# Optimal constructions for active diagnosis

Stefan Haar Serge Haddad
Tarek Melliti Stefan Schwoon

LSV, Cachan IBISC, Évry

Journée Hiding and Disclosing Information, 03/12/2013

# Diagnosis

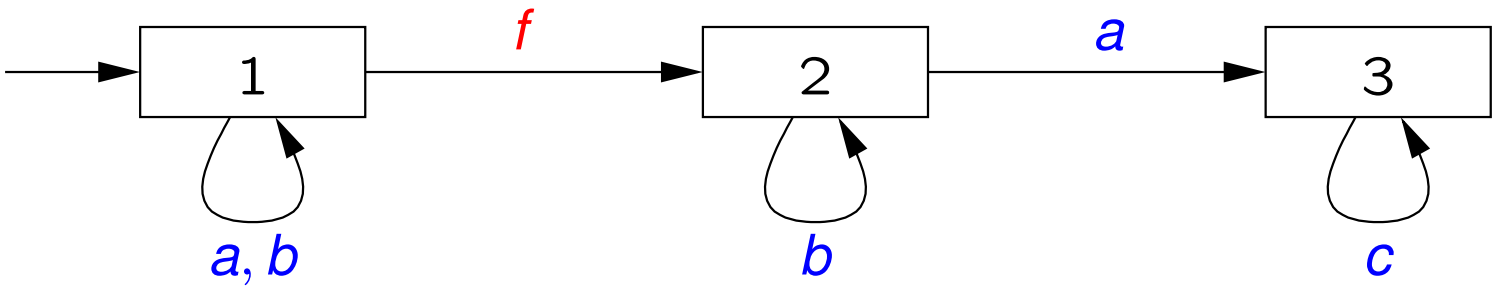
Non-deterministic system under observation


Possible behaviours well-known, current execution only partially visible

Goal: Determine, from partial observations, whether a certain event has happened in the past.

# Automata-based Diagnosis

Consider an LTS with observable and unobservable actions.



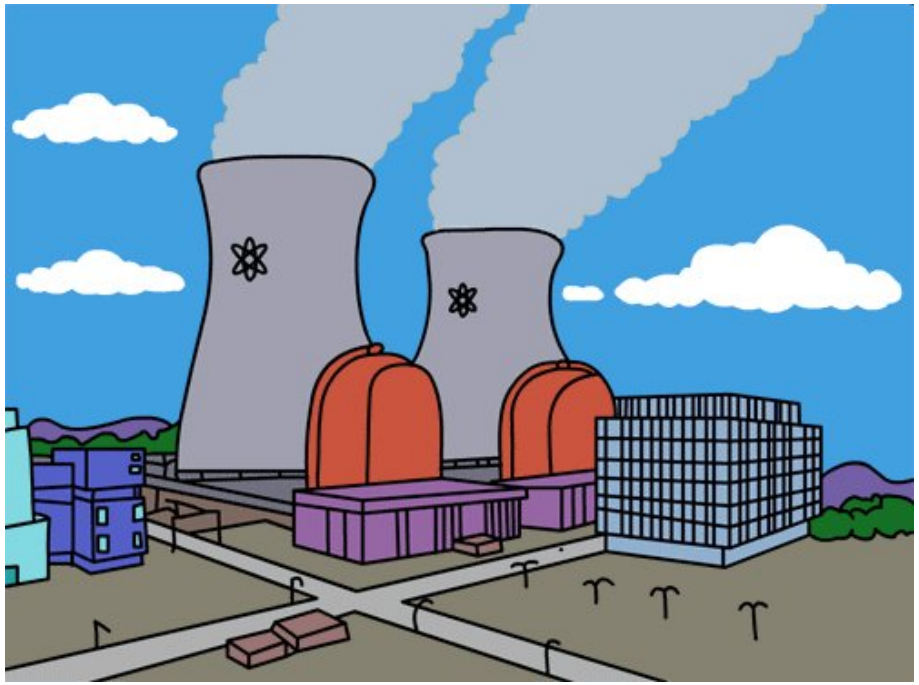

Diagnosis: Given a stream of observations from some execution of the LTS, determine whether a fault ($f$) has happened.

Examples: $ababab ac \cdots$, $a^n$ (for some $n \geq 1$), $a^\omega$, $b^\omega$

Diagnosability: Check whether an *ambiguous* sequence (like $b^\omega$) exists.

# Active Diagnosis

Suppose that certain actions are *controllable* (can be blocked).

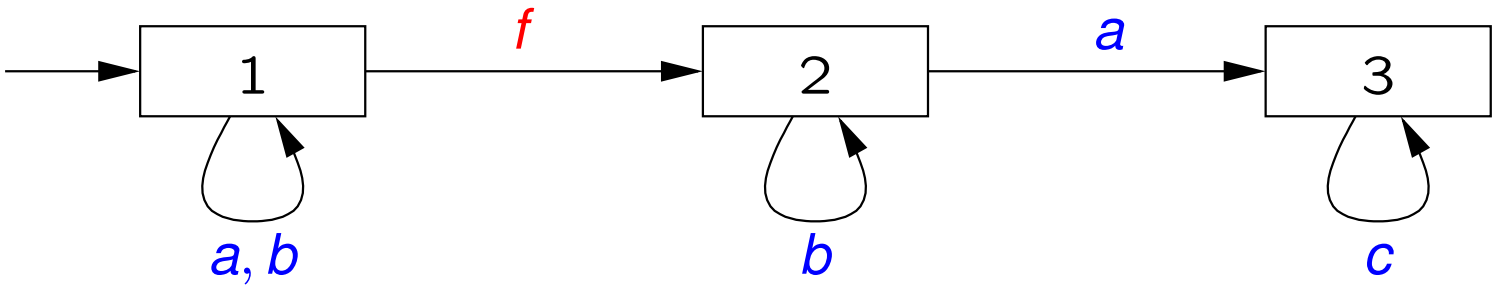


$\Rightarrow$ control the system so that faults manifest themselves through observations

$\Rightarrow$ eliminate the ambiguous sequences.

# Active Diagnosis

Example: Intuitive solution is to block all $b$ (assuming $b$ is controllable).

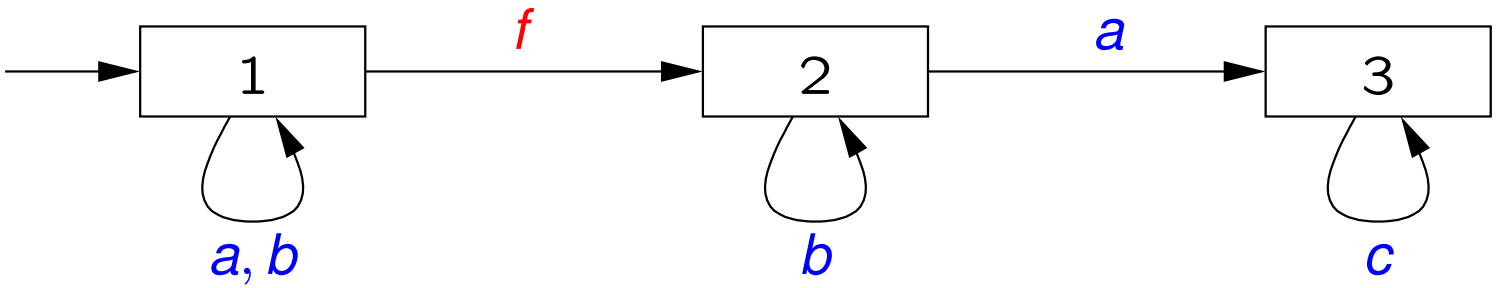



Observations:

- $\Rightarrow$ blocking all $b$ may be too restrictive to be acceptable
- $\Rightarrow$ it suffices to prevent infinite sequences of $b$

# Parametrized active diagnosis

Goal: minimally intrusive control that reveals faults within chosen delay $d$.




Example: if we permit at most $k$ uninterrupted occurrences of $b$, then the delay between fault and observation of $c$ is bounded by $k + 2$.

