an infinitary proof theory of linear logic ensuring fair termination in the linear π-calculus

Luca Ciccone, University of Torino

Luca Padovani, University of Camerino

33rd International Conference on Concurrency Theory – CONCUR 2022 – Warsaw

background: linear logic and session types

Luís Caires and Frank Pfenning, ***Session types as intuitionistic linear propositions****, CONCUR 2010*
…,Wadler [2014], Lindley and Morris [2016], …

Linear Logic		Sessions
$\mathbf{1}$	$\bot$	send/receive unit and terminate
$A \otimes B$	$A \invamp B$	send/receive payload A and continue as B
$A \oplus B$	$A \mathbin{\&} B$	send/receive choice and continue as A or B
cut reduction		communication
cut elimination		deadlock freedom, termination

Great ✔

- interactions terminate in a bounded number of steps

background: linear logic and session types

*Luís Caires and Frank Pfenning, **Session types as intuitionistic linear propositions**, CONCUR 2010*
...,Wadler [2014], Lindley and Morris [2016], ...

Linear Logic		**Sessions**
$\mathbf{1}$	$\bot$	send/receive unit and terminate
$A \otimes B$	$A \parr B$	send/receive payload A and continue as B
$A \oplus B$	$A \,\&\, B$	send/receive choice and continue as A or B
cut reduction		communication
cut elimination		deadlock freedom, termination

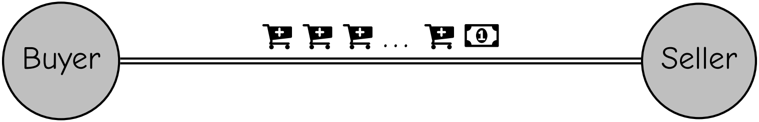
Great ✔

- interactions terminate in a bounded number of steps

Not so great ✖

- interactions terminate in a bounded number of steps

motivation



Buyer adds *n* (**fixed**) items into shopping cart and pays

- all interactions are **finite**
- well typed ✔

Buyer adds **arbitrarily many** items into shopping cart and pays

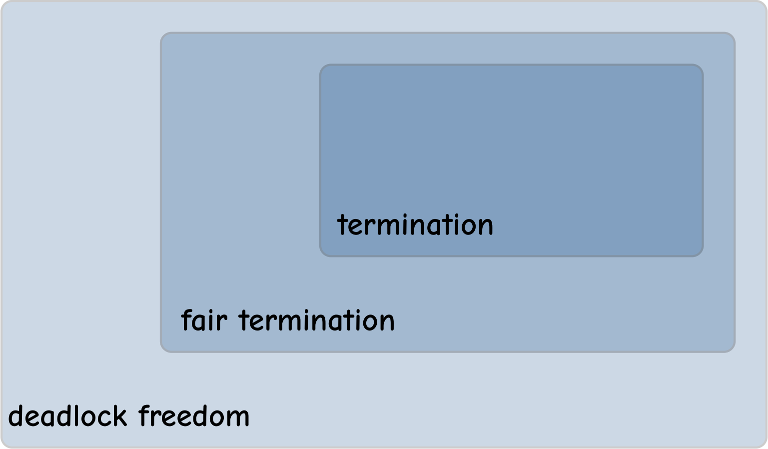
- there is an **infinite interaction** in which buyer keeps adding items into the shopping cart and never pays
- cannot be modeled or is ill typed ✖

Observation

- the infinite interaction is “unreasonable” or “unfair”

contribution

- "session" type system rooted in **linear logic**
- well-typed processes **fairly terminate**



core elements

Processes = linear π-calculus [Kobayashi et al., 1999]

- sessions are **encodable** [Kobayashi, 2002, Dardha et al., 2017]

Types = MALL with least and greatest **fixed points**

$$A, B ::= \bot \mid \top \mid \mathbf{1} \mid \mathbf{0} \mid A \oplus B \mid A \mathbin{\&} B \mid A \otimes B \mid A \parr B \mid \mu X.A \mid \nu X.A$$

- $A \otimes B$ and $A \parr B$ describe output/input of **pairs** instead of sequentiality

Proof system = $\mu\mathrm{MALL}^\infty$ [Baelde et al., 2016, Doumane, 2017]

