Making infinitary annotated proofs concise

Jan Rooduijn
ILLC, University of Amsterdam

The Proof Society Workshop
2 December 2021

Non-wellfounded proof theory for modal fixed point logics

Main idea: replace an *explicit induction rule* by allowing infinite branches (satisfying some condition).

$$
\dfrac{
  \text{iw}_L\,\dfrac{\text{id}\,\dfrac{}{p \Rightarrow p}}{p, \boxast(p \to \Box p) \Rightarrow p}
  \qquad
  \dfrac{
    \dfrac{
      \text{iw}_L\,\dfrac{\Box\,\dfrac{\dfrac{\vdots}{p, \boxast(p \to \Box p) \Rightarrow \boxast p}}{\Box p, \Box\boxast(p \to \Box p) \Rightarrow \Box\boxast p}}{p, \Box p, \Box\boxast(p \to \Box p) \Rightarrow \Box\boxast p}
      \qquad
      \dfrac{\dfrac{\dfrac{}{p \Rightarrow p}\,\text{id}}{p \Rightarrow p, \Box\boxast p}\,\text{iw}_R}{p, \Box\boxast(p \to \Box p) \Rightarrow p, \Box\boxast p}\,\text{iw}_L
    }{p, p \to \Box p, \Box\boxast(p \to \Box p) \Rightarrow \Box\boxast p}\,\to_L
  }{p, \boxast(p \to \Box p) \Rightarrow \Box\boxast p}\,\boxast_L
}{p, \boxast(p \to \Box p) \Rightarrow \boxast p}\,\boxast_R
$$

An infinite branch β is said to be *good* if it contains a good trace τ.

Connections to automata theory

Let Σ_0 be the alphabet whose characters are *rule applications* in π, *e.g*

$$\circledast_R \frac{}{p, \circledast(p \to \Box p) \Rightarrow \circledast p} \in \Sigma_0$$

The language containing precisely the good infinite branches of π is an ω-regular tree language over Σ_0.

Connections to automata theory

Let Σ_0 be the alphabet whose characters are *rule applications* in π, *e.g*

$$\boxast_R \; \frac{}{p, \boxast(p \to \Box p) \Rightarrow \boxast p} \; \in \Sigma_0$$

The language containing precisely the good infinite branches of π is an ω-regular tree language over Σ_0.

Let Σ_1 be the ranked alphabet whose characters are rule applications in any proof of some fixed sequent s. The set of proofs of s is a regular infinite tree language over the alphabet Σ_1.

Connections to automata theory

Let Σ_0 be the alphabet whose characters are *rule applications* in π, *e.g*

$$\circledast_R \frac{}{p, \circledast(p \to \Box p) \Rightarrow \circledast p} \in \Sigma_0$$

The language containing precisely the good infinite branches of π is an ω-regular tree language over Σ_0.

Let Σ_1 be the ranked alphabet whose characters are rule applications in any proof of some fixed sequent s. The set of proofs of s is a regular infinite tree language over the alphabet Σ_1.

Theorem (Rabin, 1969)

1. *The emptiness problem for regular tree languages is decidable.*
2. *Every regular tree language contains a regular tree.*

Corollary

1. *The provability of s is decidable.*
2. *If s has a proof, then it has a cyclic proof.*

Cyclic annotated proof systems

Main idea: encode the automata-theoretic trace management into the proofs.

$$
\dfrac{
\dfrac{\dfrac{}{p \Rightarrow p}\ \mathrm{id}}{p, \boxast(p \to \Box p) \Rightarrow p}\ \mathrm{iw}_L
\qquad
\dfrac{
\dfrac{
\dfrac{\dfrac{\color{red}{p, \boxast(p \to \Box p) \Rightarrow [\boxast p]}}{\Box p, \Box\boxast(p \to \Box p) \Rightarrow [\Box\boxast p]}\ \Box}{p, \Box p, \Box\boxast(p \to \Box p) \Rightarrow [\Box\boxast p]}\ \mathrm{iw}_L
\qquad
\dfrac{\dfrac{\dfrac{}{p \Rightarrow p}\ \mathrm{id}}{p \Rightarrow p, \Box\boxast p}\ \mathrm{iw}_R}{p, \Box\boxast(p \to \Box p) \Rightarrow p, \Box\boxast p}\ \mathrm{iw}_L
}{p, p \to \Box p, \Box\boxast(p \to \Box p) \Rightarrow [\Box\boxast p]}\ \to_L
}{p, \boxast(p \to \Box p) \Rightarrow [\Box\boxast p]}\ \boxast_L
}{\color{red}{p, \boxast(p \to \Box p) \Rightarrow [\boxast p]}}\ \boxast_R
$$

