Reachability analysis: Undecidability of Rectangular Hybrid Automata

Sayan Mitra

Verifying cyberphysical systems

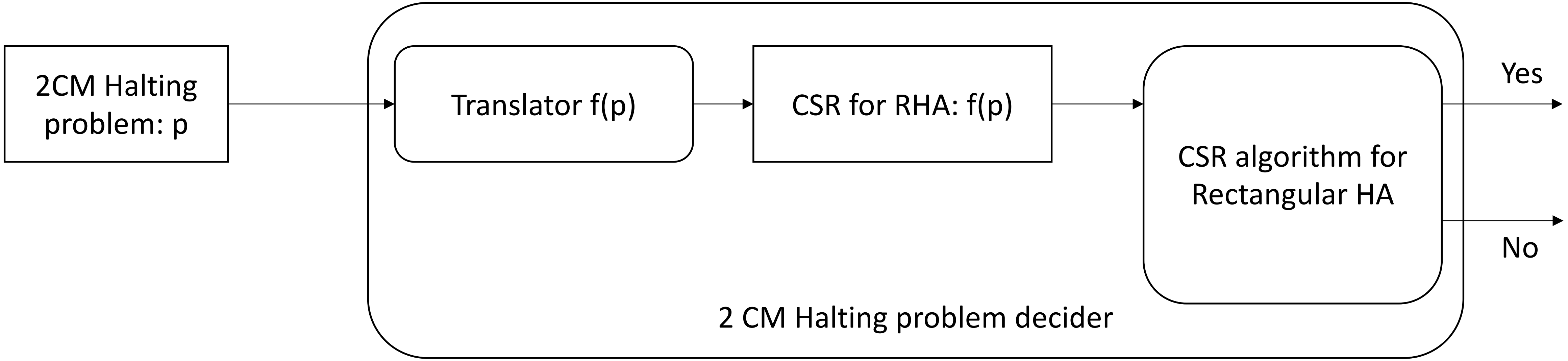
mitras@illinois.edu

- Is this problem decidable? No
  - **[Henz95]** Thomas Henzinger, Peter Kopke, Anuj Puri, and Pravin Varaiya. What's Decidable About Hybrid Automata?. Journal of Computer and System Sciences, pages 373–382. ACM Press, 1995.
- We will see that the CSR problem for rectangular hybrid automata (RHA) is undecidable
- This implies that automatic verification of invariants and safety properties is also impossible for this class of models
- The result was shown by Henzinger et al. [1995] through a *reduction from* the Halting problem of two counter machines

Recall from review of computability theory

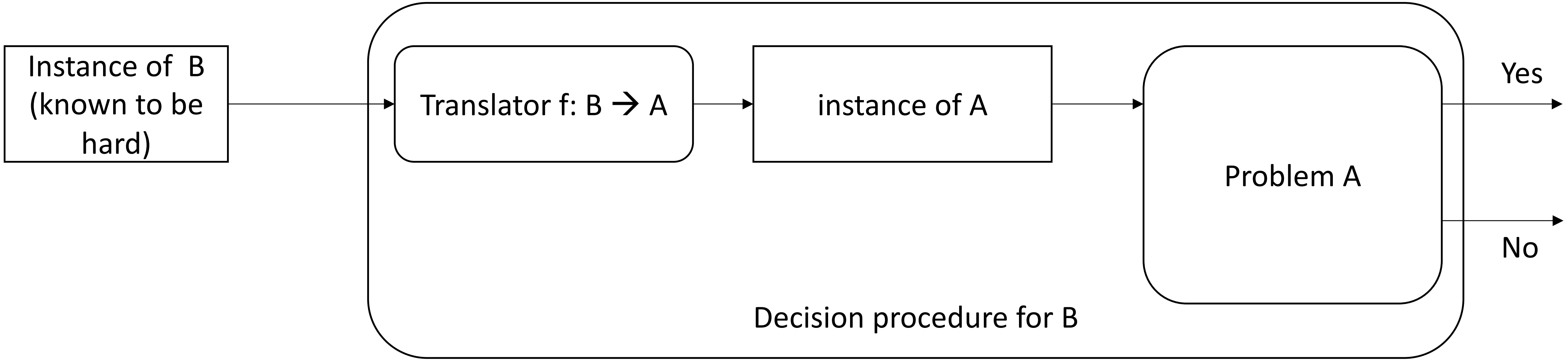
- There is a language L such that L is Recursively Enumerable (RE) but not Recursive
- That is, it halts on accepting inputs but not guaranteed to do so on all inputs
- $L_{halt} = \{\langle M \rangle \mid M \text{ } halts \text{ } on \text{ } \epsilon\}$
- This is the set strings that encode Turing Machines that halt (without any inputs)

Reduction from Halting Problem for 2CM



Suppose CSR for RHA is decidable
If we can construct a reduction from 2CM Halting Problem to CSR for RHA then 2CM Halting problem is also decidable

General reductions: Using known hard problem B to show hardness of A



Given B is known to be hard
Suppose (for the sake of contradiction) A is solvable
If we can construct a reduction f: B→A (from B to A) then B becomes easy, which is a contradiction

Counter Machines

An n-counter machine is an elementary computer with n-unbounded counters and a finite program written in a minimalistic assembly language.

