

Local-Choice HMSCs:

Don't Choose Globally,
Implement Easily

Blaise Genest & Anca Muscholl
(LIAFA, Paris 7, France)



MSCs: **graphical** specifications of communication protocols
(norm of Int. Telecomm. Union)

Client asks Firewall to access the Server, providing a password.

Firewall checks the passwd and sends a log to Server.

If passwd fails, Firewall kicks the Client & Server acknowledges log.
Client can resend a request & Server can ban user and inform
Firewall.

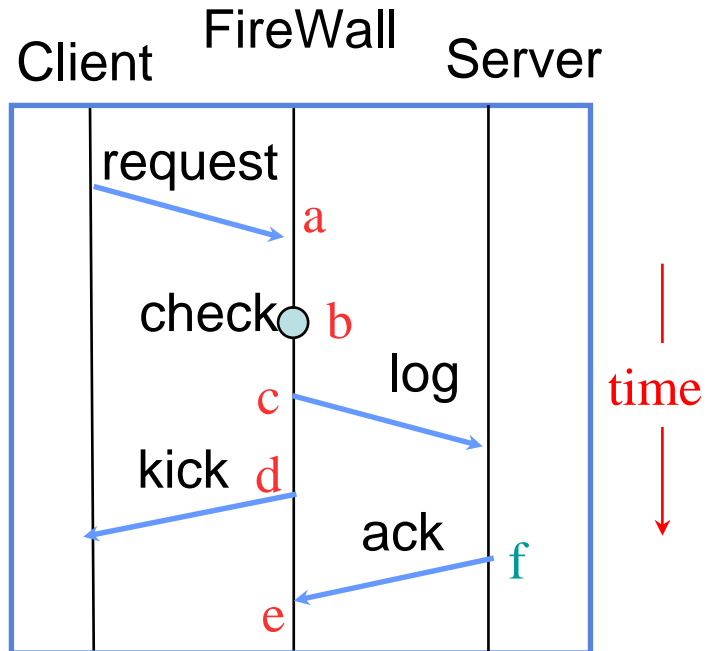
Else, Server approves the connection and Firewall grants the access.

→ **early verification**

- I Local-Choice
- II Extended Local-Choice
- III Conditional Local-Choice



Definition of MSC [ITU Z120]



MSC

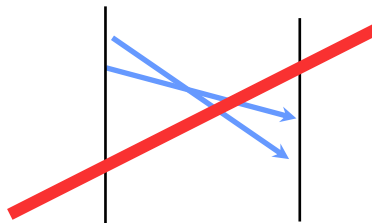
Partial order on events a,b,c...

f incomparable with d

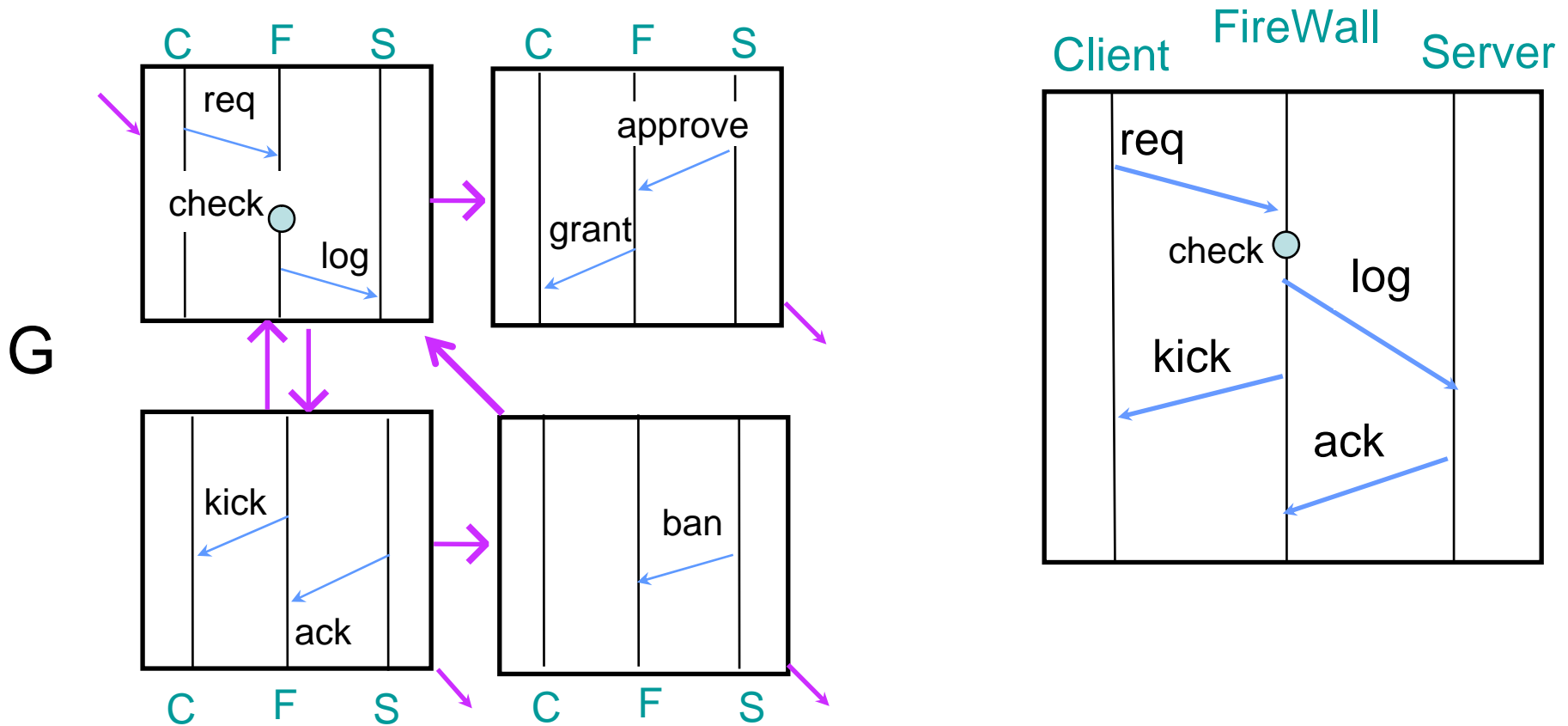
Each process: total order

$a < b < c < d < e$

FIFO channels (no overtaking)



Definition of HMSC (MSC-graph) [Z120]



$L(G)$ = set of MSCs labeling accepting paths of G



Synthesizing Executable Models

HMSC specification:

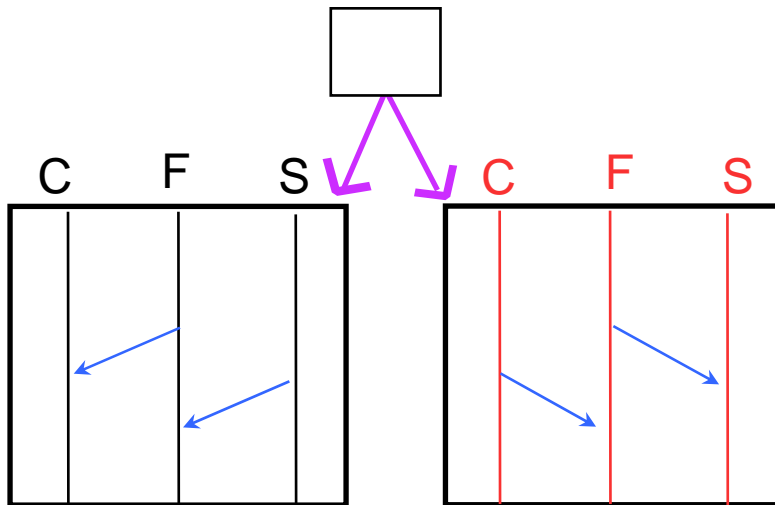
- Collection of scenarios (wanted / unwanted)
- Non-deterministic choice (environment?)
- Data abstraction (parameters)

Specification must be executable/implementable.

