Lecture 8: Model Checking

- Model Checking Problem
- Explicit State Algorithm
- Examples
- Model Checking on a Super Computer

Model Checking Problem

Let M be the state–transition graph obtained from the concurrent system.

Let f be the specification expressed in temporal logic.

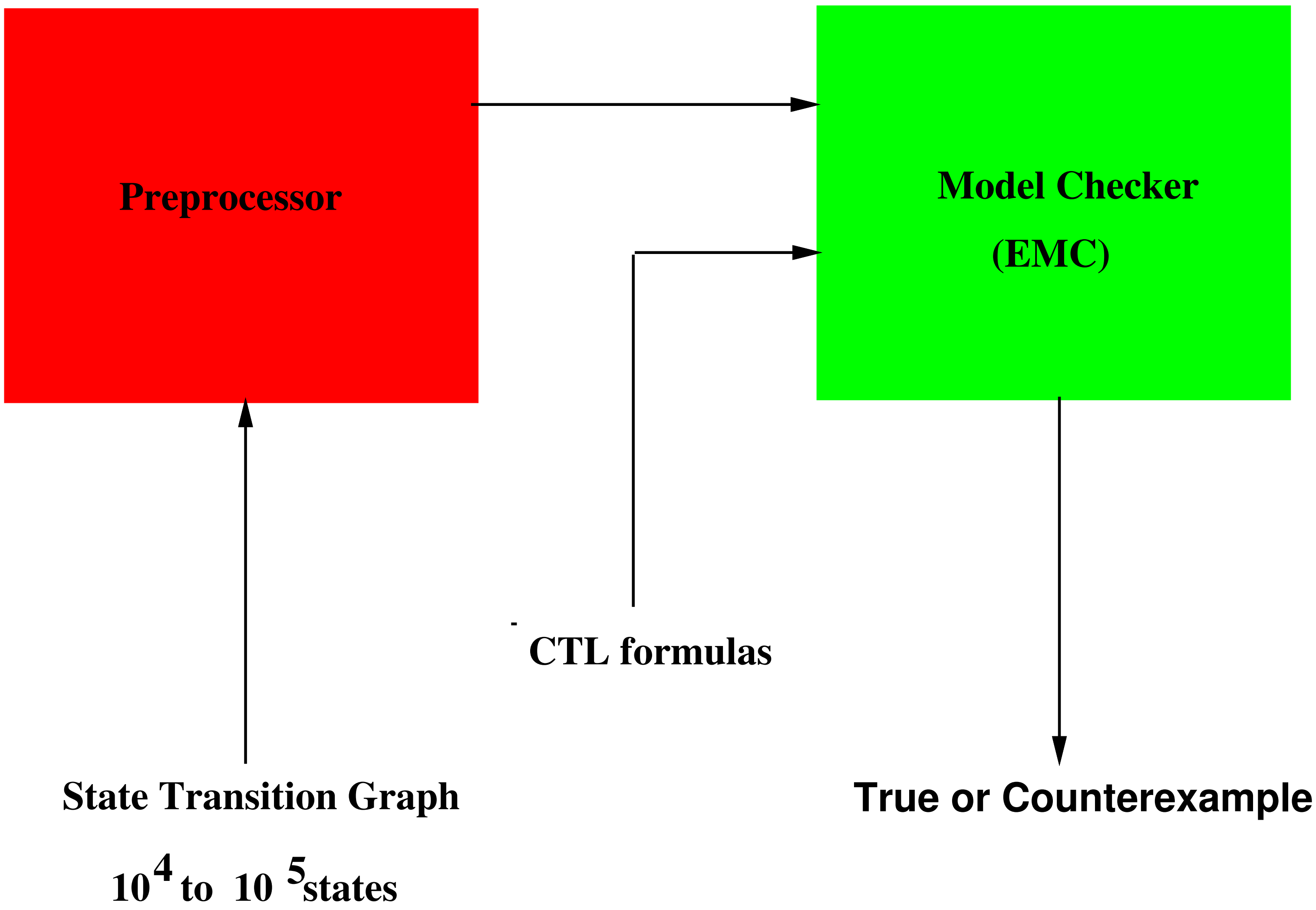
Find all states s of M such that

$$M, s \models f.$$

There exist very efficient model checking algorithms for the logic CTL.