# Related work / Contribution

Diagnosis: well-known, many papers on the subject

Active diagnosis: less well researched

- Main reference: Sampath et al 1998
- ad-hoc methods for active diagnosis
- no complexity analysis, no bounds

Contributions:

- automata- and game theoretic basis for active diagnosis
- upper and lower bounds
- *Parametrized* active diagnosis

# Controllers for active diagnosis

Given: LTS $\mathcal{A} = \langle Q, q_0, \Sigma, \delta \rangle$.

$\Sigma = \Sigma_o \uplus \Sigma_{uo}$ partitioned into observable/unobservable actions

$\Sigma_c \subseteq \Sigma_o$ *controllable* actions, *fault* $f \in \Sigma_{uo}$

Assumptions: $Q$ finite, $\mathcal{A}$ live, no loops of unobservable actions

Build a deterministic transducer $\mathcal{T}$ that reads $\Sigma_o$ and outputs control+diagnosis

control: subset of allowed controllable actions

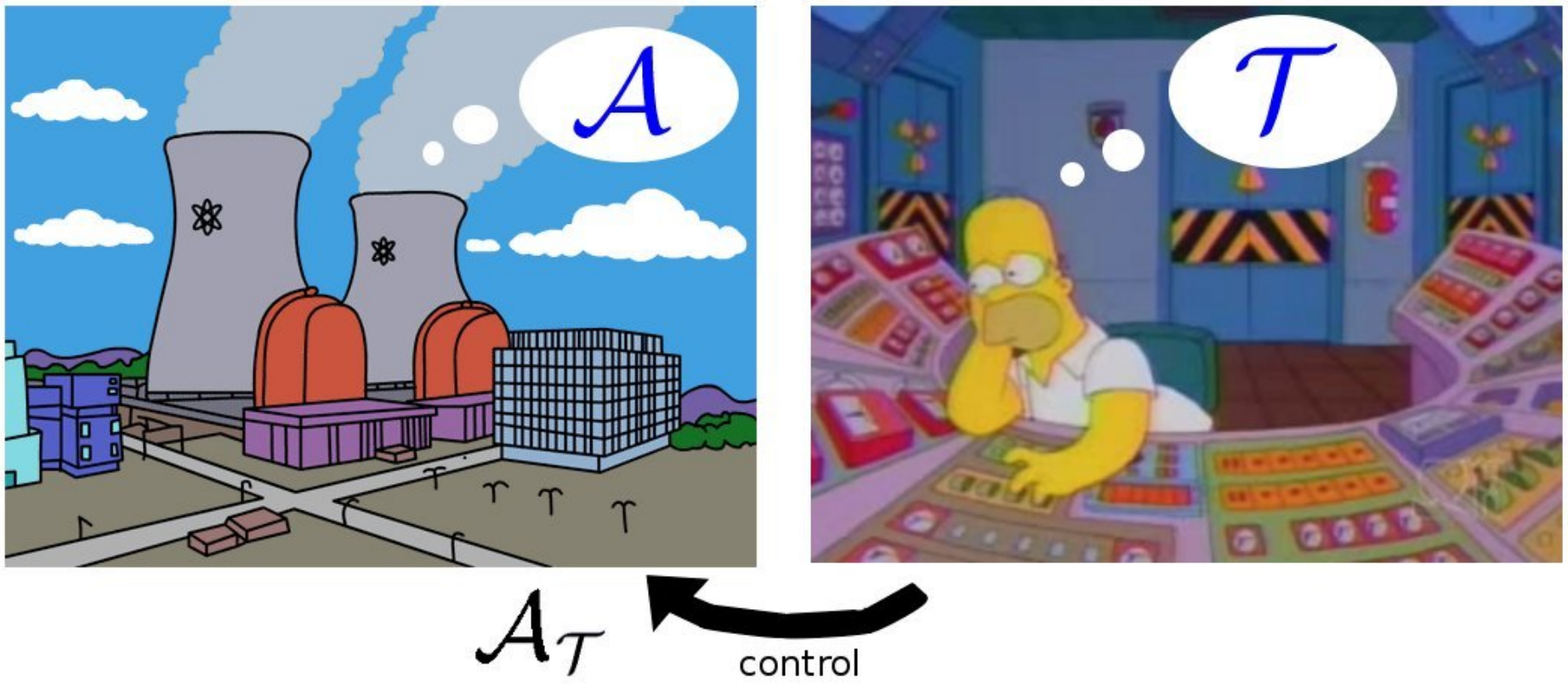
diagnosis: raise alarm when fault has surely happened

# Controllers for active diagnosis

$\mathcal{A}$ executes, $\mathcal{T}$ represents observer's knowledge.


# Controllers for active diagnosis

$\mathcal{A}$ executes, $\mathcal{T}$ represents observer's knowledge.




Observer exercises control, thereby restricting the behaviour of $\mathcal{A}$.

# Controllers for active diagnosis

Given: LTS $\mathcal{A} = \langle Q, q_0, \Sigma, T \rangle$.

$\Sigma = \Sigma_o \uplus \Sigma_{uo}$ partitioned into observable/unobservable actions

$\Sigma_c \subseteq \Sigma_o$ *controllable* actions, *fault* $f \in \Sigma_{uo}$

Assumptions: $Q$ finite, $\mathcal{A}$ live, no loops of unobservable actions

Build a deterministic transducer $\mathcal{T}$ that reads $\Sigma_o$ and outputs control+diagnosis

control: subset of allowed controllable actions

diagnosis: raise alarm when fault has surely happened

requirements: system remains live, diagnose all faults, no false alarms

or: find that no such transducer exists

# Some terminology

We say $\mathcal{A}$ is actively diagnosable if a transducer $\mathcal{T}$ satisfying all requirements exists.

Delay of $\mathcal{T}$: longest period of uncertainty in any execution admitted by $\mathcal{T}$, measured in number of observations from occurrence of fault to its revelation.

Index of $\mathcal{A}$: minimal $k$ such that there exists a transducer with delay $k$.

# Results: Lower bounds

For each of the following properties, there exists a family $(\mathcal{A}_n)_{n\geq 1}$ with $\mathcal{O}(n)$ states and:

(i) The delay of $A_n$ is $\Omega(2^n)$.

(ii) Any transducer for $A_n$ has $2^{\Omega(n)}$ states.

(iii) The minimal-delay transducer for $A_n$ has $2^{\Omega(n \log n)}$ states.

# Results: Upper bounds / Constructions

Let $\mathcal{A}$ be an actively diagnosable LTS with $n$ states.

(iv) There is a transducer for $\mathcal{A}$ with $2^{\mathcal{O}(n)}$ states.

(v) The delay of this transducer is at most two times the index of $\mathcal{A}$.

(vi) There is a minimal-delay transducer with $2^{\mathcal{O}(n^2 \log n)}$.

(vii) There is a parametrized transducer $\mathcal{T}_p$ of size $2^{\mathcal{O}(n)}$ such that $\mathcal{T}_p(d)$ has delay $2d$ (for $d \geq$ index of $\mathcal{A}$).

# Transducer construction: Overview

(iv) There is a transducer for $\mathcal{A}$ with $2^{\mathcal{O}(n)}$ states.

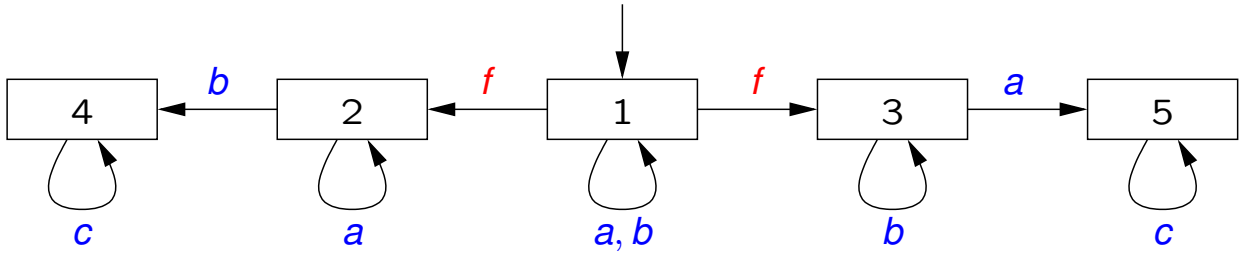
1. Construct deterministic Büchi automaton (DBA) $\mathcal{B}$.
   $\mathcal{B}$ accepts the set of "non-ambiguous" sequences.

