Local validity for circular proofs in linear logic with fixed points

Rémi Nollet[1]

IRIF, Université Paris Diderot and CNRS
Paris, France
nollet@irif.fr

This is an ongoing work, done in collaboration with Alexis Saurin and Christine Tasson.

Various logical settings have been introduced to reason about inductive and coinductive statements, both at the level of the logical languages modelling (co)induction (Martin Löf's inductive predicates vs. fixed-point logics, that is μ-calculi) and at the level of the proof-theoretical framework considered (finite proofs with (co)induction *à la* Park vs. infinite proofs with fixed-point/inductive predicate unfoldings) [8, 10, 11, 5, 2, 3]. Moreover, such proof systems have been considered over classical logic [8, 11], intuitionistic logic [12], linear-time or branching-time temporal logic [19, 18, 24, 25, 13, 15, 16] or linear logic [21, 17, 5, 4, 15].

In all those proof systems, the treatment of inductive and coinductive reasoning brings some highly complex proof figures. For instance, in proof systems using (co)induction rules *à la* Park, the rules allowing to derive a coinductive property (or dually to use an inductive hypothesis) have a complex inference of the form of fig. 1 (when presented in the setting of fixed-point logic – here we follow the one-sided sequent tradition of MALL). This inference breaks the subformula property, *i. e.* it is hiding a cut: at each coinduction rule, one has to guess an invariant (in the same way as one has to guess an appropriate induction hypothesis in usual mathematical proofs) which is problematic for automation of proof search.

Infinite (non-wellfounded) proofs have been proposed as an alternative in recent years [8, 10, 11]. By replacing the coinduction rule with simple fixed-point unfoldings and allowing for non-wellfounded branches, those proof systems address the problem of the subformula property for the cut-free systems. The cut-elimination dynamics for inductive-coinductive rules is also much simpler. Among those non-wellfounded proofs, circular proofs, that have infinite but regular derivations trees, retain the simplicity of the inferences of non-wellfounded proof systems while having simple finite representations, making it possible to have an algorithmic treatment of those proof objects.

Figure 1: Coinduction rule *à la* Park

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

However, in those proof systems when considering all possible infinite, non-wellfounded derivations (a. k. a. pre-proofs), it is straightforward to derive any sequent Γ (see example below). Such pre-proofs are therefore unsound and one needs to impose a validity criterion to distinguish, among all pre-proofs, those which are logically valid proofs from the unsound ones. This condition will actually reflect the inductive and coinductive nature of our two fixed-point connectives: a standard approach is to consider a pre-proof to be valid if every infinite branch is supported by a progressing thread. However, doing so, the logical correctness of circular proofs becomes a non-local property, much in the spirit of proof nets correctness criteria, and one has to check the validity at each cycle in the proof (obtained by placing what we will call a back-edge in the following).

Despite the need for a validity condition, circular proofs have recently received increasing interest with the simultaneous development of their applications and meta-theory: infinitary proof theory is now well-established in several proof-theoretical frameworks such as Martin Löf's inductive predicates, linear logic with fixed-points, *etc.*

$$\dfrac{\dfrac{\vdots}{\vdash \mu X.X}\,(\mu) \qquad \dfrac{\vdots}{\vdash \nu X.X,\Gamma}\,(\nu)}{\vdash \Gamma}\,(\mathsf{Cut})$$

What we will present is a contribution to two directions in the field of circular proofs:

1. the relationship between finite and circular proofs (at the level of provability and at the level of proofs themselves) and

2. the certification of circular proofs, that is the production of fast and/or small pieces of evidence to support validity of a circular pre-proof.

Comparing the finite and infinite proofs is very natural. In informal words, it amounts to wondering what is the relative strength of inductive reasoning versus infinite descent: while infinite descent is a very old form of mathematical reasoning which appeared already in Euclid's *Elements* and was systematically investigated by Fermat, making precise its relationship with mathematical induction is still an open question for many proof formalisms, known as Brotherston–Simpson's conjecture. While it is fairly straightforward to check that infinite descent (circular proofs) prove at least as many statements as inductive reasoning, the converse is complex and remains largely open. Last year, Simpson [22] on the one hand and Berardi and Tatsuta [6, 7] on the other hand made progress on this question but only in the framework of Martin Löf's inductive definitions, not in the setting of μ-calculi circular proofs in which invariant extraction is highly complex and known only for some fragments.

We motivate our study 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 fig. 2 derives sequent $\vdash F, G, H, I, J$ where $F = \mu X.(X \parr G) \,\&\, (X \parr H)$, $G = \nu X.X \oplus \bot$, $H = \nu X.\bot \oplus X$, $I = \mu Z.((Z \parr J) \oplus \bot)$, $J = \mu X.(K \parr X) \oplus \bot$ and $K = \nu Y.\mu Z.((Z \parr \mu X.(Y \parr X) \oplus \bot) \oplus \bot)$.

