# Formal Methods for Communication Protocols

## Harnessing distributed software design with behavioural contracts

Emilio Tuosto @ GSSI

– Lecture 2 –

3 - 12 March, 2026 - Novi Sad

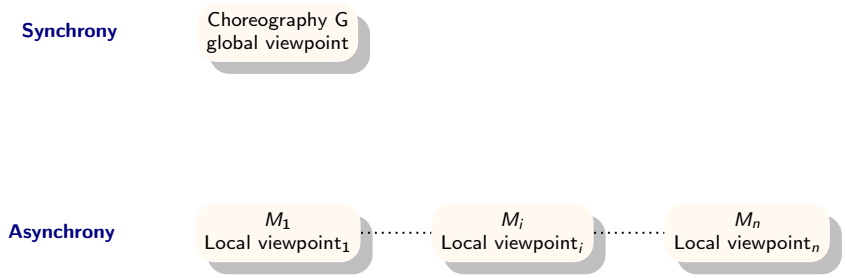
Finanziato dall'Unione europea NextGenerationEU | Ministero dell'Università e della Ricerca | Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA | DESK Developing Shared Knowledge

# – Choreographic Models –

# "Top-down"

## Quoting W3C [7]

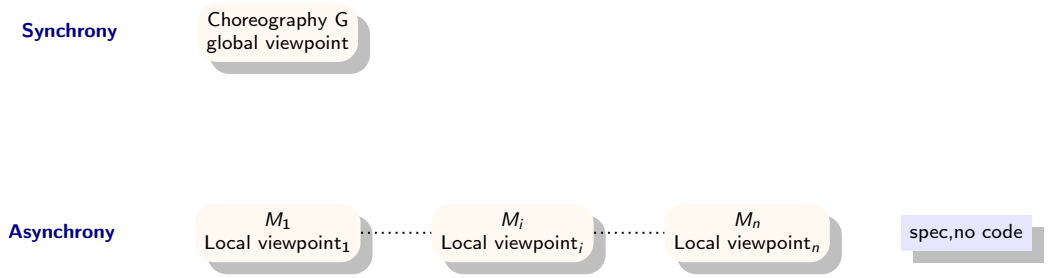
"Using the Web Services Choreography specification, a contract containing a global definition of the common ordering conditions and constraints under which messages are exchanged, is produced that describes, from a global viewpoint [...] observable behaviour of all the parties involved. Each party can then use the global definition to build and test solutions that conform to it. The global specification is in turn realised by combination of the resulting local systems [...]"



# "Top-down"

## Quoting W3C [7]

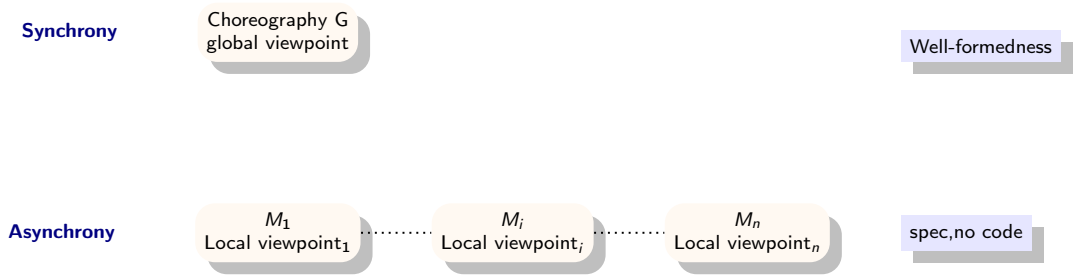
"Using the Web Services Choreography specification, a contract containing a global definition of the common ordering conditions and constraints under which messages are exchanged, is produced that describes, from a global viewpoint [...] observable behaviour of all the parties involved. Each party can then use the global definition to build and test solutions that conform to it. The global specification is in turn realised by combination of the resulting local systems [...]"



# "Top-down"

## Quoting W3C [7]

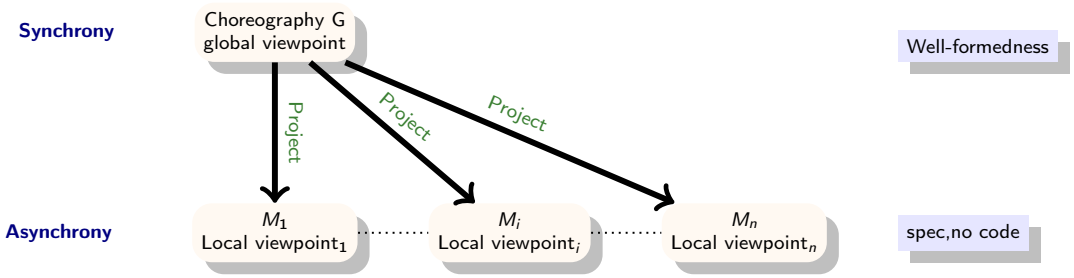
"Using the Web Services Choreography specification, a contract containing a global definition of the common ordering conditions and constraints under which messages are exchanged, is produced that describes, from a global viewpoint [...] observable behaviour of all the parties involved. Each party can then use the global definition to build and test solutions that conform to it. The global specification is in turn realised by combination of the resulting local systems [...]"



# "Top-down"

## Quoting W3C [7]

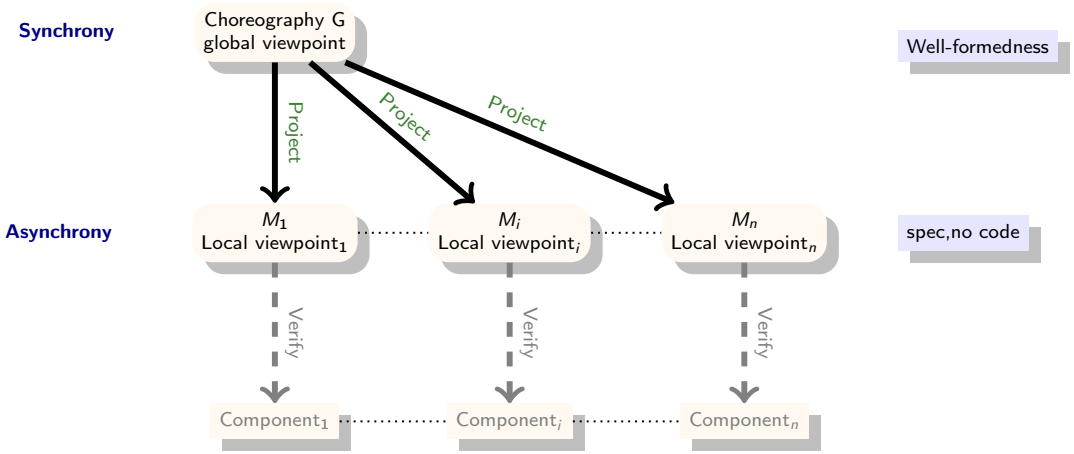
"Using the Web Services Choreography specification, a contract containing a global definition of the common ordering conditions and constraints under which messages are exchanged, is produced that describes, from a global viewpoint [...] observable behaviour of all the parties involved. Each party can then use the global definition to build and test solutions that conform to it. The global specification is in turn realised by combination of the resulting local systems [...]"



