probabilistic analysis of binary sessions

Omar Inverso, Gran Sasso Science Institute
Hernán Melgratti, Universidad de Buenos Aires
Luca Padovani, Università di Torino
Catia Trubiani, Gran Sasso Science Institute
Emilio Tuosto, Gran Sasso Science Institute

CONCUR, 1 Sep 2020

context

- session type = protocol with branching points

Accept & *Reject*

- well-typed process = protocol fidelity **along all paths**

This work

- different paths = different degrees of “success”

☺ *Accept* & *Reject* ☹

- probabilistic analysis of the session success

problem and contribution

Success probability of a session type: **easy**

$$Accept \;{}_p\& \; Reject$$

Success probability of a process: **not so easy**

- arbitrary composition of parallel, interacting processes
- dynamic network topology
- unbounded number of states
- **local choices can propagate globally** through sessions

Our contribution: bridging the gap between types and processes

$$x : Accept \;{}_p\& \; Reject \vdash P$$

processes

$P, Q ::=$	$\texttt{idle}$	inaction
$\mid$	$\texttt{done}\, x$	success
$\mid$	$x?(y).P$	message input
$\mid$	$x!y.P$	message output
$\mid$	$\texttt{case}\, x\, [P, Q]$	branch
$\mid$	$\texttt{inl}\, x.P$	left selection
$\mid$	$\texttt{inr}\, x.P$	right selection
$\mid$	$P \mid Q$	parallel composition
$\mid$	$(x)P$	session restriction
$\mid$	$P\ {}_{p}\boxplus\ Q$	probabilistic choice
$\mid$	$A\langle\overline{x}\rangle$	process invocation

processes

$$
\begin{array}{rlll}
P, Q ::= & \texttt{idle} & & \text{inaction} \\
| & \texttt{done}\, x & & \text{success} \\
| & x?(y).P & & \text{message input} \\
| & x!y.P & & \text{message output} \\
| & \texttt{case}\, x\, [P, Q] & & \text{branch} \\
| & \texttt{inl}\, x.P & & \text{left selection} \\
| & \texttt{inr}\, x.P & & \text{right selection} \\
| & P \mid Q & & \text{parallel composition} \\
| & (x)P & & \text{session restriction} \\
| & P \;{}_{p}\!\boxplus\; Q & & \text{probabilistic choice} \\
| & A\langle \overline{x} \rangle & & \text{process invocation}
\end{array}
$$

processes

$P, Q ::=$	`idle`	inaction
$\mid$	`done` x	success
$\mid$	$x?(y).P$	message input
$\mid$	$x!y.P$	message output
$\mid$	`case` $x\,[P, Q]$	branch
$\mid$	`inl` $x.P$	left selection
$\mid$	`inr` $x.P$	right selection
$\mid$	$P \mid Q$	parallel composition
$\mid$	$(x)P$	session restriction
$\mid$	$P \;{}_{p}\boxplus\; Q$	probabilistic choice
$\mid$	$A\langle \overline{x} \rangle$	process invocation

processes

$P, Q ::=$	$\texttt{idle}$	inaction
$\mid$	$\texttt{done}\ x$	success
$\mid$	$x?(y).P$	message input
$\mid$	$x!y.P$	message output
$\mid$	$\texttt{case}\ x\ [P, Q]$	branch
$\mid$	$\texttt{inl}\ x.P$	left selection
$\mid$	$\texttt{inr}\ x.P$	right selection
$\mid$	$P \mid Q$	parallel composition
$\mid$	$(x)P$	session restriction
$\mid$	$P\ {}_{p}\boxplus\ Q$	probabilistic choice
$\mid$	$A\langle\overline{x}\rangle$	process invocation

example of probabilistic choice propagation

$$(\texttt{inl}\,x\;{}_p\boxplus\;\texttt{inr}\,x) \mid \texttt{case}\,x\,[\texttt{inr}\,y.\texttt{done}\,y,\;\texttt{inl}\,y]$$

example of probabilistic choice propagation

$$(\texttt{inl}\,x \;{}_p\!\boxplus\; \texttt{inr}\,x) \mid \texttt{case}\,x\,[\texttt{inr}\,y.\texttt{done}\,y, \texttt{inl}\,y]$$

$$\preccurlyeq$$

$$(\texttt{inl}\,x \mid \texttt{case}\,x\,[\texttt{inr}\,y.\texttt{done}\,y, \texttt{inl}\,y]) \;{}_p\!\boxplus\; (\texttt{inr}\,x \mid \texttt{case}\,x\,[\dots, \dots])$$

example of probabilistic choice propagation

$$(\mathtt{inl}\,x \;{}_{p}\boxplus\; \mathtt{inr}\,x) \mid \mathtt{case}\,x\,[\mathtt{inr}\,y.\mathtt{done}\,y, \mathtt{inl}\,y]$$

