Do MSGs have an MSC in common?

set of MSCs

set of MSCs accepted by G_1

Theorem: undecidability of empty intersection

The decision problem:

for MSGs G_1 and G_2, do we have $\underline{L(G_1) \cap L(G_2) = \varnothing}$?

is undecidable.

Proof: Reduction from Post's Correspondence Problem (PCP)

. . . black board . . .

Claim: for MSGs G_1 and G_2, the decision problem: " is $L(G_1) \cap L(G_2) \neq \emptyset$ " is undecidable

Proof: ① Post's Correspondence Problem" (PCP)

② Reduction : PCP $\longrightarrow$ the emptiness problem for MSGs

③ Prove that the reduction ② is correct.

① Post's Correspondence Problem" (PCP)

Emil Post, 1946

Intuition: consider the following puzzle. We are given a finite set of tiles of the form

tile$_1$	tile$_2$	tile$_3$	tile$_4$
aba	bbb	aab	bb
a	aaa	abab	babba

Assume there are unboundedly many instances of every tile. Q: find a combination of tiles (instances thereof) such that the word in the upper parts is the <u>same</u> as the word in the lower parts when "reading" the tiles from left to right.

1	4	3	1
aba	bb	aab	aba
a	babba	abab	a

$$= \frac{ababb\;aab\;aba}{ababba\;abab\;a}$$

$\underbrace{1 \quad 4 \quad 3 \quad 1}_{\text{a solution to the given PCP puzzle}}$

1,4,3,1

1,4,3,1,1,4,3,1

Formalisation of the PCP problem:

Given: 1. Σ a finite alphabet, e.g.

$$\Sigma = \{a, b, c, \dots, t\}$$

2. $U = \{u_1, \dots, u_n\}$ with $u_i \in \Sigma^*$

3. $W = \{w_1, \dots, w_n\}$ with $w_i \in \Sigma^*$

4. $n > 0$, number of tiles

<u>Def</u> (PCP): does there exist a finite sequence of indices $i_1, i_2, \dots, i_k$ such that for $k > 0$:

$$\underbrace{u_{i_1} \circ u_{i_2} \cdots u_{i_k}}_{\text{word concatenation of } u_{i_1}, \dots, u_{i_k}} = w_{i_1} w_{i_2} \cdots w_{i_k} \; ?$$

<u>Example</u> $U = \{aba, bbb, aab, bb\}$ $\quad \Sigma = \{a, b\}$

$$W = \{\underbrace{a}_{=w_1}, \underbrace{aaa}_{=w_2}, \underbrace{abab}_{=w_3}, \underbrace{babba}_{=w_4}\}$$

Solution $i_1, i_2, i_3, i_4 = 1, 4, 3, 1$

Theorem [Post, 1946]: PCP is undecidable.

importance of this result: PCP is a popular decision problem that can be used to show the undecidability of other decision problems.

undecidable

How? take decision problems P (eg. PCP) and Q (eg. $L(G_1) \cap L(G_2) = \emptyset$? for MSGs G_1 and G_2)

Aim: prove that decision problem Q is undecidable

(P is reducible to Q) implies Q is undecidable (*)

eg PCP (undecidable)

problem for which we want to prove undecidability

What is a reduction? Need a total computable function f such that:

$$\underbrace{x \in \text{Inst}(P)}_{\text{e.g. } x \text{ is a given PCP instance}} \quad \text{iff} \quad \underbrace{f(x) \in \text{Inst}(Q)}_{\text{e.g. instance of } L(G_1) \cap L(G_2) = \emptyset \text{ for MSGs } G_1 + G_2.}$$

In our setting, we are looking for a reduction f that maps a given PCP instance onto an emptiness problem instance for two MSGs. Idea:

(2) $$\underbrace{(u, w)}_{\text{PCP instance}} \xmapsto{\ f\ } \underbrace{(G_u, G_w)}_{\text{instance of emptiness problem}}$$

such that

$$\boxed{\begin{array}{ll} (u, w) \text{ is a solution} & \\ \text{to the PCP instance} & \text{iff} \quad L(G_u) \cap L(G_w) \neq \emptyset \end{array}}$$

(3) This is the correctness statement that we need to prove of our reduction.