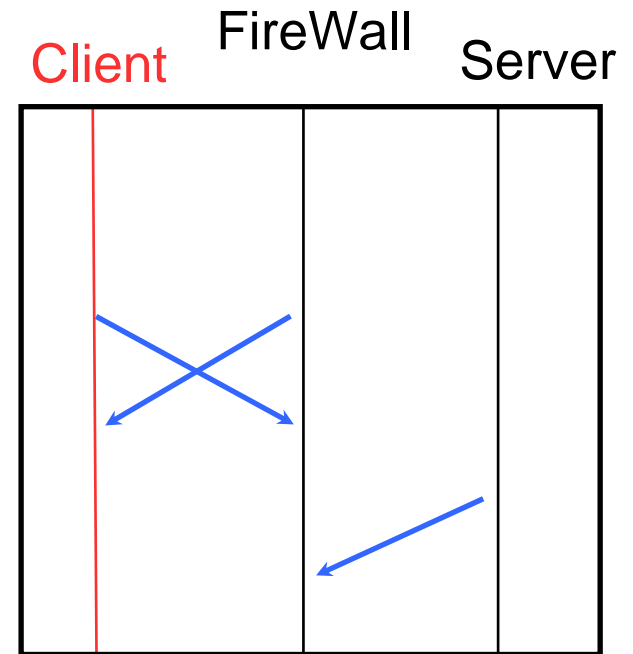
- Early test during the design process.
- Simulation & test runs.



HMSCs not Always Implementable

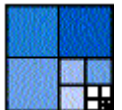


Bird eyes (global knowledge)



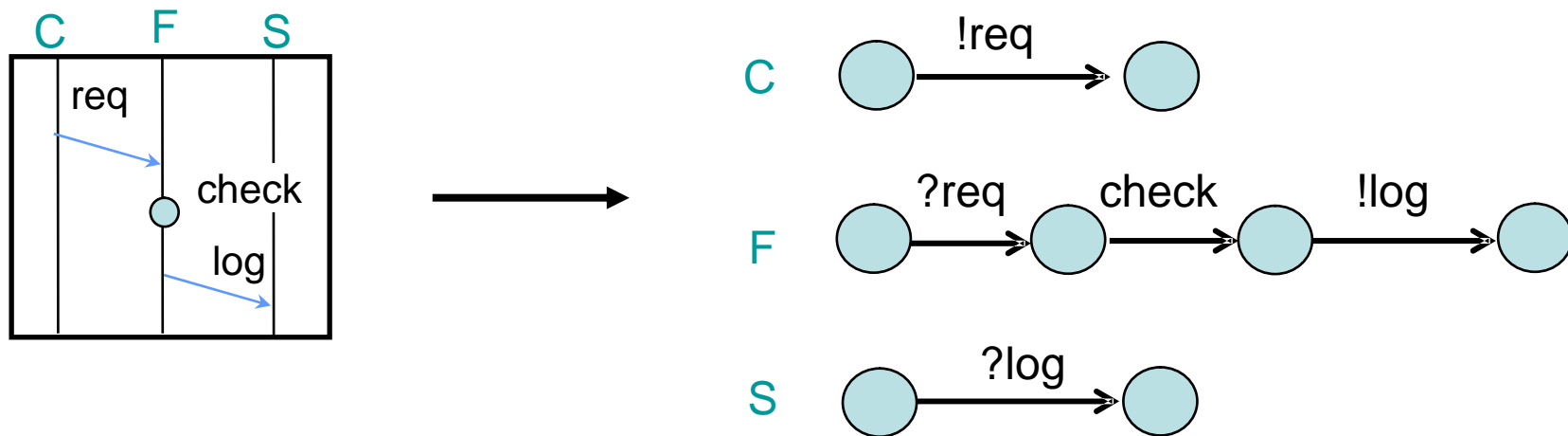
local knowledge
on each proc

Not implementable



What is an Implementation?

Implementation by Communicating Automata

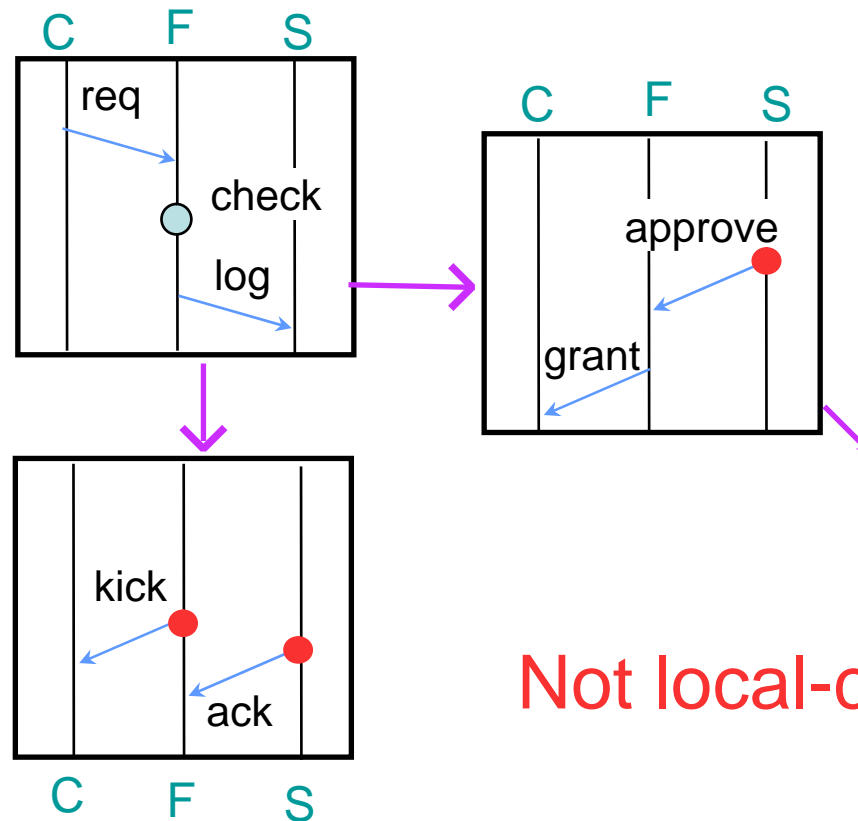


No **deadlock**: Each accessible global state is co-accessible.



Local-Choice HMSCs [Leue, Helouet]

