Recap of the previous class

Structural Operational Semantics
- regexp
- bpa

Concurrency as interleaving

Equivalences for concurrency

What about communication?

Let $A_\perp = A \cup \{\perp\}$ $\quad \perp \notin A$ $\quad$ and fix a communication function

$$\_\circ\_ : A_\perp \times A_\perp \longrightarrow A_\perp \quad \begin{cases} \circ \text{ commutative} \\ \circ \text{ associative} \\ \forall a \in A_\perp : a \circ \perp = \perp \circ a = \perp \end{cases}$$

$$(\mathrm{com}_1)\ \frac{x \xrightarrow{a} x' \qquad y \xrightarrow{b} y' \qquad a \circ b \in A}{x \parallel y \xrightarrow{a \circ b} x' \parallel y'} \qquad (\mathrm{com}_2)\ \frac{x \xrightarrow{a} 1 \qquad y \xrightarrow{b} y' \qquad a \circ b \in A}{x \parallel y \xrightarrow{a \circ b} y'}$$

$$(\mathrm{com}_3)\ \frac{x \xrightarrow{a} x' \qquad y \xrightarrow{b} 1 \qquad a \circ b \in A}{x \parallel y \xrightarrow{a \circ b} x'} \qquad (\mathrm{com}_4)\ \frac{x \xrightarrow{a} 1 \qquad y \xrightarrow{b} 1 \qquad a \circ b \in A}{x \parallel y \xrightarrow{a \circ b} 1}$$

Example

Show that $ax + by \parallel cz \xrightarrow{b} x \parallel z$ if $a \circ c = b$, $x \neq 1$, and $y \neq 1$

$$\dfrac{\dfrac{\dfrac{\dfrac{a \in A}{a \xrightarrow{a} 1}\,\text{Act}}{ax \xrightarrow{a} x}\,\text{Seq}_1}{ax + by \xrightarrow{a} x}\,\text{Cho}_1 \qquad \dfrac{\dfrac{c \in A}{c \xrightarrow{c} 1}\,\text{Act}}{cz \xrightarrow{c} z}\,\text{Seq}_2}{ax + by \parallel cz \xrightarrow{b} x \parallel z}\,\text{Com}_1$$

Immmigration course on formal methods

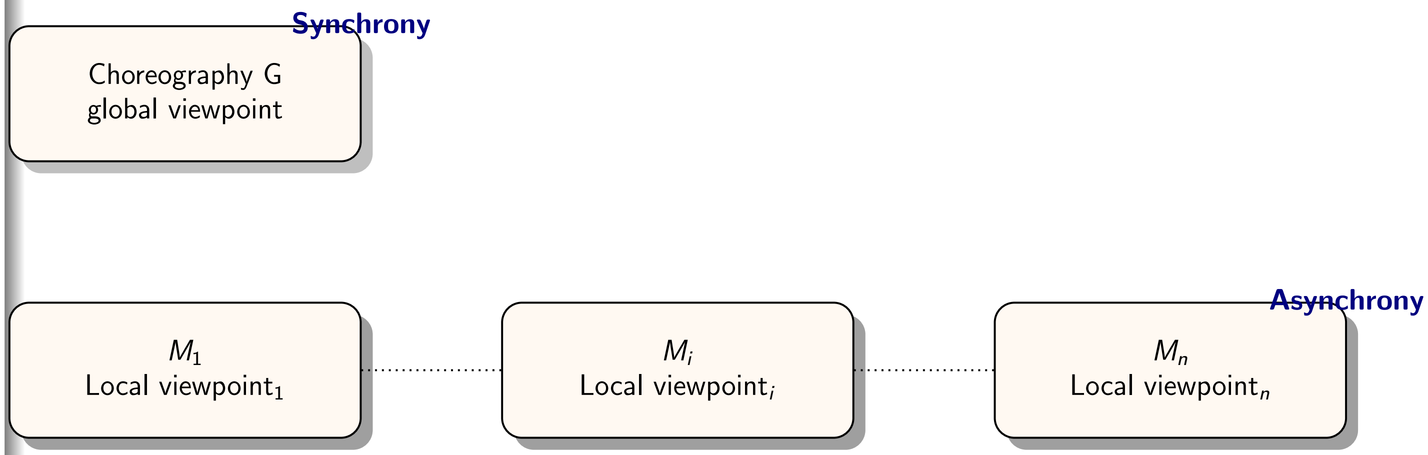
Emilio Tuosto @ GSSI

Academic year 2022/2023

“Top-down”

Quoting W3C

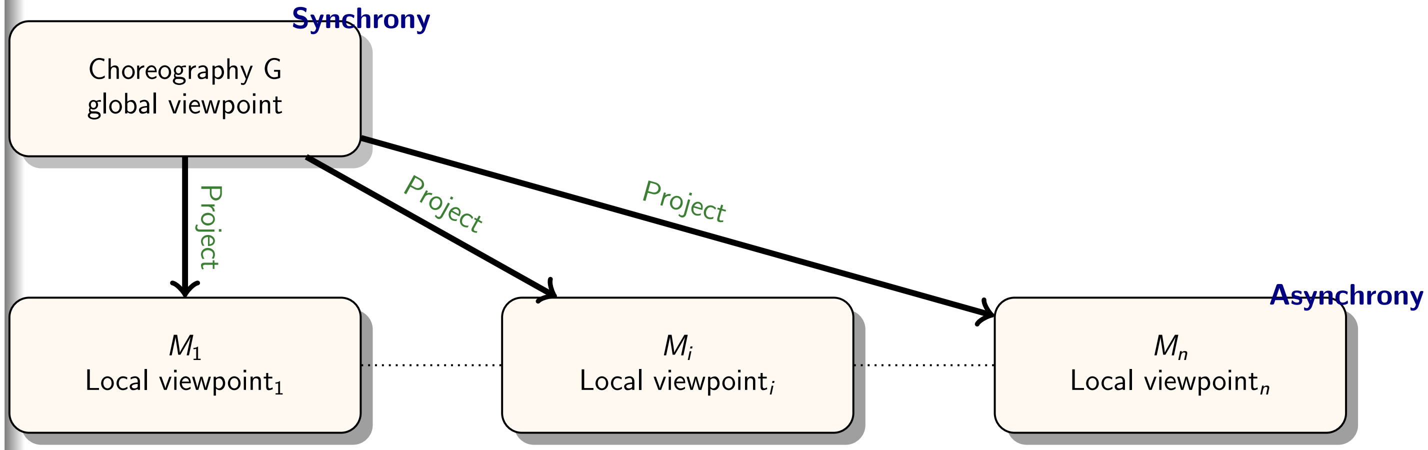
“Using the Web Services Choreography specification, a contract containing a global definition of the common ordering conditions and constraints under which messages are exchanged, is produced that describes, from a global viewpoint [...] observable behaviour of all the parties involved. Each party can 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

