Realisability of Global Models of Interaction

José Proença (CISTER & University of Porto, Portugal)

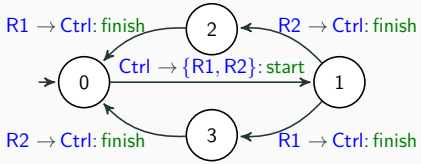
& Maurice ter Beek (ISTI-CNR, Pisa, Italy)

& Rolf Hennicker (Ludwig-Maximilians-Universität, München, Germany)

December 7
ICTAC 2023

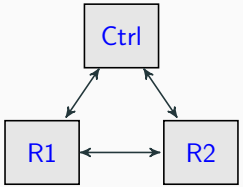
This Talk

Realisability of Global Models of Interaction



$\mathcal{G}$

realise



$\mathcal{R}$

Team Automata (TA)

[FM'03,21,23] [ICTAC'20]

[CSCW'03] [COORD.'17,20]

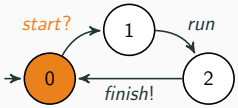
Choreographic models

- Choreography Automata
- Multiparty Session Types

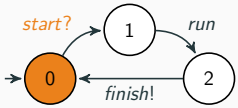
Realisability for TA

- Preserve requirements
- Realisability conditions
- Implementation

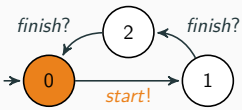
Team Automata (TA)



$\mathcal{R}unner_1$



$\mathcal{R}unner_2$



Controller

Multiparty synchronisation

Ctr $\rightarrow \{R1, R2\}$: start

Constrained synchronisation

start: $1 \rightarrow 2$

finish: $1 \rightarrow 1$

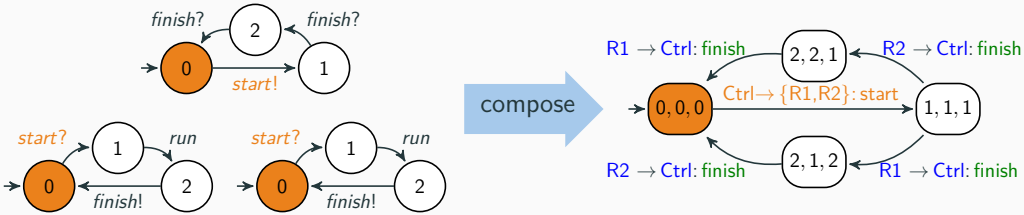
Should not get stuck

Responsiveness/receptiveness

Encoded as modal mu-calculus

mCRL2 analysing system behaviour

Team Automata (TA)



Multiparty synchronisation

Ctr $\rightarrow \{R1, R2\}$: start

Constrained synchronisation

start: $1 \rightarrow 2$

finish: $1 \rightarrow 1$

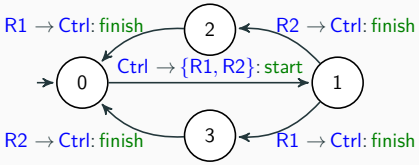
Should not get stuck

Responsiveness/receptiveness

Encoded as modal mu-calculus

mCRL2 analysing system behaviour

Choreography Automata (CA)



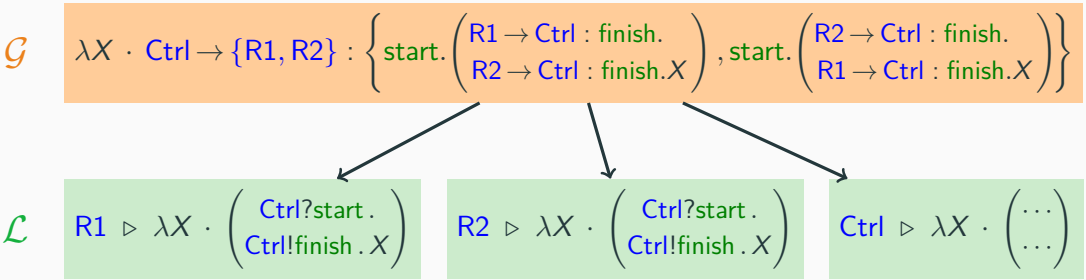
Global model of interactions

- Several results over the language of CA
- Realising = Projecting the language of CA
- F. Barbanera, I. Lanese, and E. Tuosto, *Formal Choreographic Languages* @ COORDINATION'22

