure that each of them contains an infinite thread, infinitely progressing.
⁸ It is nonetheless known that for finite representations of circular proofs, this can be
⁹ checked in finite time and space — more precisely, in polynomial space. However [Dax,
¹⁰ Hofmann, and Lange, 2006] and maybe [Lange, 2011] and [Fogarty and Vardi, 2012] must
¹¹ be checked before we claim anything to be new on this subject.

¹² Des vieux trucs

¹³ *Remark 27.* There is a way to generalise the criterion in order to validate a simple
¹⁴ unfolding of this proof. This requires to:

- ¹⁵ • dissociate the ν rule from the target-of-back-edge rule;
- ¹⁶ • follow not only one position of a ν -formula in the sequent of the back-edge, but
¹⁷ several one at once;

¹⁸ At the end you get to solve a termination problem such as:

Example 24. The following rewriting system, on $\mathbf{N} \times \mathbf{N}$, is terminating:

$$\begin{array}{lcl} a, b & \rightarrow & a - 1, b \\ a, b & \rightarrow & a, b - 1 \\ a, b & \rightarrow & b - 1, a \\ a, b & \rightarrow & b, a - 1 \\ a, b & \rightarrow & a - 1, a - 1 \\ a, b & \rightarrow & b - 1, b - 1 \end{array}$$

¹⁹ *Proof.* Use one of the following decreasing measure:

- ²⁰ • the multiset order on $[a, b]$; ¹

¹ « L'ordre multiset c'est plus fort que tout. » (Olivier Laurent)

- ¹ • the lexicographic pair $(\max\{a, b\}, \min\{a, b\})$;
- ² • the lexicographic pair $(\max\{a, b\}, a + b)$.

³

□

Example 25. among

$$\begin{array}{lcl} a, b & \rightarrow & a - 1, a \\ a, b & \rightarrow & b, b - 1 \end{array}$$

- ⁴ we can add either one of them to the previous system without breaking termination, but
⁵ not both.

- ⁶ *Proof.* • if we add the first one, consider the termination measure $(\max\{a, b\}, a + b, a)$
⁷ • if we add the second one, consider the termination measure $(\max\{a, b\}, a + b, b)$
⁸ • if we add both, see example 26

⁹

□

- ¹⁰ The general form of those rewriting system, whose termination we have to decide, is: on
¹¹ \mathbf{N}^k : a set of rewriting equations of the form $(a_1, \dots, a_k) \rightarrow (a'_1, \dots, a'_k)$ where, for all i ,
¹² a'_i is of the form a_j or $a_j - 1$ for some j .

- ¹³ And the characterisation we get is that the following are equivalent:

- ¹⁴ • the system is not terminating
¹⁵ • the preproof cannot be validated this way
¹⁶ • the preproof cannot be validated this way and we have a counter-example:
¹⁷ – with a maximal number of threads
¹⁸ – on a cyclic branch
¹⁹ – where threads never progress
²⁰ – and in the threading structure all cycles are loop and all other vertices directly
²¹ goes to a loop.

¹ Here are other examples of such rewriting systems:

² *Example 26.* The following rewriting systems are *not* terminating:

1. on \mathbf{N}^2 :

$$\begin{array}{lcl} a, b & \xrightarrow{\alpha} & a - 1, a \\ a, b & \xrightarrow{\beta} & b, b - 1 \end{array}$$

2. on \mathbf{N}^3 :

$$\begin{array}{lcl} a, b, c & \xrightarrow{\alpha} & c, c, a - 1 \\ a, b, c & \xrightarrow{\beta} & b - 1, a, a \\ a, b, c & \xrightarrow{\gamma} & b, c - 1, b \end{array}$$

3. on \mathbf{N}^3 :

$$\begin{array}{lcl} a, b, c & \xrightarrow{\alpha} & a - 1, b, b - 1 \\ a, b, c & \xrightarrow{\beta} & b - 1, b, c - 1 \end{array}$$

³ *Proof.* Consider the following cycles:

⁴ 1. $1, 0 \xrightarrow{\alpha} 0, 1 \xrightarrow{\beta} 1, 0 \xrightarrow{\alpha} \dots$

⁵ 2. $1, 0, 1 \xrightarrow{\alpha} 1, 1, 0 \xrightarrow{\beta} 0, 1, 1 \xrightarrow{\gamma} 1, 0, 1 \xrightarrow{\alpha} \dots$

⁶ 3. $1, 2, 0 \xrightarrow{\alpha} 0, 2, 1 \xrightarrow{\beta} 1, 2, 0 \xrightarrow{\alpha} \dots$

⁷

□

⁸ *Remark 28.* In such a rewriting system, the max of all coordinates is always non-increasing
⁹ along a rewriting. Therefore:

- ¹⁰ • if the rewriting system is terminating, it admits a decreasing measure in the form
¹¹ of a lexicographic pair with the max of all coordinates as first component;
- ¹² • every rewriting sequence is bounded, therefore, if the system is non-terminating, it
¹³ has a cycle.