More precisely: A 2-counter machine (2CM) is a discrete transition system with the following components:

- Two nonnegative integer counters C and D. Both are initialized to \$0\$.
- A finite program with one of these instructions at each location (or line):
  - INCC, INCD: increments counter C (or D)
  - DECC, DECD: decrements counter C (or D), provided it is not 0,
  - JNZC, JNZD [label]: moves the program control to line *label* provided that counter C (or D) is not zero.

Example 2CM for multiplication

A 2-counter machine for multiplying 2x3 is shown below.

```
INCC;
INCC;           % C = 2
INCD;           % LOOP
INCD;
INCD;
DECC;
JNZC 3;         % Jump to LOOP
                % HALT
```

Exercise: Show that any k-counter machine can be simulated by a 2CM.

Halting problem for 2CM

- A **configuration** of a 2CM is a triple (pc, C, D)
  - pc is the program counter that stores the next line to be executed
  - C, D are values of the counter
- A sequence of configurations (pc0, D0, C0), (pc1, D1, C1), … is an **execution** if the ith configuration goes to the (i+1)st configuration in the sequence executing the instruction in line pci
- Given a 2CM **M** a special halting location (pc_halt), the Halting problem requires us to decide whether all executions of **M** reach the halting location
- Theorem [Minsky 67]. The Halting problem for 2CMs is undecidable.

Reduction from 2CM to CSR-RHS

We have to construct a function (reduction) that maps instances of 2CM-Halt to instances of CSR-RHA

Reduction from 2CM to CSR-RHS

- Program counter pc
- Counters C, D
- Instructions (program)
- Halting location

- Locations, sequence of locations
- Clocks c, d that can go at some constant rates $k_1, k_2, \ldots$
- Transitions: *widgets*
- Particular location / control state (to which we will check CSR)

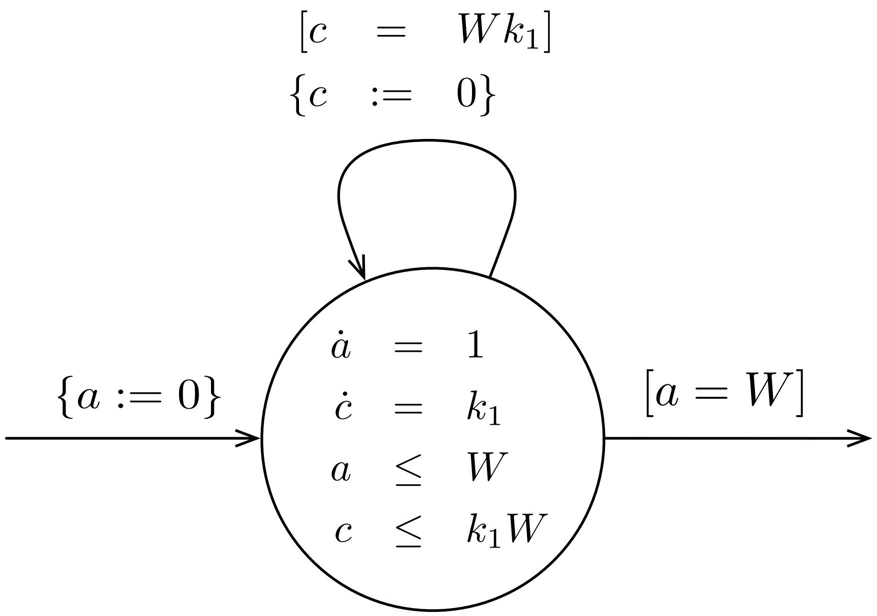
Idea of reduction (an RHA compiler)

- Two clocks
- $c \ = k_1 \left(\frac{k_2}{k_1}\right)^C$
- d $= k_1 \left(\frac{k_2}{k_1}\right)^D$