Important features of annotated proof systems:

- It suffices to check a condition between each companion and its leaf.
- Removing the annotations yields an ordinary cyclic proof.
- Every provable sequent has a concise proof.
- . . .?

Concise proofs

Definition

An annotated proof is said to be concise if the first repeat on any branch is good.

Completeness via proof-search often directly yields concise proofs:

- Jungteerapanich (2010)
- Stirling (2014)

Game-theoretic methods do not:

- Enqvist (2020)
- Marti & Venema (2021)

and neither does the method of canonical models:

- JR (2021)

We prove, in an abstract setting capturing each of the above, that every infinitary annotated proof can be made concise.

Infinitary annotated proof systems

$$
\dfrac{
\text{iw}_L\,\dfrac{\text{id}\,\dfrac{}{p \Rightarrow p}}{p, \boxast(p \to \Box p) \Rightarrow p}
\qquad
\dfrac{
\dfrac{
\text{iw}_L\,\dfrac{\Box\,\dfrac{\dfrac{\vdots}{p, \boxast(p \to \Box p) \Rightarrow [\boxast p]}}{\Box p, \Box\boxast(p \to \Box p) \Rightarrow [\Box\boxast p]}}{p, \Box p, \Box\boxast(p \to \Box p) \Rightarrow [\Box\boxast p]}
\qquad
\dfrac{\dfrac{\dfrac{}{p \Rightarrow p}\,\text{id}}{p \Rightarrow p, \Box\boxast p}\,\text{iw}_R}{p, \Box\boxast(p \to \Box p) \Rightarrow p, \Box\boxast p}\,\text{iw}_L
}{p, p \to \Box p, \Box\boxast(p \to \Box p) \Rightarrow [\Box\boxast p]}\,\to_L
}{p, \boxast(p \to \Box p) \Rightarrow [\Box\boxast p]}\,\boxast_L
}{p, \boxast(p \to \Box p) \Rightarrow [\boxast p]}\,\boxast_R
$$

Abstract definition of an infinitary annotated proof system

More precisely, we say that an *infinitary annotated proof system* P for some ranked alphabet Σ consists of:

1. An equivalence relation $\equiv$ on Σ.
2. A relation $R \subseteq \Sigma \times \Sigma^*$ such that:
    2.1 If aRw, then $\mathrm{length}(w) = \mathrm{ar}(a)$.
    2.2 If aRw and w is componentwise $\equiv$-equivalent to w', then aRw'.
3. A subset G of Σ consisting of *good words* such that:
$$\text{if } w_1 \cdot w_2 \cdot w_3 \in G \text{ and } w_2 \notin G, \text{ then } w_1 \cdot w_3 \in G.$$
4. A subset I of Σ^∞ consisting of *good infinite words* such that:
$$\text{if } w_0 \cdot w_1 \cdot w_2 \cdots \in I, \text{ then } w_n \in G \text{ for some } n \geq 0.$$

Theorem

Let P *be an infinitary annotated proof system and let T be a* P*-proof such that the set $\{l_T(u) : u \in T\}/\equiv$ is finite. Then there is a concise* P*-proof T' with an $\equiv$-equivalent root label.*

Further questions

- How should the abstract definition be restricted to ensure that the unravelling of a cyclic annotated proof is an infinitary annotated proof?
- Given a set of good words, is there a canonical definition for the set of good infinite words? (I think yes)
- How does the size of cyclic proofs obtained in this way compare to those given by automata-theoretic methods?
- Can we also get uniform proofs?

Thank you!