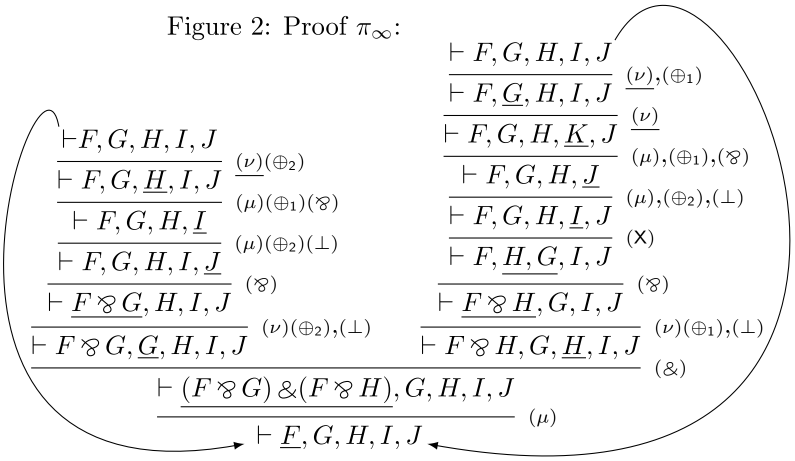
$\vdash F, G, H, I, J$
$\vdash F, \underline{G}, H, I, J$
$(\nu),(\oplus_1)$
(ν)
$\vdash F, G, H, \underline{K}, J$
$(\mu),(\oplus_1),(\parr)$
$\vdash F, G, H, \underline{J}$
$(\mu),(\oplus_2),(\bot)$
$\vdash F, G, H, \underline{I}, J$
(X)
$\vdash F, \underline{H, G}, I, J$
$(\parr)$
$\vdash \underline{F \parr H}, G, I, J$
$(\nu)(\oplus_1),(\bot)$
$\vdash F \parr H, G, \underline{H}, I, J$
$\vdash F, G, H, I, J$
$(\nu)(\oplus_2)$
$\vdash F, G, \underline{H}, I, J$
$(\mu)(\oplus_1)(\parr)$
$\vdash F, G, H, \underline{I}$
$(\mu)(\oplus_2)(\bot)$
$\vdash F, G, H, I, \underline{J}$
$(\parr)$
$\vdash \underline{F \parr G}, H, I, J$
$(\nu)(\oplus_2),(\bot)$
$\vdash F \parr G, \underline{G}, H, I, J$
$(\&)$
$\vdash \underline{(F \parr G) \,\&\, (F \parr H)}, G, H, I, J$
(μ)
$\vdash \underline{F}, G, H, I, J$

Figure 2: Proof π_∞:

This example of a circular derivation happens to be valid (it is a $\mu\mathsf{MALL}^\omega$ 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):
(i) if β *ultimately* follows always the left cycle ($A^\star \cdot l^\omega$), the unfolding of H validates β;
(ii) if β *ultimately* follows always the right cycle ($A^\star \cdot r^\omega$), the unfolding of G validates β;
(iii) if β *endlessly switches* between left and right cycles ($A^\star \cdot (r^+ \cdot l^+)^\omega$), K validates β.
The description of the thread validating this proof is thus complex and this is reflected in the difficulty to provide a local way to validate this proof and in the lack of general method to be

applied to finitize this into a $\mu\mathsf{MALL}$ proof: to our knowledge, the usual finitization methods (working only for fragments of $\mu\mathsf{MALL}$ circular proofs) do not apply here.

Contributions of this work. After providing the necessary background of infinitary and circular proof theory of multiplicative additive linear logic with least and greatest fixed points (respectively $\mu\mathsf{MALL}^{\infty}$ and $\mu\mathsf{MALL}^{\omega}$), we will introduce an approach to validity of circular proofs based on labellings of greatest fixed points, whose validity is expressed by local conditions, in contrast to the global nature of thread conditions. We will present a family of labelling systems for finite representation of circular proofs and investigate 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 fixed-points proof-theory, the best known bound for this problem being PSPACE. Our labellings rely essentially on the three following rules:

$$\frac{\vdash \Gamma[\nu^{a-}X.A]}{\vdash \Gamma[\nu X.A]}\,(\mathsf{Rec}) \qquad\qquad \frac{\vdash A[\nu^{a+}X.A],\Delta}{\vdash \nu^{a-}X.A,\Delta}\,(\nu) \qquad\qquad \frac{}{\vdash \Gamma[\nu^{a+}X.A]}\,(\circlearrowright)$$

where a back-edge in the representation must go from the conclusion of a $(\circlearrowright)$ to the premisse of a (Rec).