Solution for implementation: each choice controlled by ONE proc

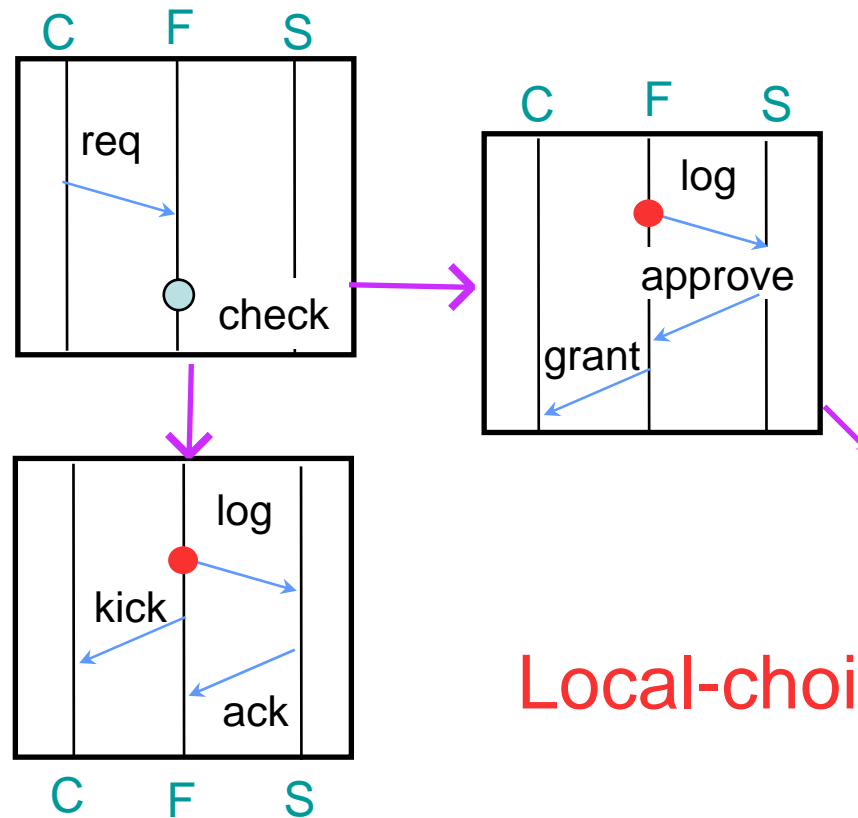


Not local-choice



Local-Choice HMSCs

Solution for implementation: each choice controlled by ONE Proc

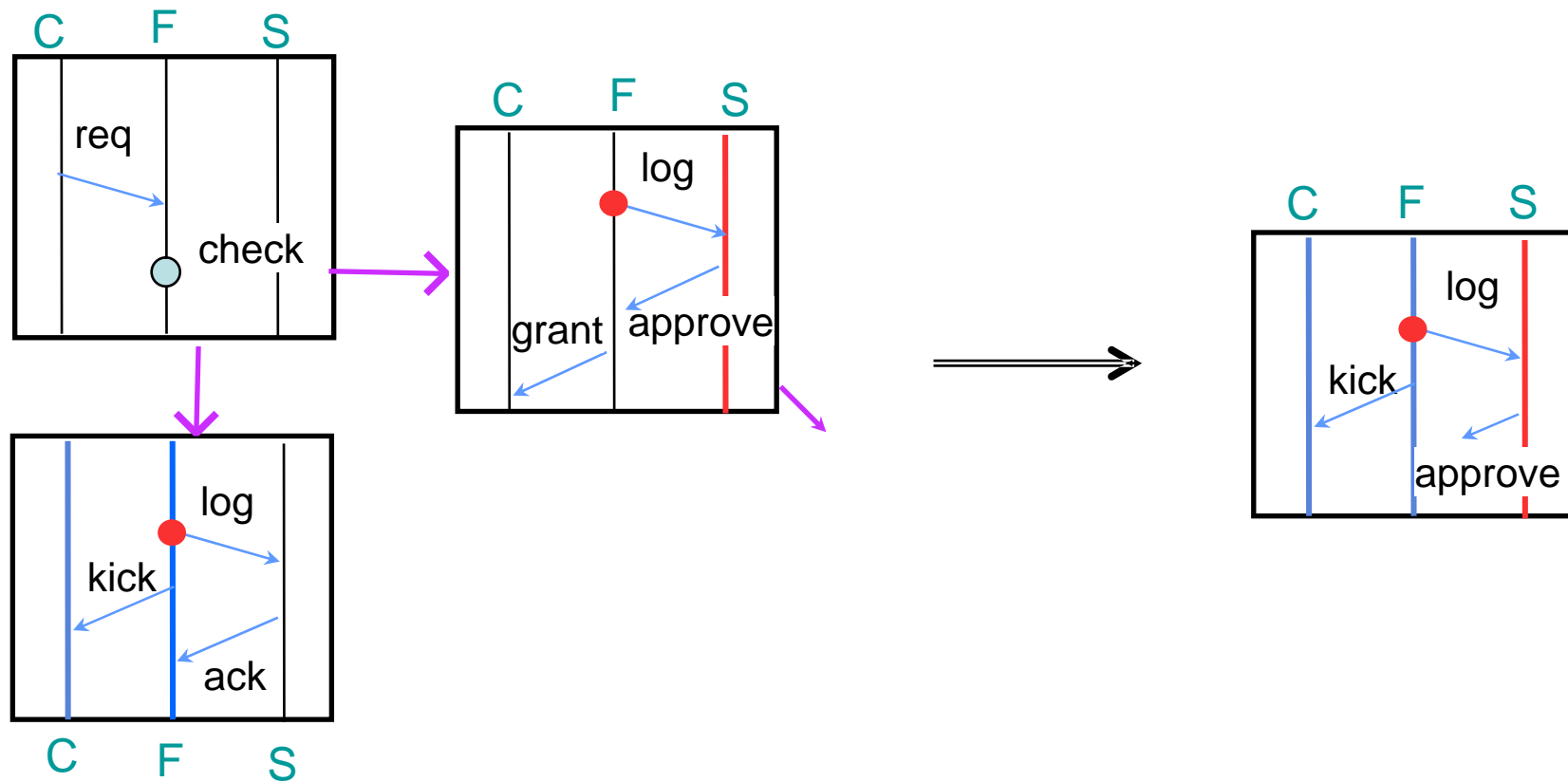


Local-choice



A Simple Implementation

- The behaviour of each automaton defined by **projections**.

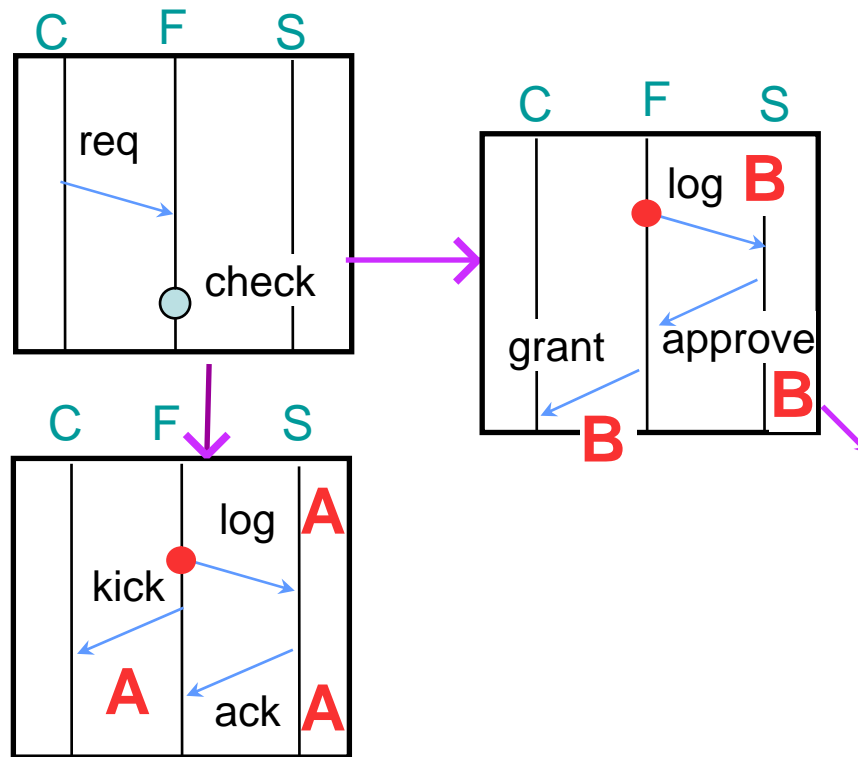


Problem: local-choice HMSC not implementable.



Extending Implementation [GMSZ02]

- Adding **messages**: too strong (everything is implementable)



- With extra **data**, local-choice HMSCs are implementable.



