Definitions and proofs of week 2 revisited

Causally ordered MSCs An MSC is causally ordered if all the messages sent to the same process are received in an order which is consistent with the causal ordering of the corresponding send events. More formally, for an MSC $M = (\mathcal{E}, \rightarrow, \lhd, \lambda)$ we define an additional binary relation $\blacktriangleleft_M \subseteq \mathcal{E} \times \mathcal{E}$ that represents a constraint under the causal ordering semantics. In particular, given two receive events f_1 and f_2, we have that $f_1 \blacktriangleleft_M f_2$ if both the following hold:

- $\lambda(f_1) \in \mathit{Rec}(\_, q, \_)$, $\lambda(f_2) \in \mathit{Rec}(\_, q, \_)$
- $e_1 \lhd f_1$ and $e_2 \lhd f_2$ for some $e_1, e_2 \in \mathcal{E}$, such that $e_1 \leq_M e_2$.

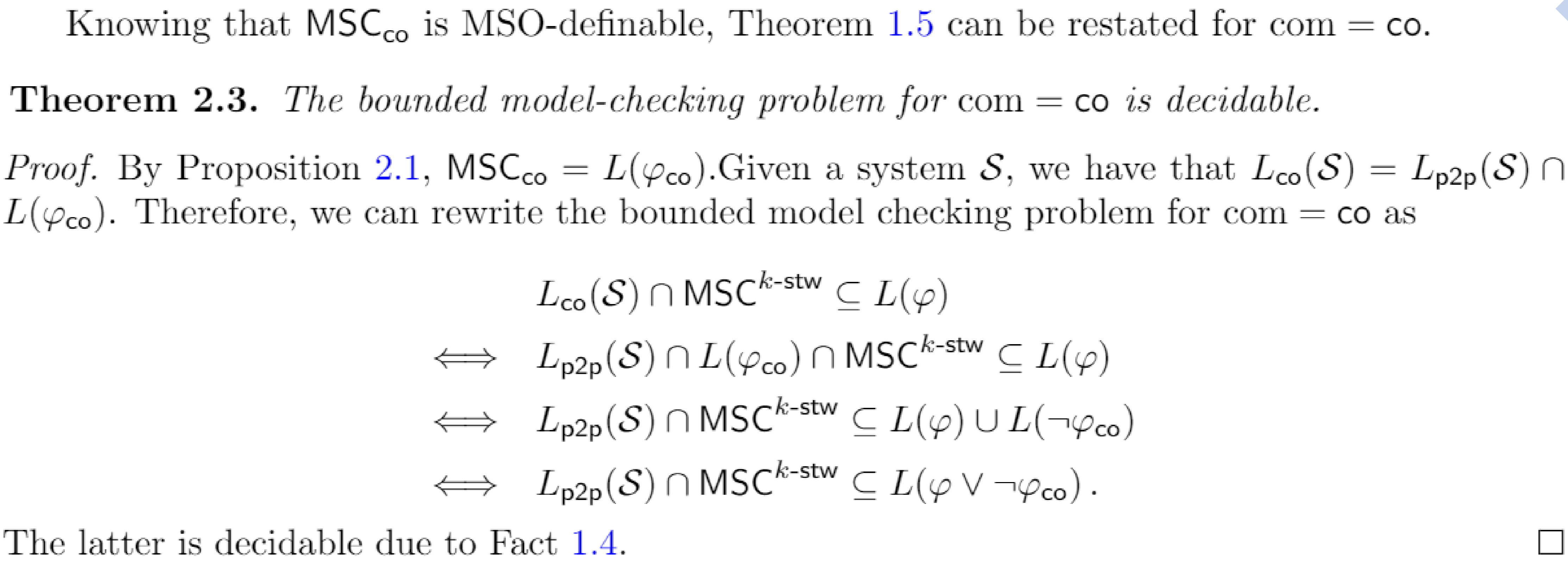
We let $\lessdot_M = (\rightarrow \cup \lhd \cup \blacktriangleleft_M)^*$. Note that $\leq_M \subseteq \lessdot_M$. We call $M \in \mathsf{MSC}$ a *causally ordered (CO) MSC* if $\lessdot_M$ is a partial order. The set of causally ordered MSCs $M \in \mathsf{MSC}$ is denoted by $\mathsf{MSC}_{\mathsf{co}}$.

