Quantitative Techniques

Emilio Tuosto

Gran Sasso Science Institute

GRAN SASSO SCIENCE INSTITUTE
SCHOOL OF ADVANCED STUDIES
Scuola Universitaria Superiore

Dagstuhl Seminar 24051

"Next Generation Protocols for Heterogeneous Systems"

29/01/2024

Agenda

- An overview of results (chronologically ordered)
    - Resource-Awareness
    - Probabilities
    - Time
- Open problems

Resources

@ LICS 18

- Das, Hoffmann, Pfenning: Work Analysis with Resource-Aware STs

- Static derivation worst-case bounds on work for communication

$$S, T ::= V \mid \oplus\{l_i^{q_i} : S\} \mid \&\{l_i^{q_i} : S\} \mid S \overset{q}{\multimap} T \mid S \overset{q}{\otimes} T \mid \mathbf{1}^{q}$$

potential energy to be transferred

- thm Soundness: Well-typed processes don't "generate" energy
- thm Progress (direct consequence of progress in SILL [Toninho, Caires, Pfenning: ESOP13])

- Case Studies

@CSF21

- Das, Balzer, Hoffmann, Pfenning, Santurkar: Resource-Aware STs for digital contracts
  - Nomos, a DSL to account for reqs of digital contracts by construction
  - a session typing discipline for resource-analysis
    - linearity to prevent duplication/deletion of assets
    - type reconstruction to automatically infer resource bounds
    - amortized resource analysis to control resource usage
  - Thm type preservation & Progress
  - Evaluation on case studies

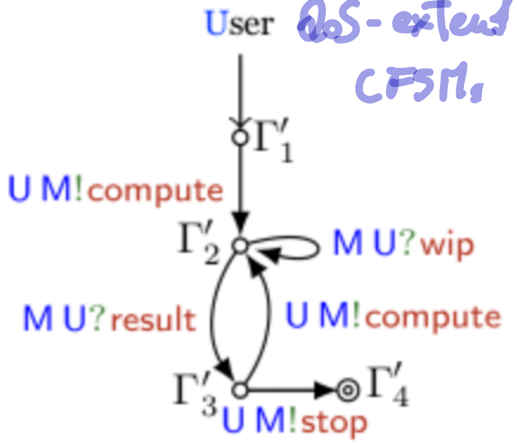
@ICTAC 23

- Lopez Pombo, Martinez Suñé, – : A Dynamic Temporal Logic for QoS in Choreographic Models

Given a distributed system for which we know the quality of service (QoS) of its components, we want to verify system-wide quality properties.

QL logic

QoS-extend CFSMs



A QoS specification $\langle \Sigma, \Gamma \rangle$ *is a (first-order) theory presentation*

$$\Sigma = \langle \{0,1\} \cup \boxed{\mathsf{Q}}, \{+,\cdot\} \cup \boxed{\{\oplus^{\mathsf{a}}\}_{\mathsf{a}\in\mathsf{Q}}}, \{<\} \rangle$$

$$\Gamma = \boxed{\Gamma_{\mathrm{RCF}}} \cup \boxed{\Gamma'}$$

Axioms of Real Closed Fields

First-order formulae over Q

Constant symbols representing QoS attributes

Aggregation operators

$$\Phi ::= \top \mid \boxed{\psi} \mid \neg\Phi \mid \Phi \vee \Phi \mid \Phi\, \mathcal{U}^{\mathsf{G}}\, \Phi$$

First-order formula over Q

Global choreography

Bounded MC (now implemented in ChorGram)

Probabilities

@FROM 19
@WOLLIC22

Amanol, Ciobanu: Probabilities in STs

probability interval

$$
\begin{array}{llll r}
\textit{Global} & G & ::= & \sum_{i\in I} q \rightarrow_{\delta_i} q' : k\langle \underline{S_i}\rangle.G_i & \text{(probValues)} \\
 & & \mid & q \rightarrow_1 q' : k\langle T@p\rangle.G' & \text{(delegation)} \\
 & & \mid & \sum_{i\in I} q \rightarrow_{\delta_i} q' : k\{l_i : G_i\} & \text{(probBranching)} \\
 & & \mid & G, G' & \text{(parallel)} \\
 & & \mid & \mu t.G & \text{(recursive)} \\
 & & \mid & t & \text{(variable)} \\
 & & \mid & \mathsf{end} & \text{(end)} \\
\textit{Sorts} & S & ::= & \textit{bool} \mid \textit{nat} \mid \ldots & \text{(value types)}
\end{array}
$$

Synchrony

prob. choiches are distributions

<u>Thm</u> Well-typed progs. don't have "probability errors"

the WOLLIC paper simplifies things using the ECOOP 22 paper of Darda, Hu, Scalas, and Yoshida

@CONCUR 20

- Inverso, Melgratti, Padovani, Trubiani, – : Probabilistic Analysis of Binary Sessions