$$\preccurlyeq$$

$$(\mathtt{inl}\,x \mid \mathtt{case}\,x\,[\mathtt{inr}\,y.\mathtt{done}\,y, \mathtt{inl}\,y]) \;{}_{p}\boxplus\; (\mathtt{inr}\,x \mid \mathtt{case}\,x\,[\dots, \dots])$$

$$\rightarrow$$

$$\mathtt{inr}\,y.\mathtt{done}\,y \;{}_{p}\boxplus\; (\mathtt{inr}\,x \mid \mathtt{case}\,x\,[\mathtt{inr}\,y.\mathtt{done}\,y, \mathtt{inl}\,y])$$

example of probabilistic choice propagation

$$(\texttt{inl}\,x \;{}_{p}\!\boxplus\; \texttt{inr}\,x) \mid \texttt{case}\,x\,[\texttt{inr}\,y.\texttt{done}\,y, \texttt{inl}\,y]$$

$$\preccurlyeq$$

$$(\texttt{inl}\,x \mid \texttt{case}\,x\,[\texttt{inr}\,y.\texttt{done}\,y, \texttt{inl}\,y]) \;{}_{p}\!\boxplus\; (\texttt{inr}\,x \mid \texttt{case}\,x\,[\dots, \dots])$$

$$\rightarrow$$

$$\texttt{inr}\,y.\texttt{done}\,y \;{}_{p}\!\boxplus\; (\texttt{inr}\,x \mid \texttt{case}\,x\,[\texttt{inr}\,y.\texttt{done}\,y, \texttt{inl}\,y])$$

$$\preccurlyeq$$

$$(\texttt{inr}\,x \mid \texttt{case}\,x\,[\texttt{inr}\,y.\texttt{done}\,y, \texttt{inl}\,y]) \;{}_{1-p}\!\boxplus\; \texttt{inr}\,y.\texttt{done}\,y$$

example of probabilistic choice propagation

$$(\mathtt{inl}\,x \;{}_{p}\!\boxplus\; \mathtt{inr}\,x) \mid \mathtt{case}\,x\,[\mathtt{inr}\,y.\mathtt{done}\,y, \mathtt{inl}\,y]$$

$$\preccurlyeq$$

$$(\mathtt{inl}\,x \mid \mathtt{case}\,x\,[\mathtt{inr}\,y.\mathtt{done}\,y, \mathtt{inl}\,y]) \;{}_{p}\!\boxplus\; (\mathtt{inr}\,x \mid \mathtt{case}\,x\,[\dots, \dots])$$

$$\rightarrow$$

$$\mathtt{inr}\,y.\mathtt{done}\,y \;{}_{p}\!\boxplus\; (\mathtt{inr}\,x \mid \mathtt{case}\,x\,[\mathtt{inr}\,y.\mathtt{done}\,y, \mathtt{inl}\,y])$$

$$\preccurlyeq$$

$$(\mathtt{inr}\,x \mid \mathtt{case}\,x\,[\mathtt{inr}\,y.\mathtt{done}\,y, \mathtt{inl}\,y]) \;{}_{1-p}\!\boxplus\; \mathtt{inr}\,y.\mathtt{done}\,y$$

$$\rightarrow$$

$$\mathtt{inl}\,y \;{}_{1-p}\!\boxplus\; \mathtt{inr}\,y.\mathtt{done}\,y$$

probabilistic session types

$$
\begin{array}{rcll}
T, S & ::= & \circ & \text{termination} \\
& | & \bullet & \text{success} \\
& | & ?t.T & \text{input} \\
& | & !t.T & \text{output} \\
& | & T\ {}_p\& \ S & \text{branch} \\
& | & T\ {}_p\oplus \ S & \text{choice}
\end{array}
$$

- **plain** termination vs **successful** termination
- **probability annotations** in branches and choices
- infinite trees with finitely many distinct sub-trees (**regularity**)
- each sub-tree contains a reachable leaf $\circ$ or $\bullet$ (**reachability**)

success probability of a session type

Definition (success probability – informal)

$[\![T]\!]$ = cumulative probability of paths from T to $\bullet$

Formally, solve this finite system of equations:

$$\begin{aligned} [\![\circ]\!] &= 0 \\ [\![\bullet]\!] &= 1 \\ [\![T \;{}_p\& \; S]\!] = [\![T \;{}_p\oplus \; S]\!] &= p[\![T]\!] + (1-p)[\![S]\!] \end{aligned}$$

Reasoning

- consider the Discrete-Time Markov Chain corresponding to T
- regularity implies that the DTMC is **finite**
- reachability implies that the DTMC is **absorbing**
- the system of equations has **exactly one** solution

success probability of a session type

Definition (success probability – informal)