Implementation: Overview of Results

Alur, Etessami, Yannakakis (ICALP'01):
safe (deadlock-free) realizability of HMSCs

- Safe realizability **EXPSpace** for regular HMSCs

Mukund, Kumar, Sohoni (Concur'00):
weak realizability of regular HMSCs with extra data

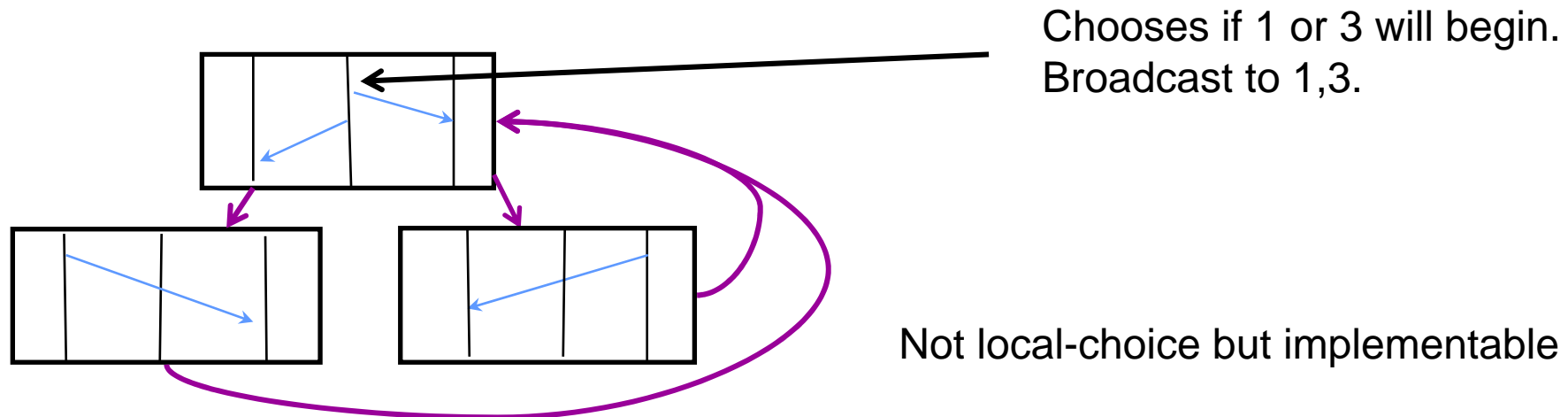
G., Muscholl, Seidl, Zeitoun (ICALP'02)

- extra data
- Local-choice: deadlock-free (safe)



Questions

- In: HMSC G Q: Is G implementable with extra data?
Open question
- In: HMSC G Q: Does there exist H local-choice
Open question with $L(G) = L(H)$?

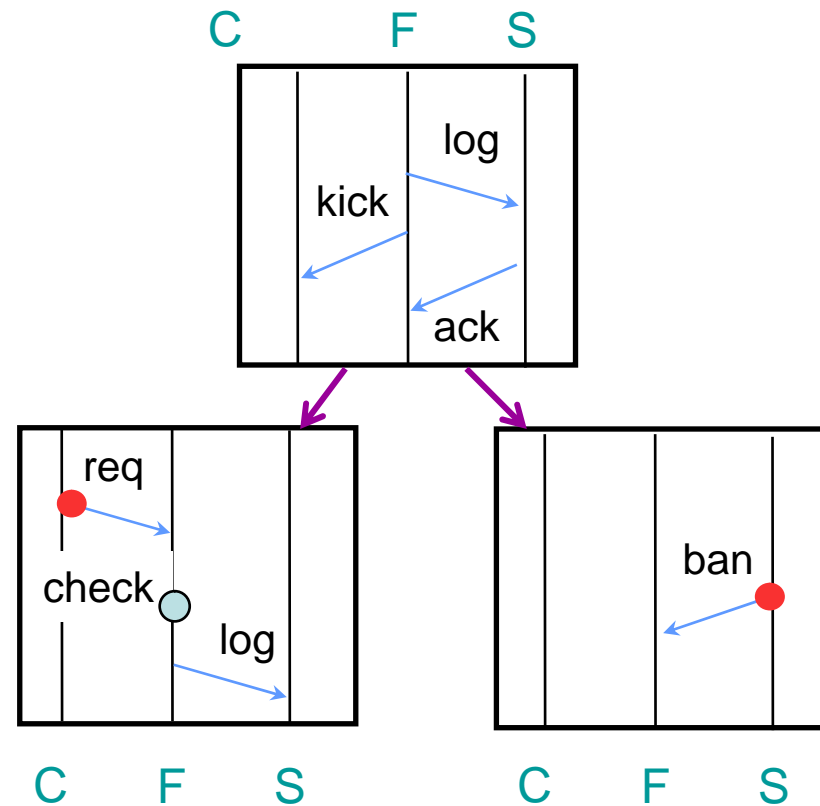


Local-choice not general enough



Extended Local-Choice [GM03]

- The minimal process after a choice can be different.



Not Local-Choice but **Extended Local-Choice**



Properties of Extended Local-Choice [GM03]

- Model-Checking: same complexity as for Local-Choice:

NLOG/PSPACE for negative/positive check

- Always implementable with extra (linear) data

- Given HMSC G .

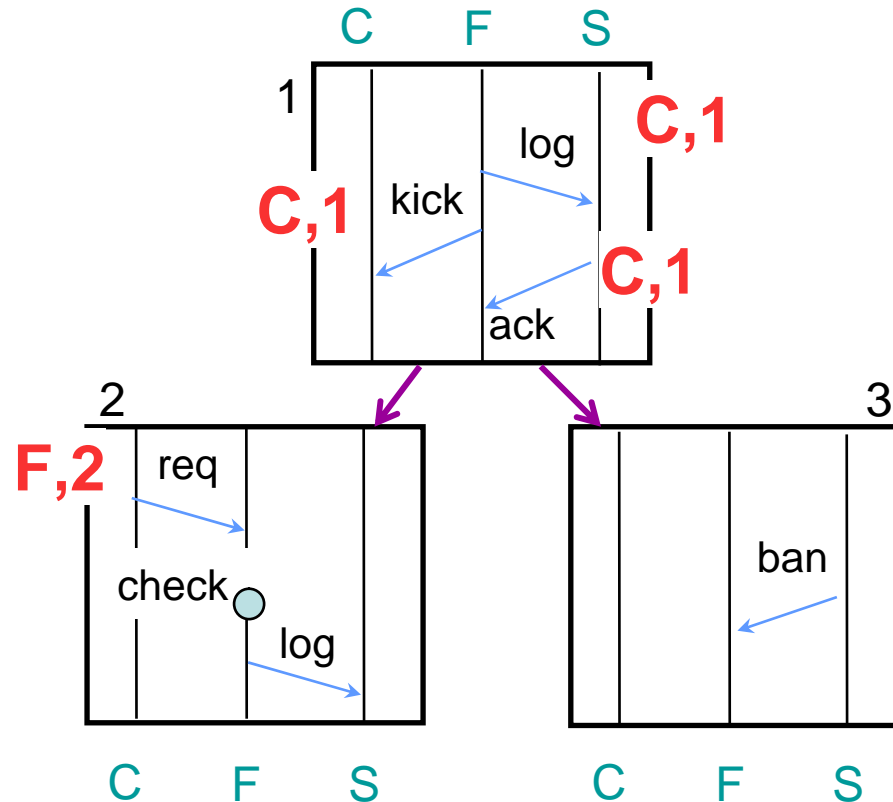
We can check if there exists **xic** H with $L(H) = L(G)$

Co-NP-complete

$|H|$ at most exponential in $|G|$



Implementation of Extended Local-Choice



Firewall decided whether the Server would ban the Client or not

↔ Not possible in real life!