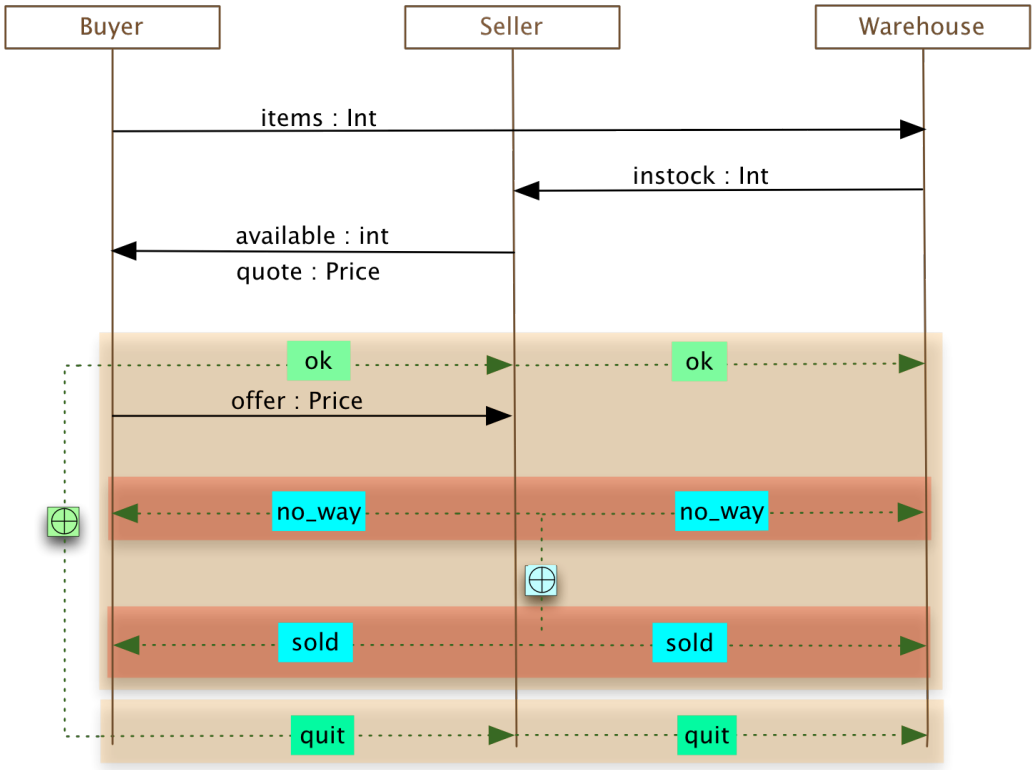
# "Top-down"

## Quoting W3C [7]

"Using the Web Services Choreography specification, a contract containing a global definition of the common ordering conditions and constraints under which messages are exchanged, is produced that describes, from a global viewpoint [...] observable behaviour of all the parties involved. Each party can then use the global definition to build and test solutions that conform to it. The global specification is in turn realised by combination of the resulting local systems [...]"