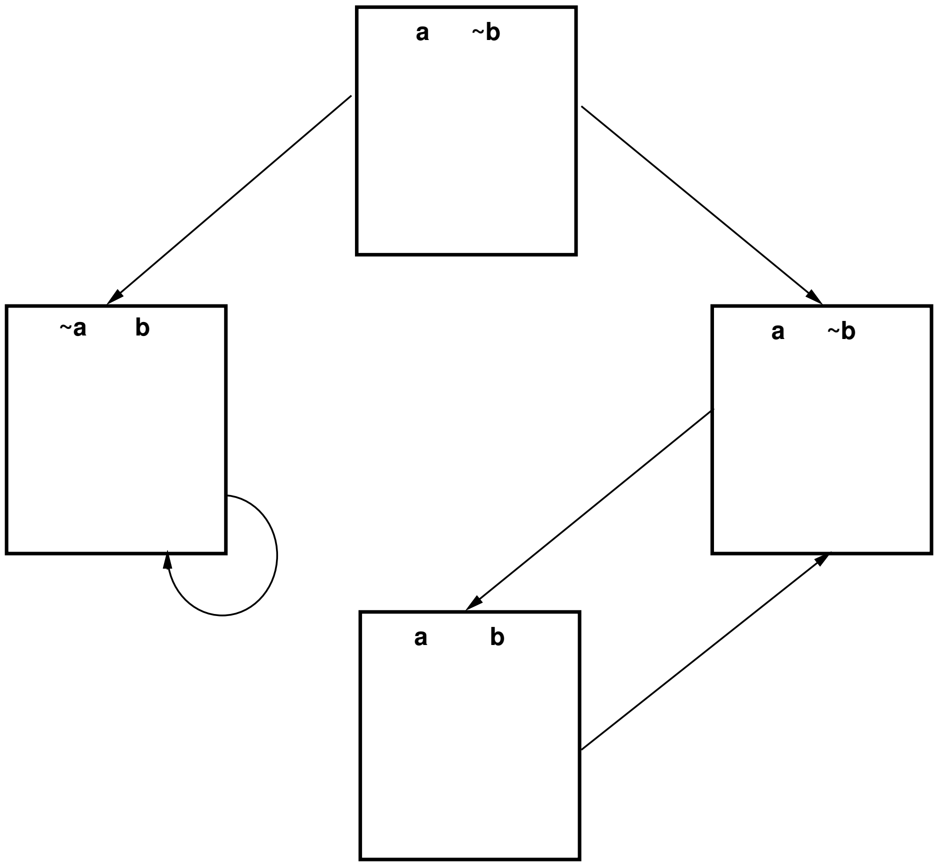
- E. M. Clarke, E. A. Emerson, and A. P. Sistla. Automatic verification of finite-state concurrent systems using temporal logic specifications. *ACM Trans. Programming Languages and Systems*, 8(2):pages 244–263, 1986.