Problems

2 meanings of a choice:

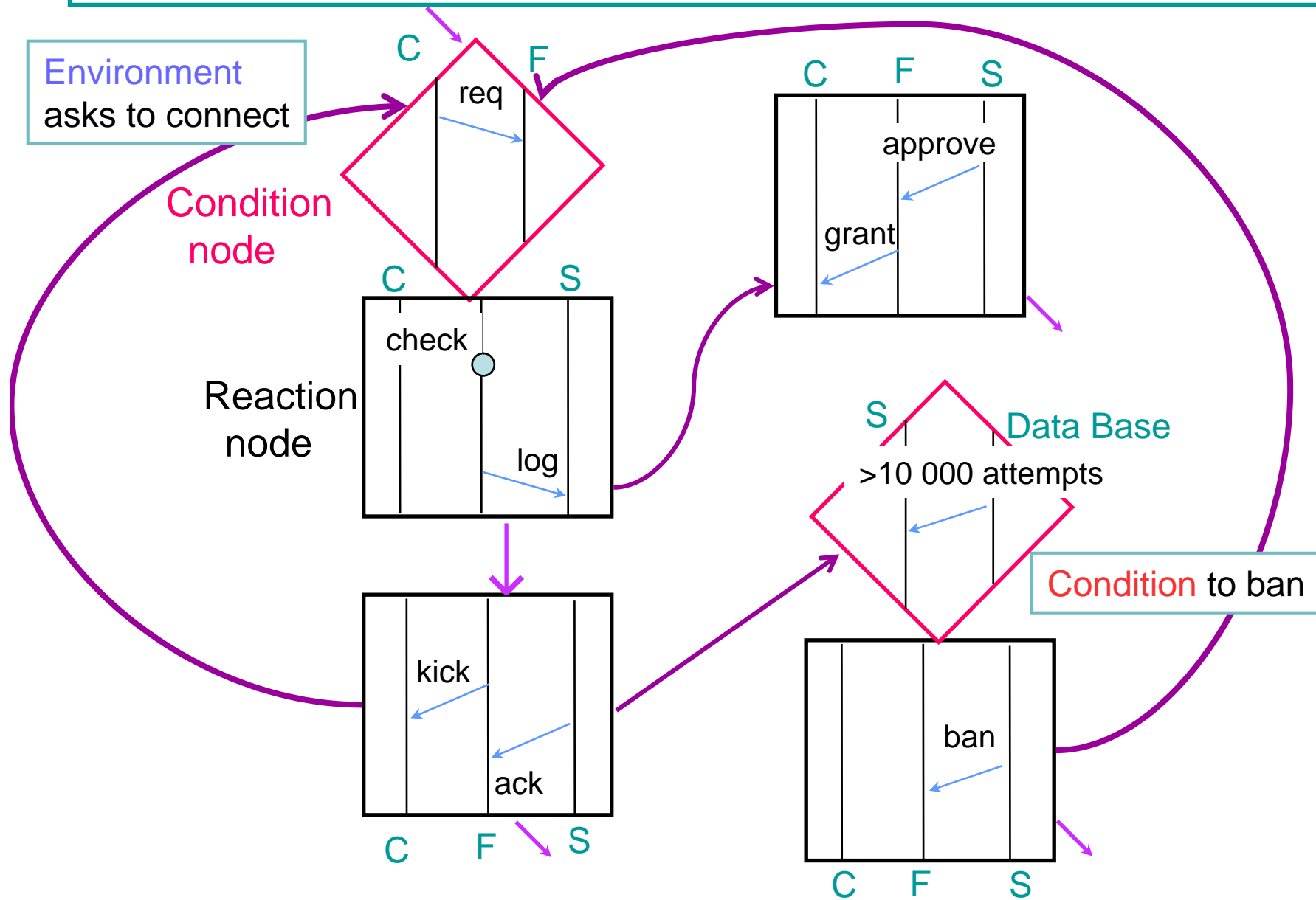
Non deterministic choice (possibility)
Reaction activated by some Condition

Environment cannot make a choice for the system.

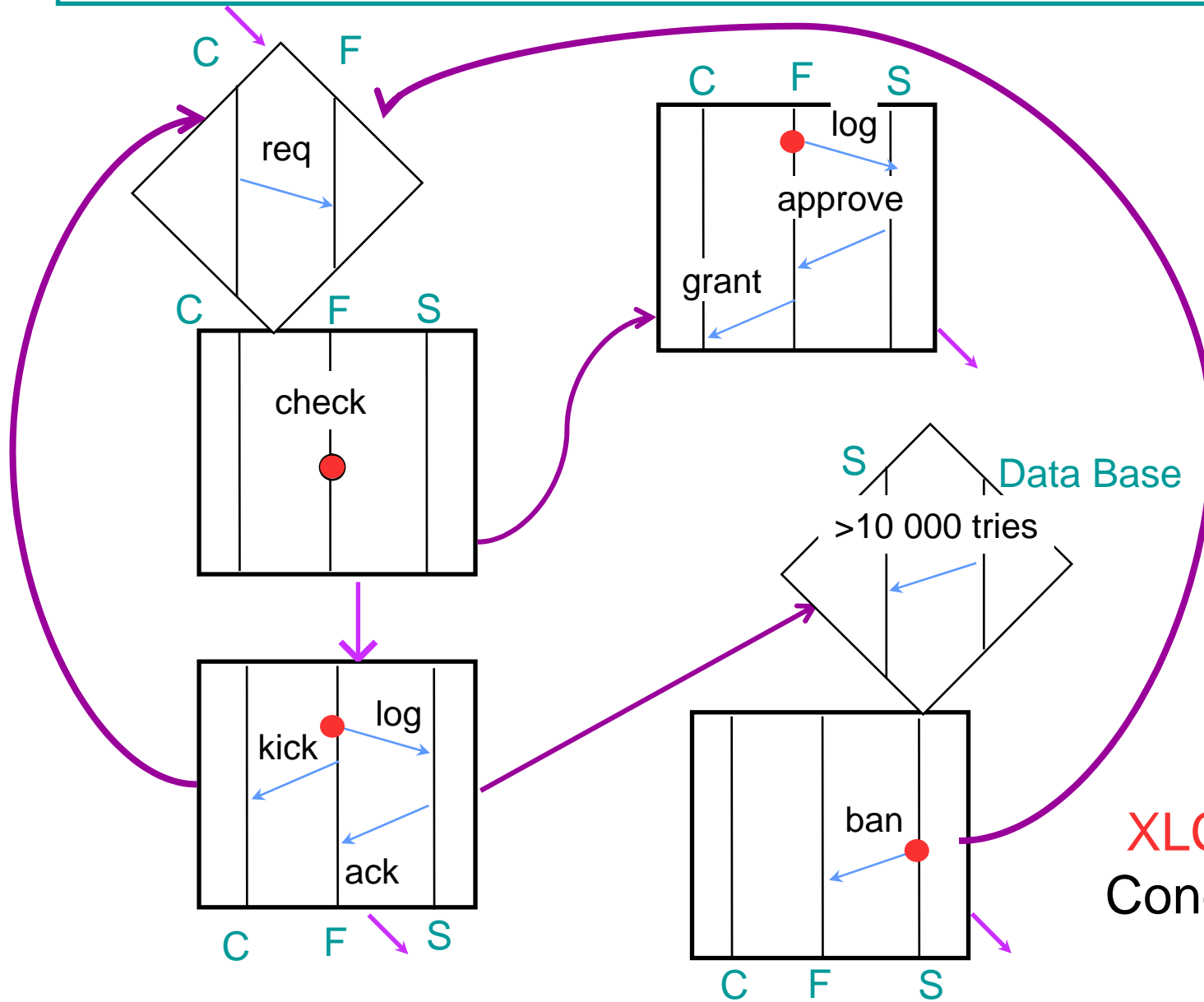
→ Express explicitly the environment & conditions.



Conditional HMSC [GM03]



