<u>Theorem</u>: the decision problem "does CMSG G have a safe, accepting path" is undecidable.

<u>Proof</u>: by a reduction from the Post's correspondence problem (PCP). Proof idea:

PCP instance $(U,W) \longmapsto$ CMSG $G_{U,W}$

such that: (U,W) has a solution

if and only if

$G_{U,W}$ has a safe, accepting path.

let $U = \{u_1, u_2, \ldots, u_n\}$ and $W = \{w_1, \ldots, w_n\}$
where $u_i \in \Sigma^*$, $w_i \in \Sigma^*$ for some alphabet Σ.

Components of the CMSG $G_{U,W}$:

$P = \{p_1, p_2, p_3, p_4\}$, set of processes

$C = \Sigma \uplus \{end\} \uplus \{1, \ldots, n\}$, set of message contents

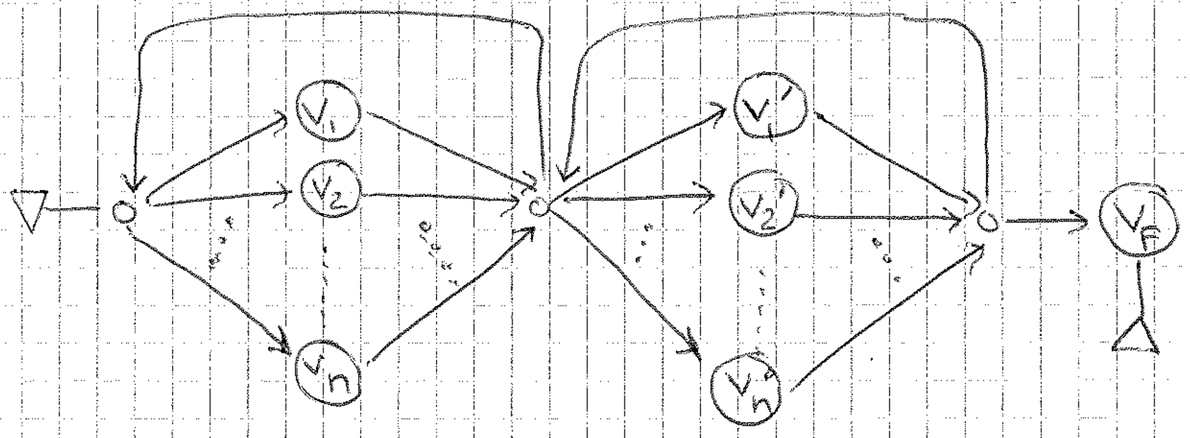
$V = \{v_1, \ldots, v_n\} \cup \{v_1', \ldots, v_n'\} \cup \{v_F\}$

$F = \{v_F\}$

$\lambda(v_i)$ = CMSG that "corresponds" to the word u_i

$\lambda(v_i')$ = " " " " " " w_i

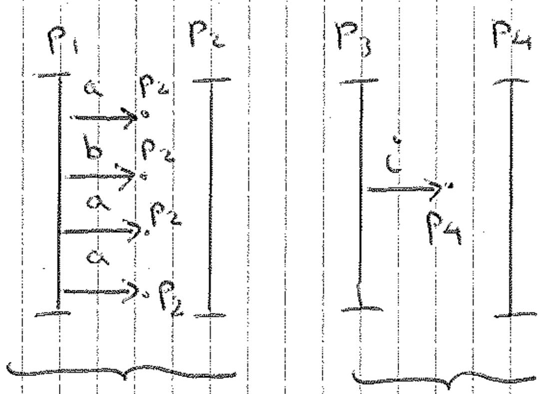
$G_{U,W}$:

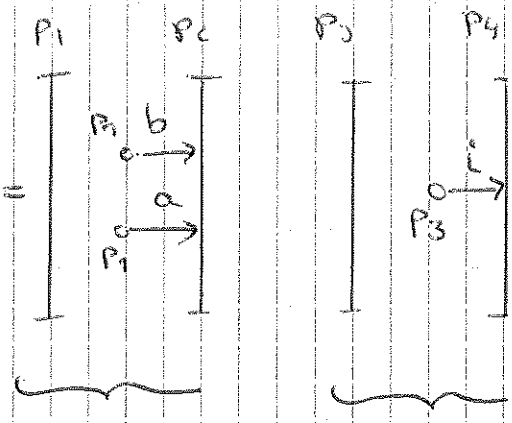


How do the vertices v_i, v_i' and v_F look like?

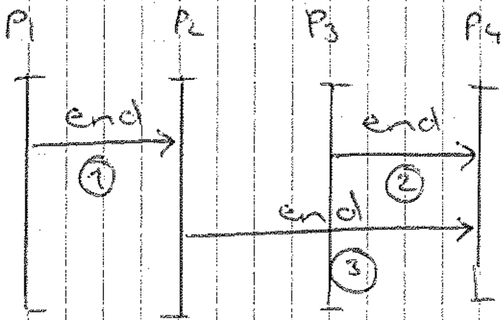
By example. Let $\Sigma = \{a, b\}$, $u_i = abaa$, $w_i = ba$

Then

$\lambda(v_i) =$ 

$\lambda(w_i) =$ 

send word $u_i =$ abaa to p_2 | send index i to p_4 | receive word $w_i = ba$ from p_1 | receive index i at p_4

$\lambda(v_F) =$ 

Intuition: (1) indicates that p_1 has sent all its messages to p_2 and if (1) is received by p_2, all receive events – possibly unmatched – have taken place at process p_2

(2) similar as (1), but now for the "index" messages (belonging to $\{1, \ldots, n\}$)

(3) indicates that all possible message transfers of symbols in Σ from p_1 to p_2 and all "index" messages between p_3 and p_4 have been transferred.