Proposition 2.1. The set $\mathsf{MSC}_{\mathsf{co}}$ of causally odered MSCs is MSO-definable.

Proof. The set of causally ordered MSCs can be defined using the MSO formula

$$\varphi_{\mathsf{co}} = \neg\exists x.\exists y. \left(\bigvee_{\substack{q \in \mathbb{P} \\ a,b \in Send(\_,q,\_)}} \lambda(x) = a \ \wedge \ \lambda(y) = b \ \wedge \ x \leq y \ \wedge \ \exists x'.\exists y'. \begin{pmatrix} x \lhd x' & \wedge \\ y \lhd y' & \wedge \\ y' \rightarrow^{+} x' & \end{pmatrix} \right)$$

The property φ_{co} says that there cannot be two send events x and y, with the same recipient, such that $x \leq y$ and their corresponding receive events x' and y' happen in the opposite order, i.e. $y' \rightarrow^{+} x'$. The set $\mathsf{MSC}_{\mathsf{co}}$ of causally ordered MSCs is therefore MSO-definable as $\mathsf{MSC}_{\mathsf{co}} = L(\varphi_{\mathsf{co}})$. □



Knowing that $\mathsf{MSC}_{\mathsf{co}}$ is MSO-definable, Theorem 1.5 can be restated for $\mathrm{com} = \mathsf{co}$.

Theorem 2.3. *The bounded model-checking problem for* $\mathrm{com} = \mathsf{co}$ *is decidable.*

Proof. By Proposition 2.1, $\mathsf{MSC}_{\mathsf{co}} = L(\varphi_{\mathsf{co}})$.Given a system $\mathcal{S}$, we have that $L_{\mathsf{co}}(\mathcal{S}) = L_{\mathsf{p2p}}(\mathcal{S}) \cap L(\varphi_{\mathsf{co}})$. Therefore, we can rewrite the bounded model checking problem for $\mathrm{com} = \mathsf{co}$ as

$$\begin{aligned} & L_{\mathsf{co}}(\mathcal{S}) \cap \mathsf{MSC}^{k\text{-}\mathsf{stw}} \subseteq L(\varphi) \\ \iff\quad & L_{\mathsf{p2p}}(\mathcal{S}) \cap L(\varphi_{\mathsf{co}}) \cap \mathsf{MSC}^{k\text{-}\mathsf{stw}} \subseteq L(\varphi) \\ \iff\quad & L_{\mathsf{p2p}}(\mathcal{S}) \cap \mathsf{MSC}^{k\text{-}\mathsf{stw}} \subseteq L(\varphi) \cup L(\neg\varphi_{\mathsf{co}}) \\ \iff\quad & L_{\mathsf{p2p}}(\mathcal{S}) \cap \mathsf{MSC}^{k\text{-}\mathsf{stw}} \subseteq L(\varphi \vee \neg\varphi_{\mathsf{co}})\,. \end{aligned}$$

The latter is decidable due to Fact 1.4. □

Decidability of bounded
model checking for p2p

New stuff

Lemma 2.1. *Every prefix of a causally ordered MSC is a causally ordered MSC.*

Proof. Let $M = (\mathcal{E}, \rightarrow, \lhd, \lambda) \in \mathsf{MSC}_{\mathsf{co}}$ and let $M_0 = (\mathcal{E}_0, \rightarrow_0, \lhd_0, \lambda_0)$ be a prefix of M. By contradiction, suppose that M_0 is not a causally ordered MSC. Then, there are distinct $e, f \in \mathcal{E}_0$ such that $e \lessdot_{M_0} f$ and $f \lessdot_{M_0} e$, with $\lessdot_{M_0} = (\rightarrow_0 \cup \lhd_0 \cup \blacktriangleleft_{M_0})^*$. As $\mathcal{E}_0 \subseteq \mathcal{E}$, we have that $\rightarrow_0 \subseteq \rightarrow$, $\lhd_0 \subseteq \lhd$, and $\blacktriangleleft_{M_0} \subseteq \blacktriangleleft_M$. Finally, we have that $\lessdot_{M_0} \subseteq \lessdot_M$ and M cannot be a causally ordered MSC, which is a contradiction. □

Lemma 1.2 can be easily extendend to $\mathrm{com} = \mathsf{co}$.