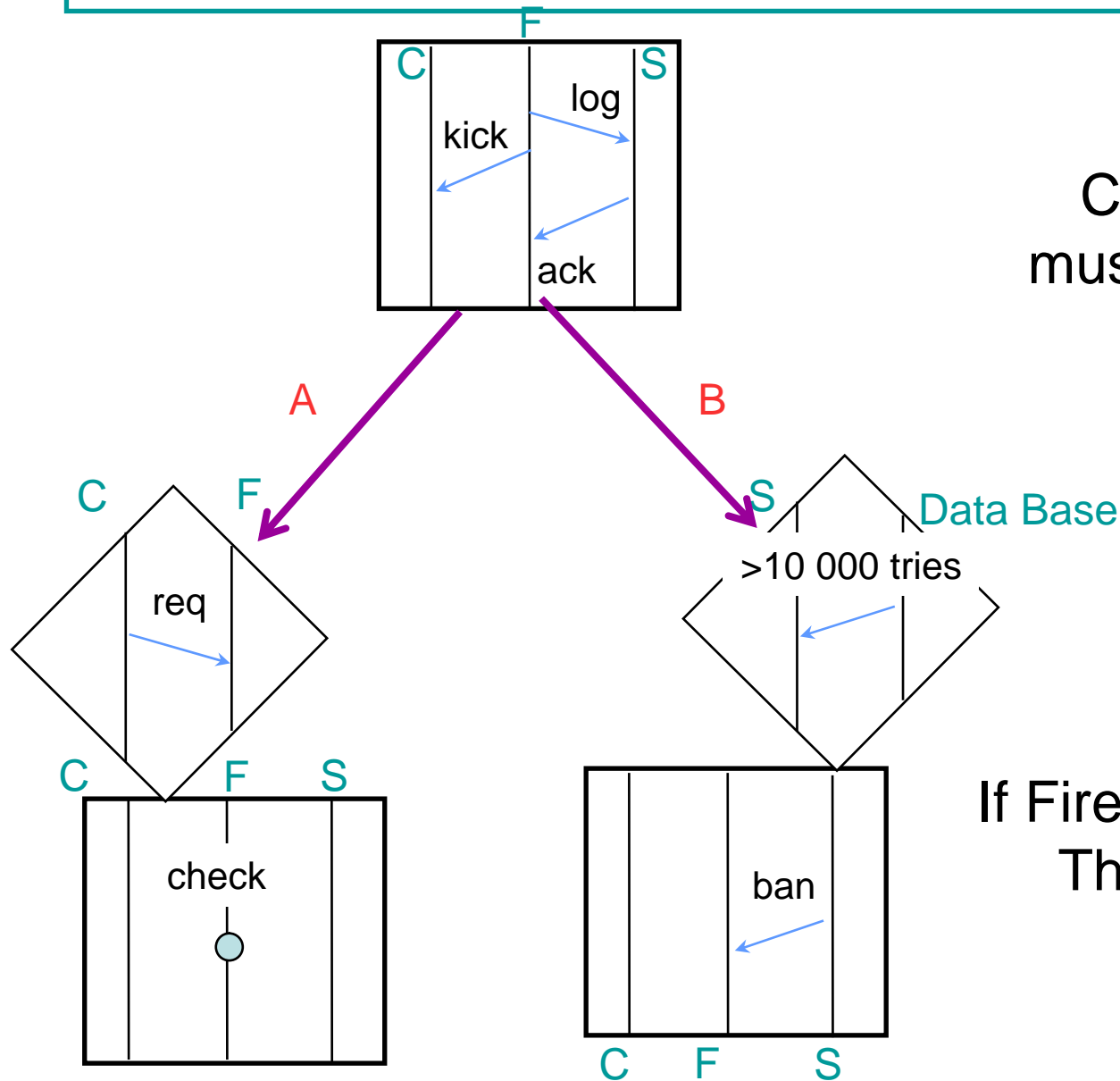
Conditional local-choice HMSC [GM03]



First :
XLC if we forget
Conditional Nodes



Conditional local-choice HMSC [GM03]



Second:
Conditional MSCs
must be **unambiguous**

If Firewall sees condition A
Then Server cannot
see condition B



Conditional local-choice HMSC

Conditional local-choice HMSC are **always implementable**

- Go to polling state
- Wait to be waken up either by environment
or by another process activated by environment

Rem: Condition 2 says two processes cannot be activated simultaneously by the environment



IV Properties of Extended Local-Choice [GM03]

- Given HMSC G .
We can check if there exists xl_c H with $L(H) = L(G)$

Co-NP-complete

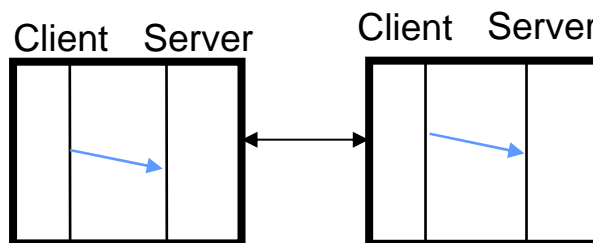
$|H|$ at most exponential in $|G|$



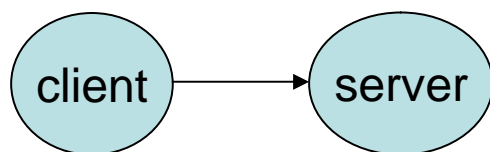
IV

Transition cooperative MSC-graphs

Communication graph of each loop is weakly connected



Communication graph



Transition Connected

Th[GMSZ02] : There exists an automaton A of exp. Size that recognizes exactly the atoms of $L(G)$.



IV

Structural Prop ! Langage Prop

A langage property :

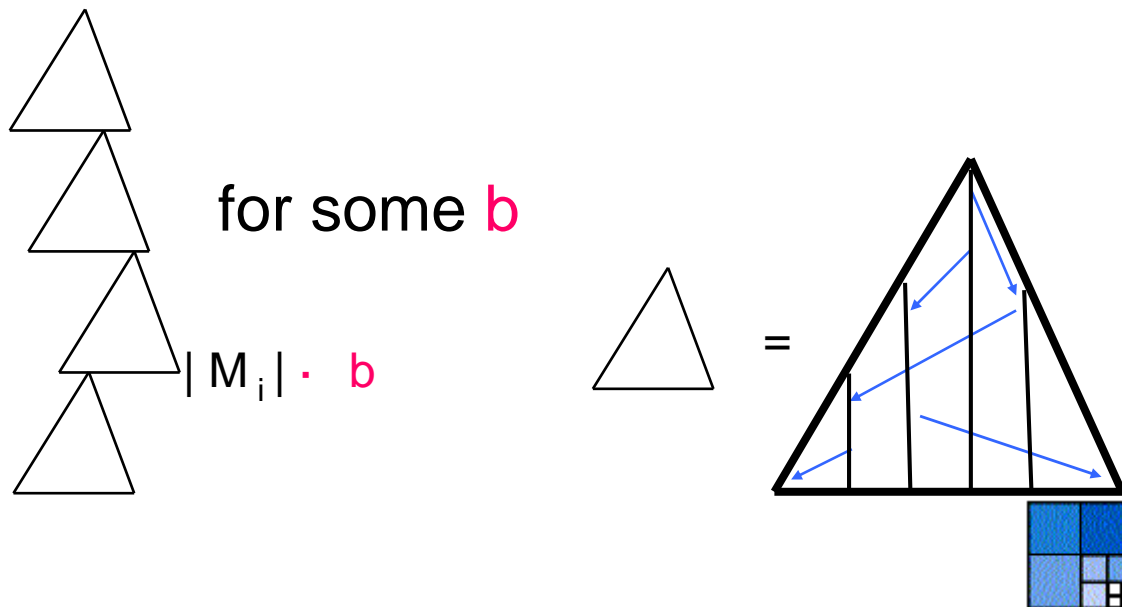
① Given L, does there exists H xlc s.t. $L(H)=L$

(L is given by a globally cooperative HMSC G)

A structural property :

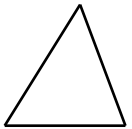
each choice controlled
by some minimal processes

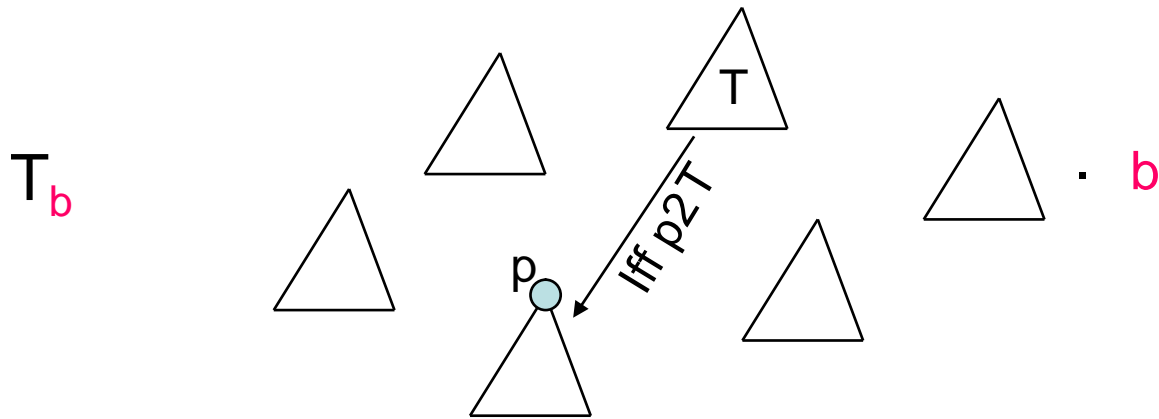
Th: ① iff for all $M \in L$, $M =$



IV

Structural Prop ! Langage Prop

Démo : ) ① (other direction is trivial)