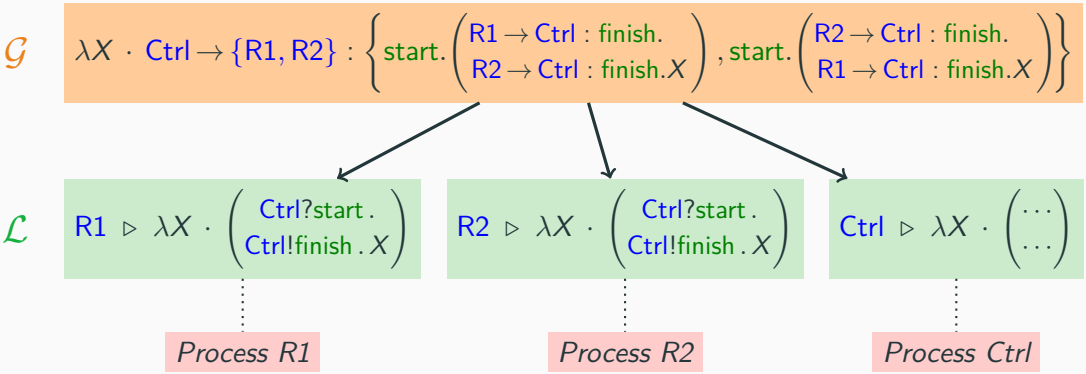
Multiparty Session Types (MPST)

$$\lambda X \cdot \mathsf{Ctrl} \to \{\mathsf{R1}, \mathsf{R2}\} : \left\{ \mathsf{start}. \begin{pmatrix} \mathsf{R1} \to \mathsf{Ctrl} : \mathsf{finish}. \\ \mathsf{R2} \to \mathsf{Ctrl} : \mathsf{finish}.X \end{pmatrix}, \mathsf{start}. \begin{pmatrix} \mathsf{R2} \to \mathsf{Ctrl} : \mathsf{finish}. \\ \mathsf{R1} \to \mathsf{Ctrl} : \mathsf{finish}.X \end{pmatrix} \right\}$$

Multiparty Session Types (MPST)



Multiparty Session Types (MPST)

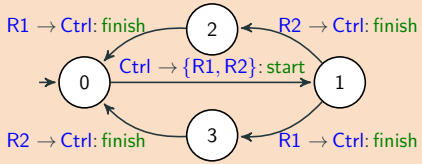


- Use projections to realise
- Often impose syntactic restrictions on global types
- M. Hüttel et al., *Foundations of Session Types and Behavioural Contracts*. ACM Comp.Surv. 2016

Realisability for Team Automata

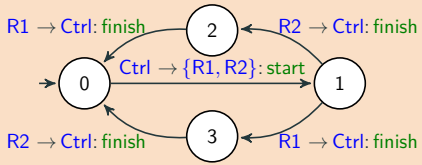
What is Realisability in TA?

Start with global $\mathcal{G}$



What is Realisability in TA?

Start with global $\mathcal{G}$



Synthesize a realisation $\mathcal{R}$

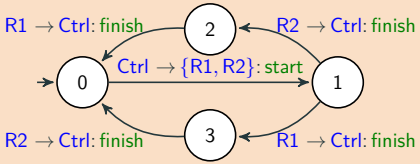
$$\mathcal{R} \;=\; \mathsf{Ctr} \;\leftrightarrow \mathsf{R1} \;\leftrightarrow\; \mathsf{R2}$$

such that

$\mathcal{R}$ *"somehow" behaves* as $\mathcal{G}$

What is Realisability in TA?