- **infinitary proof system** for MALL with fixed points
- standard rule for **non-deterministic choices**

buyer-seller in the (sugared) linear π-calculus

$$\begin{array}{rcl} \mathit{Buyer}(x) & = & \mathsf{rec}\,\overline{x}.(\mathsf{add}\,\overline{x}.\mathit{Buyer}\langle x\rangle \oplus \mathsf{pay}\,\overline{x}.\overline{x}()) \\ \mathit{Seller}(x,y) & = & \mathsf{corec}\,x.\mathsf{case}\,x\{\mathit{Seller}\langle x,y\rangle, x().\overline{y}()\} \end{array}$$

$$(x)(\mathit{Buyer}\langle x\rangle \parallel \mathit{Seller}\langle x,y\rangle)$$

Notes

- we use add and pay as labels for “left” and “right” choices
- we keep using the same name x instead of creating new continuations (just syntactic sugar, channels are **linear**)
- processes are infinite (just like proof derivations in $\mu\mathsf{MALL}^\infty$)

notions of termination

Definition (run)

A **run** of P is a *maximal* reduction sequence $P \to P_1 \to P_2 \to \cdots$

- P is **terminating** if all of its runs are finite
- P is **weakly terminating** if it has a finite run
- P is **fairly terminating** if all of its **fair** runs are finite

Definition (fair run)

A run is **fair** iff contains finitely many weakly terminating processes

- any finite run is fair
- any unfair run is infinite
- any unfair run goes through weakly terminating processes

notions of termination

Definition (run)

A **run** of P is a *maximal* reduction sequence $P \to P_1 \to P_2 \to \cdots$

- P is **terminating** if all of its runs are finite
- P is **weakly terminating** if it has a finite run
- P is **fairly terminating** if all of its **fair** runs are finite

Definition (fair run)

A run is **fair** iff contains finitely many weakly terminating processes

- any finite run is fair
- any unfair run is infinite
- any unfair run goes through weakly terminating processes

about this fairness assumption

Properties

- particular instance of **fair reachability of predicates** by Queille and Sifakis [1983]
- induces the **largest family** of fairly terminating processes

Theorem (proof method for fair termination)

P fairly terminating $\iff$ $\forall P \Rightarrow Q$ implies Q weakly terminating

Corollary

If a type system ensures weak termination, then it also ensures fair termination (under this fairness assumption)

about this fairness assumption

Properties

- particular instance of **fair reachability of predicates** by Queille and Sifakis [1983]
- induces the **largest family** of fairly terminating processes

Theorem (proof method for fair termination)

P fairly terminating $\iff$ $\forall P \Rightarrow Q$ implies Q weakly terminating

Corollary

If a type system ensures weak termination, then it also ensures fair termination (under this fairness assumption)

example: shopping

$$
\begin{aligned}
Buyer(x) &= \mathsf{rec}\,\overline{x}.(\mathsf{add}\,\overline{x}.Buyer\langle x\rangle \oplus \mathsf{pay}\,\overline{x}.\overline{x}()) \\
Seller(x,y) &= \mathsf{corec}\,x.\mathsf{case}\,x\{Seller\langle x,y\rangle, x().\overline{y}()\}
\end{aligned}
$$

$$(x)(Buyer\langle x\rangle \parallel Seller\langle x,y\rangle)$$

- there is one infinite run in which *Buyer* keeps adding items into the shopping cart
- this run is **unfair**, because *Buyer* may always pay and finish
- we want this system to be **well typed**

example: compulsive shopping

$$\begin{aligned} \mathit{CompulsiveBuyer}(x) &= \mathsf{rec}\,\overline{x}.\mathsf{add}\,\overline{x}.\mathit{CompulsiveBuyer}\langle x\rangle \\ \mathit{Seller}(x,y) &= \mathsf{corec}\,x.\mathsf{case}\,x\{\mathit{Seller}\langle x,y\rangle, x().\overline{y}()\} \end{aligned}$$

$$(x)(\mathit{CompulsiveBuyer}\langle x\rangle \parallel \mathit{Seller}\langle x,y\rangle)$$

- there is (only) one infinite run in which *CompulsiveBuyer* keeps adding items into the shopping cart
- this run is **fair**, because *CompulsiveBuyer* will never pay
- we want this system to be **ill typed**

typing rules = μMALL$^\infty$ + [choice]

Judgments

$$P \vdash \Gamma$$

1-1 correspondence with μMALL$^\infty$ proof rules

$$\frac{P \vdash \Gamma, y : A \qquad Q \vdash \Delta, z : B}{\overline{x}(y,z)(P \parallel Q) \vdash \Gamma, \Delta, x : A \otimes B}\,[\otimes] \qquad \frac{P \vdash \Gamma, y : A\{\nu X.A/X\}}{\mathsf{corec}\,x(y).P \vdash \Gamma, x : \nu X.A}\,[\nu]$$