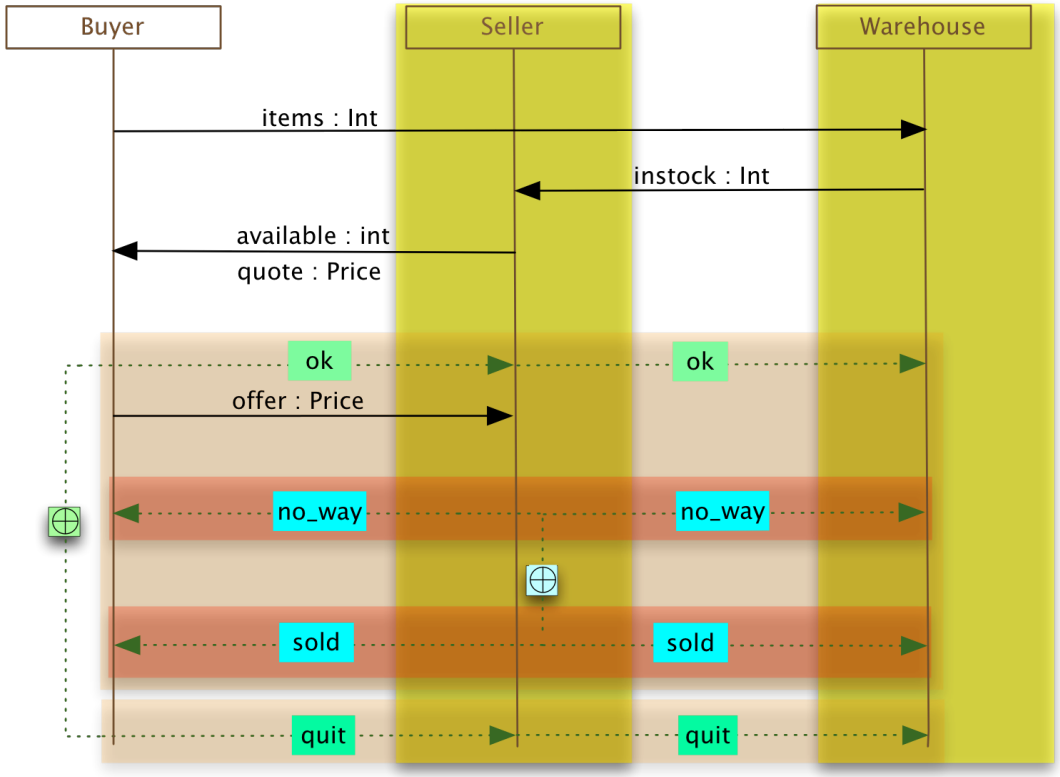


# An intuitive account...



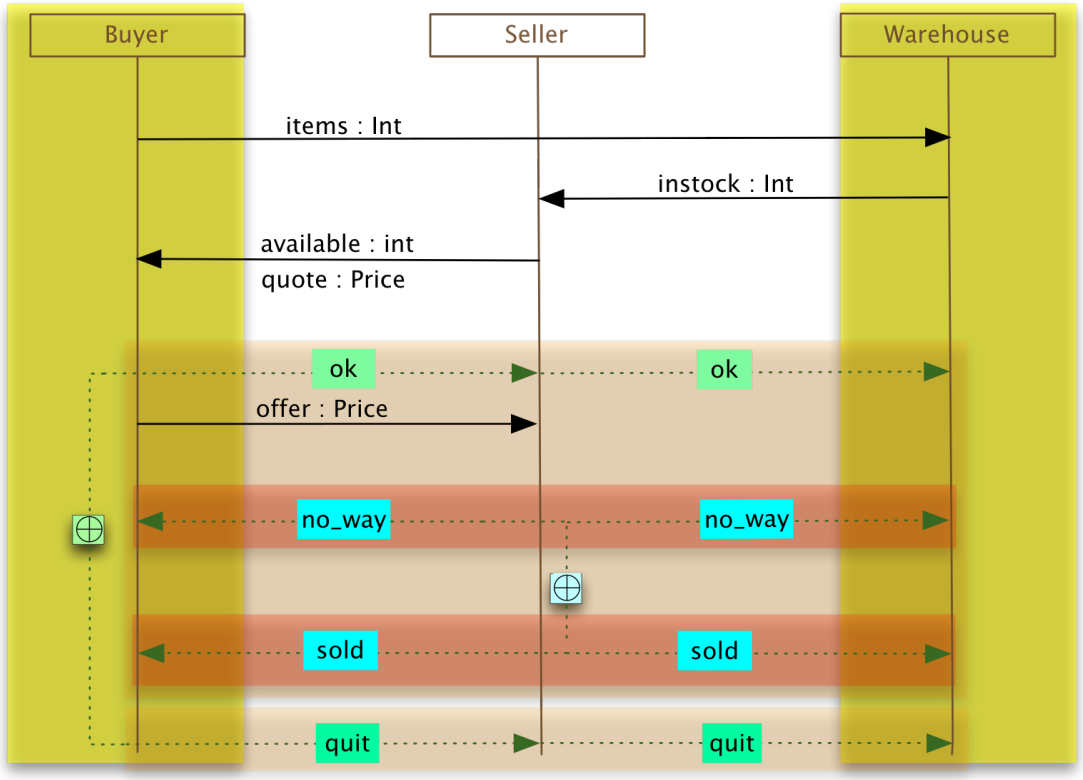

Global viewpoint

# An intuitive account...



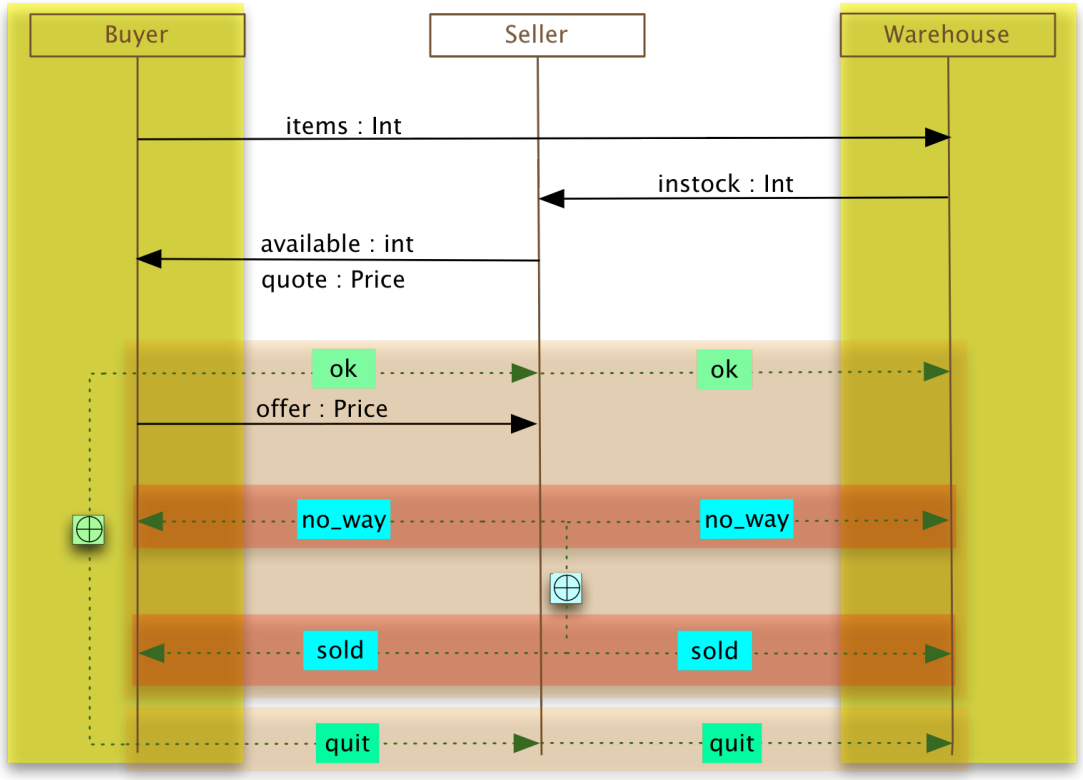

Projecting on buyer

# An intuitive account...




Projecting on seller

# An intuitive account...




Projecting on seller

Life is harder...recall the bugs of pingpong

# Global views...a bit more formally

G-choreographies [9, 5]

$$\mathsf{G}, \mathsf{G}' \ ::= \ \circledcirc \ \mid \ \mathsf{A} \to \mathsf{B} : \mathsf{m} \ \mid \ \mathsf{G} \mid \mathsf{G}' \ \mid \ \mathsf{G}; \mathsf{G}' \ \mid \ \mathsf{G} + \mathsf{G}' \ \mid \ *\mathsf{G}$$

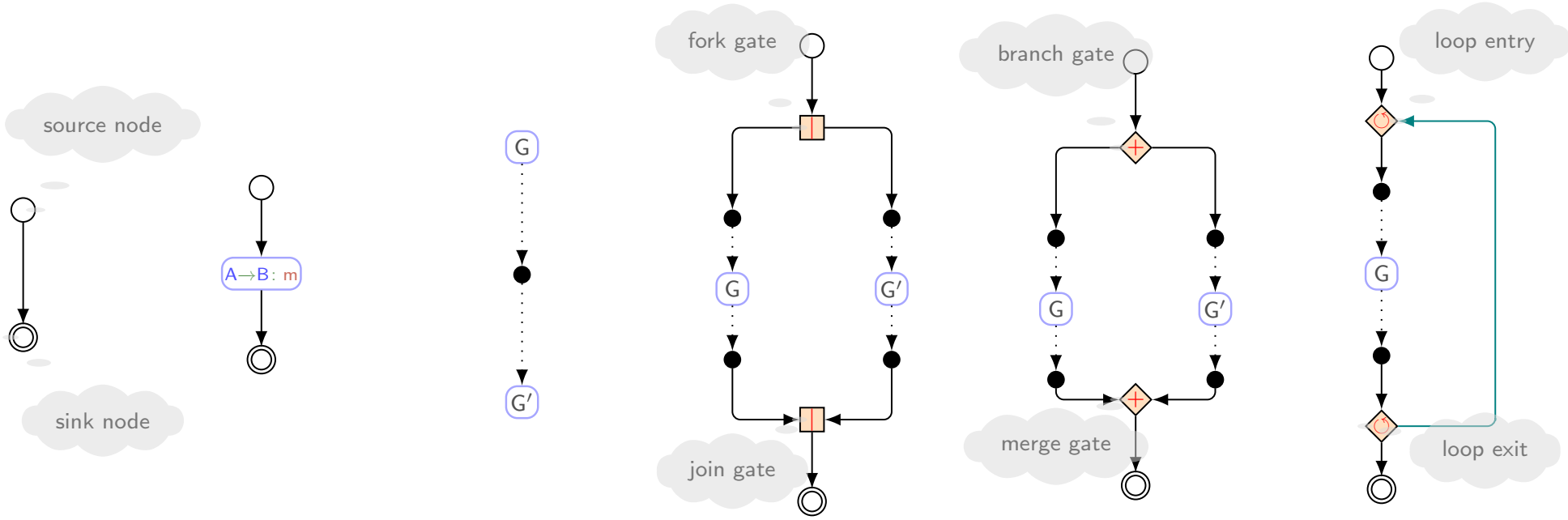
i.e., regular expressions (on an alphabet of interactions) with parallel composition