¹ It raises the following questions:

- ² • can the loop criterion be seen as a particular, but still uniform, case of this more general technique?
- ⁴ • does this extended criterion still implies the thread validity?
- ⁵ • are we able to finitize the proof validated by this extended criterion?
- ⁶ • does every regular proof have a representation valid for this extended criterion?
- ⁷ • can we make the criterion locally checkable by use of some labelling?
- ⁸ • can we generalize the form of size-change graphs so as to deal with bouncing threads?

¹⁰ This technique seems closely related to the one used by Rodolphe Lepigre in [Lepigre and Raffalli, 2016, 2019].

¹² .14 Checking finite representations vs. Circular pre-proofs

¹³ Consider the following circular pre-proofs, with $N = \mu X. \mathbf{1} \oplus X$:

$$\pi_{\text{add}}^1 = \frac{\frac{\frac{\overline{\vdash N^\perp, N} \text{ (id)}}{\vdash \perp, N^\perp, N} \text{ (\perp)} \quad \frac{\star}{\vdash N^\perp, N^\perp, N} \text{ (\mu), (\oplus_1)}}{\vdash \perp \& N^\perp, N^\perp, N} \text{ (\&)}}{(\star) \vdash N^\perp, N^\perp, N} \text{ (\nu)}$$

$$\pi_{\text{add}}^2 = \frac{\frac{\frac{\overline{\vdash N^\perp, N} \text{ (id)}}{\vdash \perp, N^\perp, N} \text{ (\perp)} \quad \frac{\star}{\vdash N^\perp, N^\perp, N} \text{ (\mu), (\oplus_1)}}{\vdash \perp \& N^\perp, N^\perp, N} \text{ (\&)}}{(\star) \vdash N^\perp, N^\perp, N} \text{ (\nu)}$$

¹⁴ Both computing the addition of two nats, corresponding respectively to:

¹⁵ let rec add1 m n = match m with
¹⁶ | Z -> n

1 | S p → S(add1 p n);;

2 and

3
 4 let rec add2 m n = match m with
 5 | Z → n
 6 | S p → S(add2 n p);;

7 It is easy to convince oneself that, while the first circular pre-proof (π_{add}^1) is presented
 8 with a finite representation satisfying the loop criterion, the finite representation used
 9 above to present the second pre-proof (π_{add}^2) does not satisfy the loop criterion. However,
 10 its alternative finite representation/unfolding does:

$$\begin{array}{c}
 \frac{}{\vdash N^\perp, N} (\text{id}) \quad \frac{\star}{\vdash N^\perp, N^\perp, N} (\text{exc}) \\
 \frac{}{\vdash \perp, N^\perp, N} (\perp) \quad \frac{\vdash N^\perp, N^\perp, N}{\vdash N^\perp, N^\perp, N} (\mu), (\oplus_1) \\
 \frac{}{\vdash \perp \& N^\perp, N^\perp, N} (\&) \\
 \frac{\vdash N^\perp, N}{\vdash \perp, N^\perp, N} (\perp) \quad \frac{\vdash N^\perp, N^\perp, N}{\vdash N^\perp, N^\perp, N} (\mu), (\oplus_1) \\
 \frac{}{\vdash \perp \& N^\perp, N^\perp, N} (\&) \\
 \frac{}{(\star) \vdash N^\perp, N^\perp, N} (\nu)
 \end{array}$$

11 Can we say something about it based on the computation of the labelling algorithm?

Alexis: En particulier, en exploitant la régularité des preuves circulaire (si je puis dire...) étant donnée une preuve circulaire dont on connaît la taille de la présentation minimale comme arbre fini avec back-edge, ne peut-on pas borner l'espace des représentations finies à vérifier?

Dans ce cas, ne peut-on pas imaginer obtenir une équivalence avec le critère des threads?

12 Another example to investigate:

$$\frac{\vdash \underline{\nu_1 X.X}, \nu_2 X.X, \mu Y.Y \& Y \quad \vdash \nu_1 X.X, \underline{\nu_2 X.X}, \mu Y.Y \& Y}{\vdash \nu_1 X.X, \nu_2 X.X, (\mu Y.Y \& Y) \& (\mu Y.Y \& Y)} (\mu) \\
 \frac{}{(\star) \vdash \nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y} (\nu)$$