It remains to prove that the reduction:

$$\text{PCP instance } (u,w) \longmapsto \text{CMSG } G_{u,w}$$

is correct. That is, we need to prove that:

(u,w) has a solution $\iff$ $G_{u,w}$ has a safe accepting path

<u>Proof</u>: "$\Rightarrow$": let index sequence $i_1 i_2 \ldots i_k$ be a solution of PCP (u,w). Then there is an accepting path

$$\pi = \underbrace{v_{i_1} v_{i_2} \ldots v_{i_k}}_{\substack{\text{traverse the} \\ \text{vertices corresponding} \\ \text{to } u_{i_1}, u_{i_2} \ldots u_{i_k}}} \; \underbrace{v'_{i_1} v'_{i_2} \ldots v'_{i_k}}_{\substack{\text{traverse the} \\ \text{vertices corresponding} \\ \text{to } w_{i_1}, w_{i_2}, \ldots, w_{i_k}}} v_F \text{ in } G_{u,w}.$$

As $i_1 i_2 \ldots i_k$ is a solution of PCP instance (u,w), and by construction of vertices v_i and v'_i it follows that

$$\lambda(v_{i_1}) \circ \lambda(v_{i_2}) \circ \ldots \circ \lambda(v_{i_k}) \circ \lambda(v'_{i_1}) \circ \lambda(v'_{i_2}) \circ \ldots \circ \lambda(v'_{i_k})$$

(all left-bracketed; remember that $\circ$ is not associative on CMSGs) is an MSC. Intuitively, this follows from the fact that all messages sent in $\lambda(v_{i_1}) \circ \ldots \circ \lambda(v_{i_k})$ are <u>all</u> received in $\lambda(v'_{i_1}) \circ \ldots \circ \lambda(v'_{i_k})$, as otherwise $i_1 i_2 \ldots i_k$ would not be solution to PCP instance (u,w).

Thus: π is safe and accepting.

"$\Leftarrow$": Let π be a safe, accepting path in $G_{u,w}$.

Assume $\pi = \underbrace{v_{i_1} v_{i_2} \cdots v_{i_m}}_{\substack{\text{traverse first part} \\ \text{of } G_{u,w} \text{ m times}}} \underbrace{v'_{j_1} v'_{j_2} \cdots v'_{j_k}}_{\substack{\text{traverse second} \\ \text{part of } G_{u,w} \\ \text{k times}}} v_F$

with $i_1, \ldots, i_m \in \{1, \ldots, n\}$ and $j_1, \ldots, j_k \in \{1, \ldots, n\}$.

Since π is safe and ends in vertex v_F it follows:

1. as $?(p_4, p_3, end)$ occurs in v_F, all unmatched sends by process p_3 in sub-path $v_{i_1} \ldots v_{i_m}$ are matched by corresponding ~~sends~~ receipts by p_4 in the sub-path $v'_{j_1} \ldots v'_{j_k}$. As in each vertex v_{i_l} one message is sent from p_3, and in each vertex v'_{j_u} one message is received at p_4 (from p_3), it follows that $\underbrace{|v_{i_1} \ldots v_{i_m}|}_{\substack{\text{length of} \\ v_{i_1} \ldots v_{i_m}}} = \underbrace{|v'_{j_1} \ldots v'_{j_k}|}_{\substack{\text{length of} \\ v'_{j_1} \ldots v'_{j_k}}}$

   and thus $\boxed{m = k}$

2. As π is safe it follows that

$$v_{i_1} \ldots v_{i_m} \; v'_{j_1} \ldots v'_{j_m} \text{ is safe and FIFO}$$

Thus all "index" messages $i_1, i_2, \ldots, i_m$ sent by P_3 in $v_{i_1} \ldots v_{i_m}$ are received by process P_4 in $v'_{j_1} \ldots v'_{j_m}$ in the same order as they were sent.

Thus $i_1 = j_1$, $i_2 = j_2$, $\ldots$, $i_m = j_m$.

So: $\pi = v_{i_1} v_{i_2} \ldots v_{i_m} v'_{i_1} v'_{i_2} \ldots v'_{i_m} v_F$ is a safe, accepting path in $G_{u,w}$

As π is completed by $?(P_4, P_2, end)$ and $!(P_2, P_4, end)$ can only occur after $?(P_2, P_1, end)$ it follows that once P_4 has received all "index" messages, P_2 has received all messages sent by process P_1 in $v_{i_1} v_{i_2} \ldots v_{i_m}$.

Process P_1 has sent the words $u_{i_1} u_{i_2} \ldots u_{i_m}$ (to P_2).

Process P_2 received the words $w_{i_1} w_{i_2} \ldots w_{i_m}$.

Since π is safe, it follows $u_{i_1} u_{i_2} \ldots u_{i_m} = w_{i_1} w_{i_2} \ldots w_{i_m}$

Thus: $i_1 i_2 \ldots i_m$ is a solution to the PCP instance (u, w)

$\boxtimes$