2. Construct a Büchi game $\mathcal{G}$ from $\mathcal{B}$.
   $\mathcal{G}$ is winnable iff $\mathcal{A}$ is actively diagnosable.

3. Construct transducer $\mathcal{T}$ by taking DBA $\mathcal{B}$
   and synthesizing control from winning strategy in $\mathcal{G}$.

# Transducer construction

Given $\mathcal{A} = \langle Q, q_0, \Sigma, \delta \rangle$:




Construct DBA $\mathcal{B} = \langle S, s_0, \Sigma_o, \eta, G \rangle$ as follows:

$S \subseteq 2^Q \times 2^Q \times 2^Q$ and $s_0 = \langle \{q_0\}, \emptyset, \emptyset \rangle$;

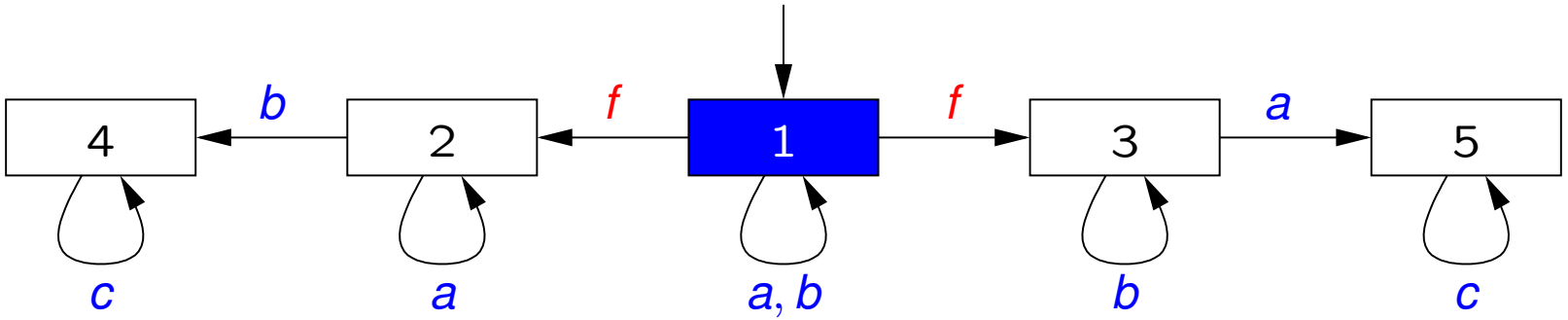
for input $w$, we reach state $s = \langle C, F, W \rangle$, where

$C \subseteq Q$ are states of $\mathcal{A}$ reached by correct sequences with observation $w$;

$F \cup W \subseteq Q$ are states reached by faulty sequences with observation $w$;

$F$ is a “waiting room”, $W$ a “worklist”.

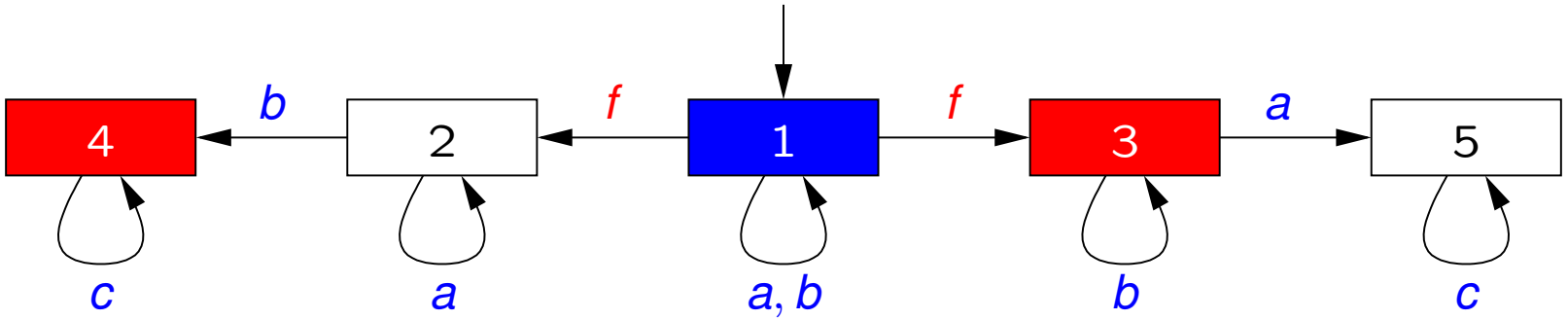
# Transducer construction: example




Initially: We can only be in state 1, without having committed a fault.

State of transducer: $\langle C, F, W \rangle = \langle \{1\}, \emptyset, \emptyset \rangle$

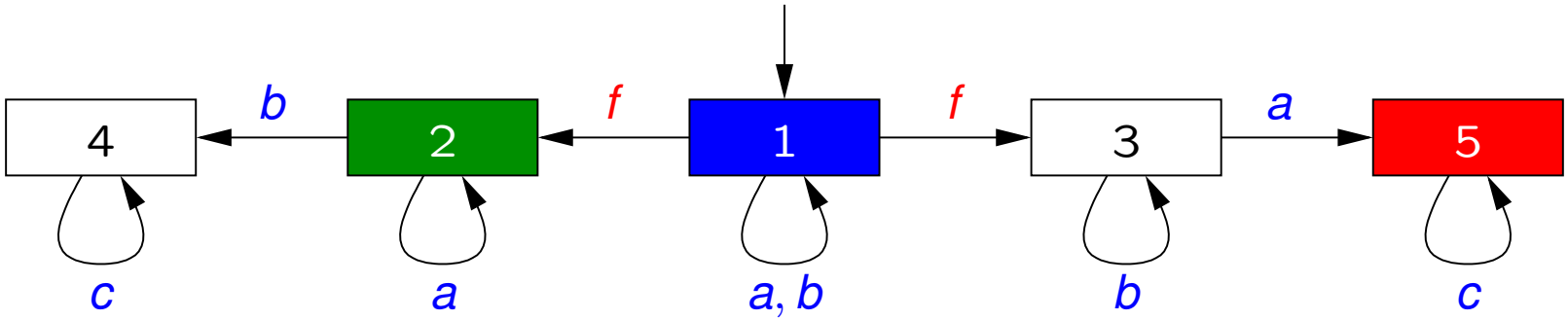
# Transducer construction: example




Suppose the first letter is $b$.

Successor state: $\langle C, F, W \rangle = \langle \{1\}, \emptyset, \{3, 4\} \rangle$

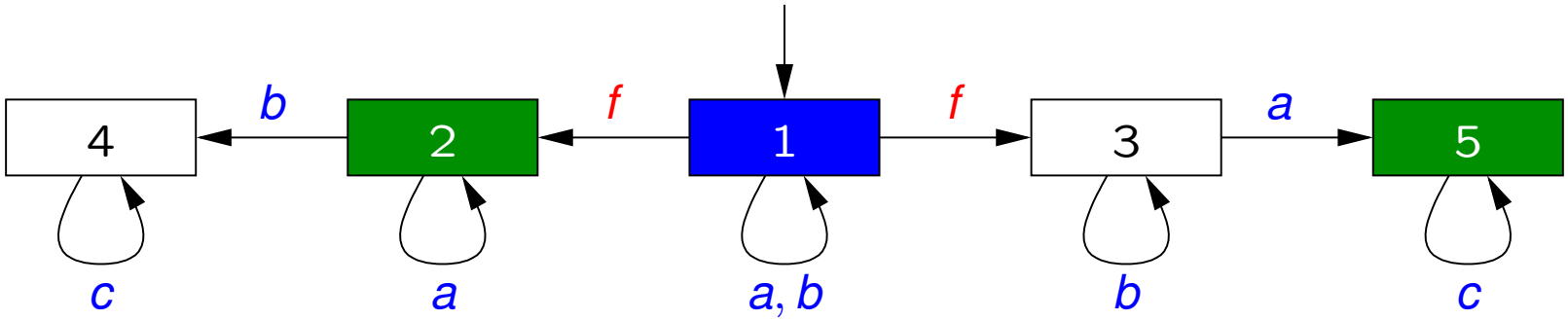
# Transducer construction: example




Suppose the second letter is $a$. We will worry about state 2 later.