Start with global $\mathcal{G}$



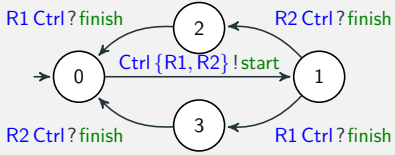
Synthesize a realisation $\mathcal{R}$

$\mathcal{R} = \text{Ctr} \leftrightarrow \text{R1} \leftrightarrow \text{R2}$

such that

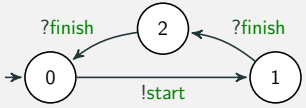
$\mathcal{R}$ *"somehow" behaves as* $\mathcal{G}$

Different agents and networks



(Ctrl with rich labels)

vs.



(Ctrl with poor labels)

How much do local agents know? Different network assumptions?

Properties and Behavioural Equivalence

Properties expressible in dynamic logic

- *No runner should finish before it has been started by the controller*
- *Any started runner should be able to finish its run*
- Receptiveness and responsiveness

[Can We Communicate? Using Dynamic Logic to Verify Team Automata, with G. Cledou @ FM'23]

Properties expressible with regular expressions

- *Runner 1 can finish immediately after Runner 2*
- *It is not possible to start the race, for runner 1 to finish, and then start another race*

Properties and Behavioural Equivalence

Properties expressible in dynamic logic

- *No runner should finish before it has been started by the controller*
- *Any started runner should be able to finish its run*
- Receptiveness and responsiveness

[Can We Communicate? Using Dynamic Logic to Verify Team Automata, with G. Cledou @ FM'23]

Properties expressible with regular expressions

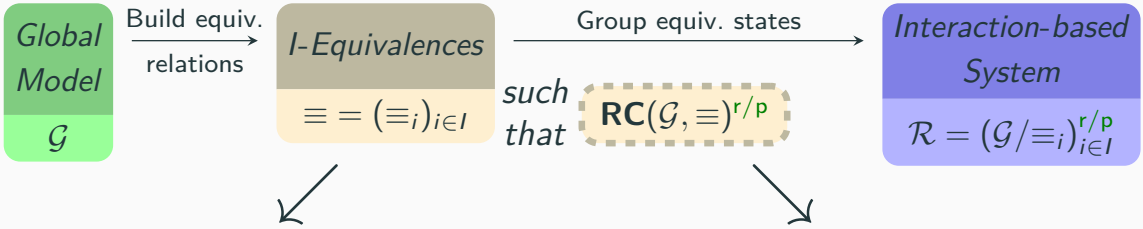
- *Runner 1 can finish immediately after Runner 2*
- *It is not possible to start the race, for runner 1 to finish, and then start another race*

Properties of $\mathcal{G}$ should also hold for $\mathcal{R}$ (and vice-versa)

- Dynamic logic: bisimilar (non-deterministic) systems obey the same formulas
- Regular expressions: language equivalent systems include the same expressions

Check realisability and system synthesis

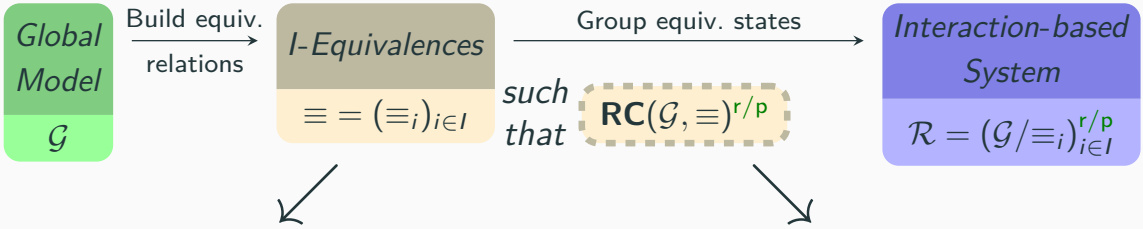
Check realisability and system synthesis