# Global views...a bit more formally

G-choreographies [9, 5]

$$\mathsf{G}, \mathsf{G}' \;::=\; \circledcirc \;\mid\; \mathsf{A}\to\mathsf{B}\colon \mathsf{m} \;\mid\; \mathsf{G} \mid \mathsf{G}' \;\mid\; \mathsf{G}; \mathsf{G}' \;\mid\; \mathsf{G} + \mathsf{G}' \;\mid\; *\mathsf{G}$$

i.e., regular expressions (on an alphabet of interactions) with parallel composition




empty | interaction | sequential | parallel | branch | iteration

# Global views' semantics as pomsets

A **pomset** on a set $\mathcal{E}$ of **events** is (an isomorphism class of) a **labelled partially-order** $(\mathcal{E}, \lambda, \leq)$, with

- $\lambda : \mathcal{E} \to \mathcal{L}$ a labelling function
- $\leq \quad \subseteq \quad \mathcal{E} \times \mathcal{E}$ reflexive, anti-symmetric, transitive

# Global views' semantics as pomsets

A **pomset** on a set $\mathcal{E}$ of **events** is (an isomorphism class of) a **labelled partially-order** $(\mathcal{E}, \lambda, \leq)$, with

- $\lambda : \mathcal{E} \to \mathcal{L}$ a labelling function
- $\leq \quad \subseteq \quad \mathcal{E} \times \mathcal{E}$ reflexive, anti-symmetric, transitive

Our basic ingredients:

# Global views' semantics as pomsets

A **pomset** on a set $\mathcal{E}$ of **events** is (an isomorphism class of) a **labelled partially-order** $(\mathcal{E}, \lambda, \leq)$, with

- $\lambda : \mathcal{E} \to \mathcal{L}$ a labelling function
- $\leq \quad \subseteq \quad \mathcal{E} \times \mathcal{E}$ reflexive, anti-symmetric, transitive

Our basic ingredients:

- a set $\mathcal{M}$ of **messages**,

# Global views' semantics as pomsets

A **pomset** on a set $\mathcal{E}$ of **events** is (an isomorphism class of) a **labelled partially-order** $(\mathcal{E}, \lambda, \leq)$, with

- $\lambda : \mathcal{E} \to \mathcal{L}$ a labelling function
- $\leq \quad \subseteq \quad \mathcal{E} \times \mathcal{E}$ reflexive, anti-symmetric, transitive

Our basic ingredients:

- a set $\mathcal{M}$ of **messages**,
- a set $\mathcal{P}$ of **participants' identities**,

# Global views' semantics as pomsets

A **pomset** on a set $\mathcal{E}$ of **events** is (an isomorphism class of) a **labelled partially-order** $(\mathcal{E}, \lambda, \leq)$, with

- $\lambda : \mathcal{E} \to \mathcal{L}$ a labelling function
- $\leq \quad \subseteq \quad \mathcal{E} \times \mathcal{E}$ reflexive, anti-symmetric, transitive

Our basic ingredients:

- a set $\mathcal{M}$ of **messages**,
- a set $\mathcal{P}$ of **participants' identities**,
- a set $\mathcal{C} = \mathcal{P} \times \mathcal{P} \setminus \{(\mathsf{A}, \mathsf{A}) \mid \mathsf{A} \in \mathcal{P}\}$ of **channels**

# Global views' semantics as pomsets

A **pomset** on a set $\mathcal{E}$ of **events** is (an isomorphism class of) a **labelled partially-order** $(\mathcal{E}, \lambda, \leq)$, with

- $\lambda : \mathcal{E} \to \mathcal{L}$ a labelling function
- $\leq \quad \subseteq \quad \mathcal{E} \times \mathcal{E}$ reflexive, anti-symmetric, transitive

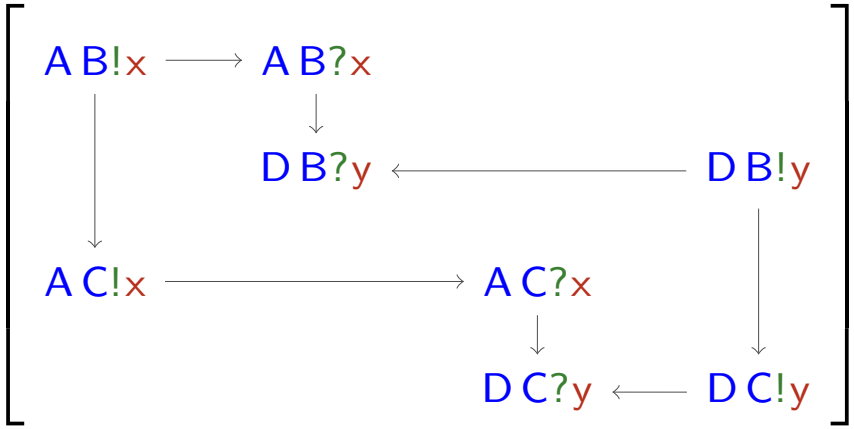
Our basic ingredients:

- a set $\mathcal{M}$ of **messages**,
- a set $\mathcal{P}$ of **participants' identities**,
- a set $\mathcal{C} = \mathcal{P} \times \mathcal{P} \setminus \{(\mathsf{A}, \mathsf{A}) \mid \mathsf{A} \in \mathcal{P}\}$ of **channels**

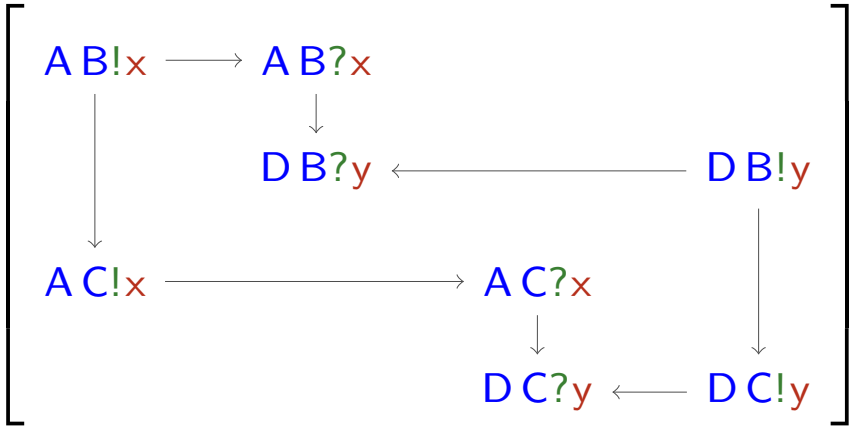
**Communication events**: $\mathcal{E} = \mathcal{E}^! \cup \mathcal{E}^?$ where

$$\begin{aligned} \mathcal{E}^! &= \mathcal{C} \times \{!\} \times \mathcal{M} \\ \mathcal{E}^? &= \mathcal{C} \times \{?\} \times \mathcal{M} \end{aligned}$$

# A simple pomset of communication events



# A simple pomset of communication events




## Exercise

Find a g-choreography that corresponds to the pomset on the left.