The EMC Verification System



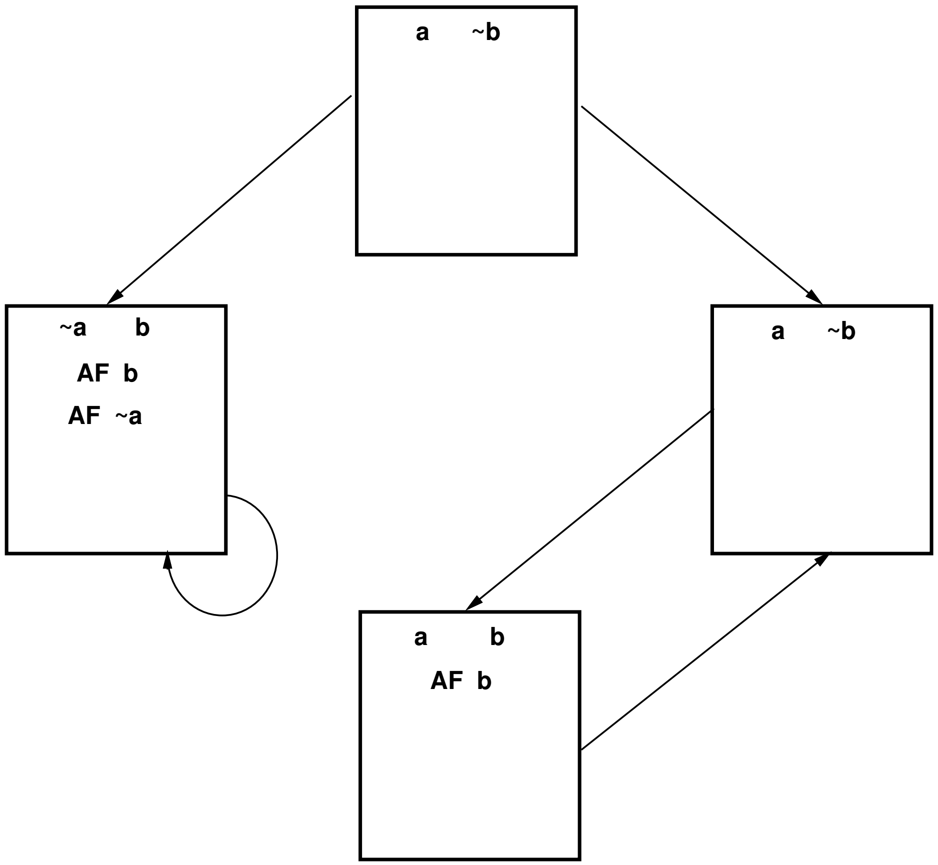
Basic Model Checking Algorithm

- $M, s_0 \models \mathbf{EG}\, a \wedge \mathbf{AF}\, b$?
- $M, s_0 \models \neg\, \mathbf{AF}\, \neg a \wedge \mathbf{AF}\, b$?



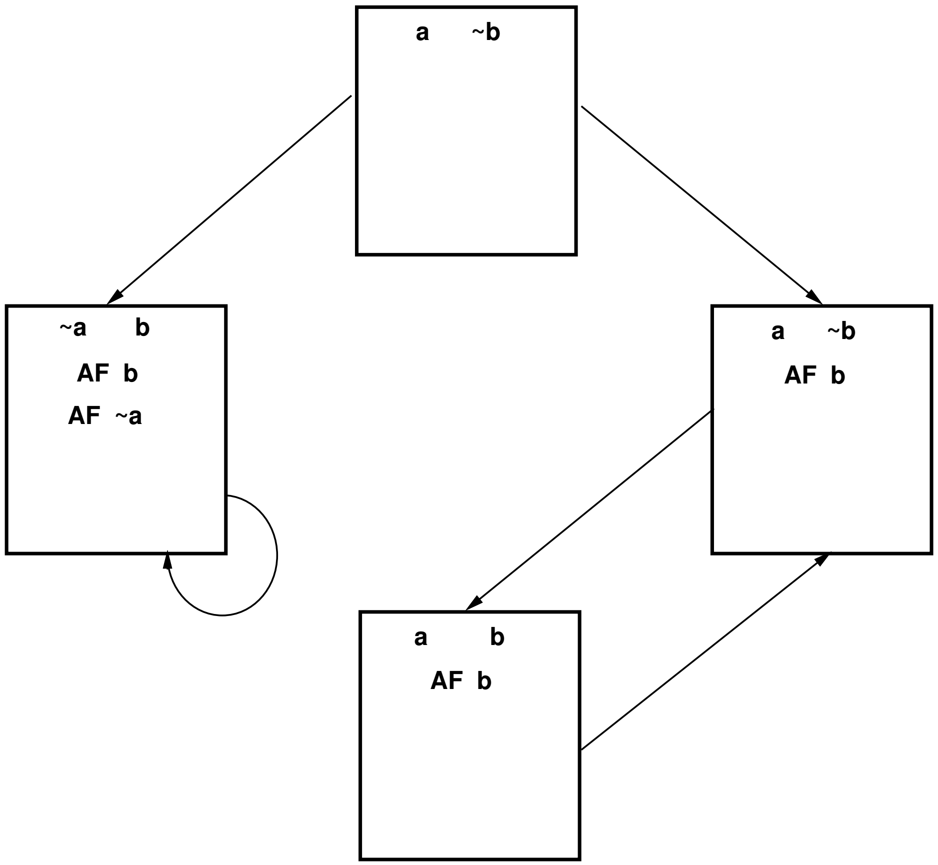
Basic Model Checking Algorithm

- $M, s_0 \models \mathbf{EG}\, a \wedge \mathbf{AF}\, b?$
- $M, s_0 \models \neg\, \mathbf{AF}\, \neg a \wedge \mathbf{AF}\, b?$