Lemma 2.2. *For all* $\mathrm{com} \in \{\mathsf{p2p}, \mathsf{mb}, \mathsf{co}\}$*,* $L_{\mathrm{com}}(\mathcal{S})$ *is prefix-closed:* $\mathit{Pref}(L_{\mathrm{com}}(\mathcal{S})) \subseteq L_{\mathrm{com}}(\mathcal{S})$.

Proof. Follows from Lemma 2.1. □

Theorem 2.6. *The following problem is undecidable: Given finite sets $\mathbb{P}$ and $\mathbb{M}$ as well as a communicating system $\mathcal{S}$, is every MSC in $L_{\mathsf{co}}(\mathcal{S})$ weakly synchronous?*

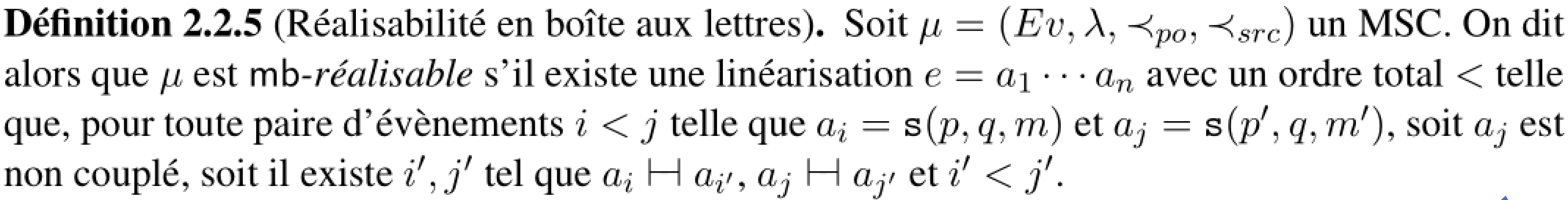
Proof. The proof is essentially identical to the p2p case. We do the same reduction from the Post correspondence problem. Recall from the proof of Theorem 1.10 that we consider a system $\mathcal{S}$ with four machines (P1, P2, V1, V2), where we have unidirectional communication channels from provers to verifiers. In particular notice that all the possible behaviours of $\mathcal{S}$ are causally ordered, i.e. $L_{\mathsf{p2p}}(\mathcal{S}) \subseteq \mathsf{MSC}_{\mathsf{co}}$; according to how we built our system $\mathcal{S}$, it is impossible to have a pair of causally-related send events of P1 and P2[1], hence the causal ordering binary relation $\blacktriangleleft_M$ will be empty for any $M \in L_{\mathsf{p2p}}(\mathcal{S})$ (i.e. causal ordering is already ensured by any possible p2p behaviour of $\mathcal{S}$). The rest of the proof is identical to the p2p case. □

[1] Notice that there is no channel between P1 and P2, and we only have unidirectional communication channels from provers to verifiers.

Proposition 2.3. The set of weakly synchronous causally ordered MSCs has unbounded special tree-width.