Another unfair question!

# Pomsets semantics of g-choreographies

We define $[\![\ ]\!] : \mathsf{G} \mapsto$ set of pomsets as

$$[\![\circledcirc]\!] = \{\epsilon\}$$

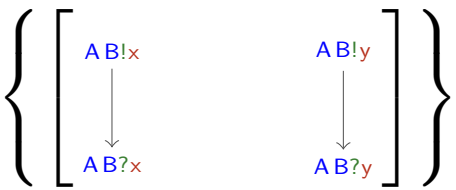
$$[\![\mathsf{A}\to\mathsf{B}:\mathsf{m}]\!] = \{[\mathsf{A}\,\mathsf{B}!\mathsf{m} \to \mathsf{A}\,\mathsf{B}?\mathsf{m}]\}$$

$$[\![\mathsf{G} \mid \mathsf{G}']\!] = \{[\text{disjoint union of } r \text{ and } r'] \mid (r, r') \in [\![\mathsf{G}]\!] \times [\![\mathsf{G}']\!]\}$$

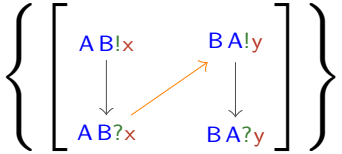
$$[\![\mathsf{G}; \mathsf{G}']\!] = \begin{cases} \bigcup_{(r,r')\in[\![\mathsf{G}]\!]\times[\![\mathsf{G}']\!]} \{\mathsf{seq}(r, r')\} & \text{if } \forall (r, r') \in [\![\mathsf{G}]\!] \times [\![\mathsf{G}']\!] : \ ws(r, r') \\ \text{undef} & \text{otherwise} \end{cases}$$

$$[\![\mathsf{G} + \mathsf{G}']\!] = \begin{cases} [\![\mathsf{G}]\!] \cup [\![\mathsf{G}']\!] & \text{if } wb(\mathsf{G}, \mathsf{G}') \\ \text{undef} & \text{otherwise} \end{cases}$$

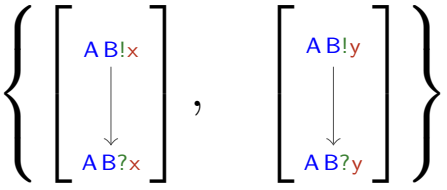
$\mathsf{A}\to\mathsf{B}:\mathsf{x} \mid \mathsf{A}\to\mathsf{B}:\mathsf{y}$




$\mathsf{A}\to\mathsf{B}:\mathsf{x};\ \mathsf{B}\to\mathsf{A}:\mathsf{y}$




$\mathsf{A}\to\mathsf{B}:\mathsf{x} + \mathsf{A}\to\mathsf{B}:\mathsf{y}$

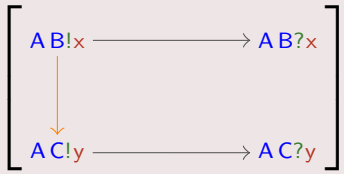


# Back to blackboard

Now we can solve the exercise on slide 18.

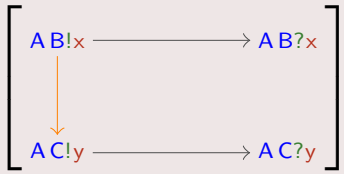
# Well-sequencedness

$A \to B : x; A \to C : y$



# Well-sequencedness

$A \to B : x; A \to C : y$

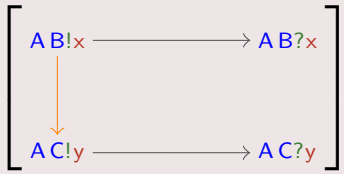



$r = [$ sbj A  sbj B $]$

$r' = [$ sbj A  sbj B $]$

# Well-sequencedness

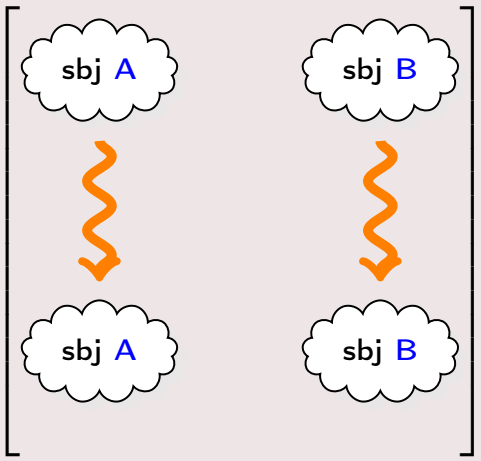
A→B : x; A→C : y




$r =$ [ sbj A  sbj B ]

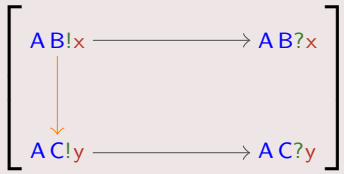
$r' =$ [ sbj A  sbj B ]

$\mathsf{seq}(r, r') =$



# Well-sequencedness

**A→B : x; A→C : y**

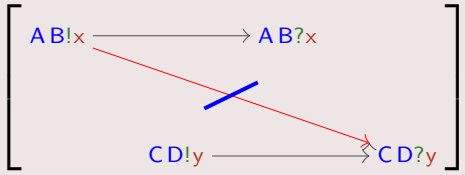



$r =$ [ sbj A  sbj B ]

$r' =$ [ sbj A  sbj B ]

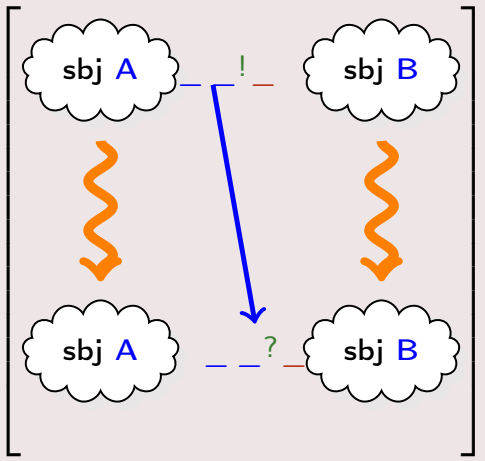
**A→B : x; C→D : y**

No minimal input "from the continuation"




(and no output in the continuation interfering with "left-inputs")