Claim: for MSGs G_1 and G_2, the decision problem: "is $L(G_1) \cap L(G_2) = \emptyset$" is undecidable

Proof: ① "Post's Correspondence Problem" (PCP) ✓

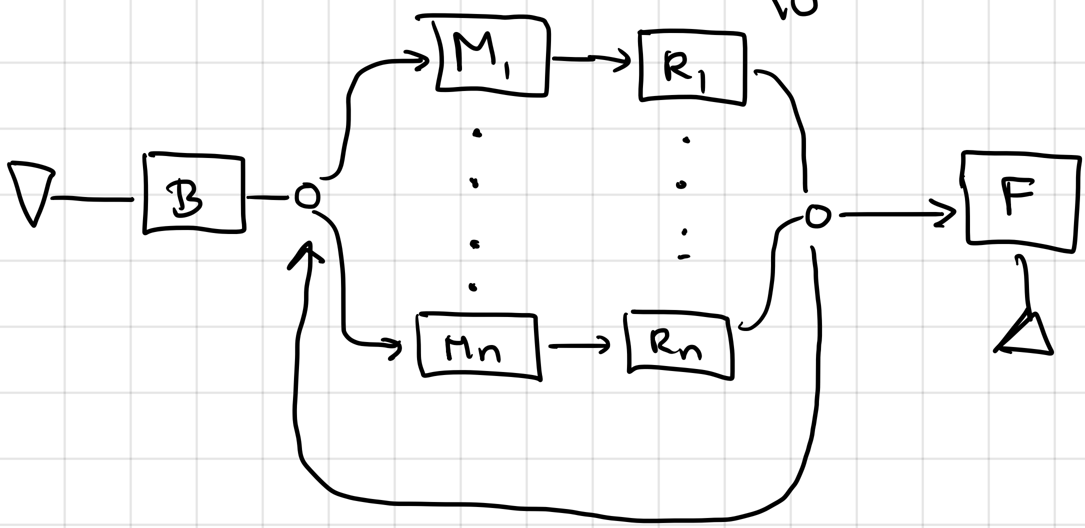
② Reduction: PCP $\longrightarrow$ the emptiness problem for MSGs ✓

③ Prove that the reduction ② is correct.

Reduction : PCP instance $(U, W) \longmapsto$ MSGs (G_U, G_W)

Explain for $\underbrace{U}_{\text{set of finite words } \{u_1, \dots, u_n\}} \longmapsto \underbrace{G_U}_{\text{MSG}}$