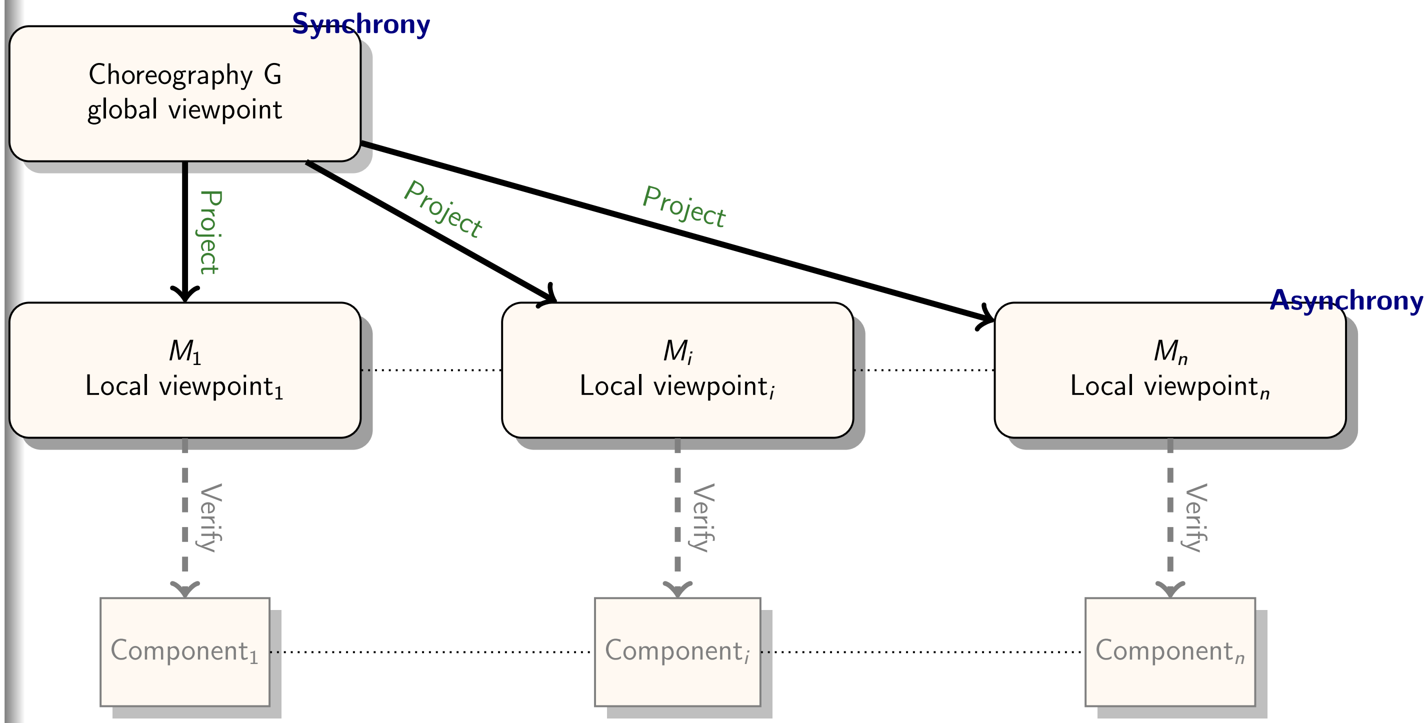
“Using the Web Services Choreography specification, a contract containing a global definition of the common ordering conditions and constraints under which messages are exchanged, is produced that describes, from a global viewpoint [...] observable behaviour of all the parties involved. Each party can 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 [...]”



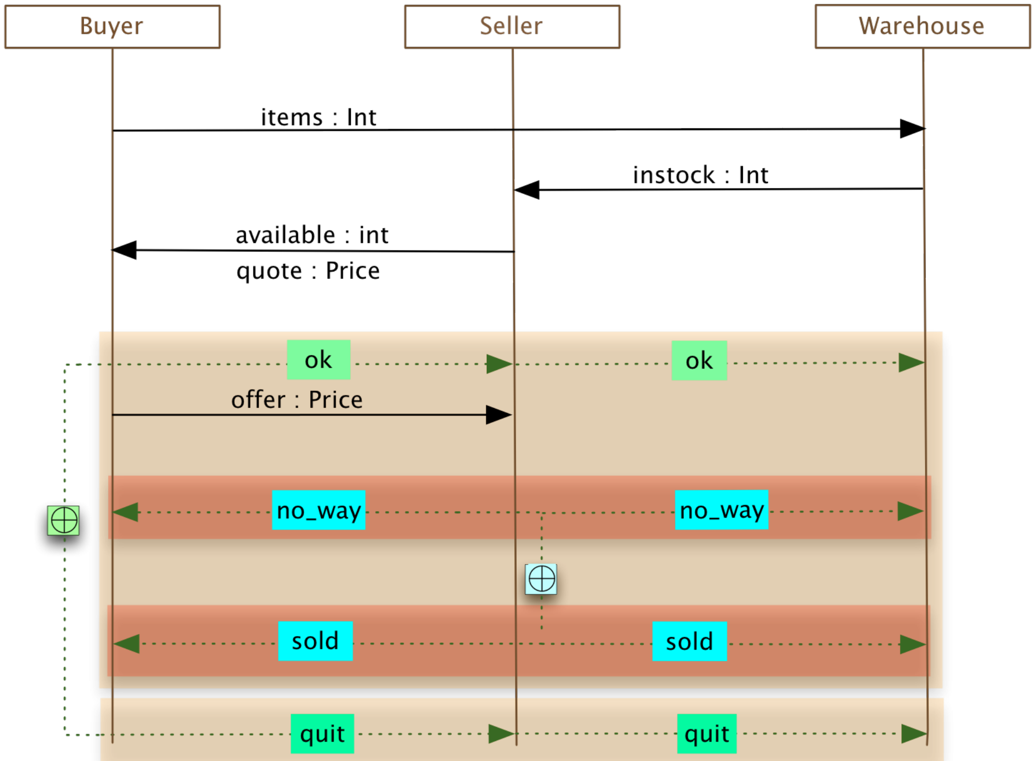
"Top-down"

Quoting W3C

"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 [...]"