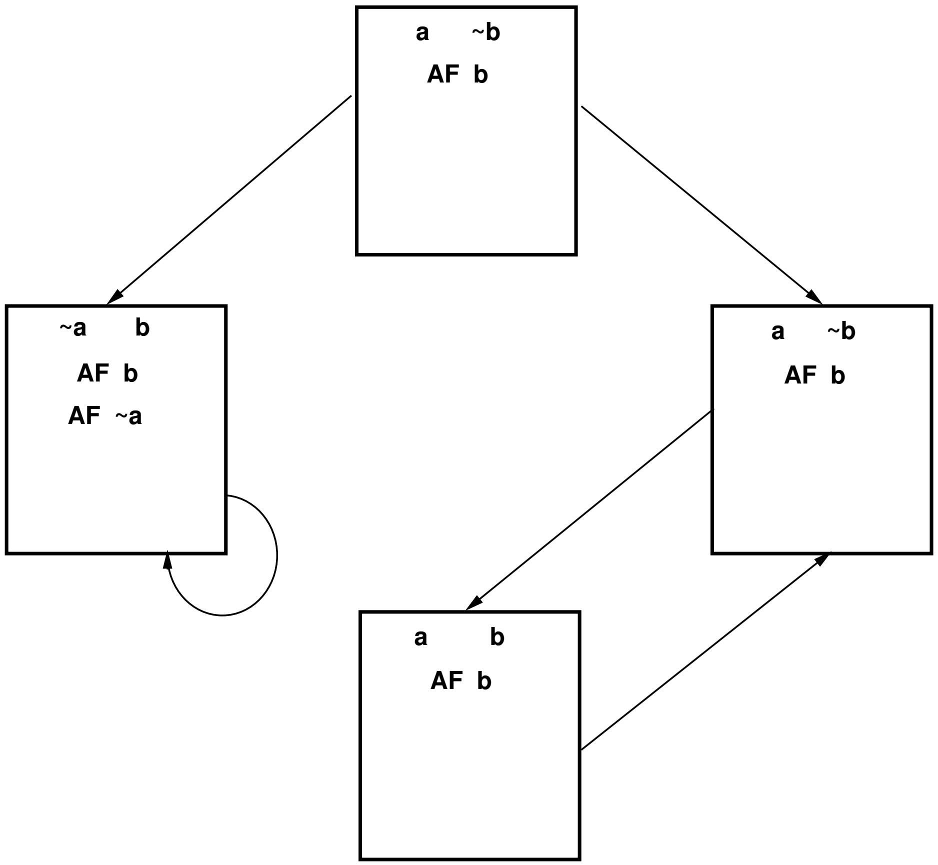
Basic Model Checking Algorithm

- $M, s_0 \models \mathbf{EG}\, a \wedge \mathbf{AF}\, b$?
- $M, s_0 \models \neg\, \mathbf{AF}\, \neg a \wedge \mathbf{AF}\, b$?