We have $L \subseteq L(T_b)$

T_b recognizes atoms of G



IV

Structural Prop ! Langage Prop

Démo :

We have $G ! A$, s.t. A recognizes atoms of G

We can build $H=A \hat{\text{A}} T_b$ with T_b

H is xlc

$$L \mu L(T_b \hat{\text{A}} A = H) \mu L(A) = L$$

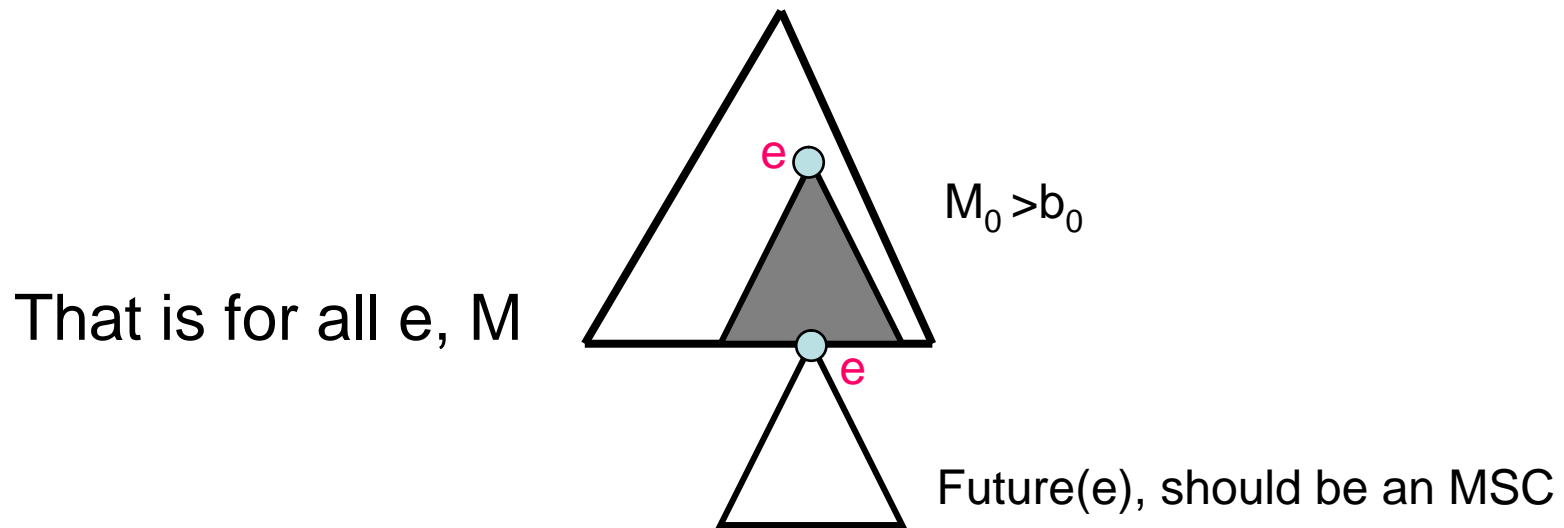
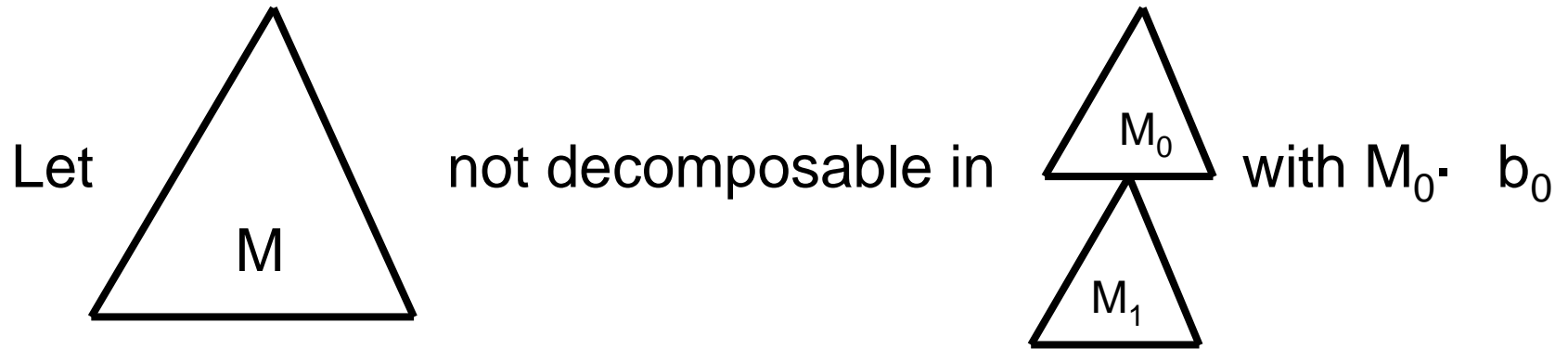
So $L=L(H)$.

H exponential in b and in G .

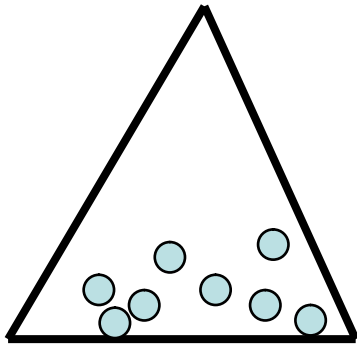


IV

b_0 of polynomial size in $|H|$ is enough

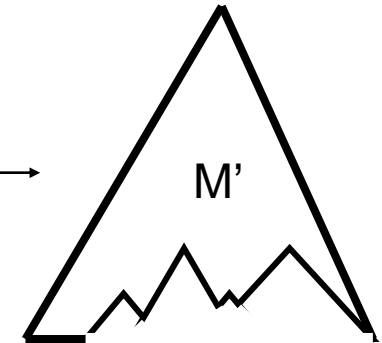
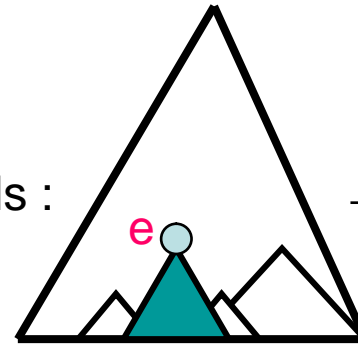


V b_0 of polynomial size in $|H|$ is enough



s.t. future \circ is an MSC.

We take the minimals :



For all e

M'_e



$$|M'| > b_0/2$$

OR

$$\text{for all } e, |M'_e| > b_0/2$$

Lemma: if $|X| > b_0/2$, then there exists a loop of H entirely in X .

We iterate the loop(s) : problem for b as big as we want.