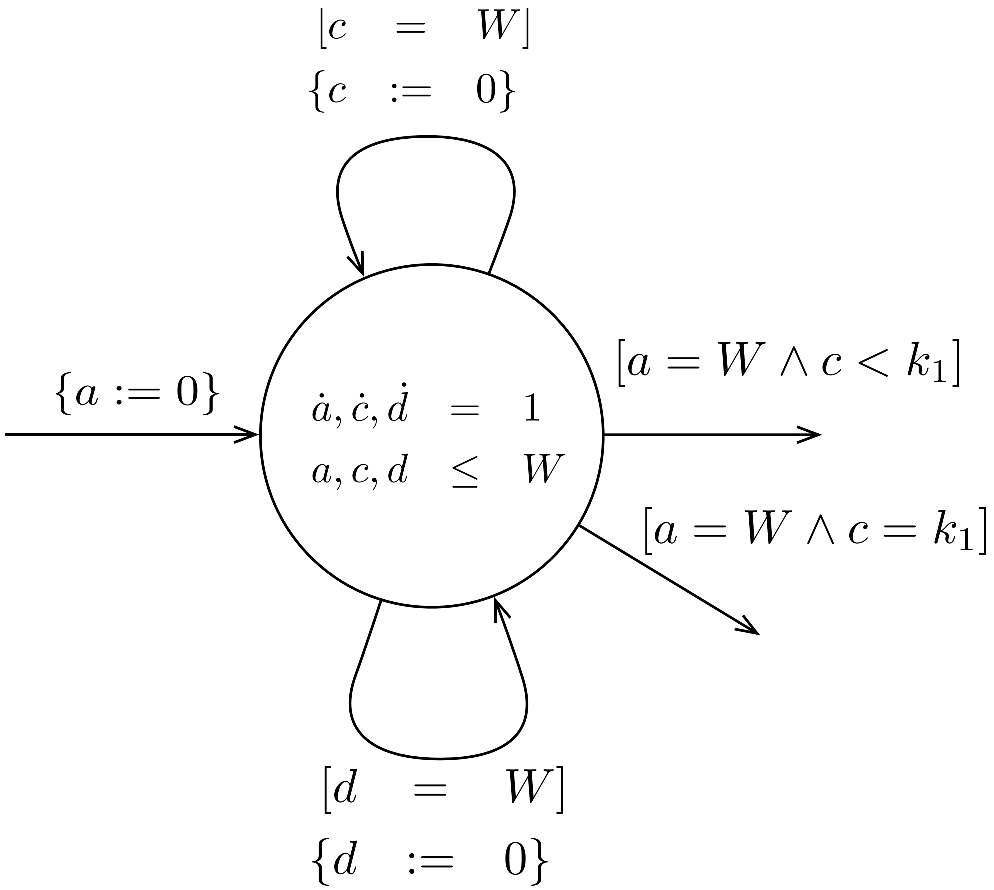
- INCC
- $k_1 \left(\frac{k_2}{k_1}\right)^{C+1} = c \left(\frac{k_2}{k_1}\right)$

- DECC
- $k_1 \left(\frac{k_2}{k_1}\right)^{C-1} = c \left(\frac{k_1}{k_2}\right)$ after checking nonzero $c < k_1$

