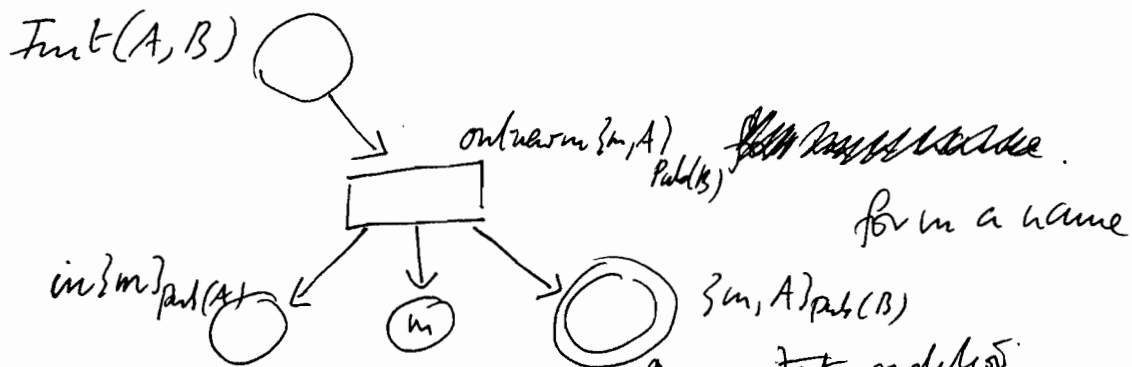
p9 q15
G-W

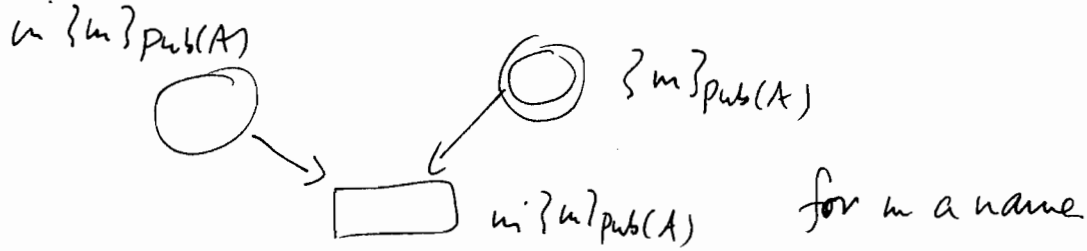
Topics in Concurrency (SPL # 2001)

(a) $Init(A,B)$ outputs a message $\{m, A\}_{pub(B)}$ with a new name m, and then inputs a message $\{m\}_{pub(A)}$.

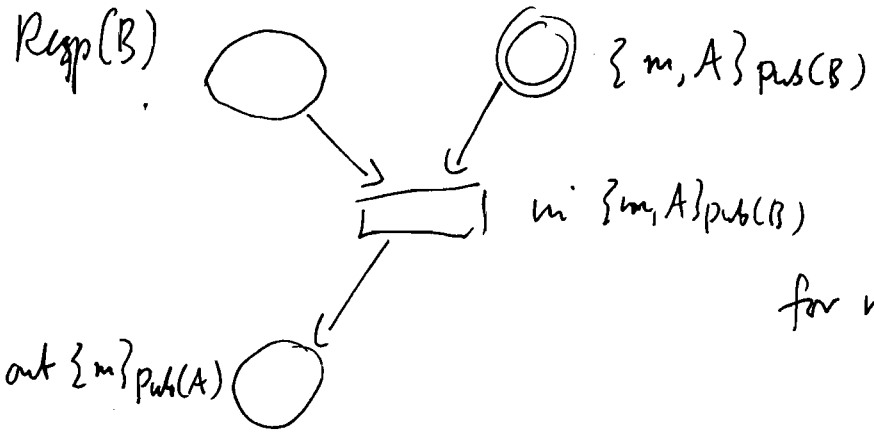
$Resp(B)$ inputs a message of the form $\{m, A\}_{pub(B)}$, and then outputs a the message $\{m\}_{pub(A)}$.

Events of $Init(A,B)$:

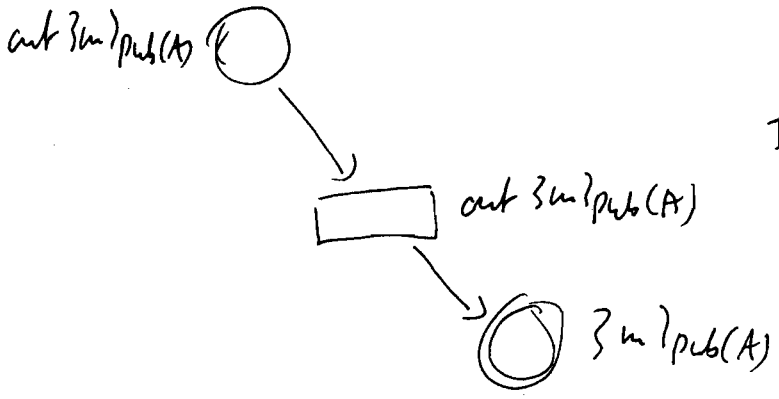




Entity Resp(B):



for m, A names.