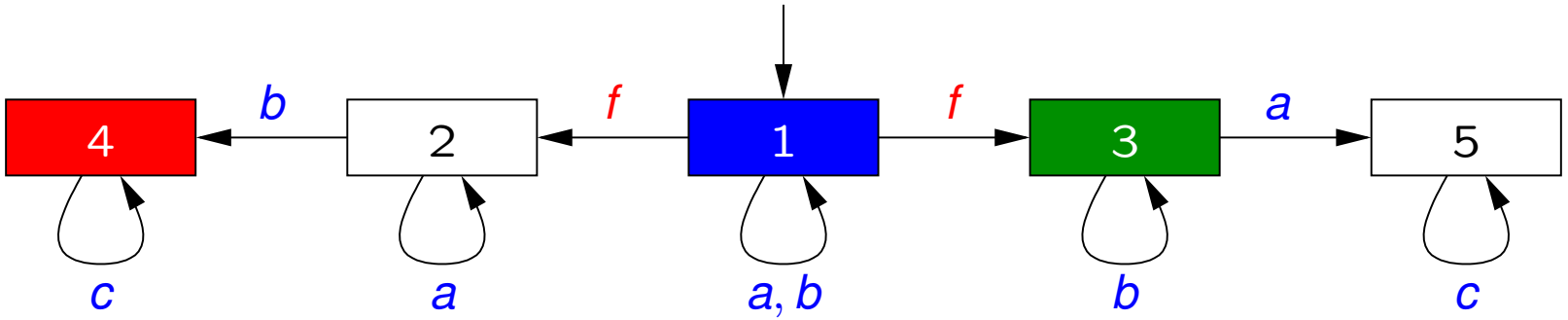
Successor state: $\langle C, F, W \rangle = \langle \{1\}, \{2\}, \{5\} \rangle$

# Transducer construction: example




We observe another *a*. Then we cannot have been in 5.

# Transducer construction: example




Situation after we observe a $b$ next.

Successor state: $\langle C, F, W \rangle = \langle \{1\}, \{3\}, \{4\} \rangle$

# Transition relation

Let $s = \langle C, F, W \rangle$ and $a \in \Sigma_o$, then $\eta(s, a) = \langle C', F', W' \rangle$, where:

$C'$ are states reached from $C$ *without fault*;

if $W \neq \emptyset$:

$F'$ are states reached from $C$ *with fault* or from $F$ *in any way*.

$W'$ are states reached from $W$ *in any way*.

if $W = \emptyset$:

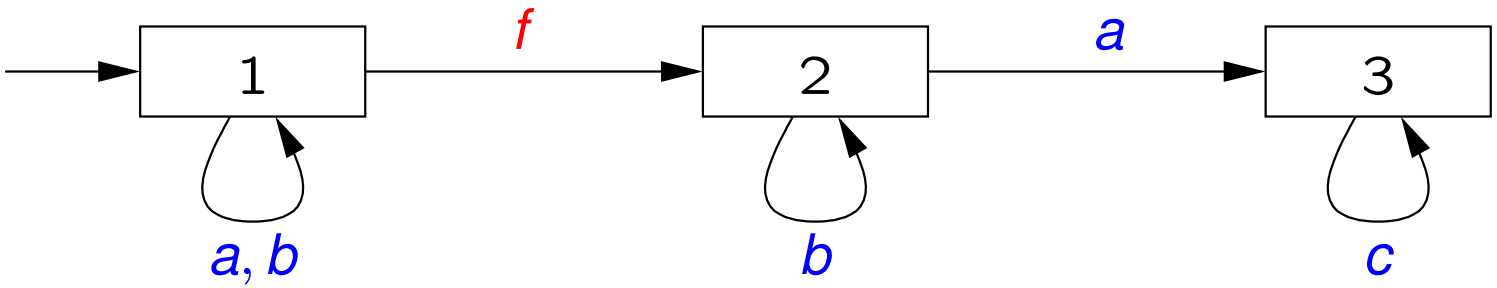
$F' = \emptyset$;

$W'$ are states reached from $C$ *with fault* or from $F$ *in any way*.

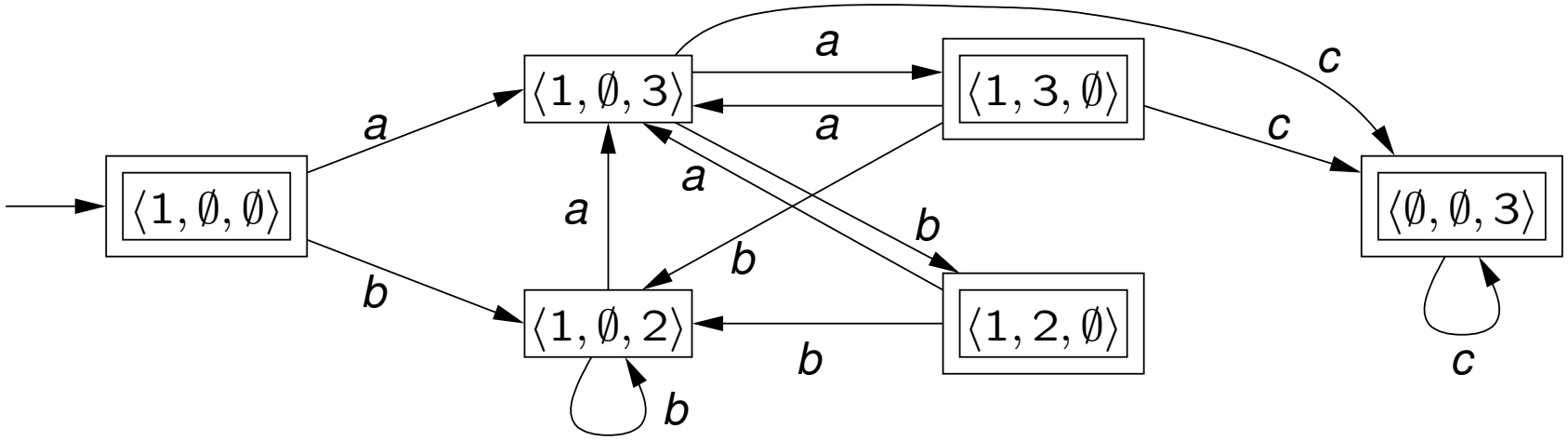
$G = \{ \langle \emptyset, F, W \rangle, \langle C, F, \emptyset \rangle \mid C, F, W \subseteq Q \}$

# Result of DBA construction

Input:




Output:



# Büchi game

Consider the following two-player Büchi game $\mathcal{G}$ on $S$:

In state $s$, Controller first chooses an "admissible" set $\Sigma' \subseteq \Sigma_c$.

Then, Environment chooses an action $a \in \Sigma' \cup (\Sigma_o \setminus \Sigma_c)$ and goes to $\eta(s, a)$.

Winning condition for Controller: infinitely often touch $G$.

Theorem: $\mathcal{A}$ is actively diagnosable iff Controller can win $\mathcal{G}$.