$ws(r, r')$



# Well-branchedness

In a branch $G_1 + G_2$

# Well-branchedness

In a branch $G_1 + G_2$

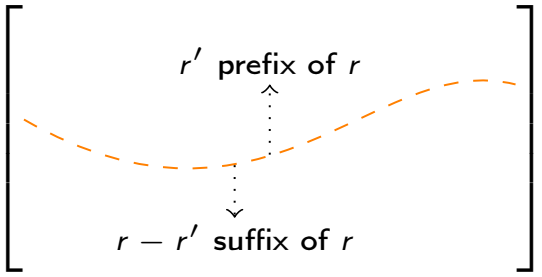
- there should be at most one active participant — non-standard

# Well-branchedness

In a branch $G_1 + G_2$

- there should be at most one active participant — non-standard
- any non-active participant should be passive — standard

Problem: Participants do not necessarily "enter" a choice "immediately"
An idea: find a "common part" of the branches for which participants behaves uniformly in $G_1$ and $G_2$

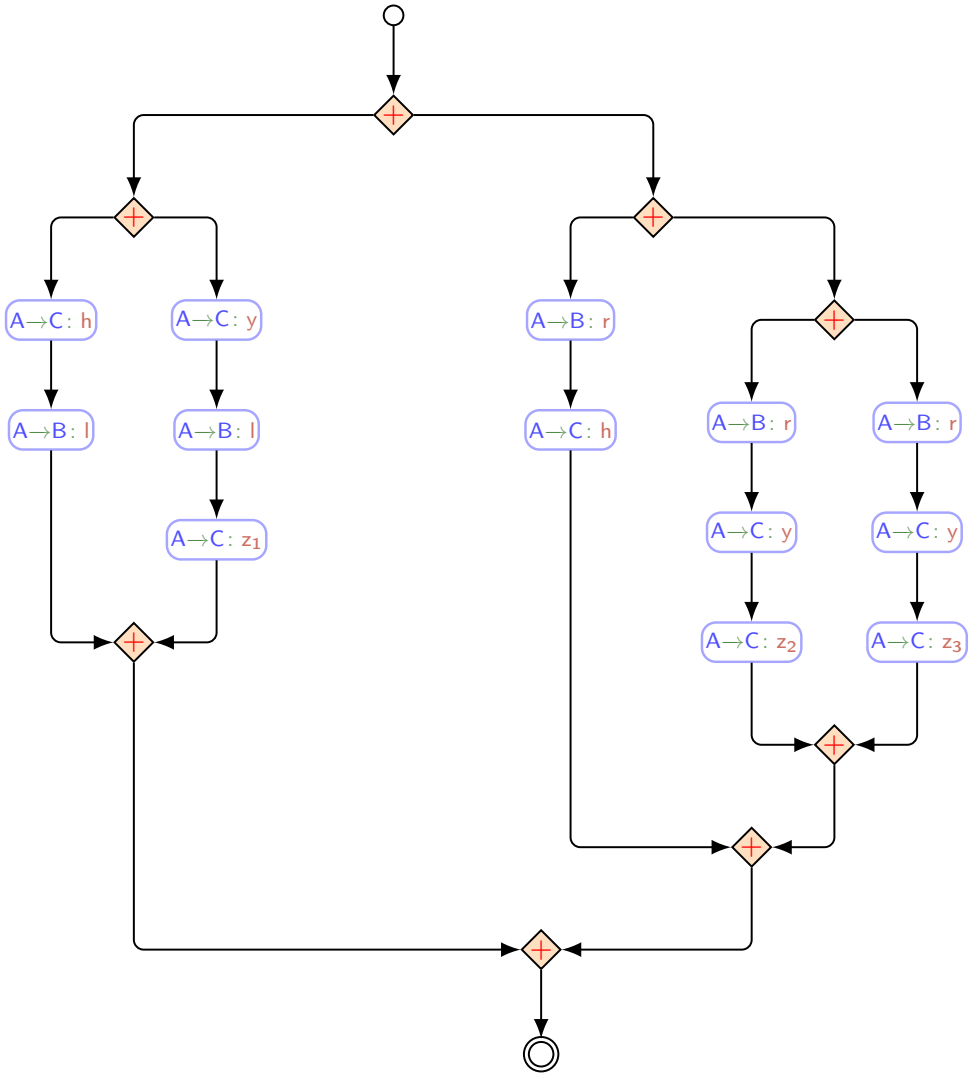
$r =$ 

# Class test

Figure out the graphical structure of the following terms and for each of them say which one is well-branched

- $G_1 = A{\to}B\colon \mathsf{int} \;+\; A{\to}B\colon \mathsf{str}$
- $G_2 = A{\to}B\colon \mathsf{int} \;+\; \circledcirc$
- $G_3 = A{\to}B\colon \mathsf{int} \;+\; A{\to}C\colon \mathsf{str}$
- $G_4 = \left( \begin{array}{l} A{\to}C\colon \mathsf{int};\, A{\to}B\colon \mathsf{bool} \\ \quad + \\ A{\to}C\colon \mathsf{str};\, A{\to}C\colon \mathsf{bool};\, A{\to}B\colon \mathsf{bool} \end{array} \right)$

# $G_{\text{😕}}$: a difficult choice




## $G_{\text{😕}} = G_1 + G_2$ where

$$G_1 = \left( \begin{array}{l} A \to C: h; A \to B: l \\ + \\ A \to C: y; A \to B: l; A \to C: z_1 \end{array} \right)$$