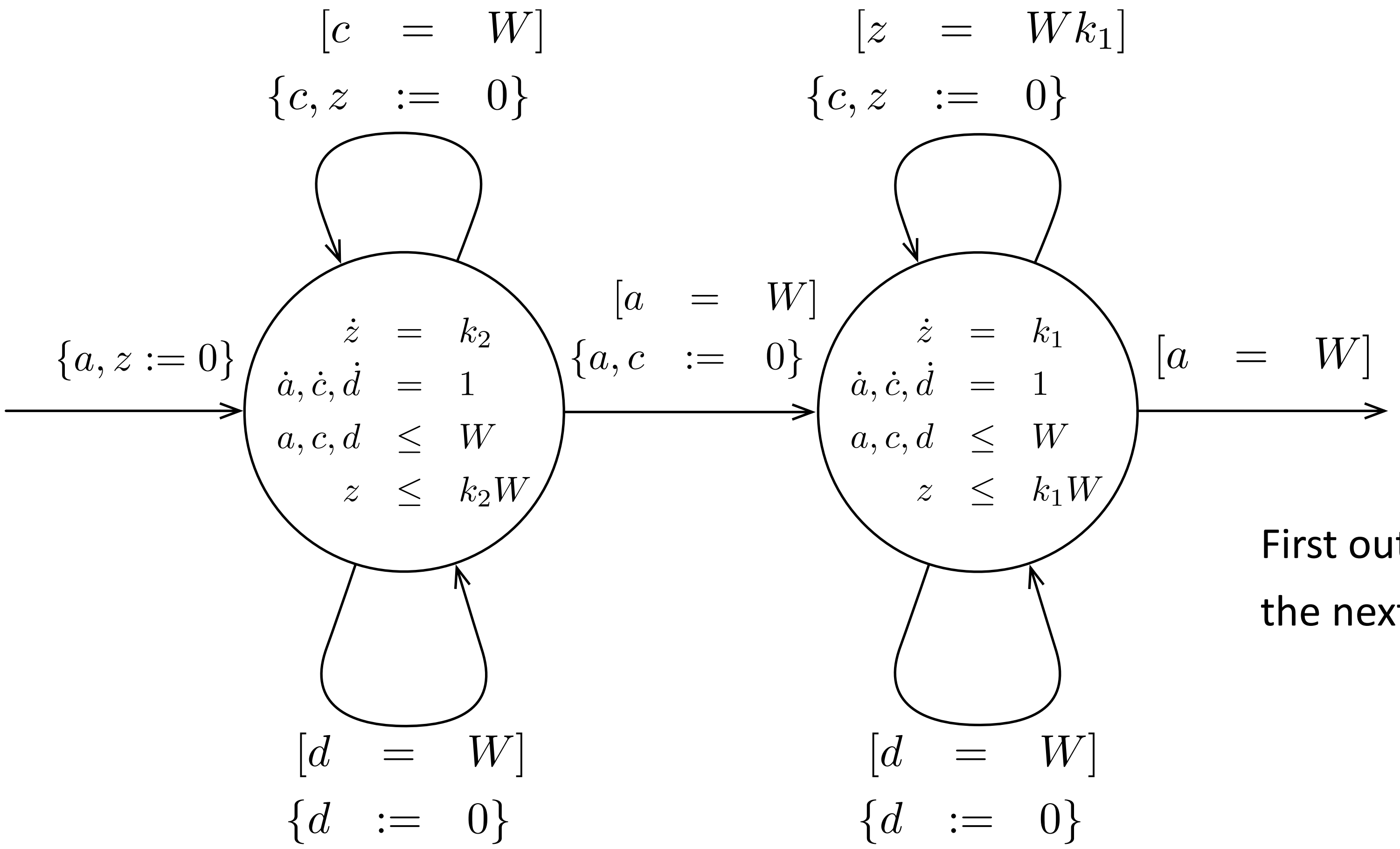
A widget that preserves the value of clock c



A widget for checking JNZC (c < k_1)

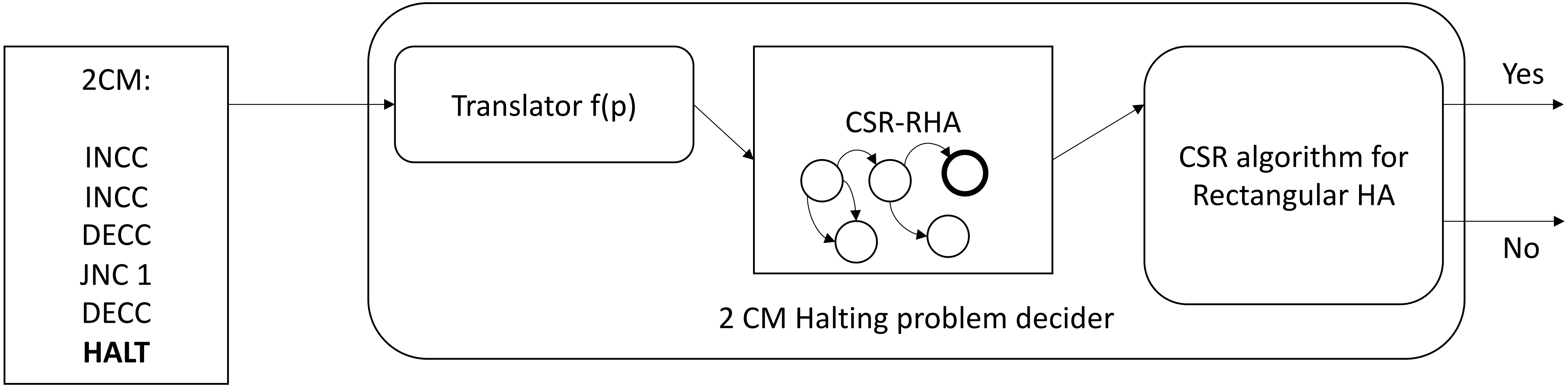


A widget implementing INCC



First outgoing transition sets $z = k_2 c$ and the next outgoing transition sets c $= z * \left(\frac{1}{k_1}\right)$

Putting it all together



Suppose CSR for RHA is decidable
If we can construct a reduction from 2CM Halting Problem to CSR for RHA then 2CM Halting problem is also decidable
Theorem: CSR for RHA is undecidable