Non-deterministic choice

$$\frac{P \vdash \Gamma \qquad Q \vdash \Gamma}{P \oplus Q \vdash \Gamma}\,[\text{choice}]$$

example: typing of buyer

Buyer | **Buyer protocol**

$$Buyer(x) = \mathsf{rec}\,\overline{x}.(\mathsf{add}\,\overline{x}.Buyer\langle x\rangle \oplus \mathsf{pay}\,\overline{x}.\overline{x}()) \qquad B \stackrel{\text{def}}{=} \mu X.X \oplus \mathbf{1}$$

$$\cfrac{\cfrac{\cfrac{\cfrac{\vdots}{Buyer\langle x\rangle \vdash x : B}}{\mathsf{add}\,\overline{x}.Buyer\langle x\rangle \vdash x : B \oplus \mathbf{1}}\,[\oplus] \qquad \cfrac{\cfrac{}{\overline{x}() \vdash x : \mathbf{1}}\,[\mathbf{1}]}{\mathsf{pay}\,\overline{x}.\overline{x}() \vdash x : B \oplus \mathbf{1}}\,[\oplus]}{\mathsf{add}\,\overline{x}.Buyer\langle x\rangle \oplus \mathsf{pay}\,\overline{x}.\overline{x}() \vdash x : B \oplus \mathbf{1}}\,[\text{choice}]}{Buyer\langle x\rangle \vdash x : B}\,[\mu]$$

example: typing of seller

Seller

$$Seller(x,y) = \mathsf{corec}\, x.\mathsf{case}\, x\{Seller\langle x,y\rangle, x().\overline{y}()\}$$

Seller protocol

$$S \stackrel{\text{def}}{=} \nu X.X \mathbin{\&} \bot$$

$$\dfrac{\dfrac{\vdots}{Seller\langle x,y\rangle \vdash x : S, y : \mathbf{1}} \qquad \dfrac{\dfrac{}{\overline{y}() \vdash y : \mathbf{1}}\,[\mathbf{1}]}{x().\overline{y}() \vdash x : \bot, y : \mathbf{1}}\,[\bot]}{\dfrac{\mathsf{case}\, x\{Seller\langle x,y\rangle, x().\overline{y}()\} \vdash x : S \mathbin{\&} \bot, y : \mathbf{1}}{Seller\langle x,y\rangle \vdash x : S, y : \mathbf{1}}\,[\nu]}\,[\&]$$

- y is used after an arbitrarily long interaction
- y is used only if the interaction eventually terminates

some typing derivations are invalid

$$
\dfrac{\dfrac{\dfrac{\vdots}{\mathit{CompulsiveBuyer}\langle x\rangle \vdash x : B}}{\mathsf{add}\,\overline{x}.\mathit{CompulsiveBuyer}\langle x\rangle \vdash x : B \oplus \mathbf{1}}\,[\oplus]}{\mathit{CompulsiveBuyer}\langle x\rangle \vdash x : B}\,[\mu]
$$

Caution

- there is a typing derivation for *CompulsiveBuyer*
- combining *CompulsiveBuyer* with *Seller* results in a **non-terminating** interaction
- a known issue of infinitary proof systems like μMALL$^{\infty}$ is that some (infinite) typing derivations compromise **cut elimination**

the validity condition in μMALL$^\infty$ [Baelde et al., 2016]

Definition (valid branch)

An infinite branch in a typing derivation is **valid** if there is a **greatest fixed point** that is unfolded **infinitely many times**

- the precise definition of valid branch is quite technical, see Baelde et al. [2016], Doumane [2017] and the paper

Definition (valid derivation)

A typing derivation is **valid** if so is every infinite branch in it

Intuition

- every greatest fixed point is **matched** by a least fixed point
- in a valid derivation there is (at least) one least fixed point that is unfolded **finitely many times**
- this finite unfolding **dominates** the duration of the interaction

which shopping is allowed?