$$G_2 = A \to B: r; A \to C: h + G_{2a} + G_{2b}$$

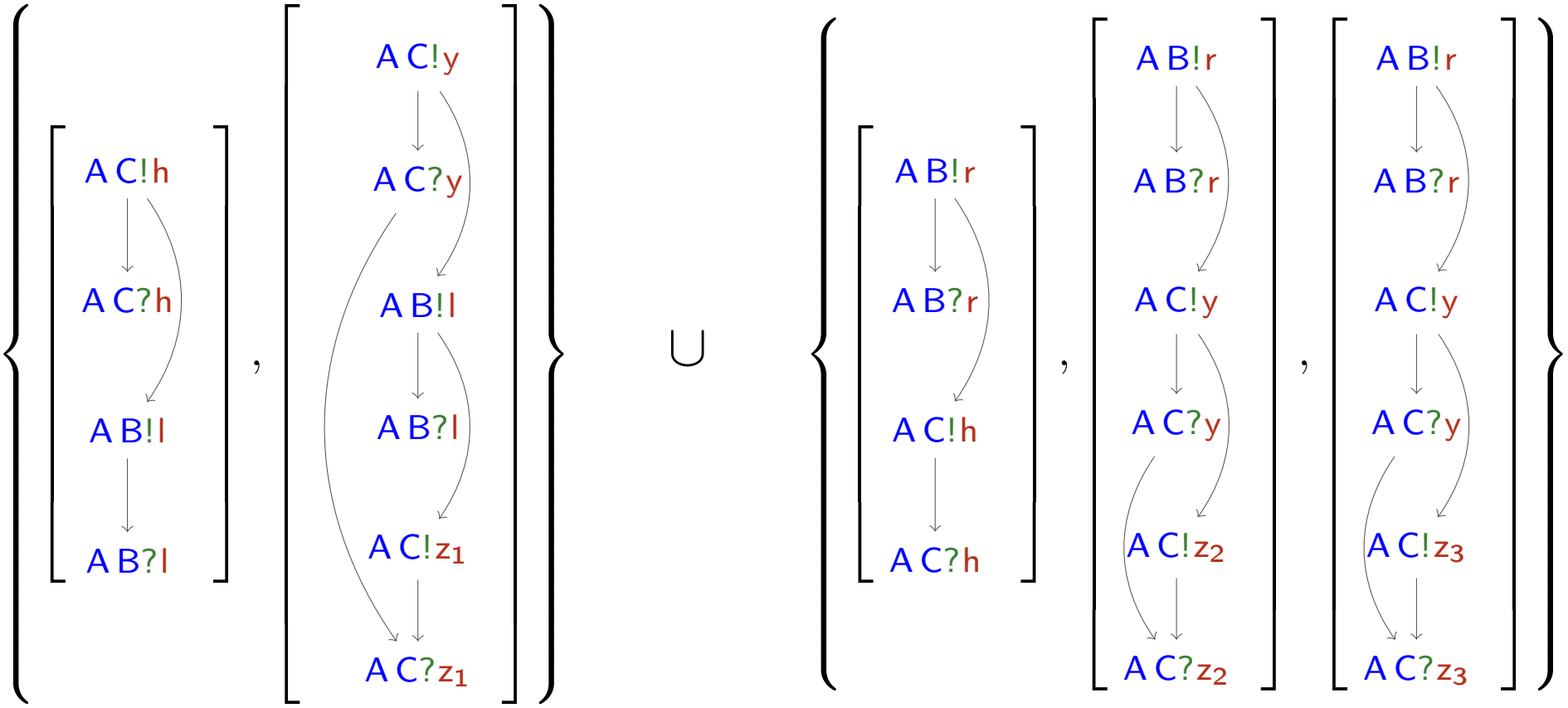
$$G_{2a} = A \to B: r; A \to C: y; A \to C: z_2$$

$$G_{2b} = A \to B: r; A \to C: y; A \to C: z_2$$

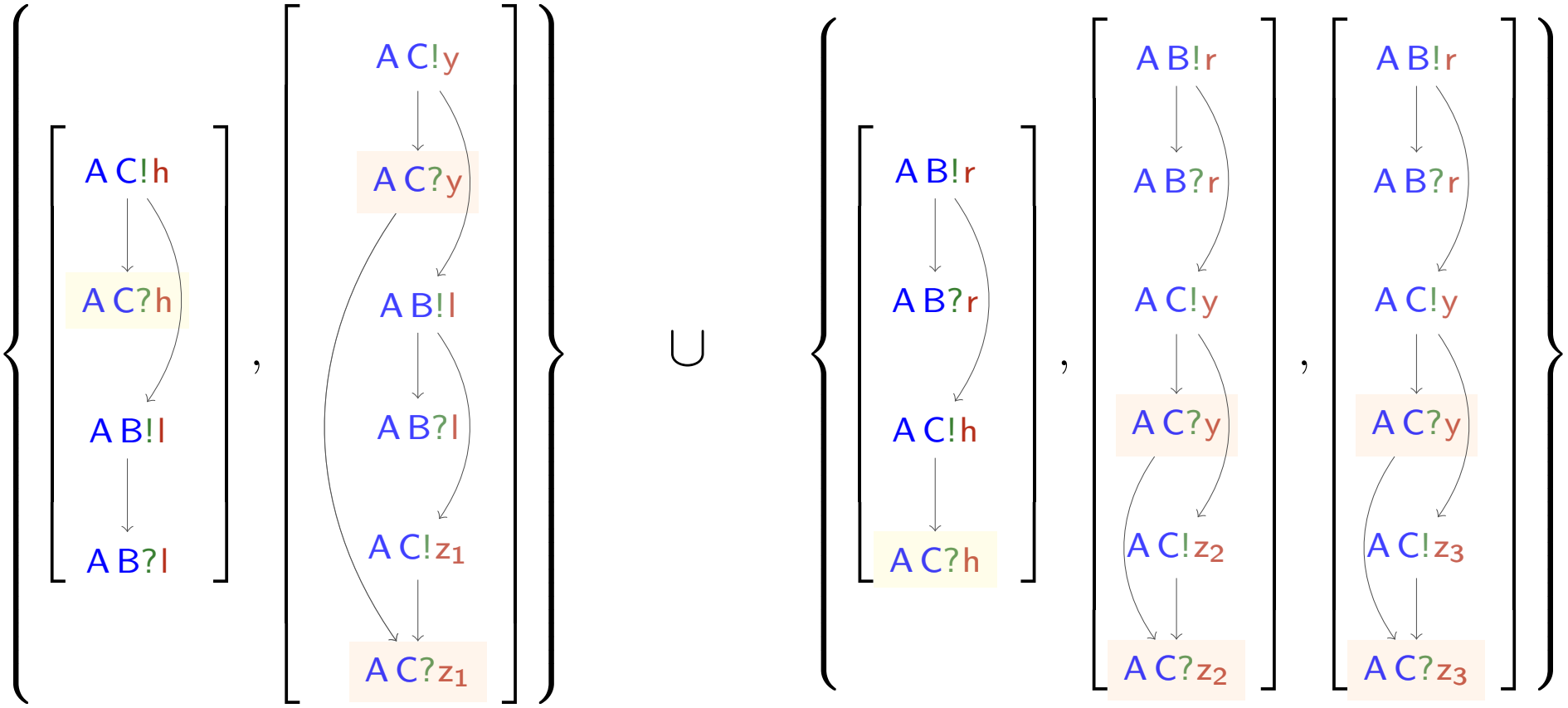
## A chooses ... and

- Whatever B gets, he won't know if A and C exchanged or not h
- If C gets h, he won't know if A and B exchanged l or r

# The pomsets of $G_{\text{😕}}$



# The pomsets of $G_{\text{😕}}$...from C's point of view



# Projecting g-choreographies

# Projecting g-choreographies

## Technicalities

- Functions $\_ \downarrow_{\mathsf{A}}$ yield the projection of g-choreographies on the participant A as triplets $(M, q_0, q_e)$ with $q_0$ and $q_e$ initial and terminal states respectively
- If $\mathsf{G}_1$ and $\mathsf{G}_2$ are sub-terms of G then we "disjointly combine" the states of $\mathsf{G}_1 \downarrow_{\mathsf{A}}$ and $\mathsf{G}_2 \downarrow_{\mathsf{A}}$; for this we define $(M, q_0, q_e) \otimes \mathbf{1}$ which transforms each state $q$ of $M$ in $(q, 1)$ (and likewise for $(M, q_0, q_e) \otimes \mathbf{2}$)