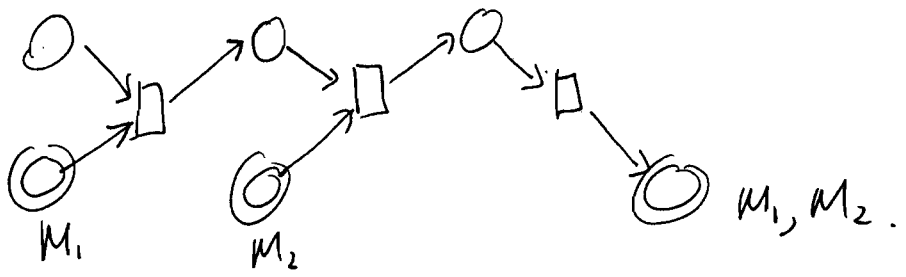


for m, A names.

(b) $Spy \equiv Spy_1 \parallel Spy_2 \parallel Spy_3 \parallel Spy_4$

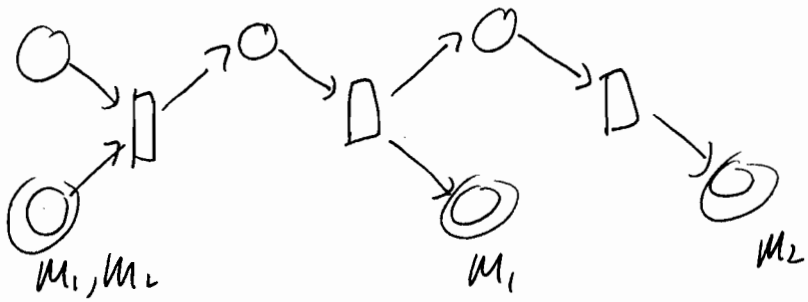
where

$Spy_1 \equiv in.\psi_1\ in.\psi_2\ out(\psi_1, \psi_2)$



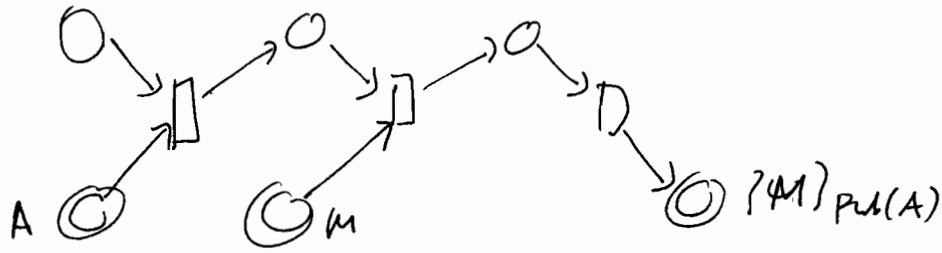
for messages M_1, M_2.

$Spy_2 \equiv in(\Psi_1, \Psi_2).out\ \Psi_1.out\ \Psi_2$

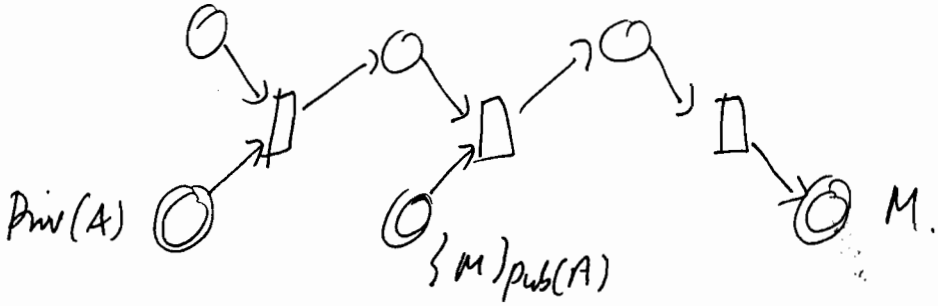


for messages M_1, M_2.

$Spy_3 \equiv in\ X.in\ \Psi.out\ \{\Psi\}_{Pub(X)}$



$Spy_4 \equiv in\ Priv(X).in\ \{\Psi\}_{Pub(X)}.out\ \Psi$



(c) $Q(t_{r-1})$ is false because ~~$e_r = t_r$~~ as a precondition of ~~e_r~~ the input event e_r the message $\{m\}_{pub(A)}$ must previously have been output and so be in t_{r-1}.

$Q(t_0)$ is true because in order ~~for~~ the input event e_r to occur A as ~~the~~ initiator must have previously performed an output $new\ n$ / $\{n, A\}_{pub(B)}$ event. Hence n ~~$\neq$~~ t_0 because n is a new name.

(d) e_i must have the form