Reasoning about session termination ... probabilistically

$$T, S ::\overset{co}{=} \circ \mid \underset{\text{success}}{\bullet} \mid ?t.T \mid !t.T \mid T\ {}_{p}\&\ S \mid T\ {}_{p}\oplus\ S$$

tech. convinience

Session types ⟶ DTMCs

also infinitary ones

Thm Typing ensures that the prob. beh. of processes respect their type

@SCP 21

- Burlò, Francalanza, Scalas, Trubiani, – : PSTMonitor : Monitor Synthesys from pST

@CONCUR22

- Dal Lago, Giusti: On Session Typing, Prob. Polynomial Time, and crypto. ex.
  - Binary STs to model cryptographic experiments
  - Extend [Cairos, Pfenning CONCUR10] with
    - polytime functions
    - probabilistic choice

    } building blocks of cryptographic protocols

Thm Subject reduction & progress of well-typed progs.

Thm Well-typed progs are confluent

internal actions lead to a unique distribution of processes

@POPL 23

- Das, Wang, Hoffmann: Probabilistic Resource Aware STs
  - Resource analysis of probabilistic systems via binary p STs
  - p ST to derive expected cost bounds of message-passing systems extending the STs in the author's LICS 18 paper
  - Both probabilistic and non-deterministic choice
  - Type preservation, progress, probability consistency
  - NomosPro with implementation and extensive evaluation

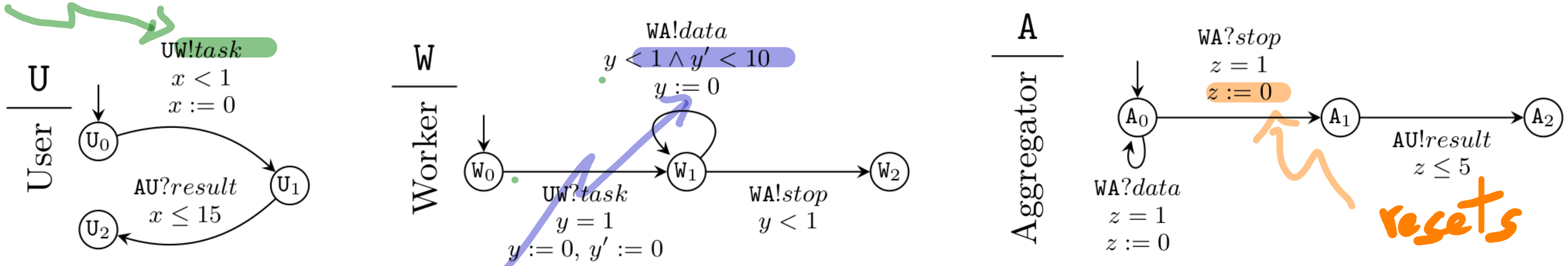
Time

Krcál, Yi @ CAV06

Communicating Timed Automata

Bocchi, Lange, Yoshida @ CONCUR 2015

I/O actions



resets

time constraints / guards on (partitioned) clocks

$$g ::= x \leq c \mid x \geq c \mid \neg g \mid g \wedge g$$

clock

rational value

Evaluations

$\nu : x \longmapsto z \in \mathbb{R}^{\geq 0}$

Asynchronous communication!

@ CONCUR14

Bocchi, Yang, Yoshida: Timed Multiparty Session Types

$$\begin{tikzcd} & MPST \arrow[r, hook] \arrow[d, squiggly] & TMPST \arrow[d, squiggly, "\text{sound \& complete projections}"'] \\ LT \arrow[r, leftrightarrow] & CA \arrow[r, hook] & CTA \end{tikzcd}$$

- time annotation increases expressiveness
- but time-error freedom with no "time-analysis"

Thm Typed programs respect timing

thm Feasibility + Wait-Freedom ⇒ time progress of typed progs

partial timed executions can be completed

if senders respect their timing then receivers don't have to wait

timed deadlock

⇓

untimed deadlock

@ CONCUR'15

Bocchi, Lange, Yoshida: Meeting Deadlines Together

CFSMs / TA $\hookrightarrow$ CTA

sound membership decision procedure
- safety = deadlock freedom + no orphan msg.
- eventual reception
- progress
- non-zenoness

> sufficient cond.

multiparty compatibility

Thm: An M.C. system is safe

Thm: S M.C. $\Longrightarrow$ $S \sim STS(S)$ ✓

timed bisimilarity

- Neykova, Bocchi, Yoshida: Timed Runtime Monitoring for Multiparty Conversations
  - tool chain for timed interaction
    - define timed protocols in Scribble
    - check for feasibility & wait-freedom
    - projections
    - derive monitor to check timing

@ FORTE 15
@ LMCS 17

- Bartoletti, Cimoli, Murgia: Timed Session Types

- Binary (synchronous) case is interesting:

  - is compatibility decidable in TST?

  - duality doesn't yield compatibility ← deadlock freedom

  - can compliant timed counterparts be found?