## Base cases

$$\mathsf{G} \downarrow_{\mathsf{A}} = \begin{cases} \rightarrow (q_0) \rightarrow & \text{if } \mathsf{G} = \circledcirc \text{ or } \mathsf{G} = \mathsf{B} \rightarrow \mathsf{C} : \mathsf{m} \\ \rightarrow (q_0) \xrightarrow{\mathsf{A}\,\mathsf{B}!\mathsf{m}} (q_e) \rightarrow & \text{if } \mathsf{G} = \mathsf{A} \rightarrow \mathsf{B} : \mathsf{m}, \text{ with } q_0 \neq q_e \\ \rightarrow (q_0) \xrightarrow{\mathsf{B}\,\mathsf{A}?\mathsf{m}} (q_e) \rightarrow & \text{if } \mathsf{G} = \mathsf{B} \rightarrow \mathsf{A} : \mathsf{m}, \text{ with } q_0 \neq q_e \end{cases}$$

# Projecting g-choreographies

## Technicalities

- Functions $\_ \downarrow_{\mathsf{A}}$ yield the projection of g-choreographies on the participant $\mathsf{A}$ as triplets $(M, q_0, q_e)$ with $q_0$ and $q_e$ initial and terminal states respectively
- If $\mathsf{G}_1$ and $\mathsf{G}_2$ are sub-terms of $\mathsf{G}$ then we "disjointly combine" the states of $\mathsf{G}_1 \downarrow_{\mathsf{A}}$ and $\mathsf{G}_2 \downarrow_{\mathsf{A}}$; for this we define $(M, q_0, q_e) \otimes \mathbf{1}$ which transforms each state $q$ of $M$ in $(q, 1)$ (and likewise for $(M, q_0, q_e) \otimes \mathbf{2}$)

## Sequential composition

$$(\mathsf{G}_1 ; \mathsf{G}_2) \downarrow_{\mathsf{A}} = \left( M_1 \sqcup \left\{ {}^{q_e^1}/_{q_0^2} \right\} M_2, q_0^1, q_e^2 \right)$$

where $(M_1, q_0^1, q_e^1) = \mathsf{G}_1 \downarrow_{\mathsf{A}} \otimes \mathbf{1}$
and $(M_2, q_0^2, q_e^2) = \mathsf{G}_2 \downarrow_{\mathsf{A}} \otimes \mathbf{2}$

# Projecting g-choreographies

## Technicalities

- Functions $\_ \downarrow_{\mathsf{A}}$ yield the projection of g-choreographies on the participant $\mathsf{A}$ as triplets $(M, q_0, q_e)$ with $q_0$ and $q_e$ initial and terminal states respectively
- If $\mathsf{G}_1$ and $\mathsf{G}_2$ are sub-terms of $\mathsf{G}$ then we "disjointly combine" the states of $\mathsf{G}_1 \downarrow_{\mathsf{A}}$ and $\mathsf{G}_2 \downarrow_{\mathsf{A}}$; for this we define $(M, q_0, q_e) \otimes \mathbf{1}$ which transforms each state $q$ of $M$ in $(q, 1)$ (and likewise for $(M, q_0, q_e) \otimes \mathbf{2}$)

## Choice

$$(\mathsf{G}_1 + \mathsf{G}_2) \downarrow_{\mathsf{A}} = \left( \left\{ {}^{q_e^2}/_{q_e^1} \right\} M_1 \sqcup \left\{ {}^{q_0^1}/_{q_0^2} \right\} M_2, q_0^1, q_e^2 \right)$$

where $(M_1, q_0^1, q_e^1) = \mathsf{G}_1 \downarrow_{\mathsf{A}} \otimes \mathbf{1}$
and $(M_2, q_0^2, q_e^2) = \mathsf{G}_2 \downarrow_{\mathsf{A}} \otimes \mathbf{2}$

# Projecting g-choreographies

## Technicalities

- Functions $\_ \downarrow_{\mathsf{A}}$ yield the projection of g-choreographies on the participant $\mathsf{A}$ as triplets $(M, q_0, q_e)$ with $q_0$ and $q_e$ initial and terminal states respectively
- If $\mathsf{G}_1$ and $\mathsf{G}_2$ are sub-terms of $\mathsf{G}$ then we "disjointly combine" the states of $\mathsf{G}_1 \downarrow_{\mathsf{A}}$ and $\mathsf{G}_2 \downarrow_{\mathsf{A}}$; for this we define $(M, q_0, q_e) \otimes \mathbf{1}$ which transforms each state $q$ of $M$ in $(q, 1)$ (and likewise for $(M, q_0, q_e) \otimes \mathbf{2}$)

## Parallel composition

$$(\mathsf{G}_1 \mid \mathsf{G}_2) \downarrow_{\mathsf{A}} = (M_1 \times M_2, (q_0^1, q_0^2), (q_e^1, q_e^2))$$

where $(M_1, q_0^1, q_e^1) = \mathsf{G}_1 \downarrow_{\mathsf{A}} \otimes \mathbf{1}$
and $(M_2, q_0^2, q_e^2) = \mathsf{G}_2 \downarrow_{\mathsf{A}} \otimes \mathbf{2}$

## Exercise

Verify that the projection of the g-choreography on 4 are the CFSM on the same slide.

# References I


[1] Gul Agha. *Actors: A Model of Concurrent Computation in Distributed Systems*.
MIT Press, Cambridge, MA, USA, 1986.

[2] Daniel Brand and Pitro Zafiropulo. On Communicating Finite-State Machines.
*JACM*, 30(2):323–342, 1983.

[3] Pierre-Malo Deniélou and Nobuko Yoshida. Multiparty session types meet communicating automata.
In *ESOP 2012*, pages 194–213, 2012.

[4] Roberto Guanciale and Emilio Tuosto. An abstract semantics of the global view of choreographies.
In *Proceedings 9th Interaction and Concurrency Experience, ICE 2016, Heraklion, Greece, 8-9 June 2016.*, pages 67–82, 2016.

[5] Roberto Guanciale and Emilio Tuosto. Realisability of pomsets.
*Journal of Logic and Algebraic Methods in Programming*, 108:69–89, 2019.

[6] Carl Hewitt, Peter Boehler Bishop, and Richard Steiger. A Universal Modular ACTOR Formalism for Artificial Intelligence.
In Nils J. Nilsson, editor, *Proceedings of the 3rd International Joint Conference on Artificial Intelligence. Standford, CA, USA, August 20-23, 1973*, pages 235–245. William Kaufmann, 1973.

[7] Nickolas Kavantzas, Davide Burdett, Gregory Ritzinger, Tony Fletcher, and Yves Lafon. Web services choreography description language version 1.0.
`http://www.w3.org/TR/2004/WD-ws-cdl-10-20041217`. Working Draft 17 December 2004.

[8] Julien Lange, Emilio Tuosto, and Nobuko Yoshida. From Communicating Machines to Graphical Choreographies.
In *POPL15*, pages 221–232, 2015.

[9] Emilio Tuosto and Roberto Guanciale. Semantics of global view of choreographies.
*Journal of Logic and Algebraic Methods in Programming*, 95:17–40, 2018. Revised and extended version of [4]. available at `http://www.cs.le.ac.uk/people/et52/jlamp-with-proofs.pdf`.