# Fine-tuning the delay

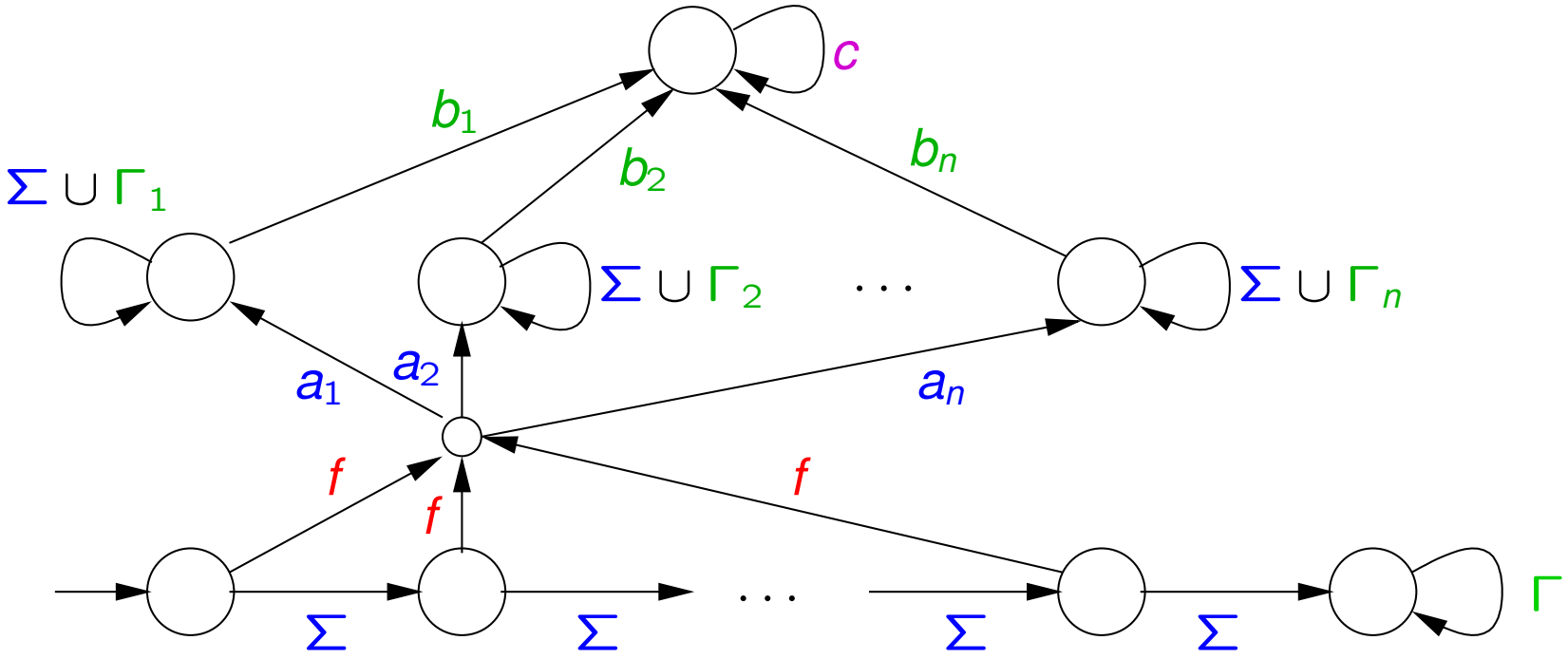
Transducer $\mathcal{T}$ – obtained from $\mathcal{B}$ and winning strategy for $\mathcal{G}$ – can have up to exponential delay.

To reduce the delay, play a quantitative variant of $\mathcal{G}$. We say Controller wins with value $d$ if he can restrict the maximal number of consecutive non-accepting states to $d$.

Theorem: Let $d_{\min}$ be the smallest number for which Controller wins. Then the index of $\mathcal{A}$ is between $d+1$ and $2d+1$.

# Lower bound for minimal delay

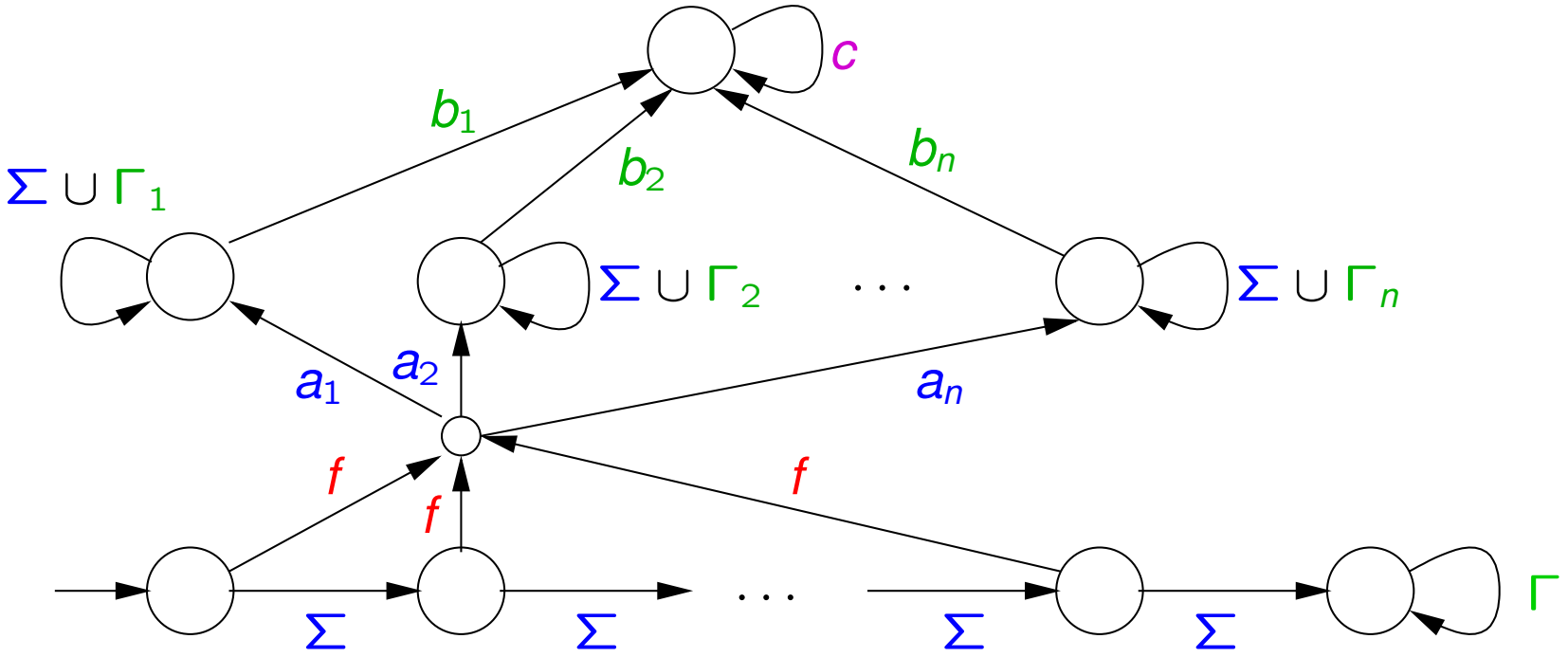
(iii) The minimal-delay transducer for $A_n$ has $2^{\Omega(n \log n)}$ states.




Definitions: $\Sigma := \{a_1, \ldots, a_n\}$, $\Gamma := \{b_1, \ldots, b_n\}$, $\Gamma_i := \Gamma \setminus \{b_i\}$