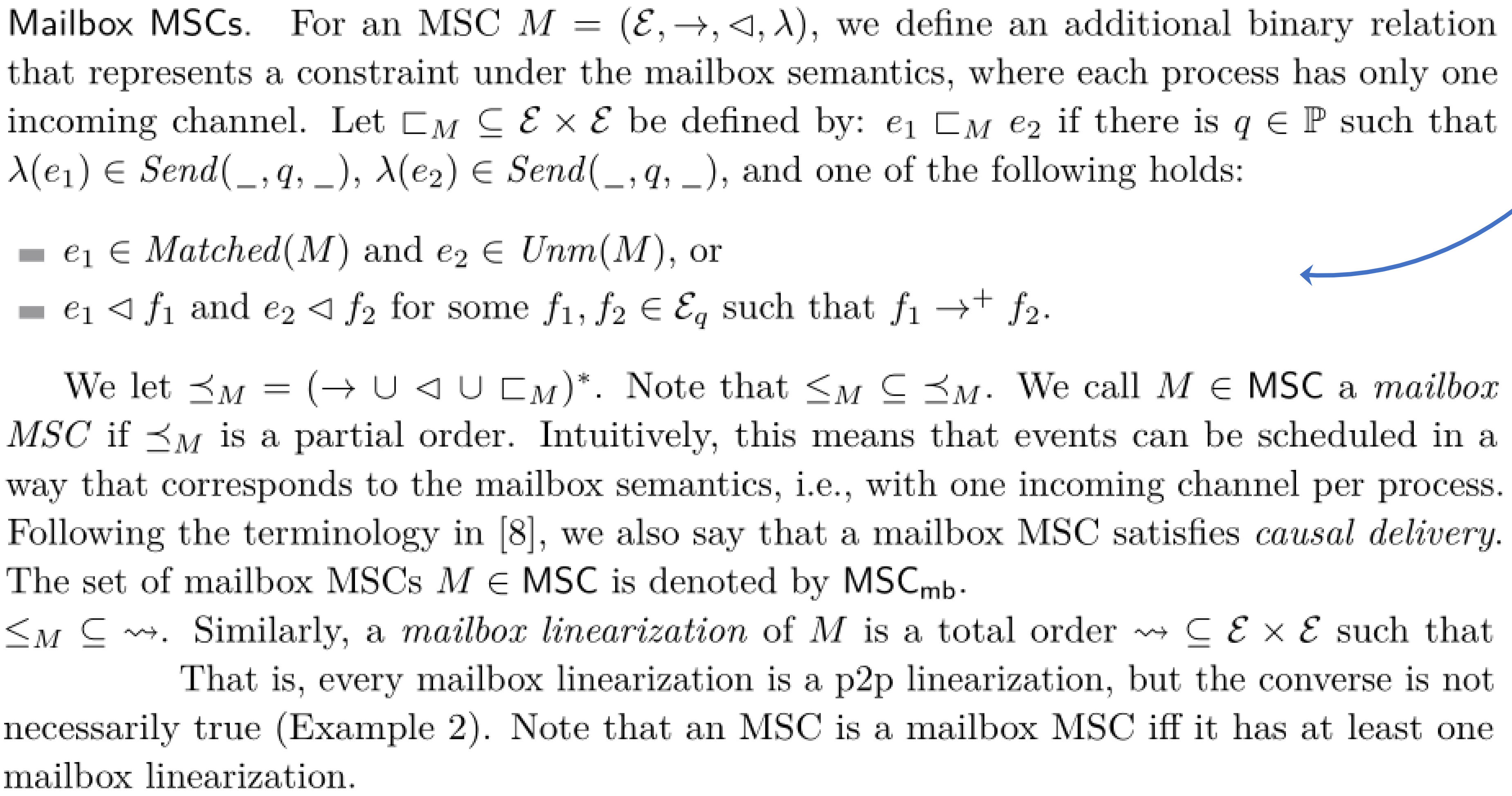
Proof. Suppose that the set of weakly synchronous causally ordered MSCs is STW-bounded. By Proposition 2.2 and Theorem 2.5, we have that the syncronicity problem for the class of weakly synchronous causally ordered MSCs would be decidable. This is a contradiction, since Theorem 2.6 states that this problem is undecidable. □

Doubts



Définition 2.2.5 (Réalisabilité en boîte aux lettres)**.** Soit $\mu = (Ev, \lambda, \prec_{po}, \prec_{src})$ un MSC. On dit alors que μ est mb-*réalisable* s'il existe une linéarisation $e = a_1 \cdots a_n$ avec un ordre total $<$ telle que, pour toute paire d'évènements $i < j$ telle que $a_i = \mathtt{s}(p, q, m)$ et $a_j = \mathtt{s}(p', q, m')$, soit a_j est non couplé, soit il existe i', j' tel que $a_i \vdash\!\dashv a_{i'}$, $a_j \vdash\!\dashv a_{j'}$ et $i' < j'$.