Next we turn to alternative characterizations of those circular proofs which can be labelled so as to provide elements concerning decidability and algorithmic construction of a labelling for a given circular representation.

Then we provide 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 into a finitary proof system with (co)induction rules *à la* Park. We provide a full finitization method in a fairly restricted labelling system which contains at least all the translations of $\mu\mathsf{MALL}$ proofs and we show how these ideas allow to translate the proof π_{∞} into a finitary proof with roughly the same structure.

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

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 be found in fixed-points approximations methods (see [14] for instance). The closest work in this direction is Stirling's annotated proofs [23] and the application Afshari and Leigh [1] made of such proofs in obtaining completeness for the modal μ-calculus. Our labelling system works quite differently since only fixed-points quantifiers are labelled while, in Stirling's annotated proofs, every formula is labelled and labels are transmitted to immediate subformulas with a label extension on greatest fixed-points.

Even though our labelling system has a very different label management from that of Stirling, one shall investigate further their relationships (in particular the role of the annotation restriction rule of Stirling's system, Definition 4 of [23]).

A less immediately connected topic is the connection between size change termination [20] and thread validity in μ-calculi: connections between those fields are not yet well understood despite early investigations from Dax et al.[14] for instance. More than a connection, this looks like an interplay: size-change termination is originally shown decidable by using Büchi automata and size-change graphs can be used to show validity of circular proofs [14]. There seems to be connections with our labelling system too.

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

Finitization of circular proofs has been recently a very active topics with many research effort on solving the so-called Brotherston-Simpson's conjecture. The following recent contributions were made in the setting of Martin-Löf's inductive definitions: firstly, Berardi and Tatsuta proved [6] that, in general, the equivalence is false by providing a counter-example inspired by the *Hydra* paradox. Secondly, Simpson [22] on the one hand and Berardi and Tatsuta [7] on the other hand provided a positive answer in the restricted frameworks when the proof system contains arithmetics. While Simpson's used tools from reverse mathematics and internalized circular proofs in a fragment of second-order arithmetics, ACA_0, with comprehension axiom on arithmetical statements, Tatsuta and Berardi proved an equivalent result by a direct proof translation relying on an arithmetical version of Ramsey theorem and Podelsky-Rybalchenko theorem.

A very natural question for future work is of course to extend the still *ad hoc* finitization method presented in the last section to the whole fragment of relaxed labelled proofs.

Circular proof search triggered interest compared to proof system with explicit inductive invariants (lacking subformula property). This has actually been turned to practice by Brotherston and collaborators [9]. We wish to investigate the potential use of labellings in circular proof-search. Indeed, there are several different labellings for a given finite derivation with back-edges where the labels are weakened. When labelling a circular representation, there are different strategies in placing the labels, which have different properties with respect to the ability to form back-edges or to validate the proof that one may exploit in proof-search.

References

[1] Bahareh Afshari and Graham E. Leigh. Cut-free completeness for modal mu-calculus. In *32nd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–12, 2017.

[2] David Baelde. On the proof theory of regular fixed points. In Martin Giese and Arild Waaler, editors, *Automated Reasoning with Analytic Tableaux and Related Methods, 18th International Conference, TABLEAUX 2009, Oslo, Norway, July 6-10, 2009. Proceedings*, volume 5607 of *Lecture Notes in Computer Science*, pages 93–107. Springer, 2009.

[3] David Baelde. Least and greatest fixed points in linear logic. *ACM Transactions on Computational Logic (TOCL)*, 13(1):2, 2012.

[4] David Baelde, Amina Doumane, and Alexis Saurin. Infinitary proof theory: the multiplicative additive case. In Jean-Marc Talbot and Laurent Regnier, editors, *25th EACSL Annual Conference on Computer Science Logic, CSL 2016, August 29 - September 1, 2016, Marseille, France*, volume 62 of *LIPIcs*, pages 42:1–42:17. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016.

[5] David Baelde and Dale Miller. Least and greatest fixed points in linear logic. In Nachum Dershowitz and Andrei Voronkov, editors, *Logic for Programming, Artificial Intelligence, and Reasoning, 14th International Conference, LPAR 2007, Yerevan, Armenia, October 15-19, 2007, Proceedings*, volume 4790 of *Lecture Notes in Computer Science*, pages 92–106. Springer, 2007.

[6] Stefano Berardi and Makoto Tatsuta. Classical system of martin-löf's inductive definitions is not equivalent to cyclic proof system. In Javier Esparza and Andrzej S. Murawski, editors, *Foundations of Software Science and Computation Structures - 20th International Conference, FOSSACS 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, April 22-29, 2017, Proceedings*, volume 10203 of *Lecture Notes in Computer Science*, pages 301–317, 2017.