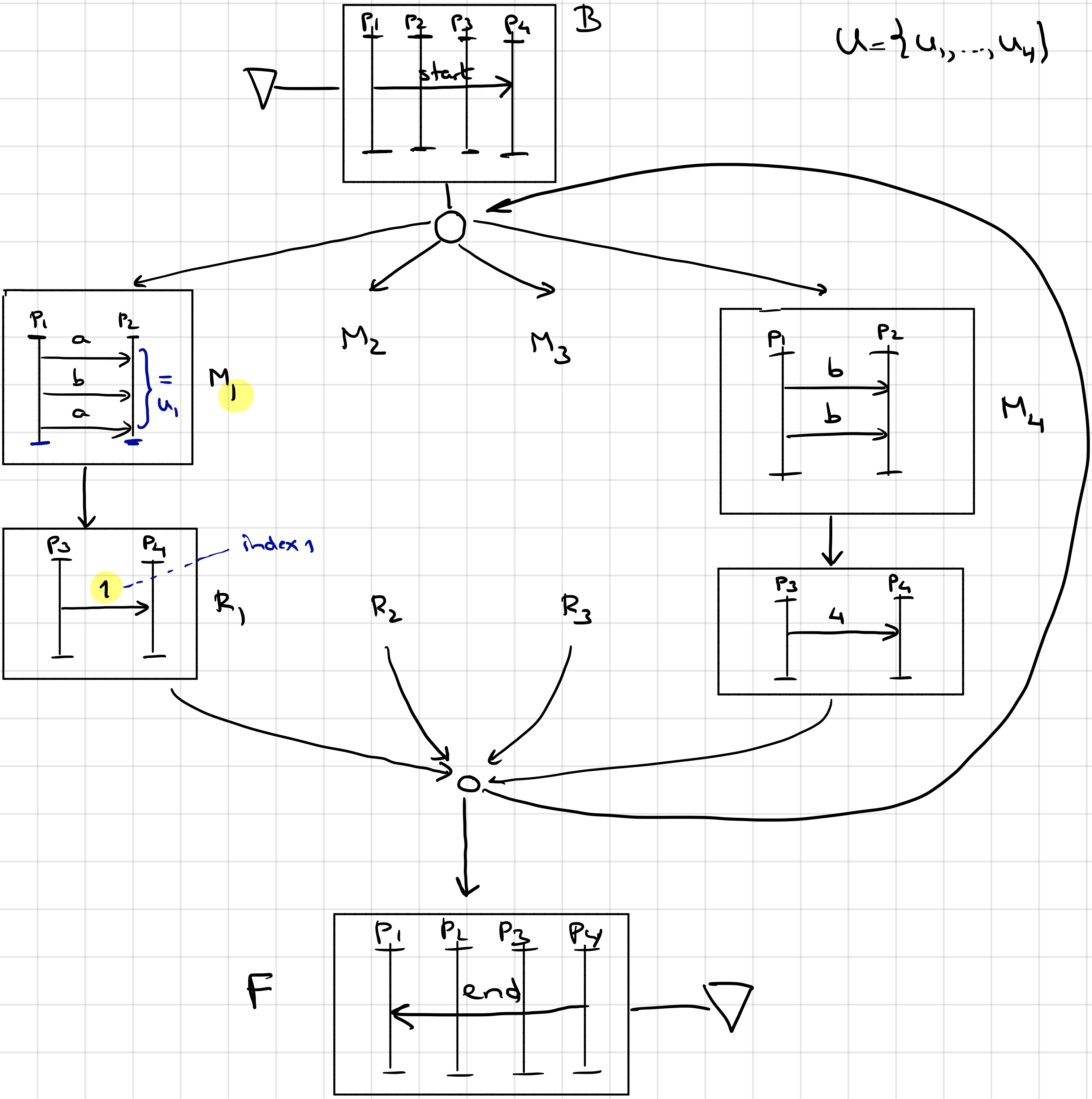
Regular expression for G_U : $B \cdot \left(\sum_{j=1}^{n} (M_j \cdot R_j) \right)^+ \cdot F$



structure of MSG G_U

Example : let $U = \{ \underbrace{aba}_{=u_1}, \underbrace{bbb}_{=u_2}, \underbrace{aab}_{=u_3}, \underbrace{bb}_{=u_4} \}$

set of processes $\mathcal{P} = \{ P_1, P_2, P_3, P_4 \}$



$$\lambda(M_i) = u_i$$

$$\lambda(R_i) = \text{"}p_1 \text{ sends index } i \text{ to } p_4\text{"}$$

<u>note:</u> $M_j \cdot R_j$

- M_j involves p_1 and p_2
- R_j involves p_3 and p_4

explains $u \longmapsto$ MSG G_u

in a similar way $w \longmapsto$ MSG G_w

③ Correctness of the reduction.

Claim:

(u, w) has a solution iff $L(G_u) \cap L(G_w) \neq \emptyset$

Proof: "$\Longrightarrow$" assume (u, w) has a solution.

That is, there exists a sequence $i_1, \dots, i_k$ such that $u_{i_1} u_{i_2} \cdots u_{i_k} = w_{i_1} w_{i_2} \cdots w_{i_k}$

Then, we can traverse MSGs G_u and G_w accordingly, i.e., by chosing branch $i_1, i_2, \dots, i_k$ (in that order) and by construction of G_u and G_w, it follows $L(G_u) \cap L(G_w) = \emptyset$.