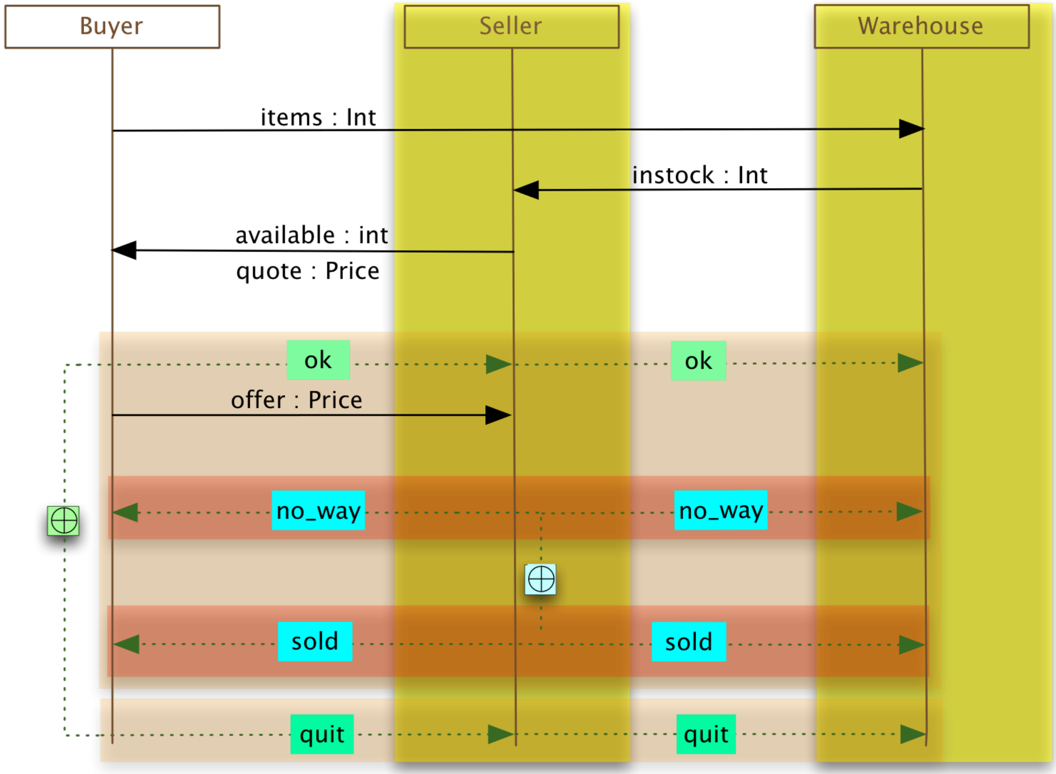


An intuitive account...



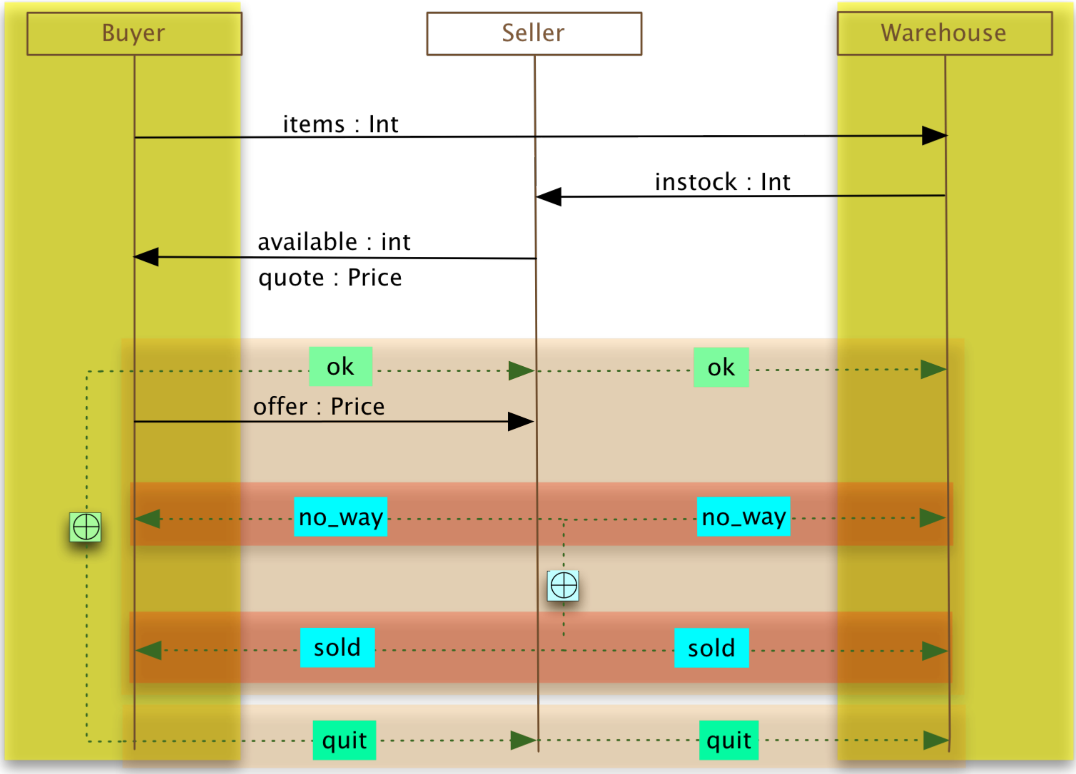
Global viewpoint

An intuitive account...



Projecting on buyer

An intuitive account...



Projecting on seller

Some considerations

Things are more complex:

- recursion/iteration
- not all global viewpoints “make sense”
  (e.g., constraints on values passing)
- interactions are “atomic” at global level, but not at local level
- ...

Desiderata

- progress (graceful termination or no-deadlock)
- no orphan messages
- no unspecified reception
- ...