I. Castellani, M. Mukund, and P.S. Thiagarajan,
Synthesizing Distributed Transition Systems
from Global Specifications @ FSTTCS'99

cf. our paper for details

Check realisability and system synthesis



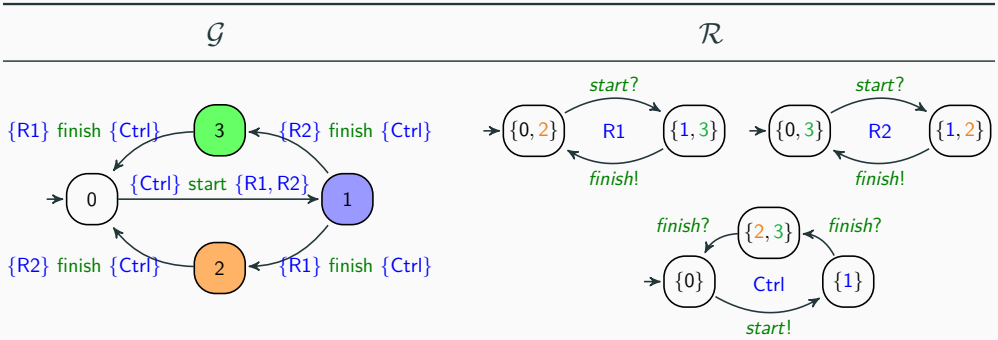
I. Castellani, M. Mukund, and P.S. Thiagarajan, Synthesizing Distributed Transition Systems from Global Specifications @ FSTTCS'99

cf. our paper for details

Theorems 2/3

If $RC(\mathcal{G}, \equiv)^{r/p}$ holds, then $\mathcal{G} \sim \otimes^{r/p}((\mathcal{G}/\equiv_i)^{r/p})_{i \in I}$

Our Approach to Synthesize a Realisation



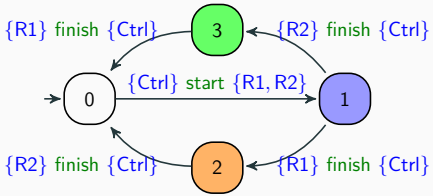
Group indistinguishable states

$R1 : 0 \equiv_{R1} 2 \; ; \; 1 \equiv_{R1} 3$

$R2 : 0 \equiv_{R2} 3 \; ; \; 1 \equiv_{R2} 2$

$Ctrl : 2 \equiv_{Ctrl} 3$

Realisability Conditions: Which States are Indistinguishable?



Group indistinguishable states

R1 : $0 \equiv_{R1} 2$; $1 \equiv_{R1} 3$

R2 : $0 \equiv_{R2} 3$; $1 \equiv_{R2} 2$

Ctrl : $2 \equiv_{Ctrl} 3$

Sufficient condition to discover equivalences

1. collapse "τ" transitions
2. $\forall$ label γ,
   participant k in γ,
   transition by k: $q \xrightarrow{\gamma\downarrow_k} q'$
   common glue g ***indistinguishable*** to each q
3. $\exists$ common g' ***indistinguishable*** to each q' s.t.

$$g \xrightarrow{\gamma} g'$$

Novelty

1. Realisations of global models with arbitrary multi-interactions supporting any kind of synchronous communication between multiple senders and multiple receivers

Novelty

1. Realisations of global models with arbitrary multi-interactions supporting any kind of synchronous communication between multiple senders and multiple receivers
2. Correctness notion for realisation based on bisimulation rather than isomorhism, so allowing to deal with non-determinism

Novelty

1. Realisations of global models with arbitrary multi-interactions supporting any kind of synchronous communication between multiple senders and multiple receivers
2. Correctness notion for realisation based on bisimulation rather than isomorhism, so allowing to deal with non-determinism
3. To construct realisations we consider, and analyse, two different localisation styles: rich and poor local actions