Seller is **valid** ✔

$$\dfrac{\dfrac{\dfrac{\vdots}{\mathit{Seller}\langle x, y\rangle \vdash x : S, y : \mathbf{1}} \qquad \dfrac{\dfrac{}{\overline{y}() \vdash y : \mathbf{1}}\,[\mathbf{1}]}{x().\overline{y}() \vdash x : \bot, y : \mathbf{1}}\,[\bot]}{\mathsf{case}\; x\{\mathit{Seller}\langle x, y\rangle, x().\overline{y}()\} \vdash x : S \,\&\, \bot, y : \mathbf{1}}\,[\&]}{\mathit{Seller}\langle x, y\rangle \vdash x : S, y : \mathbf{1}}\,[\nu]$$

CompulsiveBuyer is **invalid** ✔

$$\dfrac{\dfrac{\dfrac{\vdots}{\mathit{CompulsiveBuyer}\langle x\rangle \vdash x : B}}{\mathsf{add}\,\overline{x}.\mathit{CompulsiveBuyer}\langle x\rangle \vdash x : B \oplus \mathbf{1}}\,[\oplus]}{\mathit{CompulsiveBuyer}\langle x\rangle \vdash x : B}\,[\mu]$$

Buyer is **invalid** ✖

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\mathit{Buyer}\langle x\rangle \vdash x : B}}{\mathsf{add}\,\overline{x}.\mathit{Buyer}\langle x\rangle \vdash x : B \oplus \mathbf{1}}\,[\oplus] \qquad \dfrac{\dfrac{}{\overline{x}() \vdash x : \mathbf{1}}\,[\mathbf{1}]}{\mathsf{pay}\,\overline{x}.\overline{x}() \vdash x : B \oplus \mathbf{1}}\,[\oplus]}{\mathsf{add}\,\overline{x}.\mathit{Buyer}\langle x\rangle \oplus \mathsf{pay}\,\overline{x}.\overline{x}() \vdash x : B \oplus \mathbf{1}}\,[\mathrm{choice}]}{\mathit{Buyer}\langle x\rangle \vdash x : B}\,[\mu]$$

towards a more permissive validity condition

Let's look again at the typing derivation for *Buyer*

$$
\dfrac{
  \dfrac{\dfrac{\vdots}{\mathit{Buyer}\langle x\rangle \vdash x : B}}{\mathsf{add}\,\overline{x}.\mathit{Buyer}\langle x\rangle \vdash x : B \oplus \mathbf{1}}\,[\oplus]
  \qquad
  \dfrac{\dfrac{}{\overline{x}() \vdash x : \mathbf{1}}\,[\mathbf{1}]}{\mathsf{pay}\,\overline{x}.\overline{x}() \vdash x : B \oplus \mathbf{1}}\,[\oplus]
}{
  \dfrac{\mathsf{add}\,\overline{x}.\mathit{Buyer}\langle x\rangle \oplus \mathsf{pay}\,\overline{x}.\overline{x}() \vdash x : B \oplus \mathbf{1}}{\mathit{Buyer}\langle x\rangle \vdash x : B}\,[\mu]
}\,[\text{choice}]
$$

- the infinite branch goes through infinitely many choices
- the infinite branch corresponds to an **unfair run**
- it should not be considered as far as validity is concerned

avoiding unfair branches

Definition (process rank)

The **rank** of a process is the least number of non-deterministic choices it can possibly make before it terminates

- rank $\approx$ how far away the process is from termination
- definition is conservative, some processes have rank ∞

Definition (fair branch)

A branch in a typing derivation is **fair** if it traverses **finitely many**, **finitely-ranked** choices

Definition (valid derivation, revisited)

A typing derivation is **valid** if so is every infinite **fair** branch in it

avoiding unfair branches

Definition (process rank)

The **rank** of a process is the least number of non-deterministic choices it can possibly make before it terminates

- rank $\approx$ how far away the process is from termination
- definition is conservative, some processes have rank ∞

Definition (fair branch)

A branch in a typing derivation is **fair** if it traverses **finitely many**, **finitely-ranked** choices

Definition (valid derivation, revisited)

A typing derivation is **valid** if so is every infinite **fair** branch in it

which shopping is allowed, now?