Global views, intuitively

G-choreographies [Tuosto and Guanciale, 2018]

$$\mathsf{G}, \mathsf{G}' \ ::= \ (\mathsf{o}) \ \Big| \ \mathsf{A}{\rightarrow}\mathsf{B}\colon \mathsf{m} \ \Big| \ \mathsf{G} \parallel \mathsf{G}' \ \Big| \ \mathsf{G}; \mathsf{G}' \ \Big| \ \mathsf{G} + \mathsf{G}' \ \Big| \ \mathsf{G}^*$$

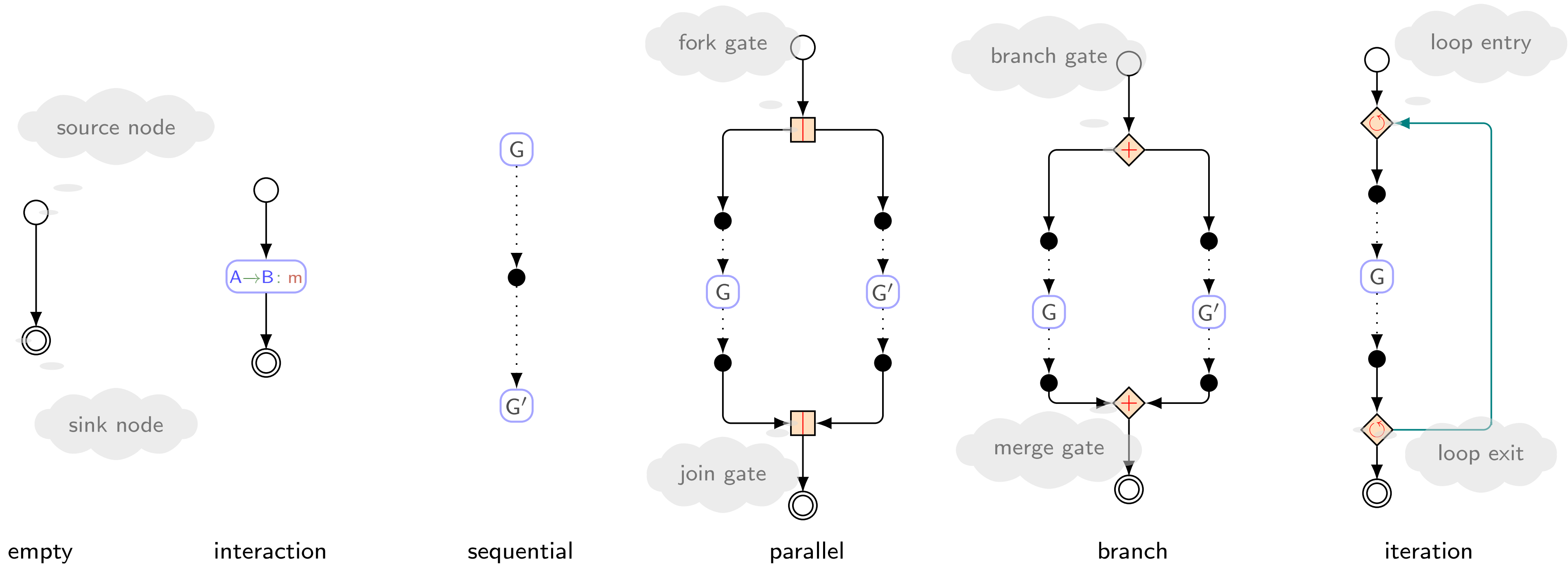
i.e., regular expressions (on an alphabet of interactions) with parallel composition
however, the semantics should account for asynchrony

Global views, intuitively

G-choreographies [Tuosto and Guanciale, 2018]

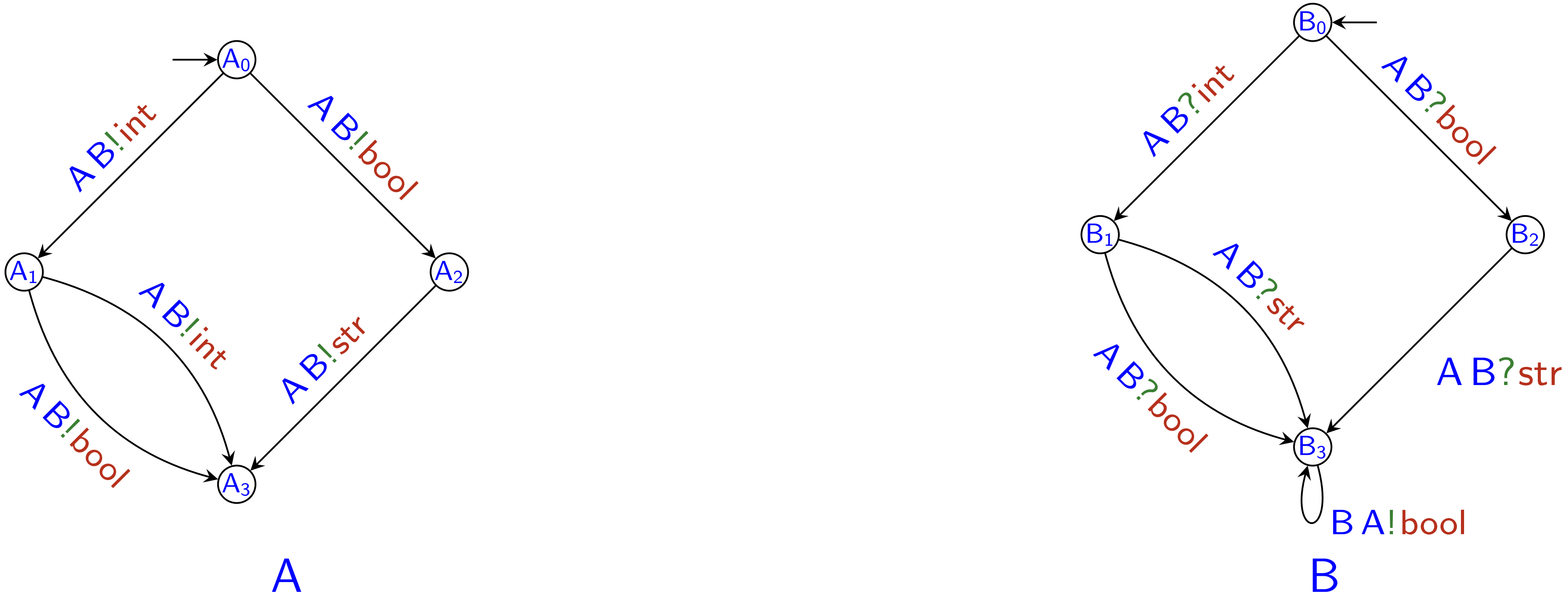
$$\mathsf{G}, \mathsf{G}' \ ::= \ (\mathsf{o}) \ \mid \ \mathsf{A} \to \mathsf{B} : \mathsf{m} \ \mid \ \mathsf{G} \parallel \mathsf{G}' \ \mid \ \mathsf{G}; \mathsf{G}' \ \mid \ \mathsf{G} + \mathsf{G}' \ \mid \ \mathsf{G}^*$$

i.e., regular expressions (on an alphabet of interactions) with parallel composition
however, the semantics should account for asynchrony