$[\![T]\!]$ = cumulative probability of paths from T to $\bullet$

Formally, solve this finite system of equations:

$$
\begin{aligned}
[\![\circ]\!] &= 0 \\
[\![\bullet]\!] &= 1 \\
[\![T \,{}_p\& \, S]\!] = [\![T \,{}_p\oplus \, S]\!] &= p[\![T]\!] + (1-p)[\![S]\!]
\end{aligned}
$$

Reasoning

- consider the Discrete-Time Markov Chain corresponding to T
- regularity implies that the DTMC is **finite**
- reachability implies that the DTMC is **absorbing**
- the system of equations has **exactly one** solution

type system

$$\Gamma \vdash P$$

- Γ is a behavioural abstraction of P (including probabilities)
- $x : T \in \Gamma \Rightarrow P$ successfully terminates x with probability $[\![T]\!]$

successul termination

$$\frac{}{x : \bullet \vdash \texttt{done}\, x}$$

deterministic choices

$$\frac{x : T \vdash P}{x : T \;{}_{1}\!\oplus S \vdash \texttt{inl}\, x.P} \qquad \frac{x : S \vdash P}{x : T \;{}_{0}\!\oplus S \vdash \texttt{inr}\, x.P}$$

- deterministic process ⇒ trivial probability

probabilistic choices

$$\frac{x : T_1 \vdash P \qquad x : T_2 \vdash Q}{x : T_1 \,{}_{p}\boxplus\, T_2 \vdash P \,{}_{p}\boxplus\, Q}$$

probabilistic combination of T_1 and T_2

$$\begin{aligned} T \,{}_{p}\boxplus\, T &= T \\ (T \,{}_{q}\oplus\, S) \,{}_{p}\boxplus\, (T \,{}_{r}\oplus\, S) &= T \,{}_{pq+(1-p)r}\oplus\, S \end{aligned}$$

- combination is **undefined** otherwise

probabilistic choices

$$\frac{x : T_1 \vdash P \qquad x : T_2 \vdash Q}{x : T_1 \ {}_p\boxplus\ T_2 \vdash P \ {}_p\boxplus\ Q}$$

probabilistic combination of T_1 and T_2

$$\begin{array}{rcl} T \ {}_p\boxplus\ T & = & T \\ (T \ {}_q\oplus\ S) \ {}_p\boxplus\ (T \ {}_r\oplus\ S) & = & T \ {}_{pq+(1-p)r}\oplus\ S \end{array}$$

- combination is **undefined** otherwise

branches and choice propagation

$$\frac{\Gamma, x : T \vdash P \qquad \Delta, x : S \vdash Q}{\Gamma \;{}_{p}\!\boxplus\; \Delta, x : T \;{}_{p}\!\& \; S \vdash \texttt{case}\, x\, [P, Q]}$$

- Γ and Δ are nearly the same
- choices in Γ and Δ affected by information received from x
- choices in Γ and Δ **weighed** by p

parallel composition

endpoint

endpoint

$$\frac{\Gamma, x : T \vdash P \qquad \Delta, x : \overline{T} \vdash Q}{\Gamma, \Delta, x : \langle [\![T]\!] \rangle \vdash P \mid Q}$$

whole session

- $\langle p \rangle$ = type of a session with success probability p

example

$$x : \circ \,{}_1\!\oplus \circ \qquad x : \circ \,{}_0\!\oplus \circ$$

$$(\overbrace{\texttt{inl}\,x}\ {}_p\boxplus\ \overbrace{\texttt{inr}\,x}) \mid \texttt{case}\,x\,[\texttt{inr}\,y.\texttt{done}\,y,\quad \texttt{inl}\,y]$$

example

$$\Big(\overbrace{\mathtt{inl}\,x}^{x\,:\,\circ\ {}_1\oplus\ \circ}\ {}_p\boxplus\ \overbrace{\mathtt{inr}\,x}^{x\,:\,\circ\ {}_0\oplus\ \circ}\Big)$$

$$\underbrace{\Big(\mathtt{inl}\,x\ {}_p\boxplus\ \mathtt{inr}\,x\Big)}_{x\,:\,\circ\ {}_p\oplus\ \circ} \mid \mathtt{case}\,x\,[\mathtt{inr}\,y.\mathtt{done}\,y,\ \ \mathtt{inl}\,y]$$

example

$x : \circ\ {}_{1}\!\oplus\ \circ$ $\quad$ $x : \circ\ {}_{0}\!\oplus\ \circ$

$$(\mathtt{inl}\,x\ \ {}_{p}\!\boxplus\ \ \mathtt{inr}\,x) \mid \mathtt{case}\,x\,[\mathtt{inr}\,y.\mathtt{done}\,y,\quad \mathtt{inl}\,y]$$