Thm T-Compliance reduced to model-check deadlock (freedom in timed-automata (→ decidable)

thm The set of evaluations of a TST admitting a compliant TST is effectively computable

Cor Canonical compliant TST can be computed

thm Subtyping is decidable

@ICE 18
@JLAMP 19

- Murgia: Input Urgent Semantics for async TST

Synchronous compliance ⇏ Asynchronous compliance
the implication holds if firable inputs are not delayed

@CONCUR 18

- Bartoletti, Bocchi, Murgia: Progress-preserving Refinements of CTA

not "really" timed STs

Refinements of CTA that { don't introduce deadlocks/livelocks
are simulated by abstract systems

@ESOP 19

- Bocchi, Murgia, Vasconcelos, Yoshida: Asynchronous Timed Session Types

Generalisation of duality & compliance based on
a urgent semantics

@ ICFP 18

- Das, Hoffmann, Pfenning: Parallel Complexity analysis with Temporal STs
  - Binary asynchronous STs with LTL-like modalities
  - $\bigcirc A$ inhabited by processes of the form

    prefixing depends on the cost model

    delay ; P

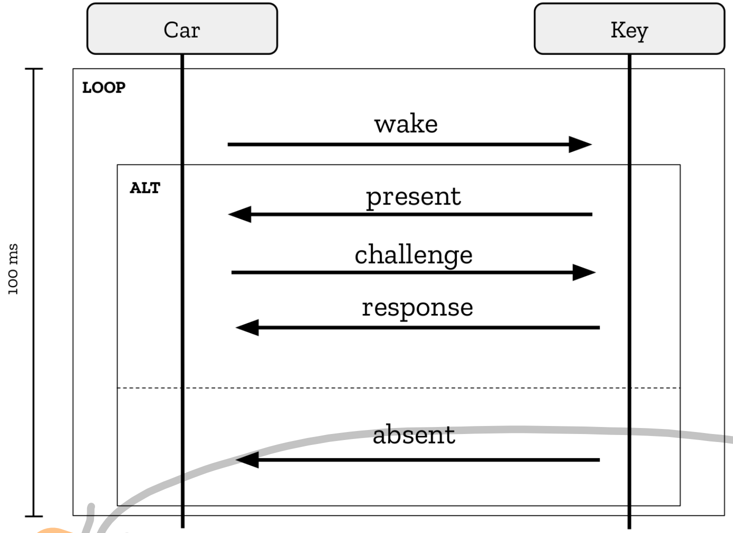
    P behaves as A after a time unit!
  - $\Box A$ = "always ready to do A"
  - $\Diamond A$ = "eventually ready to do A"
  - Generic framework for cost analysis
  - Well-typed programs enjoy progress & type-preservation
  - the cost model can be parameterised

@OOPSLA 23

Iraci, Chuang, Hu, Ziarek: Validating IoT Devices with Rate-based STs

IoT

Grant Iraci, Cheng-En Chuang, Raymond Hu, and Lukasz Ziarek



- Synchronous binary STs to reason about rates
- Simple extension: periodic recursion

T-Car = ω_{100} t.!wake.& { present: !challenge. ?response.t; absent: t }

T-Key = ω_{100} t.?wake.⊕ { present: ?challenge. !response.t; absent: t }

$\omega_n t.\,!m.t \not\approx \omega_n t.\,!m.\,!m.t$

because rates differ!

thm Well-Typed systems don't have rate-errors

@COORDINATION 23

- Pears, Bocchi, King: Safe asynchronous mixed-choice ...

  - Extend mixed sessions [Vasconcelos et al. ESOP20] to allow mixed choice in TSTs

Thm Well-typed systems have progress

assuming urgent inputs

Open Problems

(?)

Time	Probabilities	Resources
• (Inter)action duration • CPS challenges • asynchronous subtyping • Relativity	• Relative express. • Rates	• Cost analysis for QoS • Data dependent QoS
• Tooling	• binary ⇝ M.P.	• cross cut time / prob. / resources

Thank you

Details

- Async.
- Glob. time
- non-unique typing

$\oplus / \&$

$$G ::= p \to q : \{ l_i \langle S_i \rangle \{ A_i \} . G_i \}_{i \in I} \qquad T ::= p \,\square\, \{ l_i : \langle S_i \rangle \{ B_i \} . T_i \}_{i \in I}$$

$$\mid \mu t . G \qquad \mid \mu t . T$$

$$\mid t \qquad \mid t$$

$$\mid \underline{\text{end}} \qquad \mid \underline{\text{end}}$$

$(\delta_o, \lambda_o, \delta_I, \lambda_T)$

(δ, λ)

CONCUR 15

Thm: M.C. & Interaction Enabledness ⇒ Progress

1. a machine in a sending state eventually sends
2. every sent message can be received in the future

ZENO!!!!! & bottom UP!!!

CONCUR 15

"M.C., which characterizes a sound & complete correspondence with MPSTs, soundly characterizes safe CTAs and offers a basis for decidable decision procedures for progress & non-zenoness"

Open problems

- Relative expressiveness e.g. OOPSALA 23 vs ICFP 18
- Does relative time make sense?
- More expressive constraints?
- Shared clocks?

communication duration

- not much tooling