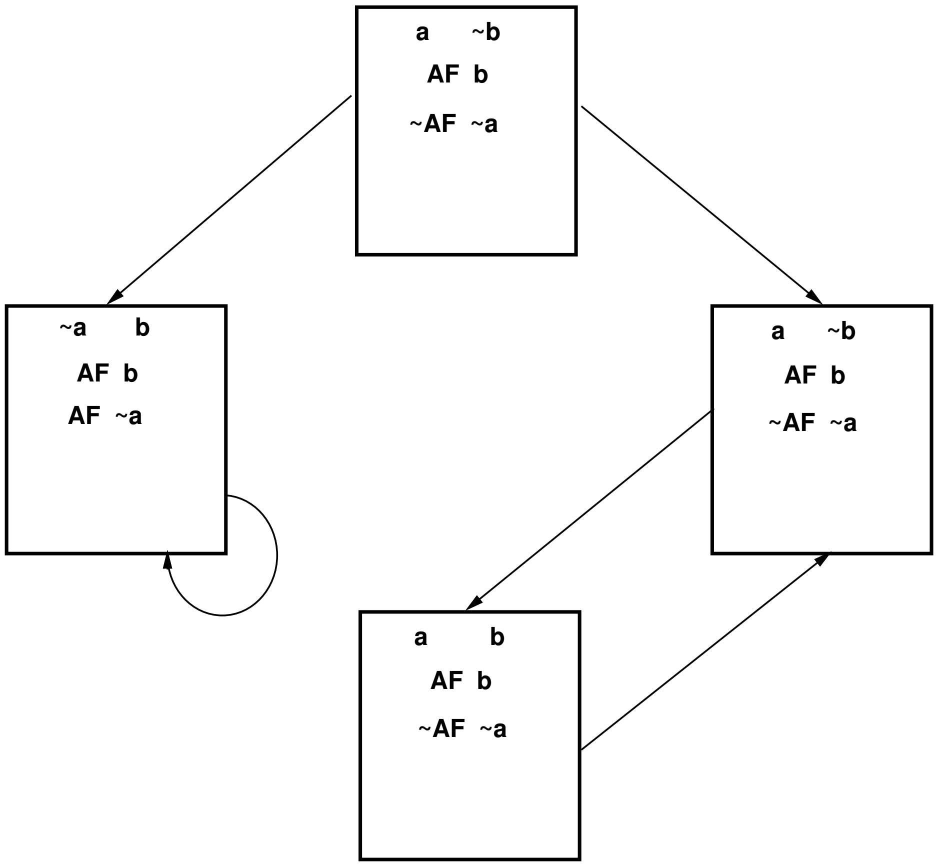
Basic Model Checking Algorithm

- $M, s_0 \models \mathbf{EG}\, a \wedge \mathbf{AF}\, b?$
- $M, s_0 \models \neg\, \mathbf{AF}\, \neg a \wedge \mathbf{AF}\, b?$