# Lower bound for minimal delay

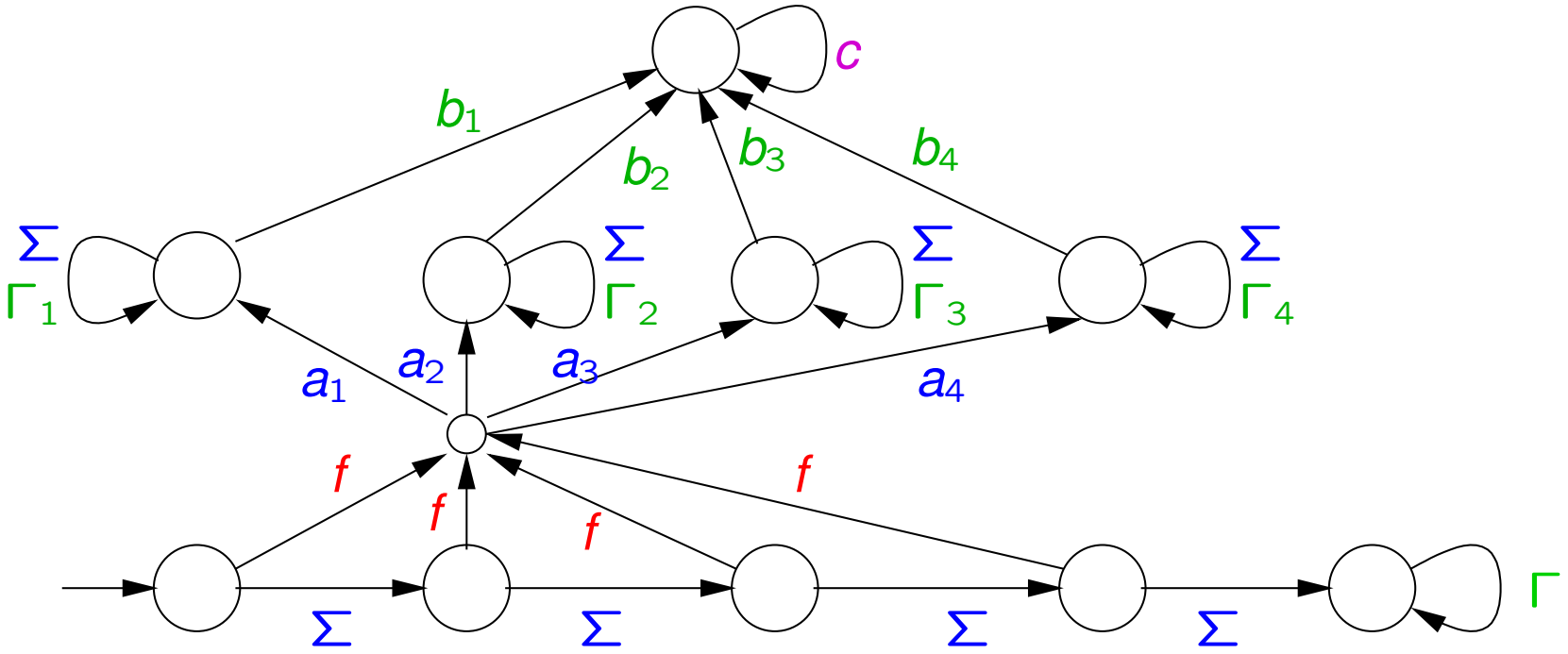
Definitions: $\Sigma := \{a_1, \ldots, a_n\}$, $\Gamma := \{b_1, \ldots, b_n\}$, $\Gamma_i := \Gamma \setminus \{b_i\}$




Observable: all except $f$, controllable: $\Gamma$

# Lower bound for minimal delay

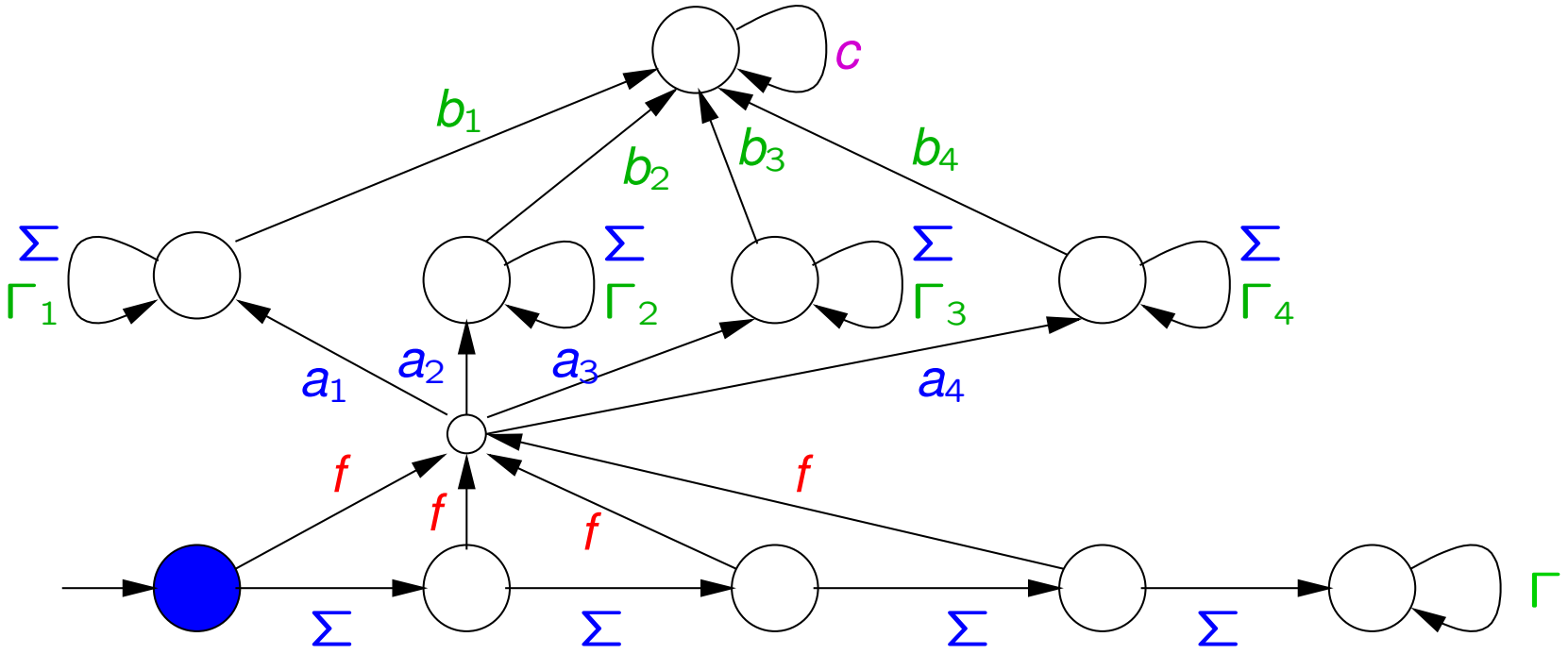
Definitions: $\Sigma := \{a_1, \ldots, a_4\}$, $\Gamma := \{b_1, \ldots, b_4\}$, $\Gamma_i := \Gamma \setminus \{b_i\}$




For $n = 4$, suppose the first $n$ observations are $a_3 a_1 a_4 a_2$.

# Lower bound for minimal delay

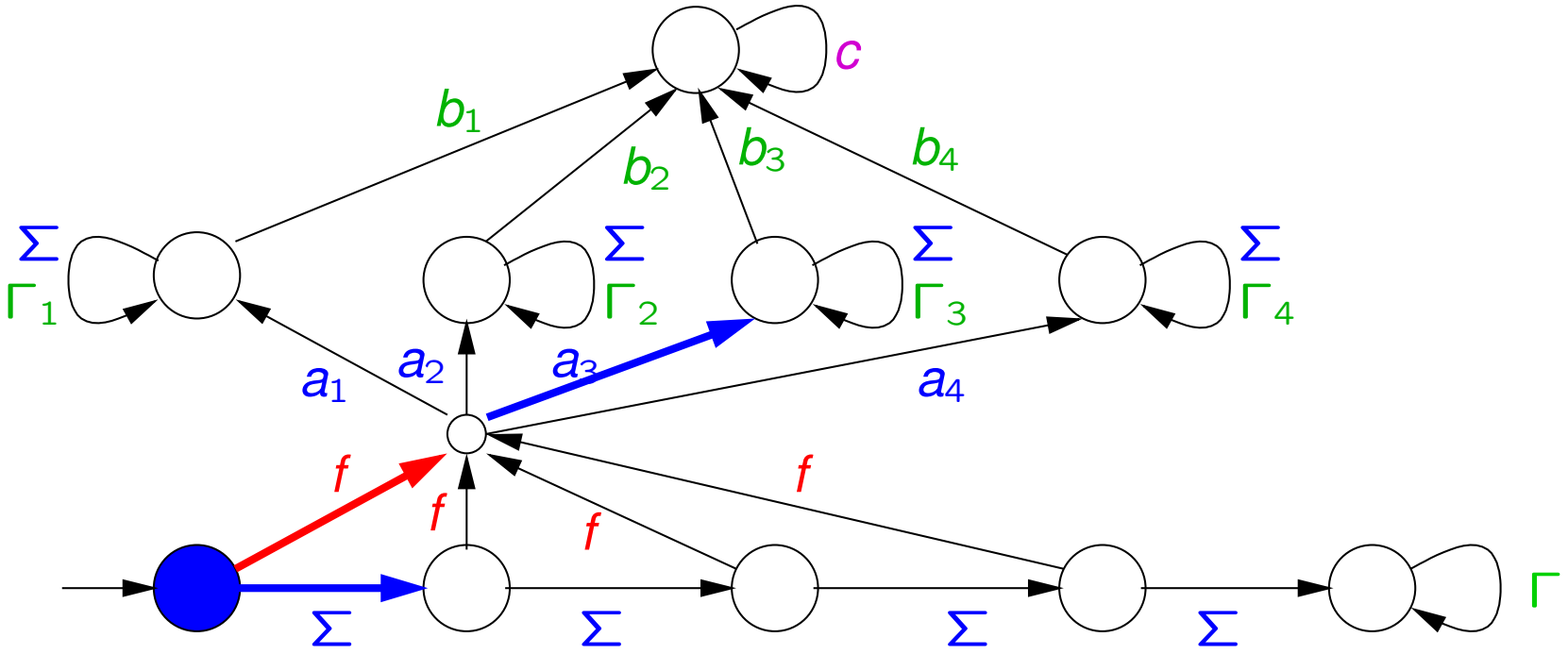
Definitions: $\Sigma := \{a_1, \ldots, a_4\}$, $\Gamma := \{b_1, \ldots, b_4\}$, $\Gamma_i := \Gamma \setminus \{b_i\}$