$\frac{\star_1}{\vdash \nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y}$	$\frac{\star_{12}}{\vdash \nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y}$	$\frac{\star_{21}}{\vdash \nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y}$
	$\frac{\vdash \nu_1 X.X, \nu_2 X.X, (\mu Y.Y \& Y) \& (\mu Y.Y \& Y)}{\vdash \nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y} \quad (\mu)$	$\frac{\vdash \nu_1 X.X, \nu_2 X.X, (\mu Y.Y \& Y) \& (\mu Y.Y \& Y)}{\vdash \nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y} \quad (\mu)$
\star_1	$\frac{\vdash \nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y}{(\star_{12}) \vdash \nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y} \quad (\nu)$	$\frac{\vdash \nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y}{(\star_{21}) \vdash \nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y} \quad (\nu)$
	$\frac{\vdash \nu_1 X.X, \nu_2 X.X, (\mu Y.Y \& Y) \& (\mu Y.Y \& Y)}{\vdash \nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y} \quad (\mu)$	$\frac{\vdash \nu_1 X.X, \nu_2 X.X, (\mu Y.Y \& Y) \& (\mu Y.Y \& Y)}{\vdash \nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y} \quad (\mu)$
$(\star_1) \vdash \underline{\nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y}$		$\frac{\vdash \nu_1 X.X, \nu_2 X.X, (\mu Y.Y \& Y) \& (\mu Y.Y \& Y)}{\vdash \nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y} \quad (\mu)$
	$\frac{\vdash \nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y}{\vdash \nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y} \quad (\nu)$	$\frac{\vdash \nu_1 X.X, \nu_2 X.X, (\mu Y.Y \& Y) \& (\mu Y.Y \& Y)}{\vdash \nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y} \quad (\mu)$
	$\frac{\vdash \nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y}{(\star_2) \vdash \nu_1 X.X, \nu_2 X.X, \mu Y.Y \& Y}$	

Figure .3

- ¹ Which is a pre-proof valid for the loop criterion when presented in a clever way as in figure .3

.15 Searching for circular proofs

- #### 4 (d) About proof-search:

- in $\mu\text{MALL}_{\text{lab}}^{\curvearrowleft}$

- 7 Justify that it is

- simpler than for μ MALL
 - simpler than for μ MALL $^\omega$.
 - compare with Brotherston's approach

Alexis: ajouté!

- ¹² Extrait du papier de Brotherston et al. *A Generic Cyclic Theorem Prover*, section
¹³ “4 Proof search issues and experimental results”:

- ## • 4.1 Global search strategy

- ¹ • 4.2 Soundness checking
- ² • 4.3 Forming back-links
- ³ • 4.4 Order of rule applications
- ⁴ • 4.5 Predicate folding/lemma application
- ⁵ • 4.6 Limitations
- ⁶ • 4.7 Experimental results
- ⁷ • (+ voir les related works)

⁸ .16 Quelques Remarques d'Orthographe et de Style

- ⁹ • légendes des figures (et barbe par rapport à la couverture) : en dessous ou au dessus
¹⁰ ? Réponse : LIPICs et Springer s'accordent sur le fait que : “Figure captions have
¹¹ to be placed below the figures. Table captions (and also captions of other text-like
¹² floating environments like listings and algorithms) have to be placed above the
¹³ table.”
- ¹⁴ • pluriels : “formulas”, “criteria”
- ¹⁵ • “premise”, plural: “premises”
- ¹⁶ • adjectif : “labelled” (UK)
- ¹⁷ • “preproof” ou “pre-proof” ? Le premier : plus simple à lire comme à écrire.
- ¹⁸ • définitions: utiliser la commande defname pour souligner les termes définis
- ¹⁹ • On Capitalise les Titres de Sections (en général, c'est la règle appliquée précédem-
²⁰ ment qui est utilisée par les éditeurs il me semble, spécification molle.)
- ²¹ • penser à déclarer une référence pour chaque définition ou résultat, pour permettre
²² facilement des les citer dans les discussions et preuves du papier.
- ²³ • pour annexes/version longue: avec David et Amina, on utiliser une commande
²⁴ qui permet de reciter facilement un résultat en annexe tout en conservant la
²⁵ numérotation: voir quand on introduit cela...

- ¹ • notation: $\nu X.A$

² Rémi: Du coup est-ce qu'on note $A[\nu X.A]$ ou $A[\nu X.A[X]]$ ou $A[\nu X.A/X]$?

- ³ • pour annotations: à trancher, note en cours.

⁴ Les ensembles dont on a besoin de parler :

- ⁵ • prépreuves infinies

- ⁶ • prépreuves infinies étiquetées

- ⁷ • preuves infinies

- ⁸ • preuves étiquetées infinies

- ⁹ • prépreuves circulaires

- ¹⁰ • preuves circulaires

- ¹¹ • prépreuves circulaires étiquetées

- ¹² • preuves circulaires étiquetées

- ¹³ • représentations de prépreuves circulaires

- ¹⁴ • représentations étiquetées de prépreuves circulaires

- ¹⁵ • représentations de preuves circulaires

- ¹⁶ • représentations de preuves circulaires étiquetées

- ¹⁷ • preuves finitaires

¹⁸ **.16.1 Terminology**

- ¹⁹ • En accord avec wikipedia et ncatlab on dit “fixed point”, “pre-fixed point” et
²⁰ “post-fixed point”.

- ²¹ • “order” ou “preorder” désigne la relation. L’ensemble équipé de cette relation est
²² un “ordered set” ou “preordered set”.

- ¹ • “endofunction” est bien. (On peut aussi dire “self-mapping” d’apres le nlab.)
- ² • Si (E, \leq) est un ordre ou un préordre, les $x \in E$ sont des “elements” plutôt que des “points”.
- ³

⁴ .16.2 Dialogues

- ⁵ Notes en commentaires