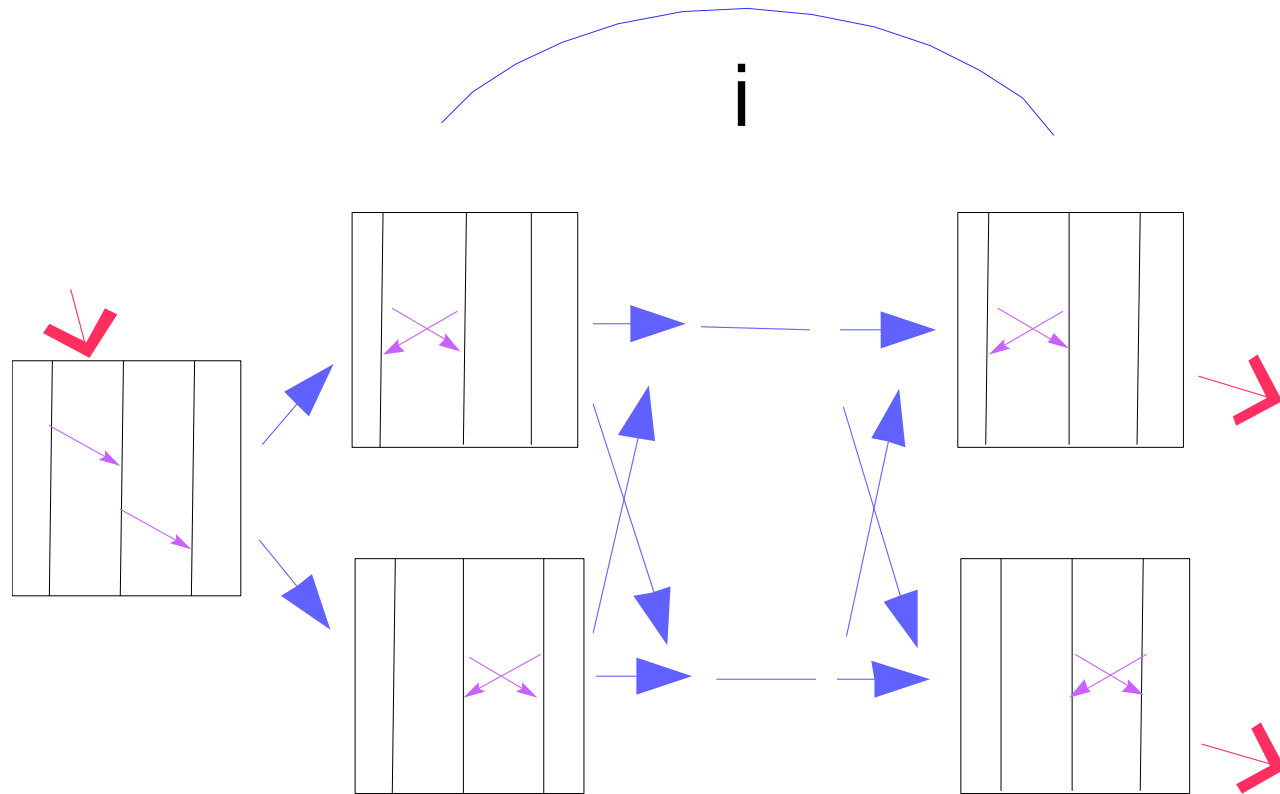


Directions for future work

- HMSC specifications as **open** systems: environment, uncontrollable processes
- Implementation: controller synthesis
- Strategy: add data or messages **only** on controllable processes

IV

We cannot do better than exp. in G

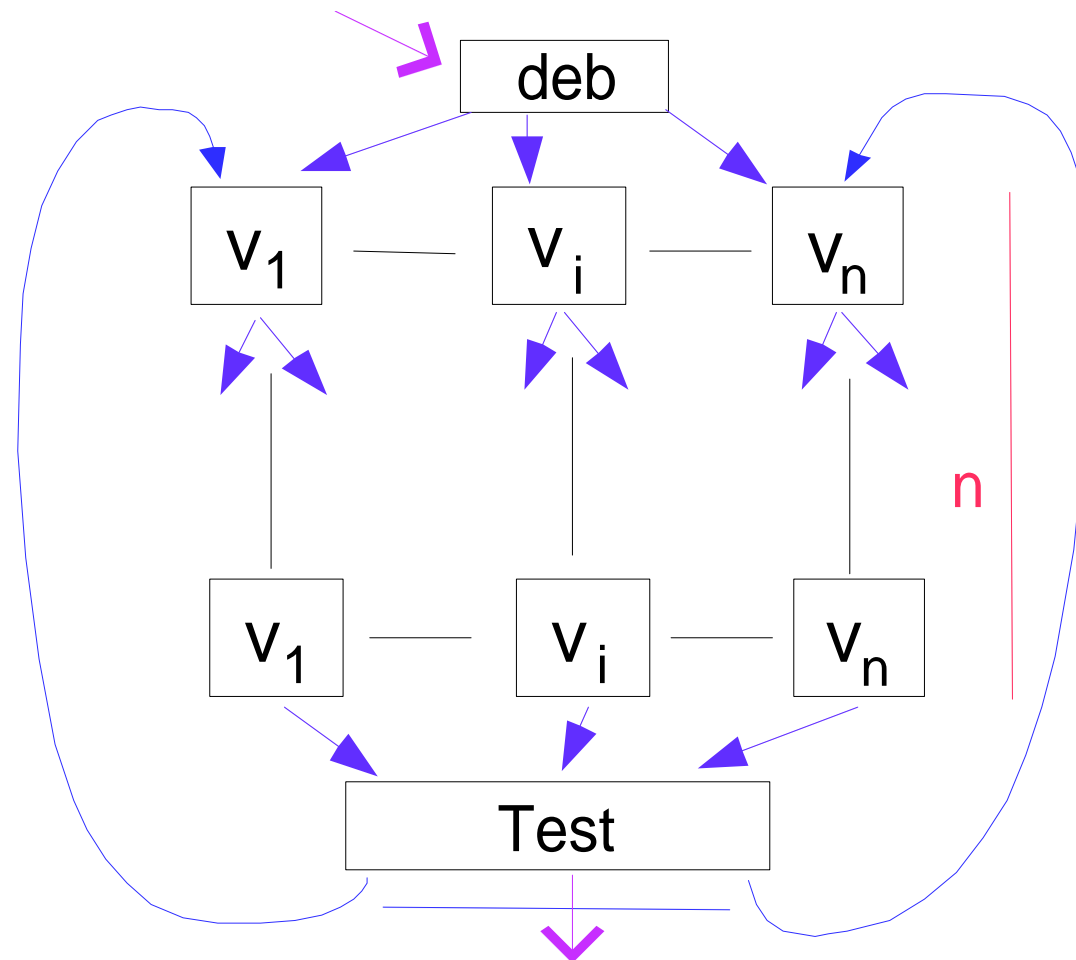


IV

Co-NP hardness

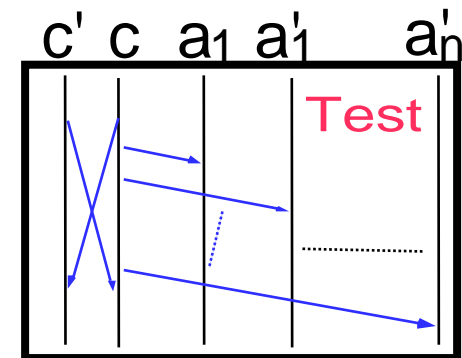
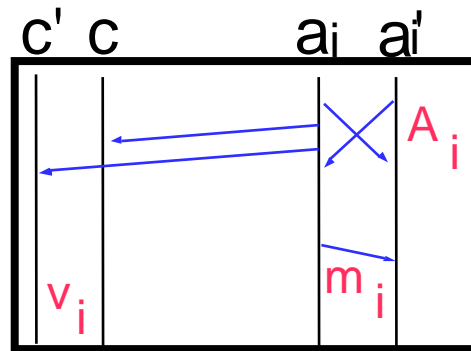
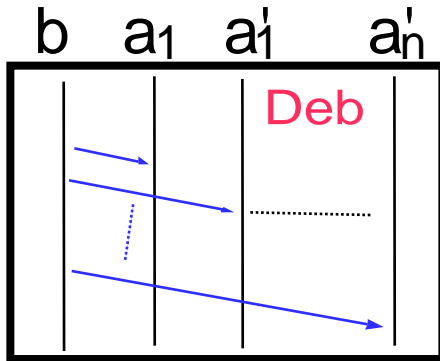
Reduction with co-hamiltonian path:

- No hamiltonian path if twice the same node in each n-path



IV

Co-NP hardness



IV

Co-NP hardness

Twice A_i