Initial state of the system...

# Lower bound for minimal delay

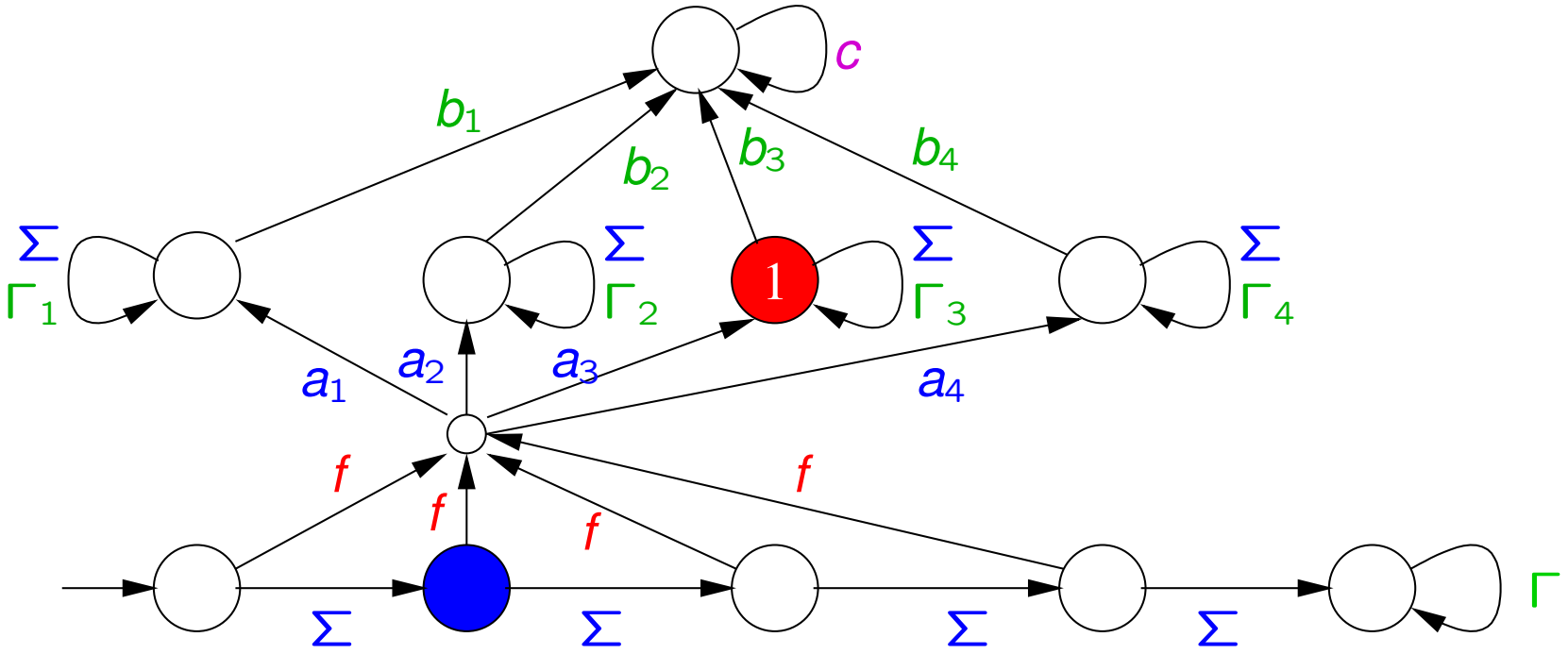
Definitions: $\Sigma := \{a_1, \ldots, a_4\}$, $\Gamma := \{b_1, \ldots, b_4\}$, $\Gamma_i := \Gamma \setminus \{b_i\}$




Observation of $a_3$...

# Lower bound for minimal delay

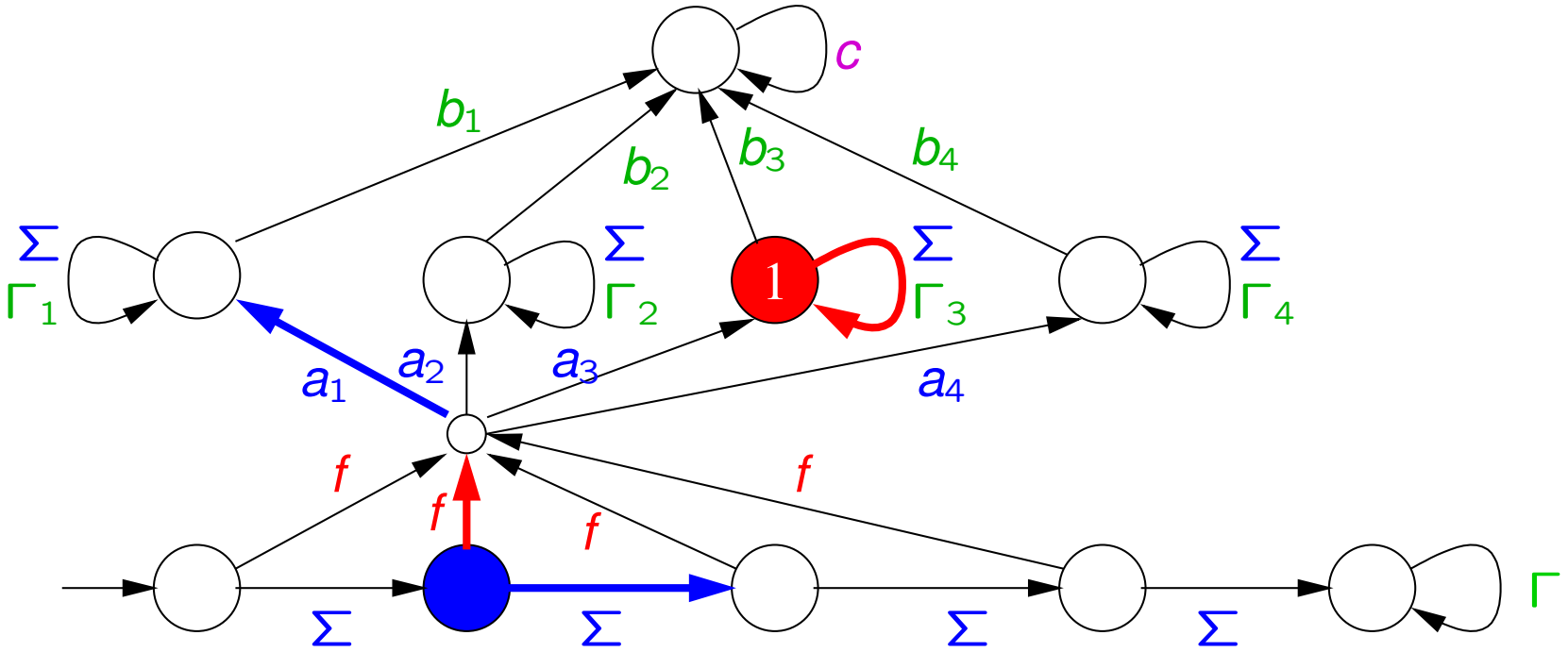
Definitions: $\Sigma := \{a_1, \ldots, a_4\}$, $\Gamma := \{b_1, \ldots, b_4\}$, $\Gamma_i := \Gamma \setminus \{b_i\}$




Possible states after observing $a_3$.