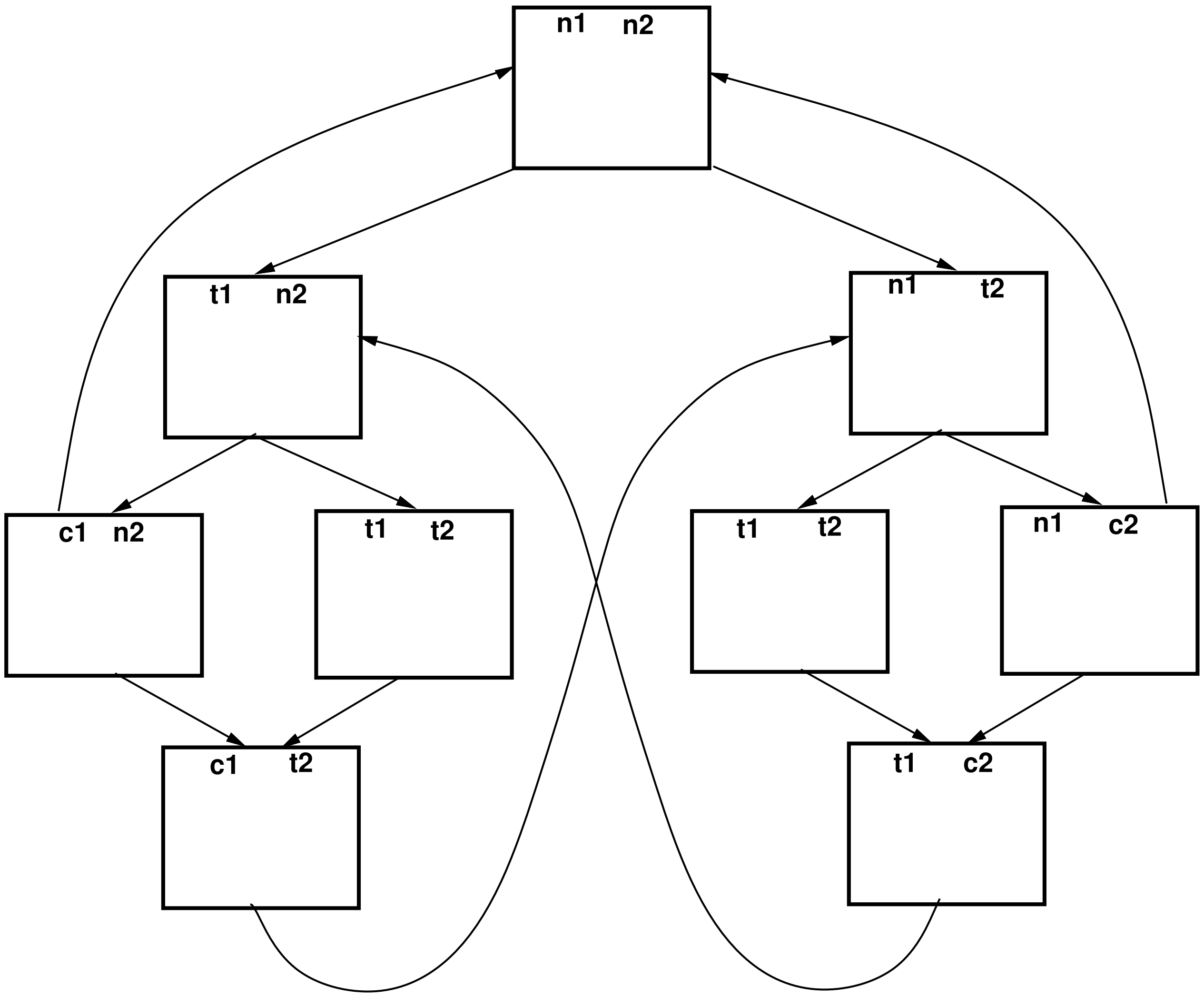


Basic Model Checking Algorithm

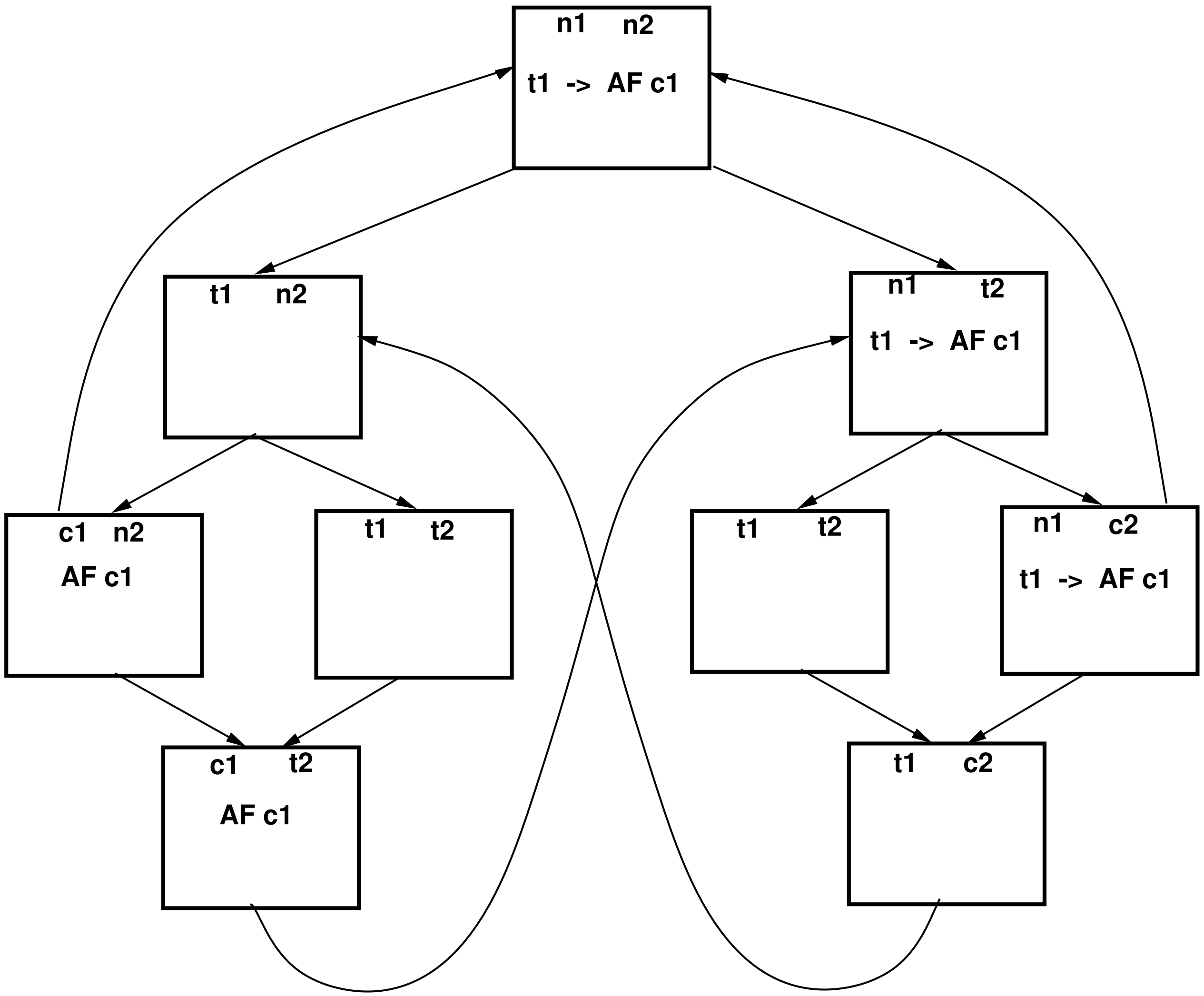
- $M, s_0 \models \mathbf{EG}\, a \wedge \mathbf{AF}\, b$?
- $M, s_0 \models \neg\, \mathbf{AF}\, \neg a \wedge \mathbf{AF}\, b$?