Seller is **valid** ✔
infinite branch fair & valid

$$\dfrac{\dfrac{\dfrac{\vdots}{\mathit{Seller}\langle x, y\rangle \vdash x : S, y : \mathbf{1}} \qquad \dfrac{\dfrac{}{\overline{y}() \vdash y : \mathbf{1}}\,[\mathbf{1}]}{x().\overline{y}() \vdash x : \bot, y : \mathbf{1}}\,[\bot]}{\mathsf{case}\; x\{\mathit{Seller}\langle x, y\rangle, x().\overline{y}()\} \vdash x : S \mathbin{\&} \bot, y : \mathbf{1}}\,[\&]}{\mathit{Seller}\langle x, y\rangle \vdash x : S, y : \mathbf{1}}\,[\nu]$$

CompulsiveBuyer is **invalid** ✔
infinite branch fair & invalid

$$\dfrac{\dfrac{\dfrac{\vdots}{\mathit{CompulsiveBuyer}\langle x\rangle \vdash x : B}}{\mathsf{add}\;\overline{x}.\mathit{CompulsiveBuyer}\langle x\rangle \vdash x : B \oplus \mathbf{1}}\,[\oplus]}{\mathit{CompulsiveBuyer}\langle x\rangle \vdash x : B}\,[\mu]$$

Buyer is **valid** ✔
rank 1 – the infinite branch is **unfair**

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\mathit{Buyer}\langle x\rangle \vdash x : B}}{\mathsf{add}\;\overline{x}.\mathit{Buyer}\langle x\rangle \vdash x : B \oplus \mathbf{1}}\,[\oplus] \qquad \dfrac{\dfrac{}{\overline{x}() \vdash x : \mathbf{1}}\,[\mathbf{1}]}{\mathsf{pay}\;\overline{x}.\overline{x}() \vdash x : B \oplus \mathbf{1}}\,[\oplus]}{\mathsf{add}\;\overline{x}.\mathit{Buyer}\langle x\rangle \oplus \mathsf{pay}\;\overline{x}.\overline{x}() \vdash x : B \oplus \mathbf{1}}\,[\mathrm{choice}]}{\mathit{Buyer}\langle x\rangle \vdash x : B}\,[\mu]$$

properties of well-typed processes

Theorem (subject reduction)

If $P \Vdash \Gamma$ *and* $P \rightarrow Q$ *then* $Q \Vdash \Gamma$

Theorem (weak termination)

If $P \Vdash x : \mathbf{1}$ *then* $P \Rightarrow \overline{x}()$

Proof.

From cut elimination of $\mu\mathsf{MALL}^{\infty}$ $\square$

Theorem (fair termination)

If $P \Vdash x : \mathbf{1}$ *then* P *is fairly terminating*

Proof.

From weak termination and proof principle of fair termination $\square$

concluding remarks

Summary

- minimal and **conservative extension** of μMALL$^\infty$
- well-typed processes **fairly terminate**
- fair termination entails **deadlock/lock/junk freedom**

In the (extended version of the) paper (online)

- omitted details and **proofs**
- more examples (**fork/join parallelism**, **context-free protocols**)
- **decidability algorithm** for proof validity with fair branches
- alternative calculus with **finite representation of processes**

references

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 für Informatik, 2016.

Luís Caires, Frank Pfenning, and Bernardo Toninho. Linear logic propositions as session types. *Math. Struct. Comput. Sci.*, 26(3): 367–423, 2016.

Ornela Dardha, Elena Giachino, and Davide Sangiorgi. Session types revisited. *Inf. Comput.*, 256:253–286, 2017.

references (cont.)

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. URL `https://tel.archives-ouvertes.fr/tel-01676953`.

Naoki Kobayashi. Type systems for concurrent programs. In *10th Anniversary Colloquium of UNU/IIST*, LNCS 2757, pages 439–453. Springer, 2002. Extended version at `http://www.kb.ecei.tohoku.ac.jp/~koba/papers/tutorial-type-extended.pdf`.

Naoki Kobayashi, Benjamin C. Pierce, and David N. Turner. Linearity and the pi-calculus. *ACM Trans. Program. Lang. Syst.*, 21(5):914–947, 1999.

references (cont.)

Sam Lindley and J. Garrett Morris. Talking bananas: structural recursion for session types. In Jacques Garrigue, Gabriele Keller, and Eijiro Sumii, editors, *Proceedings of the 21st ACM SIGPLAN International Conference on Functional Programming, ICFP 2016, Nara, Japan, September 18-22, 2016*, pages 434–447. ACM, 2016.

Zesen Qian, G. A. Kavvos, and Lars Birkedal. Client-server sessions in linear logic. *Proc. ACM Program. Lang.*, 5(ICFP):1–31, 2021.

Jean-Pierre Queille and Joseph Sifakis. Fairness and related properties in transition systems - A temporal logic to deal with fairness. *Acta Informatica*, 19:195–220, 1983.

Philip Wadler. Propositions as sessions. *J. Funct. Program.*, 24(2-3): 384–418, 2014.