Novelty

1. Realisations of global models with arbitrary multi-interactions supporting any kind of synchronous communication between multiple senders and multiple receivers
2. Correctness notion for realisation based on bisimulation rather than isomorhism, so allowing to deal with non-determinism
3. To construct realisations we consider, and analyse, two different localisation styles: rich and poor local actions
4. A prototypical tool Ceta checks the realisability conditions and, if they are satisfied, generates local quotients and hence realisations

`https://github.com/arcalab/choreo/tree/ceta`

`https://lmf.di.uminho.pt/ceta`

Tooling @ https://lmf.di.uminho.pt/ceta

Choreographic Extended Team Automata

Choreography

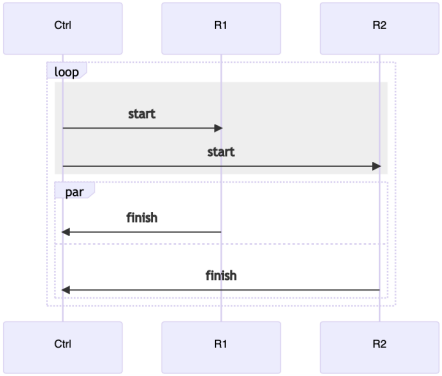
```
1 // Race example
2 (
3  (Ctrl->R1,R2: start);
4  (R1->Ctrl:finish ||
5   R2->Ctrl:finish)
6 )*
```

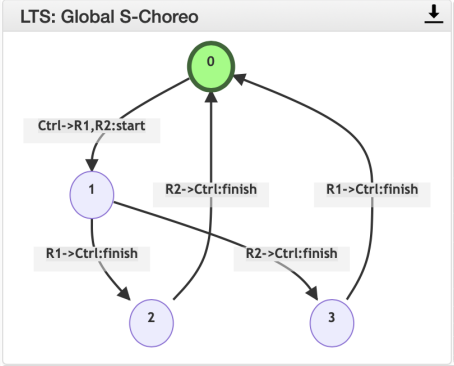
A controller starts 2 runners at the same time, and receives a finish message from each runner at a time.

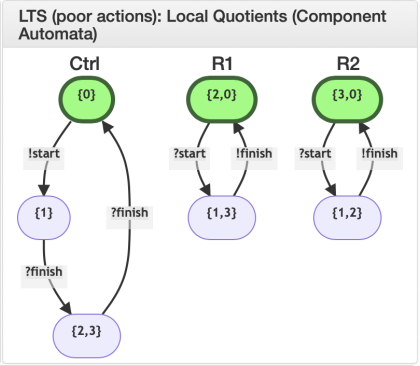
Examples

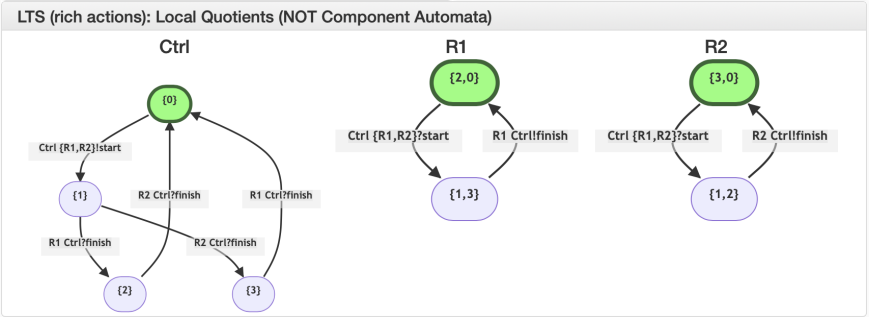
Race (simple) | Race (R1-first) | Race (once, simple) | Toss | Gossip (bad) | Gossip (good) | Cast-v1 | Cast-v2 | ab+cb+ca | ab;ac | ab|ac | ab;cd | ab|cd

Sequence Diagram




LTS: Global S-Choreo
0
Ctrl->R1,R2:start
1
R2->Ctrl:finish
R1->Ctrl:finish
R1->Ctrl:finish
R2->Ctrl:finish
2
3