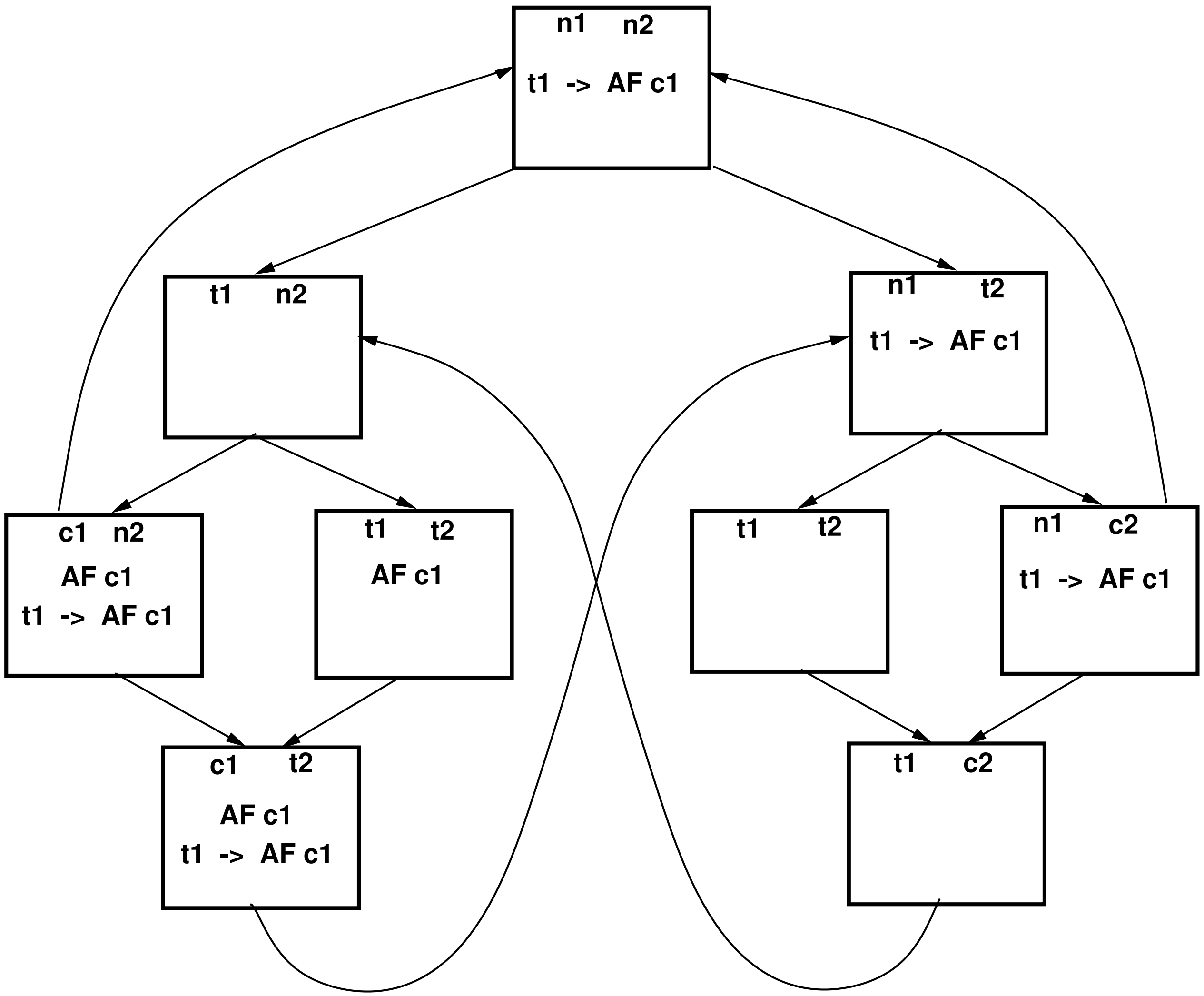
Mutual Exclusion Example



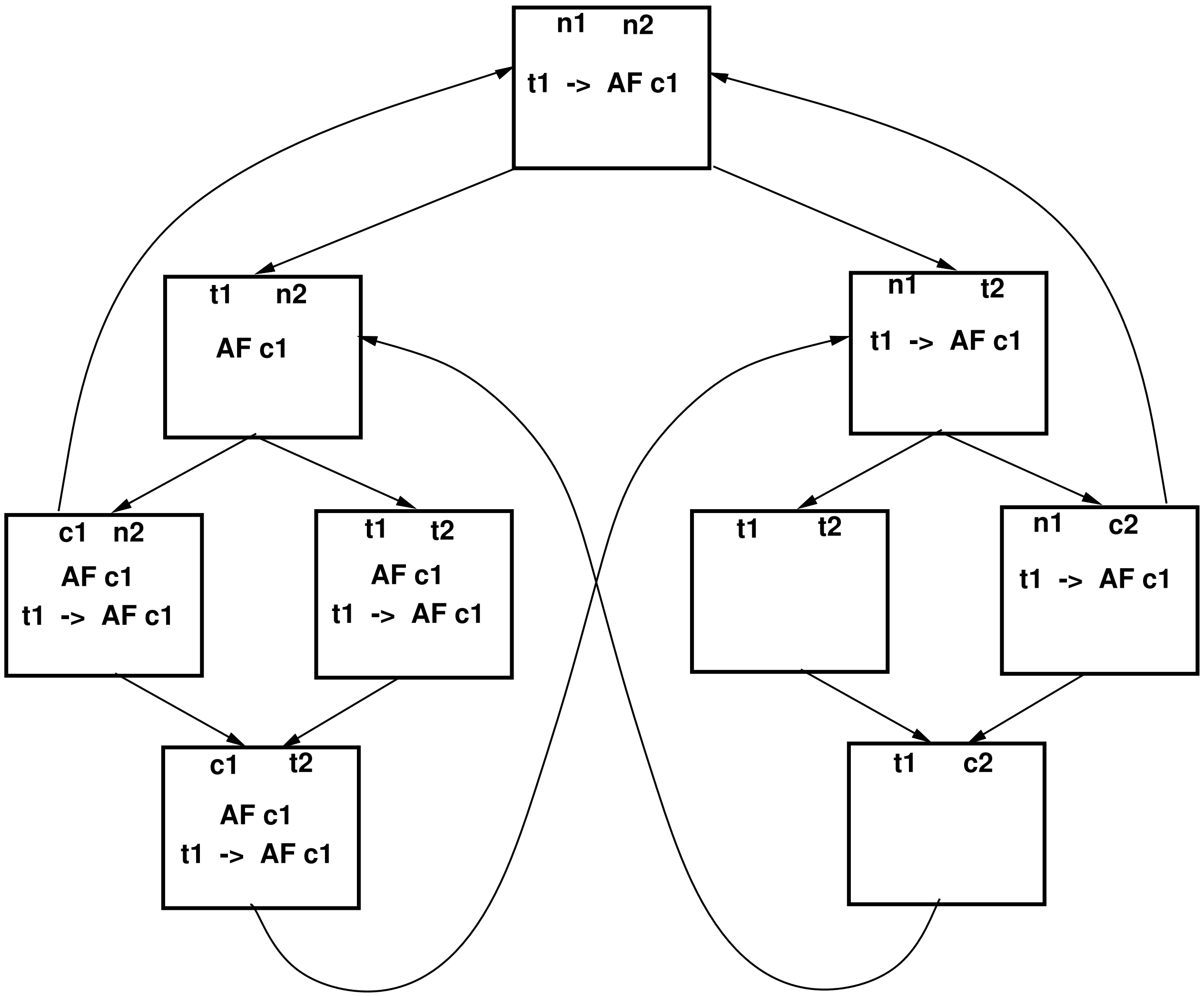
Mutual Exclusion Example



Mutual Exclusion Example



Mutual Exclusion Example



The Kyoto University Verifier

Vectorized version of *EMC* algorithm on Fujitsu FACOM VP400E using an explicit representation of the state–transition graph.

State Machine size:

- 131,072 states
- 67,108,864 transitions
- 512 transitions from each state on the average.

CTL formula:

- 113 different subformulas.

Time for model checking:

- 225 seconds!!