[7] Stefano Berardi and Makoto Tatsuta. Equivalence of inductive definitions and cyclic proofs under arithmetic. In *32nd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2017, Reykjavik, Iceland, June 20-23, 2017*, pages 1–12. IEEE Computer Society, 2017.

[8] James Brotherston. *Sequent Calculus Proof Systems for Inductive Definitions.* PhD thesis, University of Edinburgh, November 2006.

[9] James Brotherston, Nikos Gorogiannis, and Rasmus Lerchedahl Petersen. A generic cyclic theorem prover. In *Programming Languages and Systems - 10th Asian Symposium, APLAS 2012, Kyoto, Japan, December 11-13, 2012. Proceedings*, volume 7705 of *Lecture Notes in Computer Science*, pages 350–367. Springer, 2012.

[10] James Brotherston and Alex Simpson. Complete sequent calculi for induction and infinite descent. In *22nd IEEE Symposium on Logic in Computer Science (LICS 2007), 10-12 July 2007, Wroclaw, Poland, Proceedings*, pages 51–62. IEEE Computer Society, 2007.

[11] James Brotherston and Alex Simpson. Sequent calculi for induction and infinite descent. *J. Log. Comput.*, 21(6):1177–1216, 2011.

[12] Pierre Clairambault. Least and greatest fixpoints in game semantics. In *FOSSACS*, volume 5504 of *Lecture Notes in Computer Science*, pages 16–31. Springer, 2009.

[13] Christian Dax, Martin Hofmann, and Martin Lange. A proof system for the linear time μ-calculus. In S. Arun-Kumar and Naveen Garg, editors, *FSTTCS 2006: Foundations of Software Technology and Theoretical Computer Science, 26th International Conference, Kolkata, India, December 13-15, 2006, Proceedings*, volume 4337 of *Lecture Notes in Computer Science*, pages 273–284. Springer, 2006.

[14] Christian Dax, Martin Hofmann, and Martin Lange. A proof system for the linear time μ-calculus. In S. Arun-Kumar and Naveen Garg, editors, *FSTTCS 2006: Foundations of Software Technology and Theoretical Computer Science, 26th International Conference, Kolkata, India, December 13-15, 2006, Proceedings*, volume 4337 of *Lecture Notes in Computer Science*, pages 273–284. Springer, 2006.

[15] Amina Doumane. *On the infinitary proof theory of logics with fixed points. (Théorie de la démonstration infinitaire pour les logiques à points fixes).* PhD thesis, Paris Diderot University, France, 2017.

[16] Amina Doumane, David Baelde, Lucca Hirschi, and Alexis Saurin. Towards Completeness via Proof Search in the Linear Time mu-Calculus. Accepted for publication at LICS, January 2016.

[17] Jérôme Fortier and Luigi Santocanale. Cuts for circular proofs: semantics and cut-elimination. In Simona Ronchi Della Rocca, editor, *Computer Science Logic 2013 (CSL 2013), CSL 2013, September 2-5, 2013, Torino, Italy*, volume 23 of *LIPIcs*, pages 248–262. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2013.

[18] Roope Kaivola. A simple decision method for the linear time mu-calculus. In Jörg Desel, editor,

Structures in Concurrency Theory, Workshops in Computing, pages 190–204. Springer London, 1995.

[19] Dexter Kozen. Results on the propositional mu-calculus. *Theor. Comput. Sci.*, 27:333–354, 1983.

[20] 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.

[21] Luigi Santocanale. A calculus of circular proofs and its categorical semantics. In Mogens Nielsen and Uffe Engberg, editors, *Foundations of Software Science and Computation Structures*, volume 2303 of *Lecture Notes in Computer Science*, pages 357–371. Springer, 2002.

[22] Alex Simpson. Cyclic arithmetic is equivalent to peano arithmetic. In Javier Esparza and Andrzej S. Murawski, editors, *Foundations of Software Science and Computation Structures - 20th International Conference, FOSSACS 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, April 22-29, 2017, Proceedings*, volume 10203 of *Lecture Notes in Computer Science*, pages 283–300, 2017.

[23] Colin Stirling. A tableau proof system with names for modal mu-calculus. In *HOWARD-60: A Festschrift on the Occasion of Howard Barringer's 60th Birthday*, volume 42 of *EPiC Series in Computing*, pages 306–318. EasyChair, 2014.

[24] Igor Walukiewicz. On completeness of the mu-calculus. In *LICS*, pages 136–146. IEEE Computer Society, 1993.

[25] Igor Walukiewicz. Completeness of Kozen's axiomatisation of the propositional mu-calculus. In *Proceedings, 10th Annual IEEE Symposium on Logic in Computer Science, San Diego, California, USA, June 26-29, 1995*, pages 14–24. IEEE Computer Society, 1995.