

Compositional Reasoning

Comp of aut.

$$\cdot \text{sig}(A) = \prod_{i \in I} \text{sig}(A_i) \quad \left\{ \begin{array}{l} \text{out}(A) = \bigcup_{i \in I} \text{out}(A_i) \\ \text{in}(A) = \bigcup_{i \in I} \text{in}(A_i) \\ \quad - \bigcup \text{out}(A_i) \end{array} \right.$$

Comp of trace prop.

$$\cdot \text{sig}(P) = \prod_{i \in I} \text{sig}(P_i)$$

· traces(P) is the set of seq. of ext. actions of P s.t. $\rho \upharpoonright \text{acts}(P_i) \in \text{traces}(P_i) \forall i \in I$

$A \rightarrow \text{comp.}, P \rightarrow \text{comp trace}$

a) if $\text{extsig}(A_i) = \text{sig}(P_i) \ \& \ \text{traces}(A_i) \subseteq \text{traces}(P_i) \ \forall i.$
 then $\text{extsig}(A) = \text{sig}(P) \ \& \ \text{traces}(A) \subseteq \text{traces}(P)$

Proof : $\rho \in \text{traces}(A)$
 $\rho \upharpoonright A_i \in \text{traces}(A_i) \ \forall i \in I$
 \Downarrow
 $\rho \upharpoonright A_i \in \text{traces}(P_i) \ \forall i$
 $\rho \upharpoonright \text{acts}(P_i) \in \text{ " } \ \forall i \Rightarrow \rho \in \text{traces}(P)$

send(m) $C_{i,j}$ \rightarrow receive(m)

send(m_1), send(m_2), receive(m_1)

m_1, m_2

m_1

2nd \rightarrow how can you prove that a particular
seqⁿ of actions is actually the trace of a comp.

3rd → comp. proof of safety prop.

Defn - An automaton "preserving" a safety prop. P

$$P \text{ is s.t. } a) \text{ acts}(P) \cap \text{int}(A) = \emptyset$$

$$b) \text{ in}(P) \cap \text{out}(A) = \emptyset \rightarrow .$$

⊆ A preserves P if for every seq. β of actions

(β doesn't have int. acts of A) $\exists \forall \pi \in \text{out}(A)$
the fol. holdy

If $\beta / \text{acts}(P) \in \text{traces}(P)$ & $\beta \pi / A \in \text{traces}(A)$ then
 $\beta \pi / \text{acts}(P) \in \text{traces}(P)$

Thm 8.11 \div A is a comp. & P be a seq. ppty.
 (a) & (b) conditions hold for P

i) If A_i preserves $P \forall i \in I$ then A preserves P .

sketch: $\rho|_{\text{acts}(P)} \in \text{traces}(P)$

& $\pi \in \text{out}(A) \quad \pi \in \text{out}(A_j)$

$\rho\pi \in \text{traces}(A).$ $j = j_1, j_2, \dots, j_\ell$

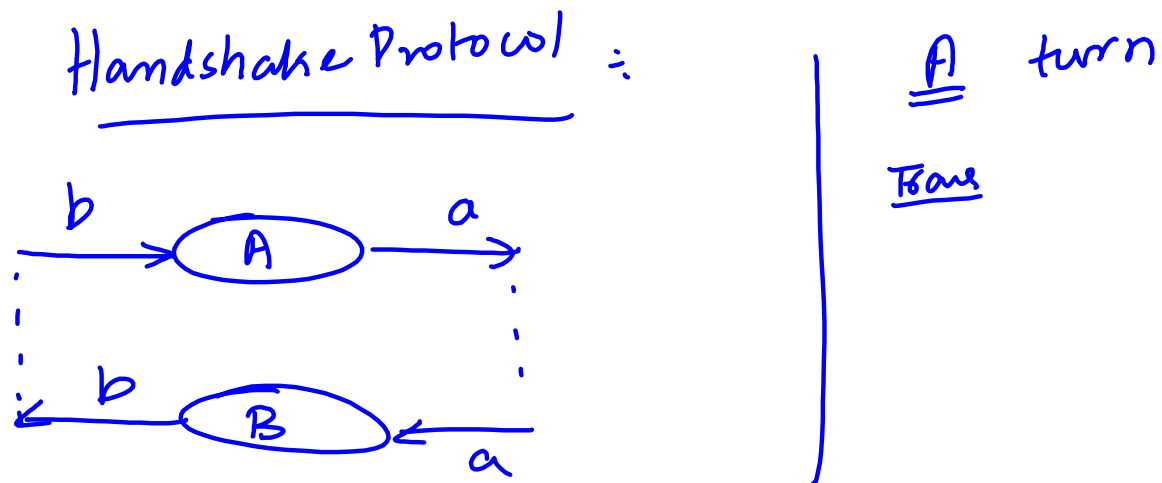
$\rightarrow \rho\pi|_{\text{acts}(A_j)} \in \text{traces}(P)$

$\rho\pi|_{\text{acts}(A_i)} \in \text{traces}(P) \forall i$

- Assumptions
- (1) $\rho \upharpoonright \text{acts}(P) \in \text{traces}(P)$.
 - (2) $\pi \in \text{out}(A)$ & $\rho \pi \upharpoonright A \in \text{traces}(A)$
 - (x) A_i preserves P .

To prove: $\rho \pi \upharpoonright \text{acts}(P) \in \text{traces}(P)$.

$\pi \in \text{out}(A_i)$ for some i
 From (2) $\rho \pi \upharpoonright A_i \in \text{traces}(A_i)$.
 From (x) $\rho \pi \upharpoonright \text{acts}(P) \in \text{traces}(P)$.



P: $\text{sig}(P) :$ $\text{in}(P) = \emptyset$
 $\text{out}(P) = \{a, b\}$

$\text{traces}(P) \rightarrow$ set of all finite & infinite
 seq. of alternating a's & b's

→ A & B are two I/O automata with same ext. interface
 f is a binary relation over $\text{states}(A)$ & $\text{states}(B)$

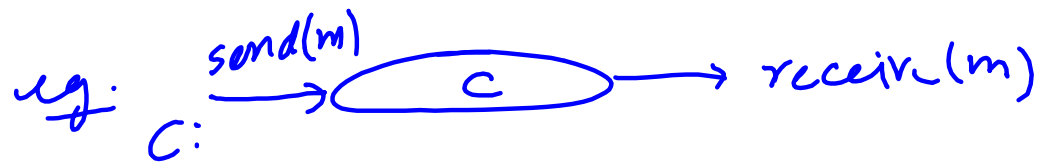
f is a sim. relation from $A \rightarrow B$

a) if $s \in \text{start}(A)$, then $f(s) \cap \text{start}(B) \neq \emptyset$

b) s is a reachable state of A . $u \in f(s)$ is a reachable state of B

$(s, \pi, s') \in \text{trans}(A)$,

then there is an exec. frag. α of B
 starting with u & ending with $u' \in f(s')$
 s.t. $\text{trace}(\alpha) = \text{trace}(\pi)$



$u \rightarrow \text{state } C$

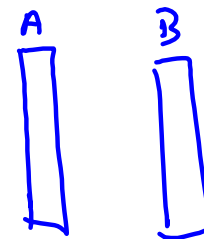
S.A. s.B are states of A & B

$u.\text{queue} \xrightarrow{\text{cat}} \text{s.A. queue} \leftarrow \text{s.B. queue}$

1) $\pi = \text{send}(m)$.

$\alpha \rightarrow u \text{ send}(m) u'$

2) $\pi = \text{receive}(m)$



(3) $\pi = \text{pass}(m)$.