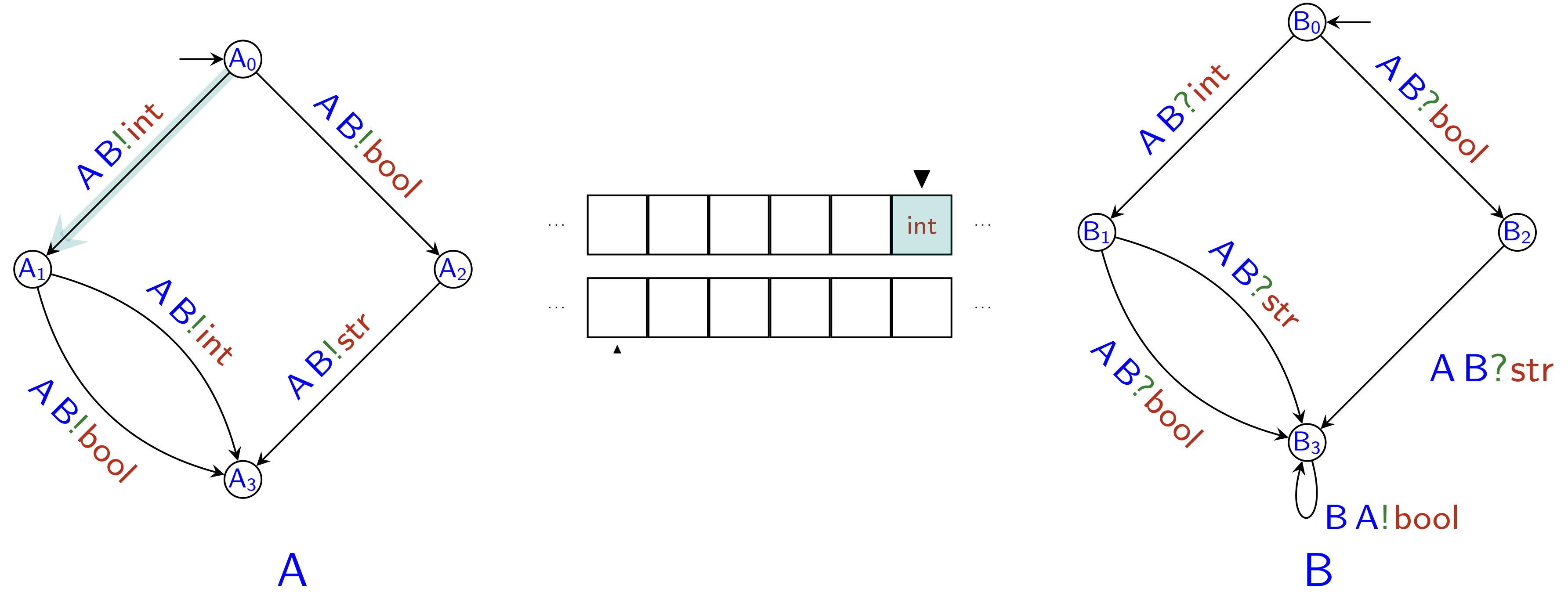
Local views, intuitively

Communicating systems [Brand and Zafiropulo, 1983]



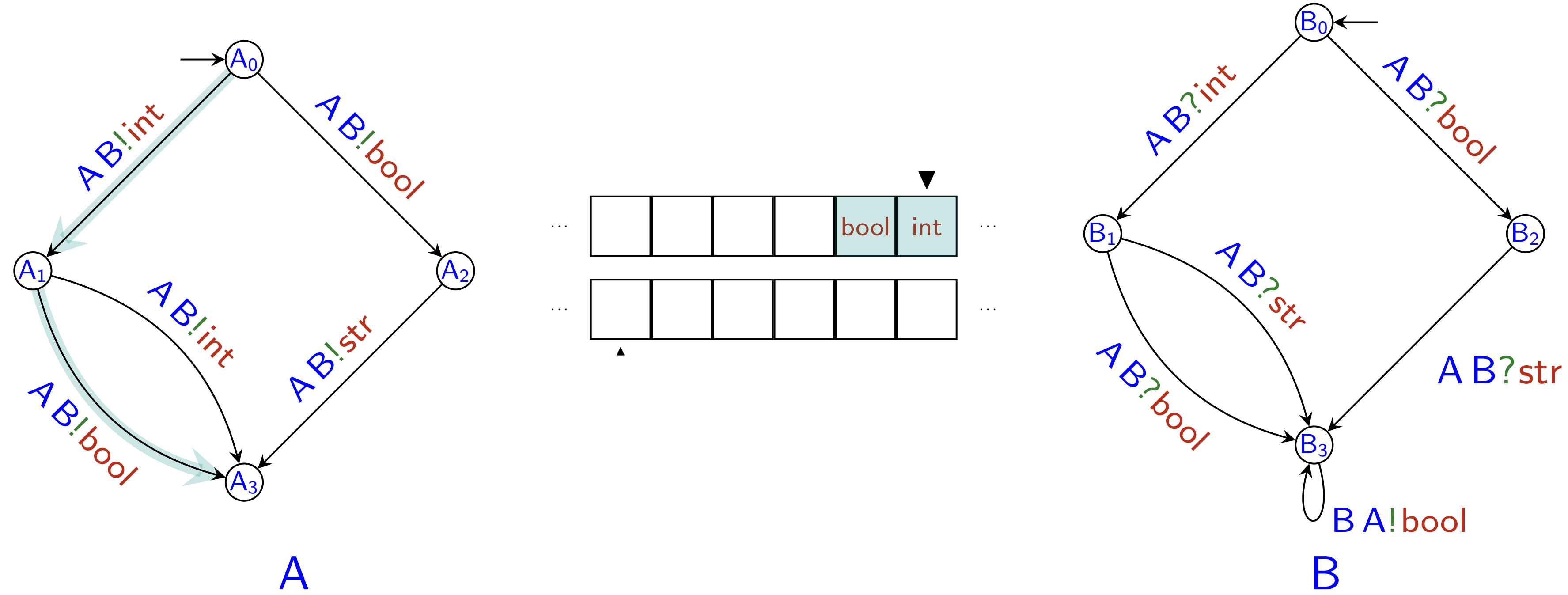
Local views, intuitively

Communicating systems [Brand and Zafiropulo, 1983]