=



Mailbox MSCs. For an MSC $M = (\mathcal{E}, \rightarrow, \lhd, \lambda)$, we define an additional binary relation that represents a constraint under the mailbox semantics, where each process has only one incoming channel. Let $\sqsubset_M \subseteq \mathcal{E} \times \mathcal{E}$ be defined by: $e_1 \sqsubset_M e_2$ if there is $q \in \mathbb{P}$ such that $\lambda(e_1) \in \mathit{Send}(\_, q, \_)$, $\lambda(e_2) \in \mathit{Send}(\_, q, \_)$, and one of the following holds:

- $e_1 \in \mathit{Matched}(M)$ and $e_2 \in \mathit{Unm}(M)$, or
- $e_1 \lhd f_1$ and $e_2 \lhd f_2$ for some $f_1, f_2 \in \mathcal{E}_q$ such that $f_1 \rightarrow^+ f_2$.

We let $\preceq_M = (\rightarrow \cup \lhd \cup \sqsubset_M)^*$. Note that $\leq_M \subseteq \preceq_M$. We call $M \in \mathsf{MSC}$ a *mailbox MSC* if $\preceq_M$ is a partial order. Intuitively, this means that events can be scheduled in a way that corresponds to the mailbox semantics, i.e., with one incoming channel per process. Following the terminology in [8], we also say that a mailbox MSC satisfies *causal delivery*. The set of mailbox MSCs $M \in \mathsf{MSC}$ is denoted by $\mathsf{MSC}_{\mathsf{mb}}$.

$\leq_M \subseteq \rightsquigarrow$. Similarly, a *mailbox linearization* of M is a total order $\rightsquigarrow \subseteq \mathcal{E} \times \mathcal{E}$ such that

That is, every mailbox linearization is a p2p linearization, but the converse is not necessarily true (Example 2). Note that an MSC is a mailbox MSC iff it has at least one mailbox linearization.

Définition 2.3.3 (Exécution causalement ordonnée [Charron-Bost et al., 1996]). Soit un MSC $\mu = (Ev, \lambda, \prec_{po}, \prec_{src})$, μ admet une exécution causalement ordonnée si, pour deux messages $m, m' \in \mathbb{V}$, tels que $\mathbf{m} = \{s, r\}$ et $\mathbf{m}' = \{s', r'\}$:

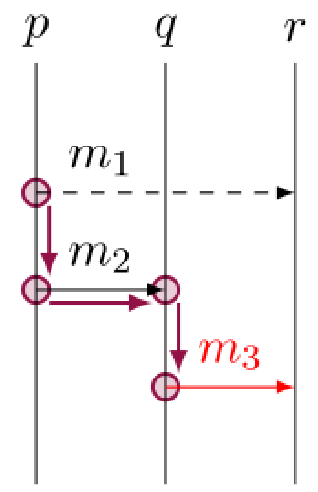
$$(\mathsf{proc}_{\mathsf{R}}(\mathbf{m}) = \mathsf{proc}_{\mathsf{R}}(\mathbf{m}')) \wedge (s \prec s') \implies r \prec r' \tag{2.2}$$

≠

Définition 2.3.6 (Livraison causale [Bouajjani et al., 2018a]). Soit $\mu = (Ev, \lambda, \prec_{po}, \prec_{src})$ un MSC, μ vérifie la livraison causale si, pour deux messages $m, m' \in \mathbb{V}$, tels que $\mathbf{m} = \{s, r\}$ et $s' \in \mathbf{m}'$:

$$(s \prec s') \wedge (\mathsf{proc}_{\mathsf{R}}(\mathbf{m}) = \mathsf{proc}_{\mathsf{R}}(\mathbf{m}')) \implies (\mathbf{m}' = \{s'\}) \vee (\mathbf{m}' = \{s', r'\} \wedge (r' \not\prec r)) \tag{2.4}$$

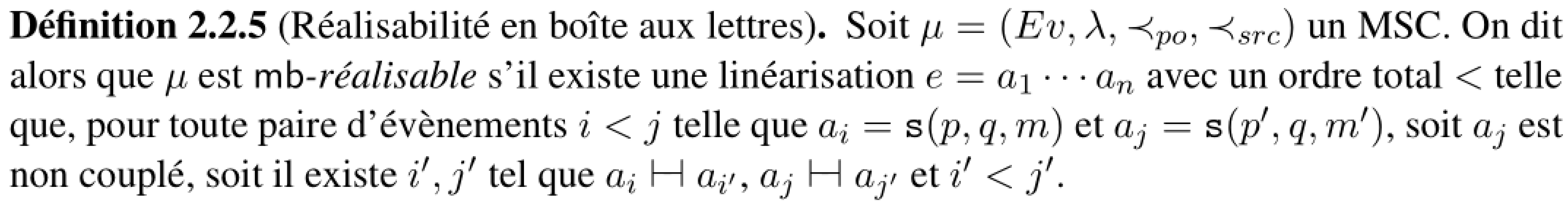
Definition 4 (Causal Delivery). *Let $(Ev, \lambda, \prec)$ be an MSC. We say that it satisfies causal delivery if the MSC has a linearisation $e = a_1 \ldots a_n$ such that for any two events $i \prec j$ such that $a_i = send(p, q, \mathbf{v})$ and $a_j = send(p', q, \mathbf{v}')$, either a_j is unmatched, or there are i', j' such that $a_i \vdash\!\dashv a_{i'}$, $a_j \vdash\!\dashv a_{j'}$, and $i' \prec j'$.*



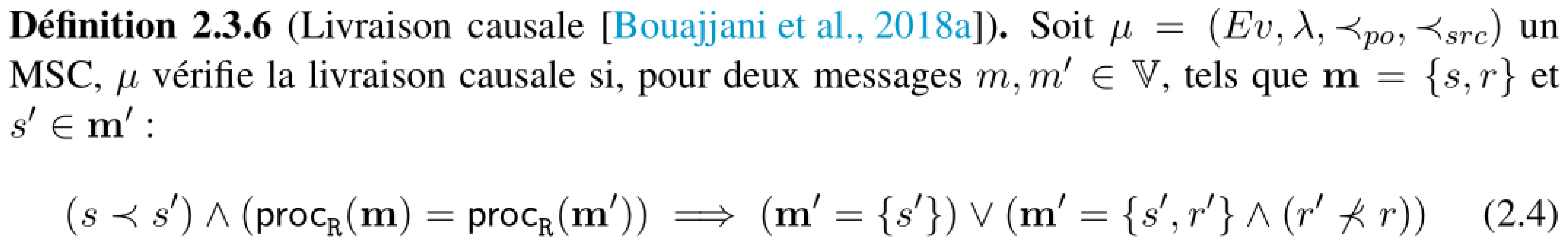
(a)

!1 !2 ?2 !3 ?3

Verifies **def 2.3.6**, but not **def 4**



Définition 2.2.5 (Réalisabilité en boîte aux lettres). Soit $\mu = (Ev, \lambda, \prec_{po}, \prec_{src})$ un MSC. On dit alors que μ est mb-*réalisable* s'il existe une linéarisation $e = a_1 \cdots a_n$ avec un ordre total $<$ telle que, pour toute paire d'évènements $i < j$ telle que $a_i = \mathtt{s}(p, q, m)$ et $a_j = \mathtt{s}(p', q, m')$, soit a_j est non couplé, soit il existe i', j' tel que $a_i \vdash\!\dashv a_{i'}$, $a_j \vdash\!\dashv a_{j'}$ et $i' < j'$.

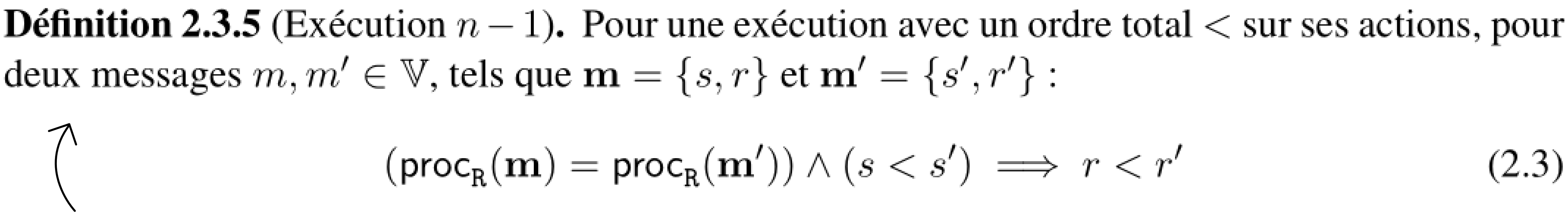


Définition 2.3.6 (Livraison causale [Bouajjani et al., 2018a]). Soit $\mu = (Ev, \lambda, \prec_{po}, \prec_{src})$ un MSC, μ vérifie la livraison causale si, pour deux messages $m, m' \in \mathbb{V}$, tels que $\mathbf{m} = \{s, r\}$ et $s' \in \mathbf{m}'$:

$$(s \prec s') \wedge (\mathsf{proc}_{\mathsf{R}}(\mathbf{m}) = \mathsf{proc}_{\mathsf{R}}(\mathbf{m}')) \implies (\mathbf{m}' = \{s'\}) \vee (\mathbf{m}' = \{s', r'\} \wedge (r' \not\prec r)) \tag{2.4}$$

Mailbox → Causal delivery

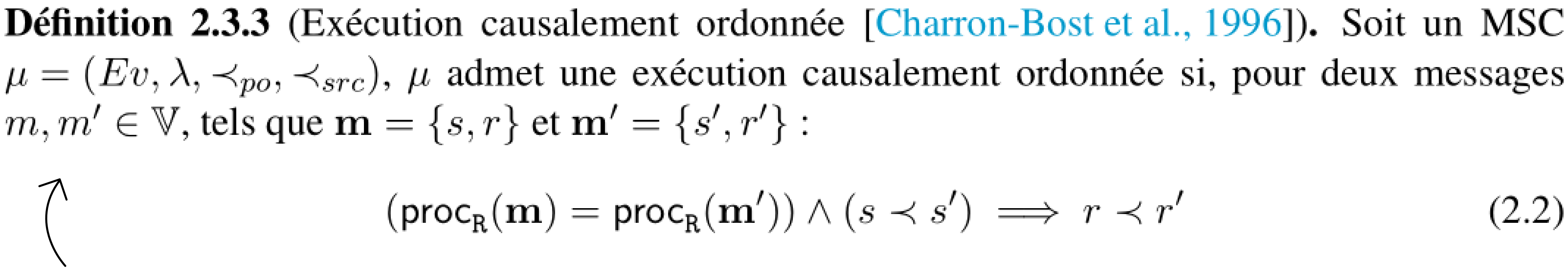
Causal delivery ↛ Mailbox



Définition 2.3.5 (Exécution $n-1$). Pour une exécution avec un ordre total $<$ sur ses actions, pour deux messages $m, m' \in \mathbb{V}$, tels que $\mathbf{m} = \{s, r\}$ et $\mathbf{m}' = \{s', r'\}$:

$$(\mathsf{proc}_{\mathrm{R}}(\mathbf{m}) = \mathsf{proc}_{\mathrm{R}}(\mathbf{m}')) \wedge (s < s') \implies r < r' \tag{2.3}$$

Mailbox without taking into consideration unmatched messages



Définition 2.3.3 (Exécution causalement ordonnée [Charron-Bost et al., 1996]). Soit un MSC $\mu = (Ev, \lambda, \prec_{po}, \prec_{src})$, μ admet une exécution causalement ordonnée si, pour deux messages $m, m' \in \mathbb{V}$, tels que $\mathbf{m} = \{s, r\}$ et $\mathbf{m}' = \{s', r'\}$:

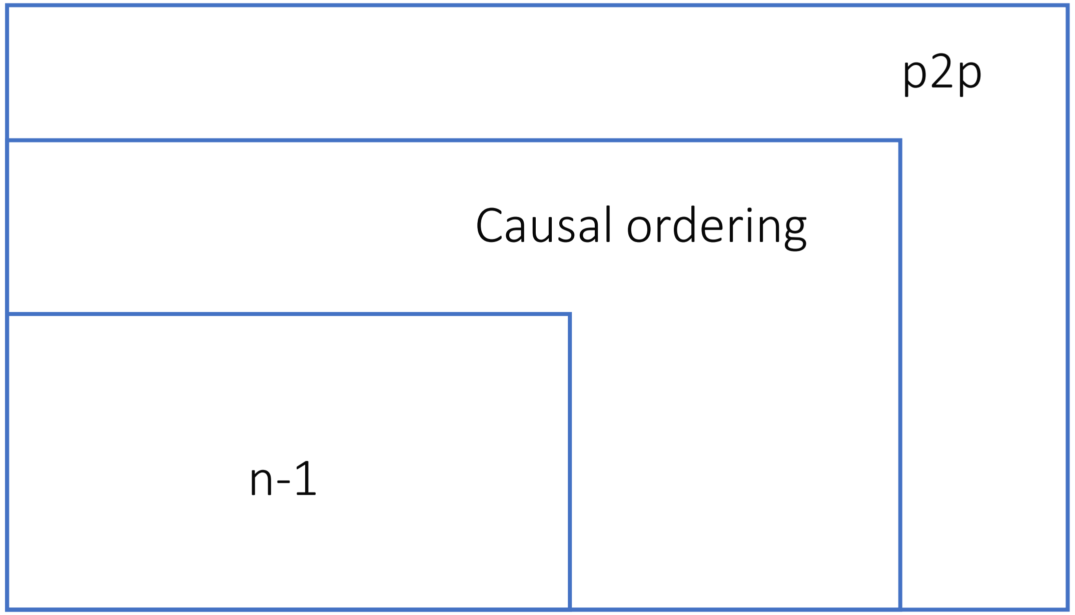
$$(\mathsf{proc}_{\mathrm{R}}(\mathbf{m}) = \mathsf{proc}_{\mathrm{R}}(\mathbf{m}')) \wedge (s \prec s') \implies r \prec r' \tag{2.2}$$

Causal delivery without taking into consideration unmatched messages

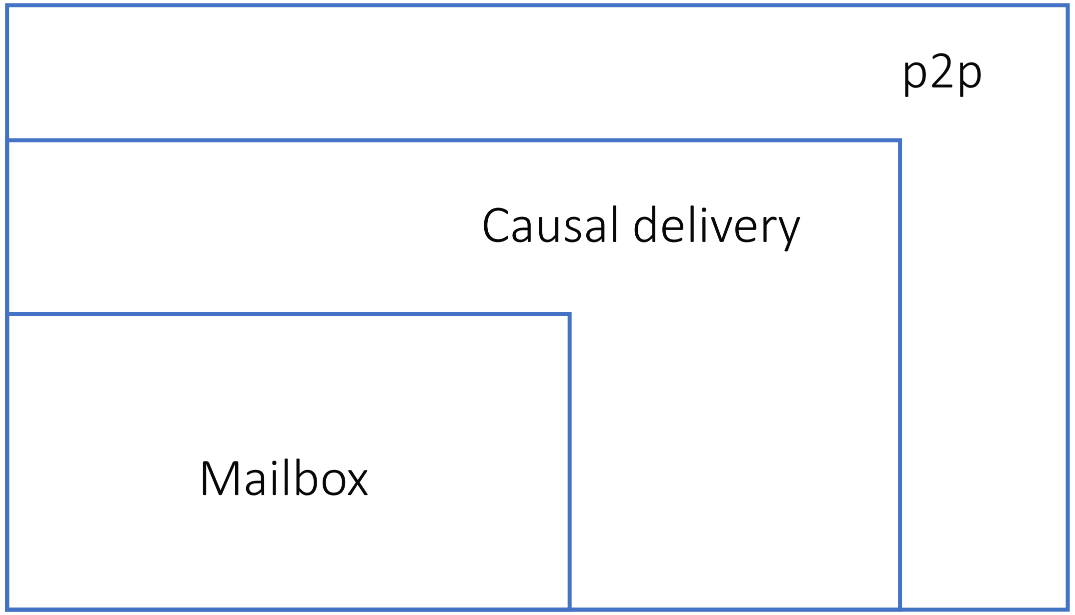
n-1 → Causal ordering

Causal ordering ↛ n-1

MSCs hierarchy



No unmatched messages



With unmatched messages