$x : \circ\ {}_{p}\!\oplus\ \circ$ $\quad$ $x : \circ\ {}_{p}\!\&\ \circ$

example

$x : \circ \ {}_1\!\oplus\ \circ$ $\quad x : \circ \ {}_0\!\oplus\ \circ$ $\quad y : \circ \ {}_0\!\oplus\ \bullet$ $\quad y : \circ \ {}_1\!\oplus\ \bullet$

$$(\texttt{inl}\ x \ \ {}_p\!\boxplus\ \ \texttt{inr}\ x) \mid \texttt{case}\ x\ [\texttt{inr}\ y.\texttt{done}\ y,\ \ \texttt{inl}\ y]$$

$x : \circ \ {}_p\!\oplus\ \circ$ $\quad x : \circ \ {}_p\&\ \circ$

example

$$\underbrace{(\overbrace{\mathtt{inl}\,x}^{x : \circ\,{}_{1}\!\oplus\,\circ}\ {}_{p}\!\boxplus\ \overbrace{\mathtt{inr}\,x}^{x : \circ\,{}_{0}\!\oplus\,\circ})}_{x : \circ\,{}_{p}\!\oplus\,\circ} \mid \underbrace{\mathtt{case}\,x\,[\overbrace{\mathtt{inr}\,y.\mathtt{done}\,y}^{y : \circ\,{}_{0}\!\oplus\,\bullet},\ \overbrace{\mathtt{inl}\,y}^{y : \circ\,{}_{1}\!\oplus\,\bullet}]}_{y : \circ\,{}_{1-p}\!\oplus\,\bullet}$$

subject reduction

Informally

Types – not just typing – are preserved by reductions.

Theorem

If $\Gamma \vdash P$ *and* $P \rightarrow Q$*, then* $\Gamma \vdash Q$*.*

Particular instance

If $x : \langle p \rangle \vdash P$ and $P \rightarrow Q$, then $x : \langle p \rangle \vdash Q$.

- **unresolved** prob. choices $\Rightarrow$ **steady** success probabilities
- suitable design choice for specifying **invariants**

soundness

Definition

We write $P \uparrow_p^x$ iff P has a top-level $\texttt{done}\, x$ with probability p, that is

$$P \uparrow_p^x \iff P \preccurlyeq \texttt{done}\, x \;{}_p\boxplus\; Q$$

Theorem

If $x : \langle p \rangle \vdash P$ and $P \not\rightarrow$, then $P \uparrow_p^x$.

Remarks

- deadlock freedom is a **necessary condition**
  - type system enforces an acyclic (tree-like) network topology
- useless when P reduces forever

soundness

Definition

We write $P \uparrow_p^x$ iff P has a top-level $\texttt{done}\, x$ with probability p, that is

$$P \uparrow_p^x \iff P \preccurlyeq \texttt{done}\, x \;{}_p\boxplus\; Q$$

Theorem

If $x : \langle p \rangle \vdash P$ *and* $P \not\rightarrow$*, then* $P \uparrow_p^x$*.*

Remarks

- deadlock freedom is a **necessary condition**
  - type system enforces an acyclic (tree-like) network topology
- useless when P reduces forever

probabilistic termination

$$A(x) := \mathtt{done}\, x \;{}_p\!\boxplus\; A\langle x\rangle$$

Fact: $A\langle x\rangle$ reduces forever

$$A\langle x\rangle \rightarrow \mathtt{done}\, x \;{}_p\!\boxplus\; (\mathtt{done}\, x \;{}_p\!\boxplus\; A\langle x\rangle) \rightarrow \cdots$$

Fact: if $p > 0$, the probability of reaching an irreducible state is 1

$$p + (1-p)p + (1-p)^2 p + \cdots = \frac{p}{1-(1-p)} = 1$$

limit soundness

Definition (eventual success of a session)

Let $P \Uparrow_p^x$ if $P = P_0 \rightarrow P_1 \rightarrow P_2 \rightarrow \cdots$ and

1. $P_n \uparrow_{p_n}^x$ for all $n \in \mathbb{N}$
2. $\lim_{n \to \infty} p_n = p$

Theorem

If $x : \langle p \rangle \vdash P$ and P terminates with probability 1, then $P \Uparrow_p^x$.

- Conclusion holds also if the termination probability is $p < 1$ and the successful completion probability is 1 (see paper).

Wrap up

With which probability P terminates session x successfully?

- easy to do from session types, less so for processes
- type system fills the gap

Future work

- type inference
- subtyping

Wrap up

With which probability ***P*** terminates session ***x*** successfully?

- easy to do from session types, less so for processes
- type system fills the gap

Future work

- type inference
- subtyping

thank you