Formally,

$$M_u = B \cdot \underbrace{(M^u_{i_1} \cdot R^u_{i_1}) \cdot (M^u_{i_2} \cdot R^u_{i_2}) \cdot \ldots \cdot (M^u_{i_k} \cdot R^u_{i_k})}_{\text{in MSG } G_u} \cdot F$$

Similarly,

$$M_w = B \cdot \underbrace{(M^w_{i_1} \cdot R^w_{i_1}) \cdot (M^w_{i_2} \cdot R^w_{i_2}) \cdot \ldots \cdot (M^w_{i_k} \cdot R^w_{i_k})}_{\text{vertices in MSG } G_w.} \cdot F$$

It follows that MSC $M_u = M_w$

since $\underbrace{M^u_{i_1} \cdot \ldots \cdot M^u_{i_k}}_{\text{encodes } u_{i_1} \ldots u_{i_k}} = \underbrace{M^w_{i_1} \cdot \ldots \cdot M^w_{i_k}}_{\text{encodes } w_{i_1} \ldots w_{i_k}}$

$$u_{i_1} \ldots u_{i_k} = w_{i_1} \ldots w_{i_k}$$

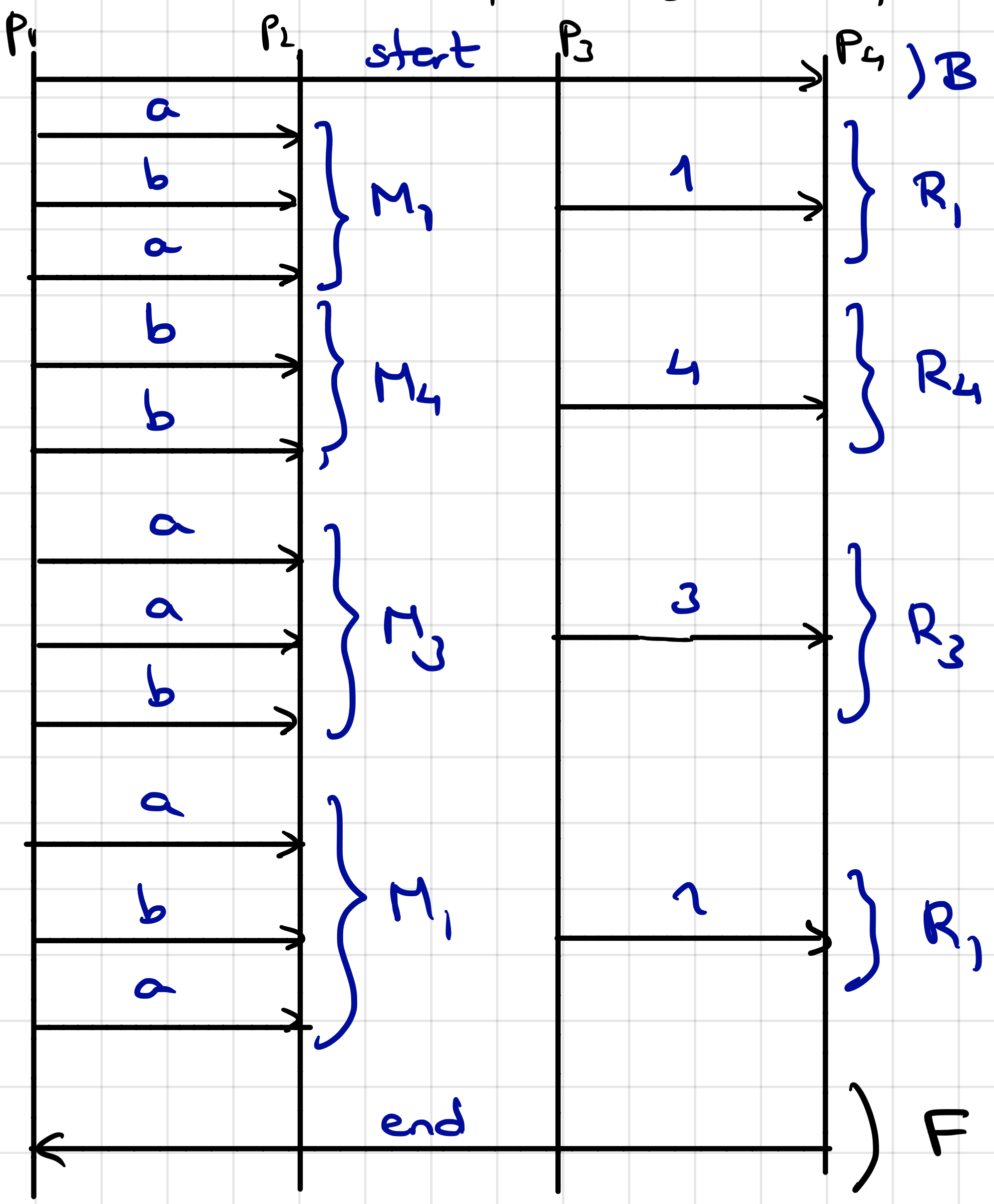
and

$\underbrace{R^u_{i_1} \cdot \ldots \cdot R^u_{i_k}}_{\text{encodes } i_1, \ldots, i_k} = \underbrace{R^w_{i_1} \cdot \ldots \cdot R^w_{i_k}}_{\text{encodes } i_1, \ldots, i_k}$

$$i_1, \ldots, i_k = i_1, \ldots, i_k$$