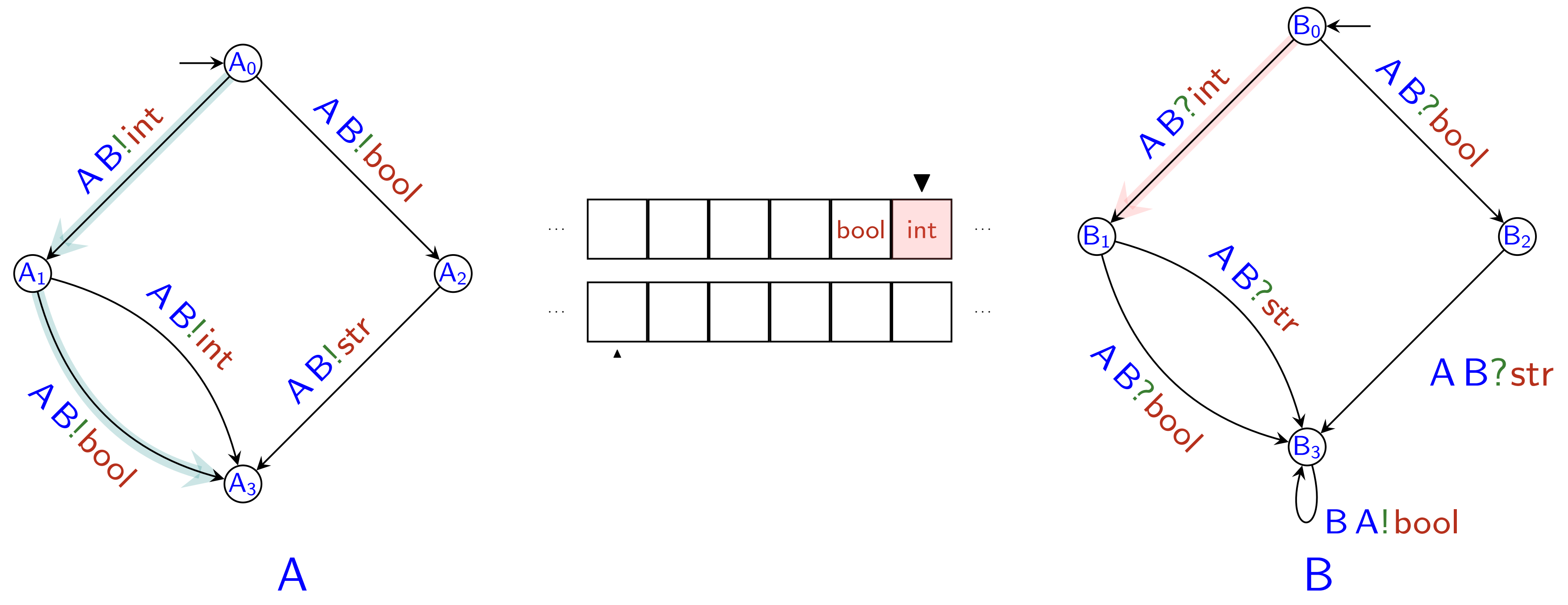
Local views, intuitively

Communicating systems [Brand and Zafiropulo, 1983]



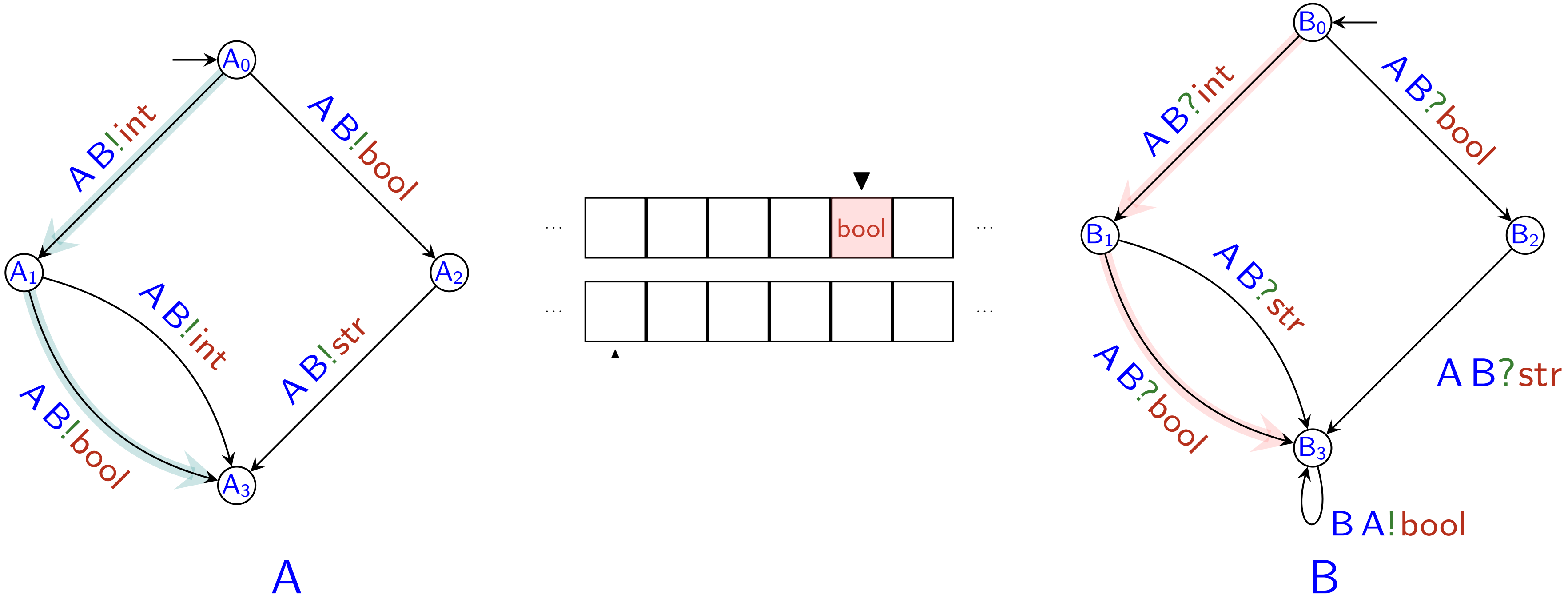
Local views, intuitively

Communicating systems [Brand and Zafiropulo, 1983]