LTS (poor actions): Local Quotients (Component Automata)
Ctrl
{0}
!start
{1}
?finish
?finish
{2,3}
R1
{2,0}
?start
!finish
{1,3}
R2
{3,0}
?start
!finish
{1,2}

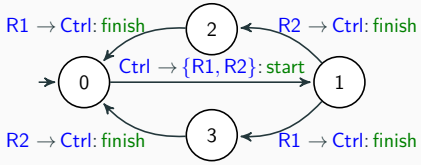

LTS (rich actions): Local Quotients (NOT Component Automata)
Ctrl
{0}
Ctrl {R1,R2}!start
{1}
R2 Ctrl?finish
R1 Ctrl?finish
R1 Ctrl?finish
R2 Ctrl?finish
{2}
{3}
R1
{2,0}
Ctrl {R1,R2}?start
R1 Ctrl!finish
{1,3}
R2
{3,0}
Ctrl {R1,R2}?start
R2 Ctrl!finish
{1,2}

Some Challenges

- compact representation of the global $\mathcal{G}$
  e.g., $\Big(\mathsf{Ctrl} \to \{\mathsf{R1}, \mathsf{R2}\} : \mathsf{start} \;\; ; \;\; (\mathsf{R1} \to \mathsf{Ctrl} : \mathsf{finish} \;||\; \mathsf{R2} \to \mathsf{Ctrl} : \mathsf{finish})\Big)^*$
- other network assumptions (e.g., asynchronous, causal channels, lossy, ...)
- heterogeneous agents (different assumptions/realisations)
- variability: global representation for any number of runners
  (to match the flexibility of synchronisation types, e.g., start: $[1] \to [2..*]$)
- refine realisations: can we make the local behaviour *"more specific"*, such that its composition is weakly bisimilar to the global behaviour?

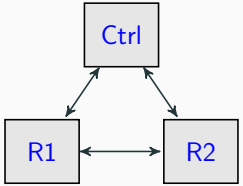
Wrap Up

Realisability of Global Models of Interaction



$\mathcal{G}$

realise



$\mathcal{R}$

Team Automata (TA)

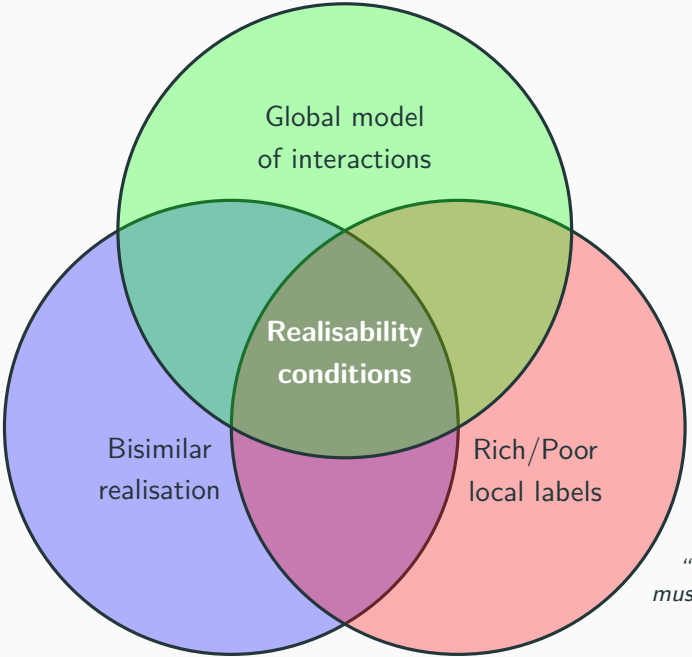
[FM'03,21,23] [ICTAC'20]
[CSCW'03] [COORD.'17,20]

Choreographic models

- Choreography Automata
- Multiparty Session Types

Realisability for TA

- Preserve requirements
- Realisability conditions
- `https://lmf.di.uminho.pt/ceta`



"Every good presentation must have a Venn diagram"

E.B. Johnsen

Thank you for your attention!

And thanks to the other team members of the work presented here: