Notiztitel 30.09.2015

(1) "Design Meets Verification" for Real-Time Systems

Mani Swaminathan, University of Oldenburg

[Joint Work with Ernst-Rüdiger Olderog]

- R1 Workpackage on "Structure and Hierarchy"
- Interplay of 5 Structural Transformations for Extended Timed Automata (ETA)
  - Separation
  - Layering (+)
  - Flattening
  - Expansion
  - Timed Layering (<)

[ETA = Timed Automata + (shared) data]

- Example: Enhanced Fischer's Mutex for 2 CS
- AVACS Phase 3 Paradigm: "Design Meets Verification"

(2) The "Design meets Verification" Paradigm

* Parallelism a main source of system complexity
  - interactions between system components & between system and environment.

* Possible solution : reduce parallelism by examining dependencies. Sequential system much easier to verify! } Side-conditions & equivalences

  [Structural Transformations]

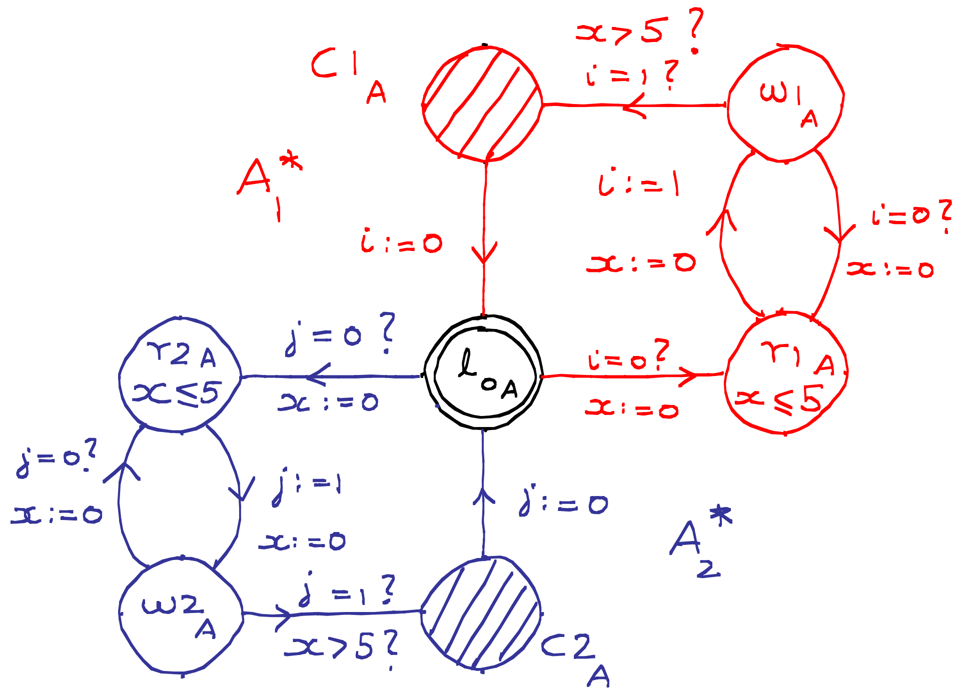
* "Design meets Verification" : restructure system's design to simplify verification

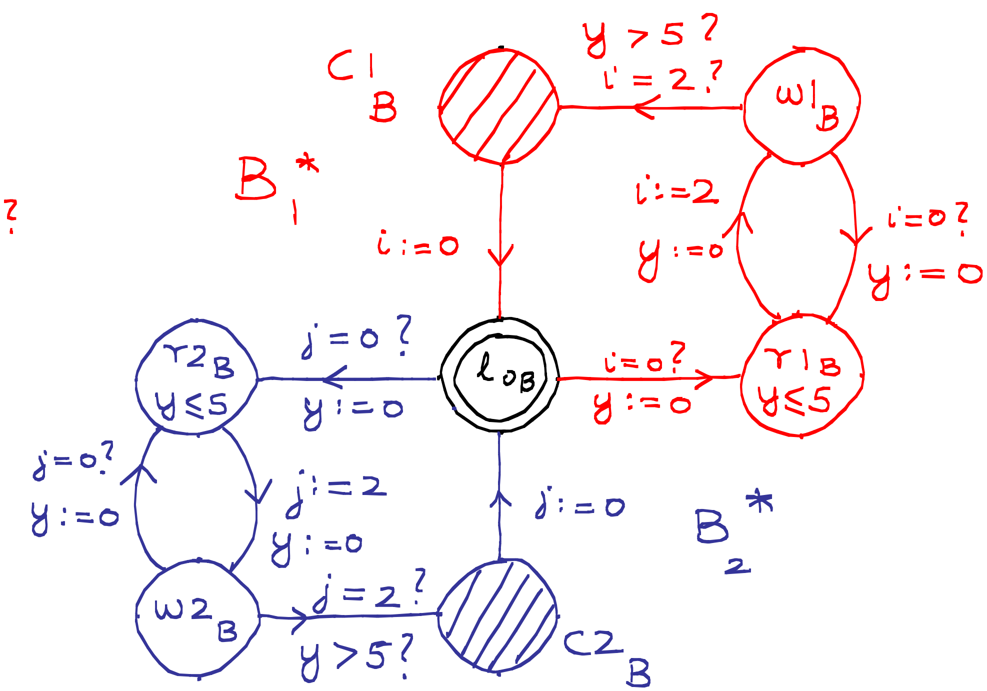
* Disjoint Parallelism : $\underbrace{A_1 \| A_2}_{\text{complex}} \underbrace{\equiv_{po}}_{\text{equivalence}} \underbrace{A_1 ; A_2}_{\text{simple}}$ if $\underbrace{A_1 \pitchfork A_2}_{\text{side-condition}}$

* Design meets Verification for real-time systems

[Extended Timed Automata ; locations + clocks + shared data variables

(3) Example : Fischer's Mutex for two Critical Sections





$$DF = \begin{pmatrix} A_1^* \\ \cup \\ A_2^* \end{pmatrix} \underbrace{|||}_{} \begin{pmatrix} B_1^* \\ \cup \\ B_2^* \end{pmatrix}$$

[Clocks x & y sync.]

CCS-style [UPPAAL]

A_1^* & A_2^* glued together at ℓ_{0A} by $\cup$

B_1^* & B_2^* glued together at ℓ_{0B} by $\cup$

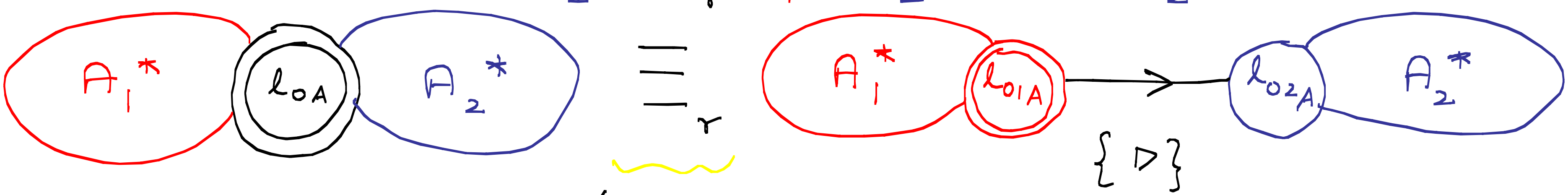
A_1^* & B_1^* share i, $MX_1 = \Box\neg(c1_A \wedge c1_B)$

A_2^* & B_2^* share j, $MX_2 = \Box\neg(c2_A \wedge c2_B)$

$DMX = MX_1 \wedge MX_2$

(4) Separation of ETA: From $\cup$ to $\triangleright$

Sep. Theorem: $A_1^* \cup A_2^* \equiv_r A_1^* \triangleright A_2^*$ if A_1^*, A_2^* memoryless at l_{0A}



not a congruence w.r.t $||$

same sets of reachable states modulo location renaming

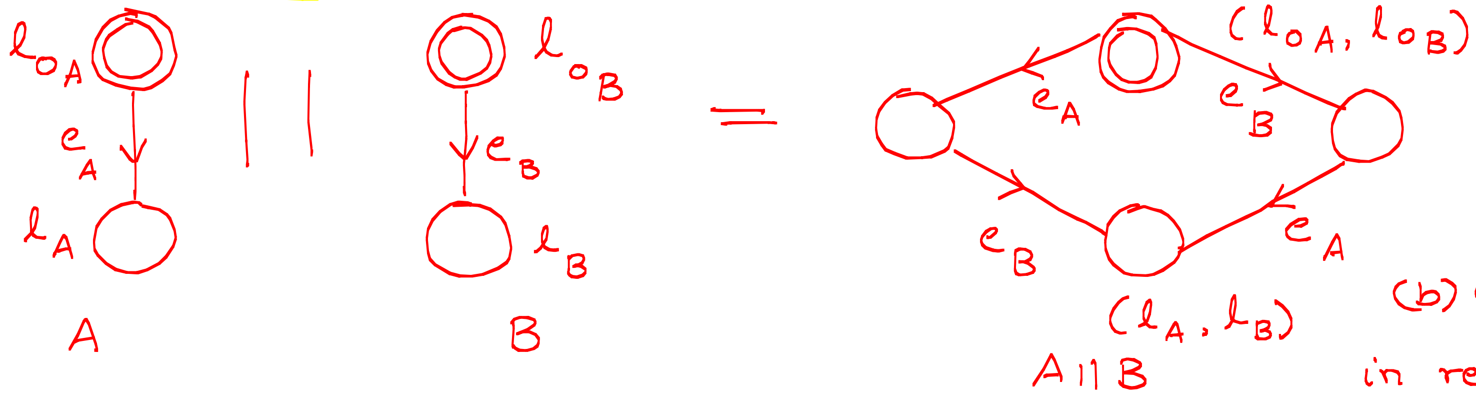
Memoryless at l_{0A} $\Longrightarrow$ initial conditions established upon (re-)entering l_{0A} $\left.\right\}$ $Inv(l_{0A}) = Inv(l_{01A}) = Inv(l_{02A})$

Double Fischer however comprises of $||$ instances of $\cup$!

Aim: Identify additional (syntactic) conditions enabling local ETA separation in a parallel context $\left.\right\}$ while still preserving $\equiv_r$

(5) Independence ($\pitchfork$) in ETA

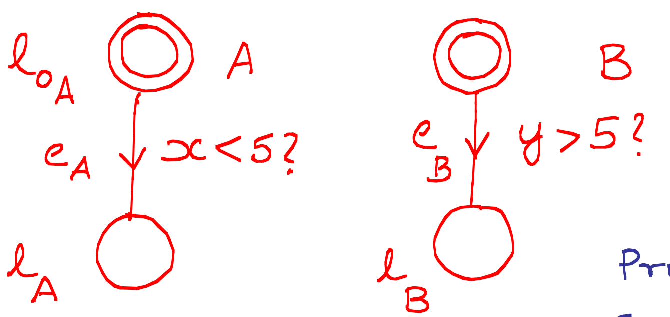
- Dependencies ($\frown$) in ETA due to shared data, sync. actions, & clocks
- Independence ($\pitchfork$) as in partial order reduction
  - enabledness
  - commutativity



(a) e_A & e_B do not disable each other

(b) e_A & e_B commute in reaching (l_A, l_B)

- Synchronously evolving clocks $\Longrightarrow$ timing-induced dependencies!



x & y are synchronous $\Longrightarrow e_A \frown e_B$

So disjoint clocks & data & no sync. actions do not suffice for $\pitchfork$ with global time

Proposed solution for TA P.O.R.

[Bengtsson et al 98, & many others]

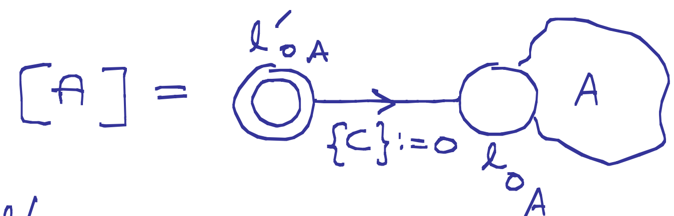
$\frac{dx}{dt}$ indep. of $\frac{dy}{dt}$ $\rightarrow$ - Local time semantics!

(6) Wrapping an ETA [A] for $\pitchfork$ with Sync. Clocks

- ✗ Local time semantics as in p.o.r introduces extra reference clocks for sync.
- ✗ UPPAAL most naturally supports globally sync. clocks
- ✗ Local time semantics not applicable to our case-study

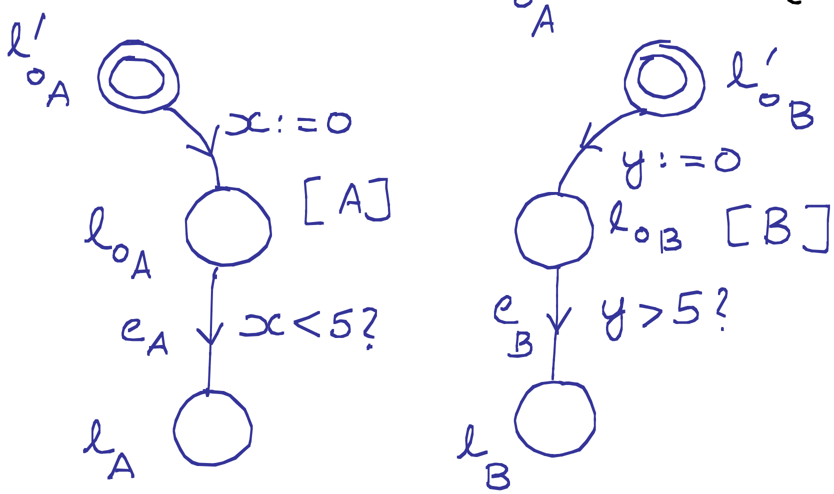
  But eliminating timing-induced $\frown$ still desirable

- ✓ Solution: Wrap ETA to mimic local time with sync. clocks



→ Eliminates timing-induced dependencies

$Inv(l'_{0A}) = true$ permits arbitrary idling at l'_{0A}



Thus $e_A \pitchfork e_B$ in $[A] \parallel [B]$

So by wrapping ETA, $\pitchfork$ reduces to a syntactic inspection of shared data & sync. actions

(7) Local Separation in a Parallel Context : $\cup$ to $\triangleright$ under $\|$

Separation Theorem with $\|$:

$$\begin{pmatrix} A_1^* \\ \cup \\ A_2^* \end{pmatrix} \| \begin{pmatrix} B_1^* \\ \cup \\ B_2^* \end{pmatrix} \equiv_r \begin{pmatrix} A_1^* \\ \triangleright \\ A_2^* \end{pmatrix} \| \begin{pmatrix} B_1^* \\ \triangleright \\ B_2^* \end{pmatrix} \quad \text{when}$$

$$\text{DF} \quad \equiv_r \quad \text{SDF}$$

(a) A_1^*, B_1^*, A_2^*, B_2^* are all memoryless at l_{0A} & l_{0B}

(b) A_2^* & B_2^* inherently wrapped : $[A_2^*] \equiv_r A_2^*$, $[B_2^*] \equiv_r B_2^*$

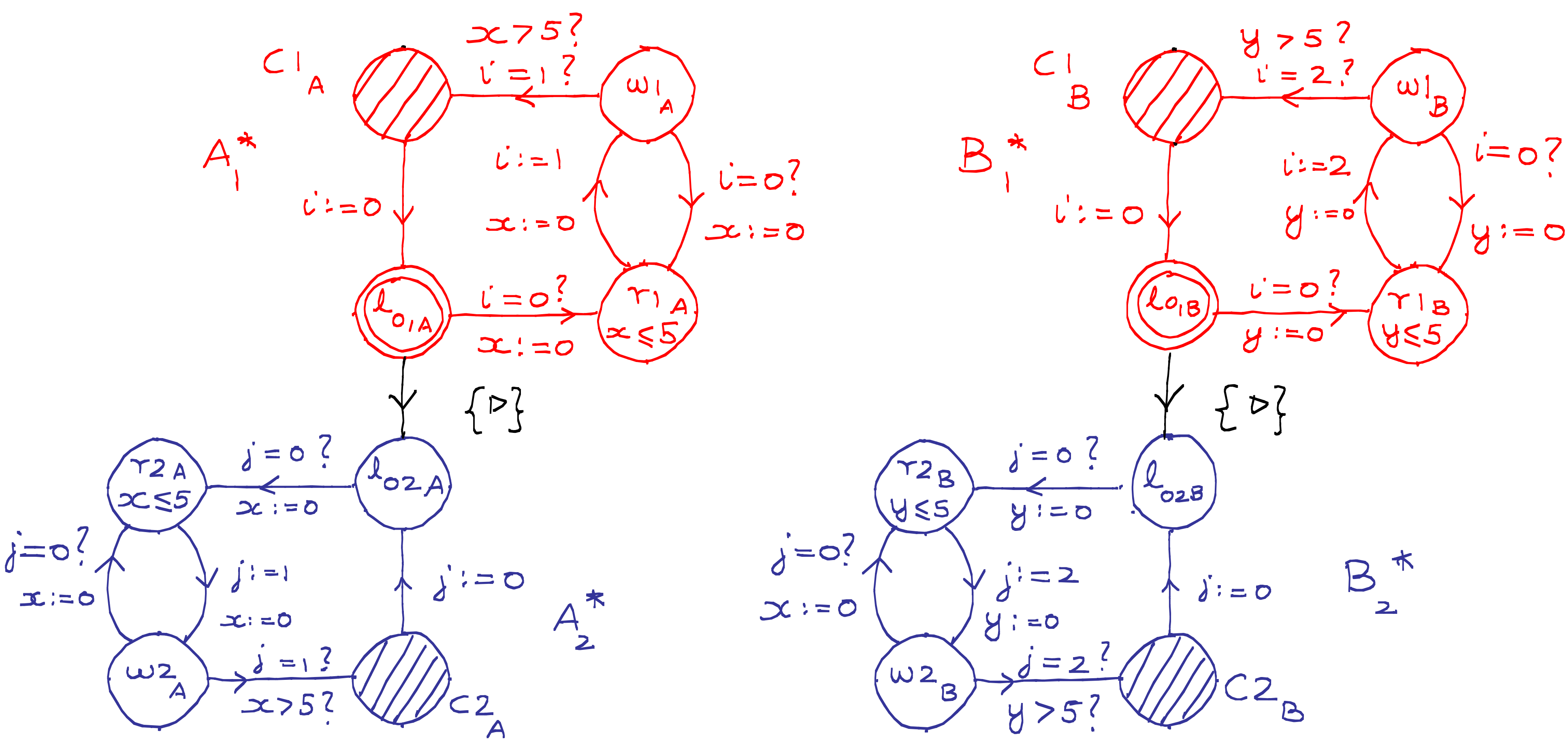
(c) $A_1^* \pitchfork B_2^*$

(d) $B_1^* \pitchfork A_2^*$

$\Big\}$ In DF: A_1^* & B_1^* access only i; A_2^* & B_2^* access only j

- Proof intuition: Memorylessness & $\pitchfork$ with wrapping permit re-ordering of executions so as to preserve $\equiv_r$
- DF satisfies (a) – (d) & $\equiv_r$ preserves DMX

(8) Local Separation applied to Double Fischer



$$DF \equiv_r SDF = \begin{pmatrix} A_1^* \\ \triangleright \\ A_2^* \end{pmatrix} \Big|\Big| \begin{pmatrix} B_1^* \\ \triangleright \\ B_2^* \end{pmatrix}$$

(9) Layering under $\pitchfork$ with wrapping

Layering Theorem under $\pitchfork$

$$\underbrace{\begin{pmatrix} A_1^* \\ \triangleright \\ A_2^* \end{pmatrix} \Big\| \begin{pmatrix} B_1^* \\ \triangleright \\ B_2^* \end{pmatrix}}_{\text{SDF}} \equiv_L \underbrace{\begin{matrix} (A_1^* \parallel B_1^*) \\ \triangleright \\ (A_2^* \parallel B_2^*) \end{matrix}}_{\text{LDF}} \qquad \equiv_r \implies \equiv_L$$

$DMX = MX_1 \wedge MX_2$

$L_1 = A_1^* \parallel B_1^*$ $\quad L_2 = A_2^* \parallel B_2^*$

$\equiv_L$: location reachability properties that do not "cross layers"

(b) A_2^* & B_2^* inherently wrapped : $[A_2^*] \equiv_r A_2^*$, $[B_2^*] \equiv_r B_2^*$

(c) $A_1^* \pitchfork B_2^*$

(d) $B_1^* \pitchfork A_2^*$

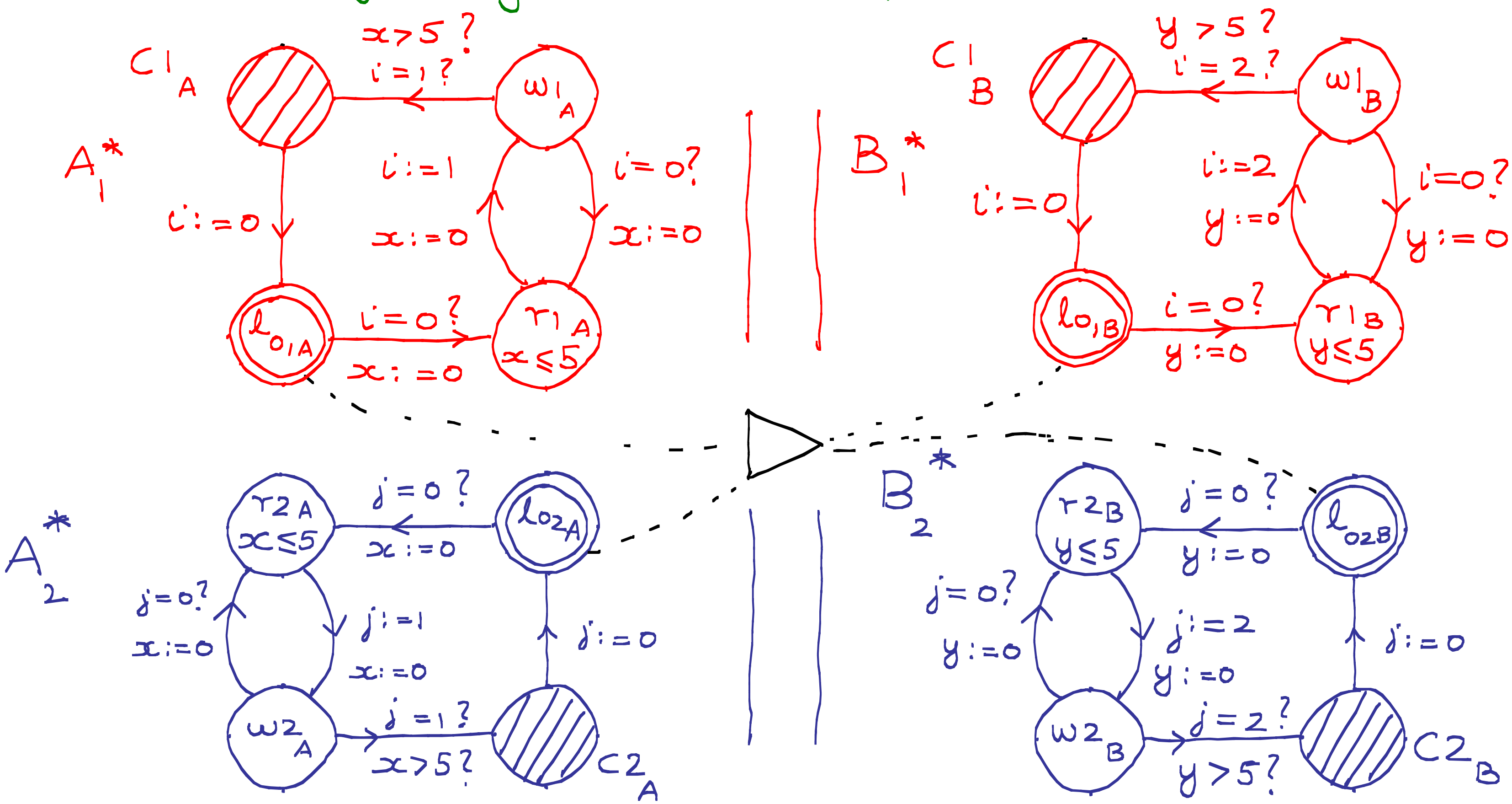
In SDF: A_1^* & B_1^* access only i

A_2^* & B_2^* access only j

- Proof intuition: $\pitchfork$ with wrapping permits re-ordering of executions so as to preserve $\equiv_L$

SDF satisfies (b) – (d) & $\equiv_L$ preserves DMX

(10) Layering under $\rhd$ applied to SDF



$\rhd$ between $(lo1_A, lo1_B)$ & $(lo2_A, lo2_B)$ $L_1 = A_1^* \| B_1^*$ $L_2 = A_2^* \| B_2^*$

$SDF \equiv_L LDF = L_1 \rhd L_2 \models ?\ DMX = MX_1 \wedge MX_2$, preserved by $\equiv_L$

So it suffices to show $L_1 \models MX_1 \wedge L_2 \models MX_2$!

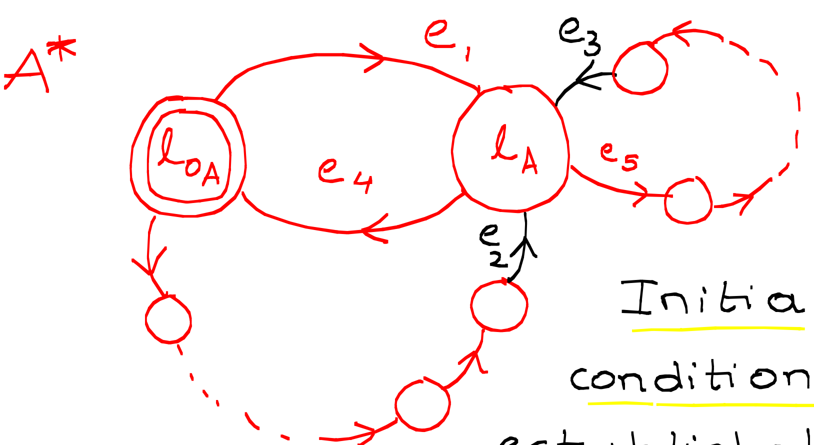
(11) Flattening ETA

Idea: Exploit memorylessness to remove superfluous edges

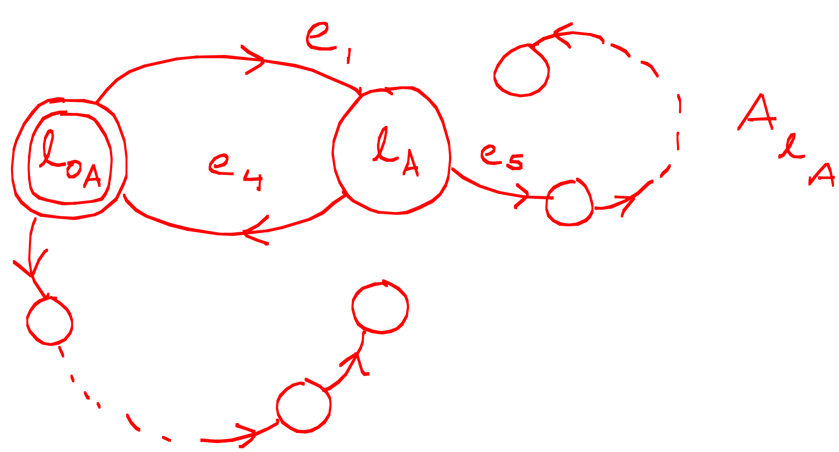
– possibly eliminates cycles thro' memoryless locations

- $A^* \equiv_r A_{\ell_A}$ when A^* is memoryless at ℓ_A [Flattening Thm]

- A_{ℓ_A} obtained from A^* by removing those edges entering ℓ_A having ℓ_A as their target, while retaining syntactic reachability of ℓ_A from ℓ_{oA} $\Big\}$ $\equiv_r$ w.r.t identity ~ on locations



$\equiv_r$



Initial conditions established at ℓ_A by e_1, e_2, e_3

(12) Local Flattening in a Parallel Context

- $\equiv_r$ not a congruence w.r.t $\|$, so more conditions needed
- Flattening Thm under $\|$: $A^* \| B \equiv_{loc} A_{\ell_A} \| B$ if

(a) A^* memoryless at A_{ℓ_A} $\rightarrow$ completely syntactic ✓✓✓

(b) Each location of A^* is reachable from ℓ_{0A} w/o visiting ℓ_A more than once, while B stays in ℓ_{0B}

(c) If a transition entering ℓ_A enables a transition of B with target ℓ_B, then each location of A^* is reachable from ℓ_A w/o visiting ℓ_A more than once, while B stays in ℓ_B

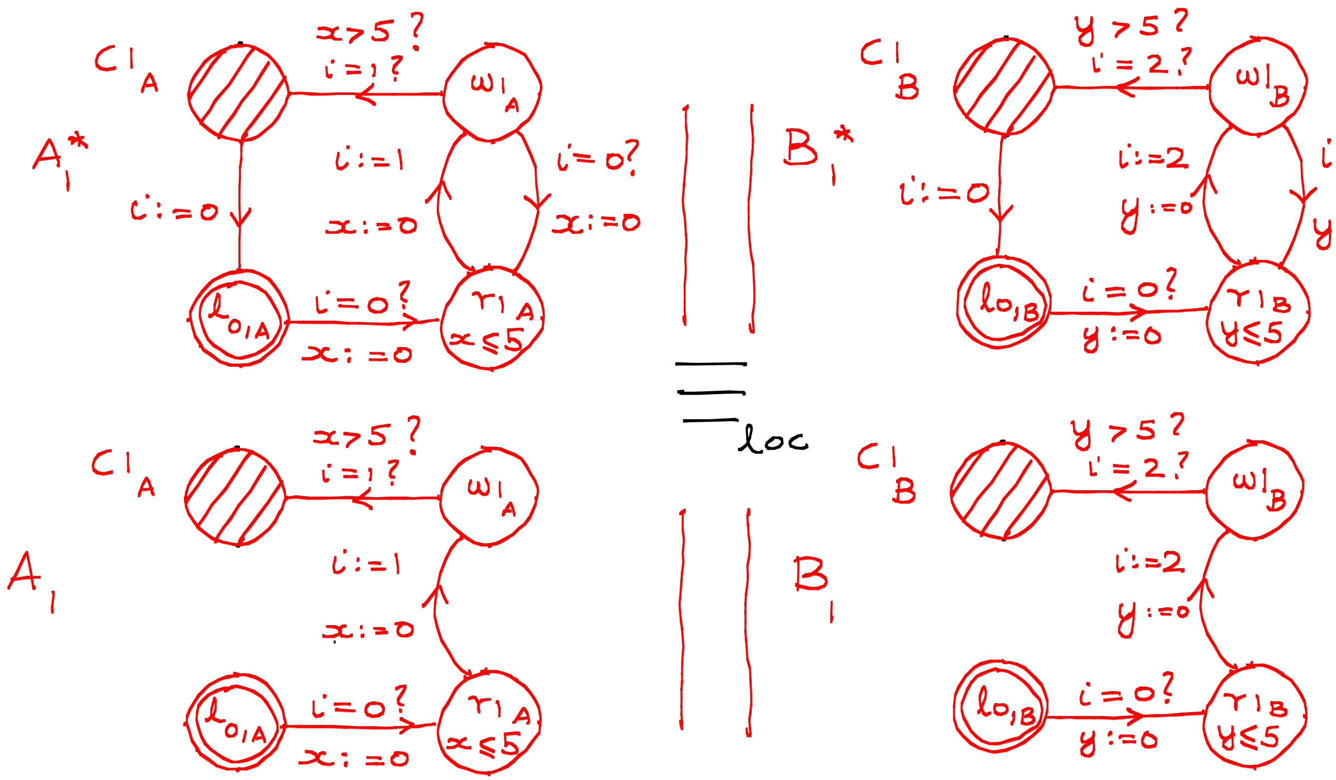
(b), (c): Local reachability checks on A^* with control fixed at ℓ_{0B} resp. ℓ_B – thus no resolution of $\|$ ✓✓

(d) Each location of B is reachable from ℓ_{0B} while A^* stays in A_{ℓ_A} – Limited resolution of $\|$ within a layer

(d): B might involve multiple ETA ✓ [3 or more CS]

(13) Local Flattening at Layer L_1

- $L_1 = A_1^* \| B_1^*$ $\equiv_{loc}$ Both A_1^* & B_1^* satisfy conditions (a), (b), (c), (d) for local flattening
- $FL_1 = A_1 \| B_1$ at $l_{01A}, r_{1A}, l_{01B}, r_{1B}$
- $\equiv_r \Rightarrow \equiv_{loc} \Rightarrow \equiv_L$, thus $\equiv_{loc}$ preserves MX_1

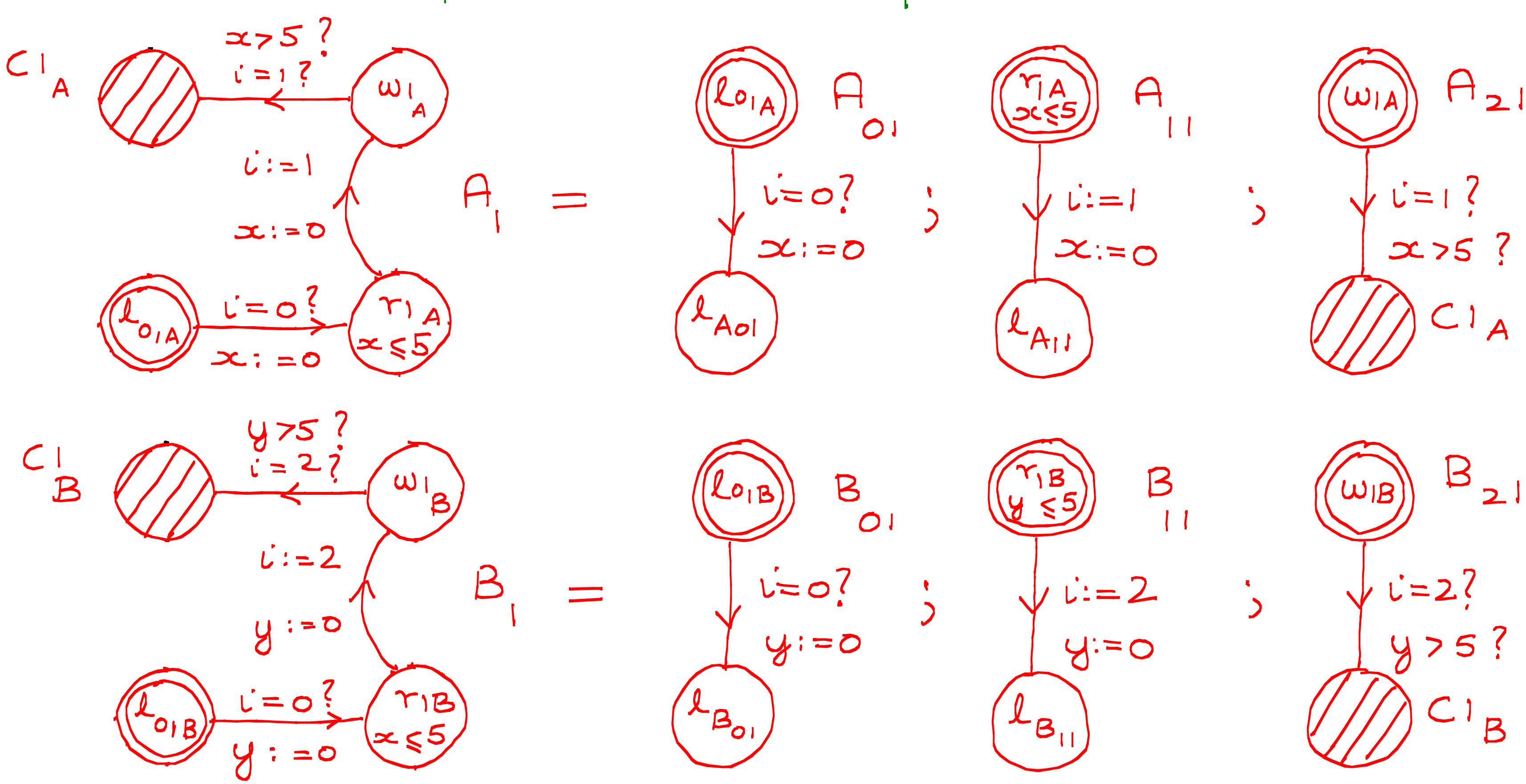


$L_1 = A_1^* \| B_1^*$

$\equiv_{loc}$

$FL_1 = A_1 \| B_1$

(14) Expansion of FL_1 : $||$ into $+$ and ;

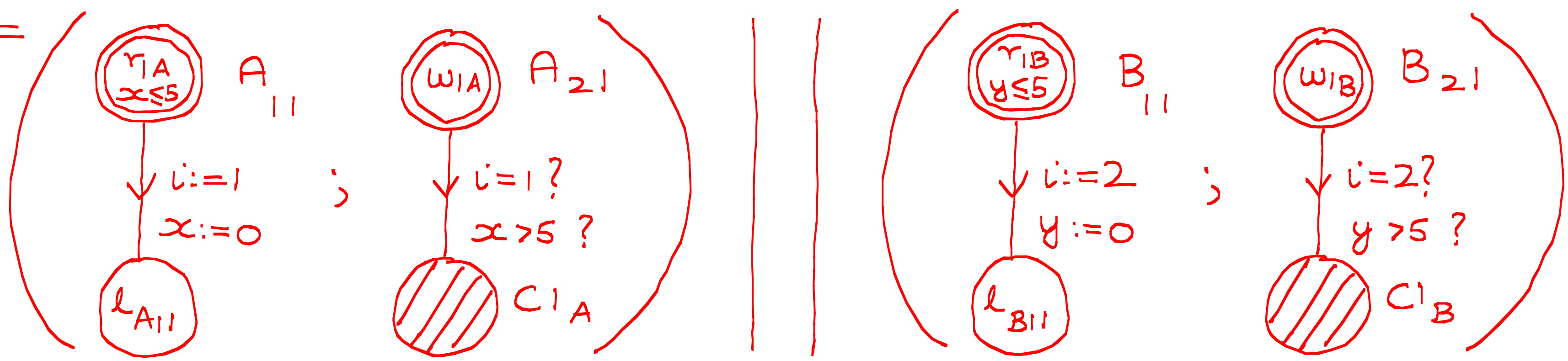


- $A_1 = A_{01} ; A_{11} ; A_{21}$ $\quad B_1 = B_{01} ; B_{11} ; B_{21}$ [Step in $\triangleright$ vs. merger in ;]
- ETA Expansion : $A \,||\, B \equiv_r A ; B + B ; A$ [no ?! sync, A, B atomic]
- $FL_1 = A_1 \,||\, B_1 \equiv_r (A_{01} ; A_{11} ; A_{21}) + (B_{01} ; B_{11} ; B_{21}) + (A_{01} \,||\, B_{01}) ; [(A_{11} ; A_{21}) \,||\, (B_{11} ; B_{21})]$

(15) Satisfaction of MX_1 under Expansion of FL_1

- $FL_1 \equiv_r A_1 + B_1 + (L_{01} ; L_{11 \frown 21})$ where $L_{01} = A_{01} \| B_{01}$, $L_{11 \frown 21} = (A_{11} ; A_{21}) \| (B_{11} ; B_{21})$
- So $FL_1 \models MX_1$ iff $\underbrace{A_1 \models MX_1 \wedge B_1 \wedge MX_1}_{\text{trivial}} \wedge (\underbrace{L_{01}}_{\text{trivial}} ; L_{11 \frown 21}) \models MX_1$

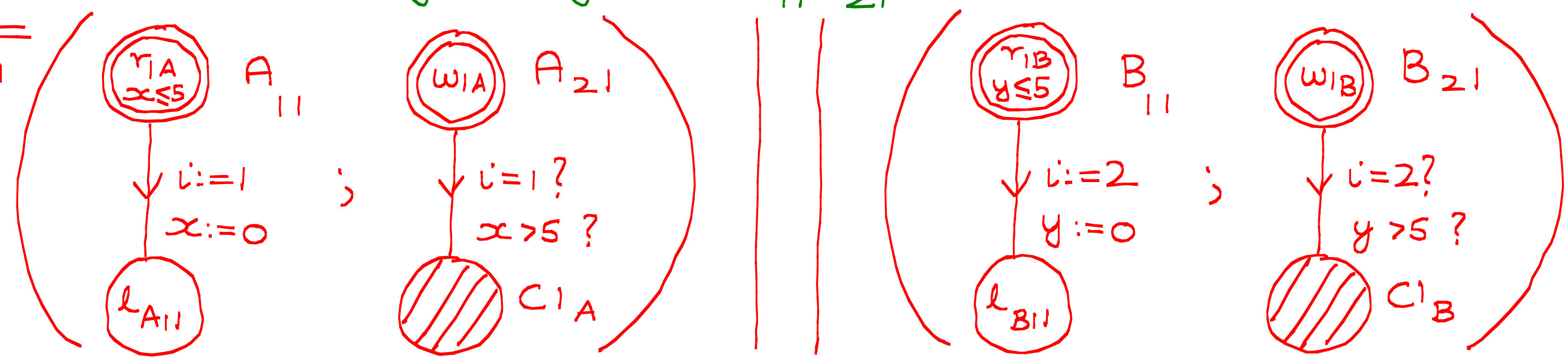
  trivial as MX_1 is contained in $L_{11 \frown 21}$
- So $FL_1 \models MX_1$ iff $L_{11 \frown 21} \models MX_1$
- $L_{11 \frown 21} =$



- Layering under $\pitchfork$ does not apply; $A_{11}, A_{21}, B_{11}, B_{21}$ all access i

(16) Timed Layering of $L_{11 \frown 21}$ under Precedence $\prec$

• $L_{11 \frown 21} =$



• x & y are sync., so B_{21} can't start before A_{11} finishes

A_{21} can't start before B_{11} finishes

$\left.\right\}$ $A_{11} \prec_{A_{21}, B_{11}} B_{21}$, $B_{11} \prec_{A_{11}, B_{21}} A_{21}$

• Precedence $\prec$ in a parallel context enforced by timing

• $\equiv \Rightarrow$ equal sets of reachable states at each iteration depth

• $\equiv \Rightarrow \equiv_r \Rightarrow \equiv_{loc} \Rightarrow \equiv_L$, thus good enough for MX,

• Timed Layering Theorem

$$L_{11 \frown 21} = \begin{pmatrix} A_{11} \\ ; \\ A_{21} \end{pmatrix} \,||\, \begin{pmatrix} B_{11} \\ ; \\ B_{21} \end{pmatrix} \equiv \left.\begin{matrix} (A_{11} \,||\, B_{11}) = L_{11} \\ ; \qquad\qquad ; \\ (A_{21} \,||\, B_{21}) = L_{21} \end{matrix}\right\} \begin{matrix} A_{11} \prec B_{21} \\ \\ B_{11} \prec A_{21} \end{matrix}$$

(17) Preservation of DMX by Double Fischer

- $$\left.\begin{array}{l} L_{11\frown 21} \equiv (A_{11} \parallel B_{11}) = L_{11} \\ \qquad\qquad\quad ; \qquad\qquad\quad ; \\ \qquad\qquad (A_{21} \parallel B_{21}) = L_{21} \end{array}\right\}$$ by Timed Layering, so $L_{11\frown 21} \models MX_1$ iff $\underbrace{L_{11} \models MX_1 \wedge L_{21} \models MX_1}$

  trivial as MX_1 is contained within L_{21}

- Thus $L_1 = (A_1^* \parallel B_1^*) \models MX_1$

- Similarly, $L_2 = (A_2^* \parallel B_2^*) \models MX_2$

- Altogether, $$\begin{array}{c} DF = \\ \models \\ DMX \end{array} \begin{pmatrix} A_1^* \\ \cup \\ A_2^* \end{pmatrix} \Big|\Big| \begin{pmatrix} B_1^* \\ \cup \\ B_2^* \end{pmatrix} \equiv_L \begin{array}{c} L_1 \models MX_1 \\ \triangleright \\ L_2 \models MX_2 \end{array}$$

(18) Summary

	Compositions	Conditions	Equivalences
• Separation	$\cup$ to $\rhd$ under $\parallel$	Memoryless & $\pitchfork$ with wrapping	$\equiv_r$
• Layering	$\parallel$ domination to $\rhd$ domination	$\pitchfork$ with wrapping	$\equiv_L$
• Flattening	Edge removal under $\parallel$	Memoryless & local reach. checks	$\equiv_{loc}$
• Expansion	$\parallel$ to $+$ & $;$	Atomicity & no action sync.	$\equiv_r$
• Timed Layering	$\parallel$ domination to $;$ domination	$\prec$	$\equiv$

• $= \;\Rightarrow\; \equiv \;\Rightarrow\; \equiv_r \;\Rightarrow\; \equiv_{loc} \;\Rightarrow\; \equiv_L$; Proofs exploit reordering

(19) Extensions and Perspectives

* "Design meets Verification" by means of 5 Structural Transformations : Separation, Layering, Flattening, Expansion, Timed Layering for the model of Extended Timed Automata [real-valued clocks + shared data]

* Layering extended to probabilistic automata [with J.-P. Katoen] [randomized mutual exclusion]

* Layering extended to UML Sequence Diagrams [Weak & strict sequencing] [Univ. of Ottawa]

* Layering for (probabilistic) modal specifications [RWTH Aachen]

* Computational & Conceptual simplification of state-space
* Shorter traces – easier debugging & diagnostics

"Design meets Verification"

(20) Other Related Work

- Separation studied by [Cohen '00] for Kleene Algebras
- Non-local Flattening for TA by [Comon & Jurski '99]
- Layering studied by [Elrad & Francez '82], [Janssen et al '90s]
- "TA with disjoint activity" studied by [Muniz, Westphal, Podelski '12]
- Fischer's mutex analysed using [Larsen, Steffen, Weise '96] Timed Modal Specifications
- A form of non-local flattening applied to Fischer's mutex [Mahdi, Westphal, Fränzle, '14]

(21) Many thanks

- to the funding agency (DFG),
- to the Autumn School Organizers, and
- for your interest and attention!

- Our results published in Formal Asp. Comp. ['12, '15]

  – AVACS DB.