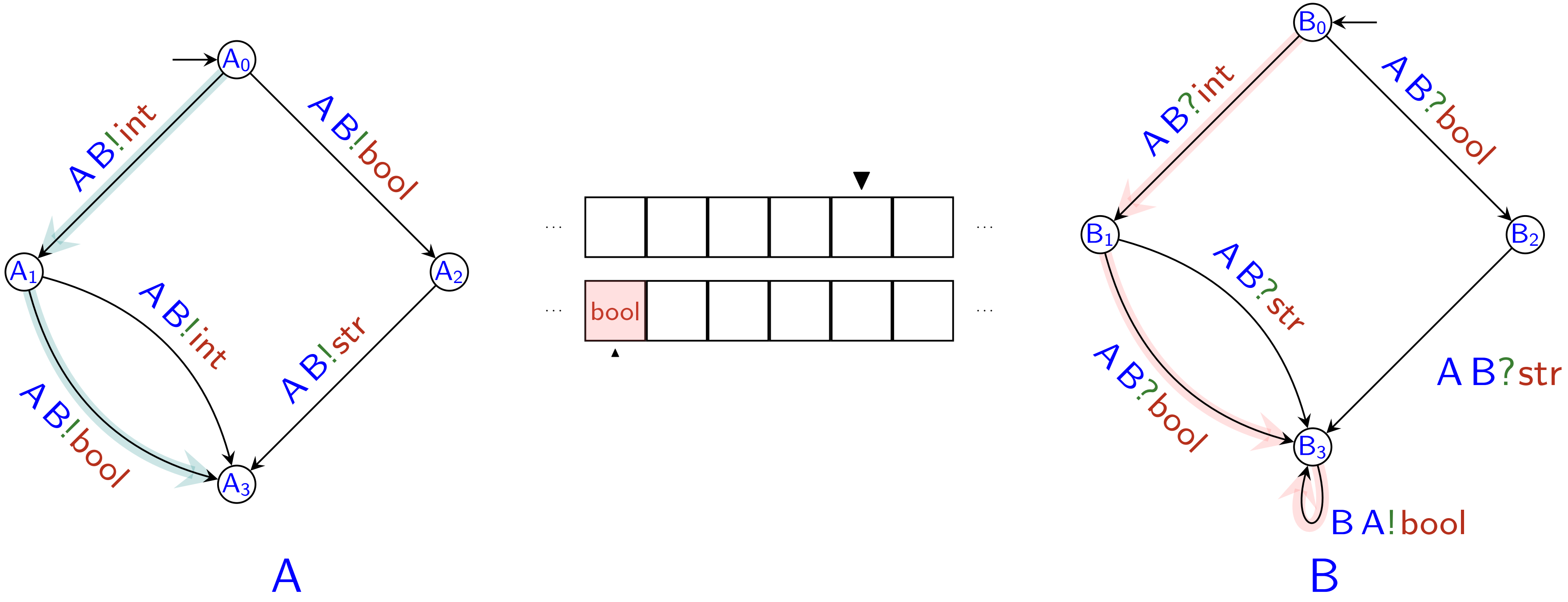
Local views, intuitively

Communicating systems [Brand and Zafiropulo, 1983]



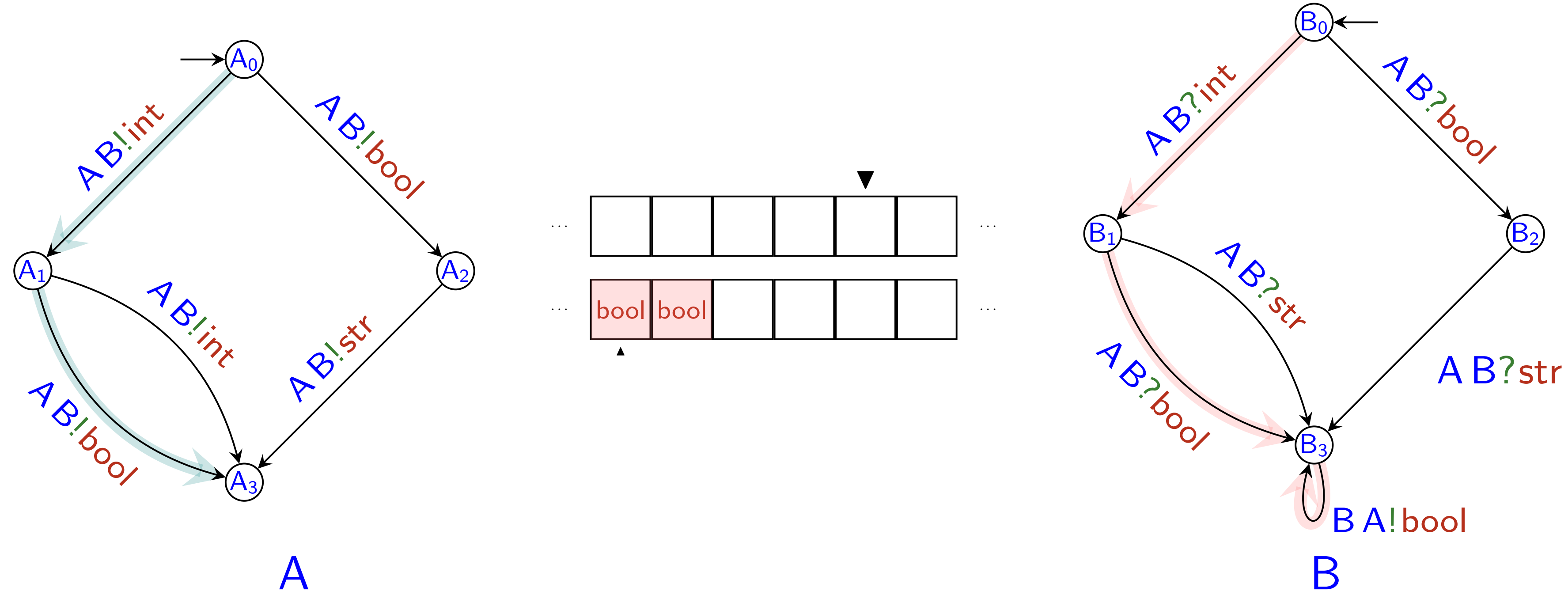
Local views, intuitively

Communicating systems [Brand and Zafiropulo, 1983]