$\underline{\text{Example}}$ $u = \underbrace{aba}_{=u_1} \; \underbrace{bb}_{=u_4} \; \underbrace{aab}_{=u_3} \; \underbrace{aba}_{=u_1}$ $\quad \underbrace{1, 4, 3, 1}_{\substack{\text{index} \\ \text{order} \\ i_1, \dots, i_4}}$

MSC of a run of MSG G_u



$$MSC \in L(G_u)$$

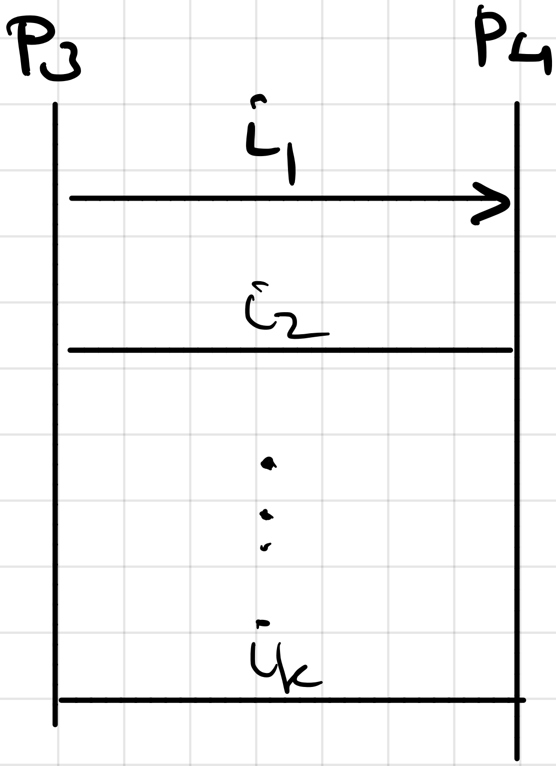
in a similar way, we traverse G_w where

$$\underbrace{a}_{w_1} \; \underbrace{babba}_{=w_4} \; \underbrace{aba}_{=w_3} \; \underbrace{a}_{=w_1}$$

$$MSC \in L(G_u) \cap L(G_w) \neq \emptyset$$

"$\Leftarrow$" Assume $L(G_u) \cap L(G_w) \neq \emptyset$.

Then by construction of G_u and G_w the message contents between P_3 and P_4 yield



$$R^{u}_{i_1} \cdot \ldots \cdot R^{u}_{i_k} = R^{w}_{i_1} \cdot \ldots \cdot R^{w}_{i_k}$$

as $R^{u}_{i_j} = R^{w}_{i_j}$ for all $1 \leq j \leq k$

G_u and G_w can only produce the same index sequence $i_1, i_2, \ldots, i_k$ if the correspondig message between P_1 and P_2 are exchanged, so $M \in \underbrace{L(G_u) \cap L(G_w)}_{\neq \emptyset}$ yields

$$u_{i_1} u_{i_2} \cdots u_{i_k} = w_{i_1} w_{i_2} \cdots w_{i_k}$$

Thus, (u, w) has a solution. $\square$.