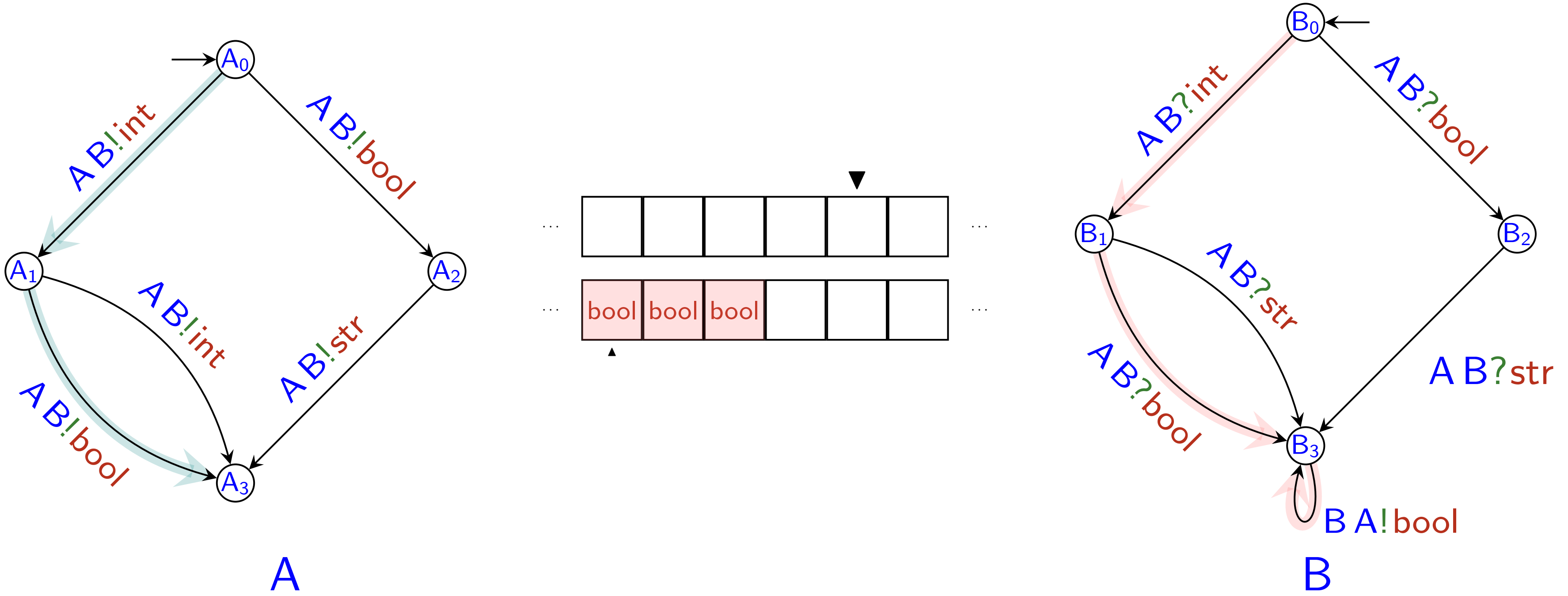
Local views, intuitively

Communicating systems [Brand and Zafiropulo, 1983]



Local views, intuitively

Communicating systems [Brand and Zafiropulo, 1983]



Formally,

- a communicating finite-state machine (CFSM) is an FSA whose transitions are input/output actions executed by a single participant and whose states are all accepting
- a communicating system is a finite map assigning to a participant A a CFSM executing communications of A

Well-formedness, intuitively

To G or not to G?

Ehm...in a distributed choice $G_1 + G_2 + \cdots$

- there should be one active participant
- any non-active participant should be passive

Well-formedness, intuitively

To G or not to G?

Ehm...in a distributed choice $G_1 + G_2 + \cdots$

- there should be one active participant
- any non-active participant should be passive

Def. A is active when it locally decides which branch to take in a choice

Def. B is passive when

- either B behaves uniformly in each branch
- or B "unambiguously understands" which branch A opted for through the information received on each branch

Well-formedness, intuitively

To G or not to G?

Ehm...in a distributed choice $G_1 + G_2 + \cdots$

- there should be one active participant
- any non-active participant should be passive

Def. A is active when it locally decides which branch to take in a choice

Def. B is passive when

- either B behaves uniformly in each branch
- or B "unambiguously understands" which branch A opted for through the information received on each branch

Well-branchedness

When the above holds true for each choice, the choreography is well-branched. This enables correctness-by-design.

Class test

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

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

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 G_1 and 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

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

Projecting g-choreographies

Technicalities

- Functions $\_\downarrow_{\mathsf{A}}$ yield the projection of g-choreographies on the participant A as triplets (M, q_0, q_e) with q_0 and q_e initial and terminal states respectively
- If G_1 and 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 $(M, q_0, q_e) \otimes \mathbf{2}$)

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 $\_\downarrow_{A}$ 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 G_1 and G_2 are sub-terms of G then we "disjointly combine" the states of $G_1 \downarrow_{A}$ and $G_2 \downarrow_{A}$; 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

$$(G_1 + G_2) \downarrow_{A} = \left(\left\{ {}^{q_e^2}/_{q_e^1} \right\} M_1 \sqcup \left\{ {}^{q_0^1}/_{q_0^2} \right\} M_2, q_0^1, q_e^2 \right)$$

where $(M_1, q_0^1, q_e^1) = G_1 \downarrow_{A} \otimes \mathbf{1}$
and $(M_2, q_0^2, q_e^2) = G_2 \downarrow_{A} \otimes \mathbf{2}$

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 G_1 and 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 $(M, q_0, q_e) \otimes \mathbf{2}$)

Parallel composition

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

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

Brand, D. and Zafiropulo, P. (1983).
On Communicating Finite-State Machines.
JACM, 30(2):323–342.

Guanciale, R. and Tuosto, E. (2016).
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.

Tuosto, E. and Guanciale, R. (2018).
Semantics of global view of choreographies.
Journal of Logic and Algebraic Methods in Programming, 95:17–40.
Revised and extended version of [Guanciale and Tuosto, 2016].