# Lower bound for minimal delay

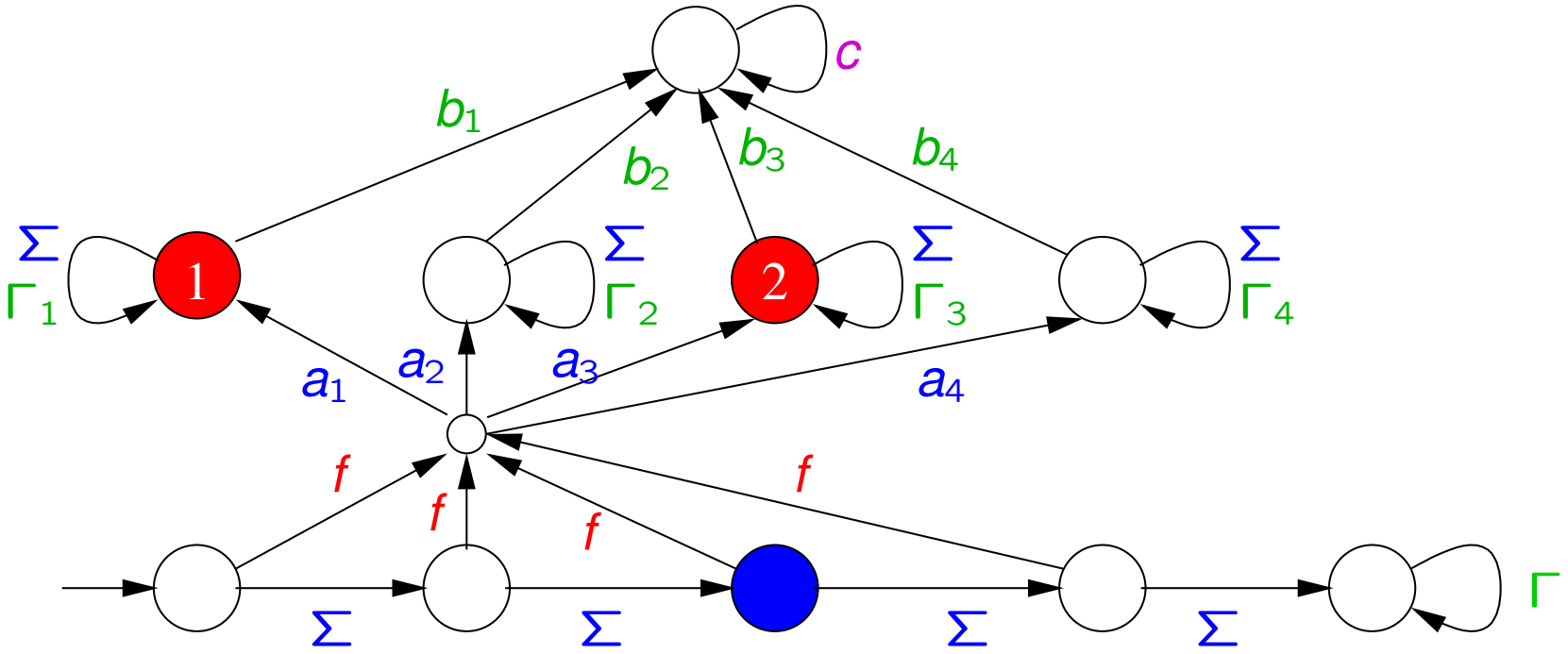
Definitions: $\Sigma := \{a_1, \ldots, a_4\}$, $\Gamma := \{b_1, \ldots, b_4\}$, $\Gamma_i := \Gamma \setminus \{b_i\}$




Observation of $a_1 \ldots$

# Lower bound for minimal delay

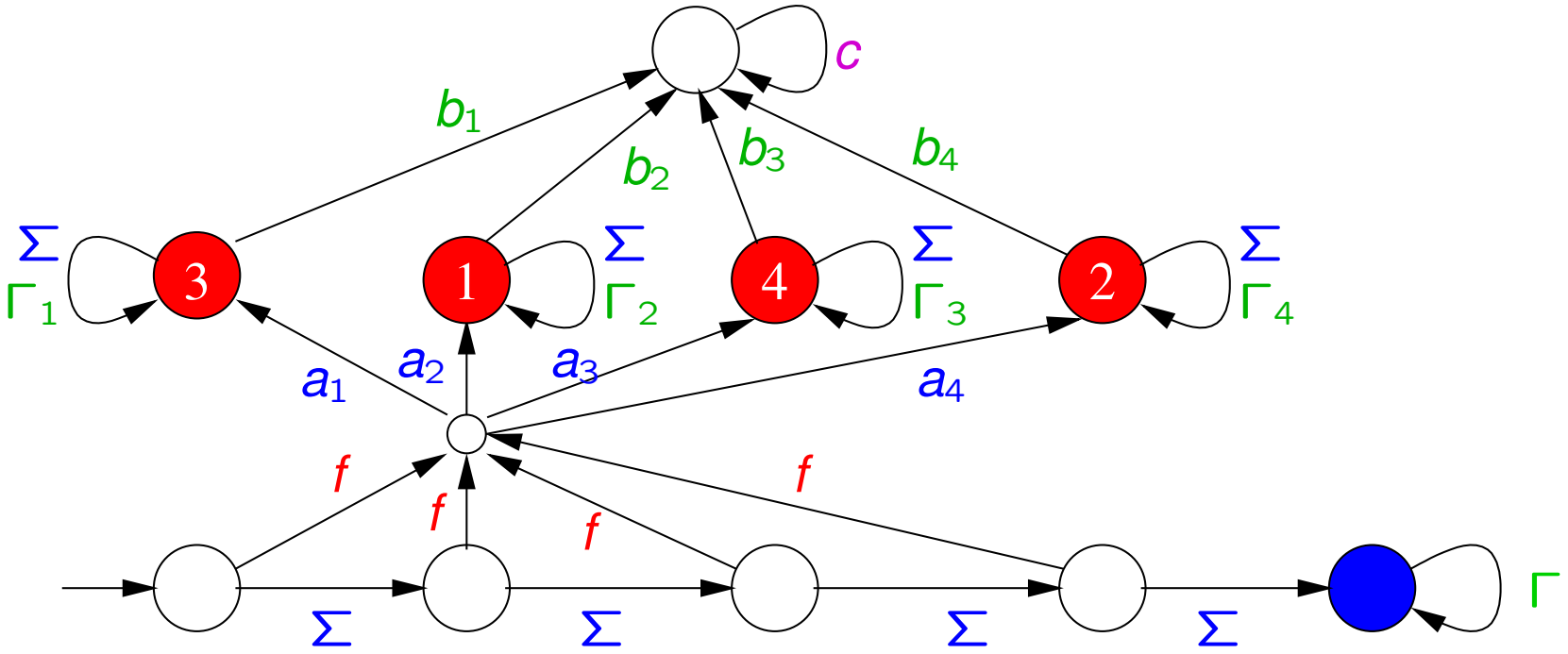
Definitions: $\Sigma := \{a_1, \ldots, a_4\}$, $\Gamma := \{b_1, \ldots, b_4\}$, $\Gamma_i := \Gamma \setminus \{b_i\}$




Possible states after observing $a_3 a_1$.

# Lower bound for minimal delay

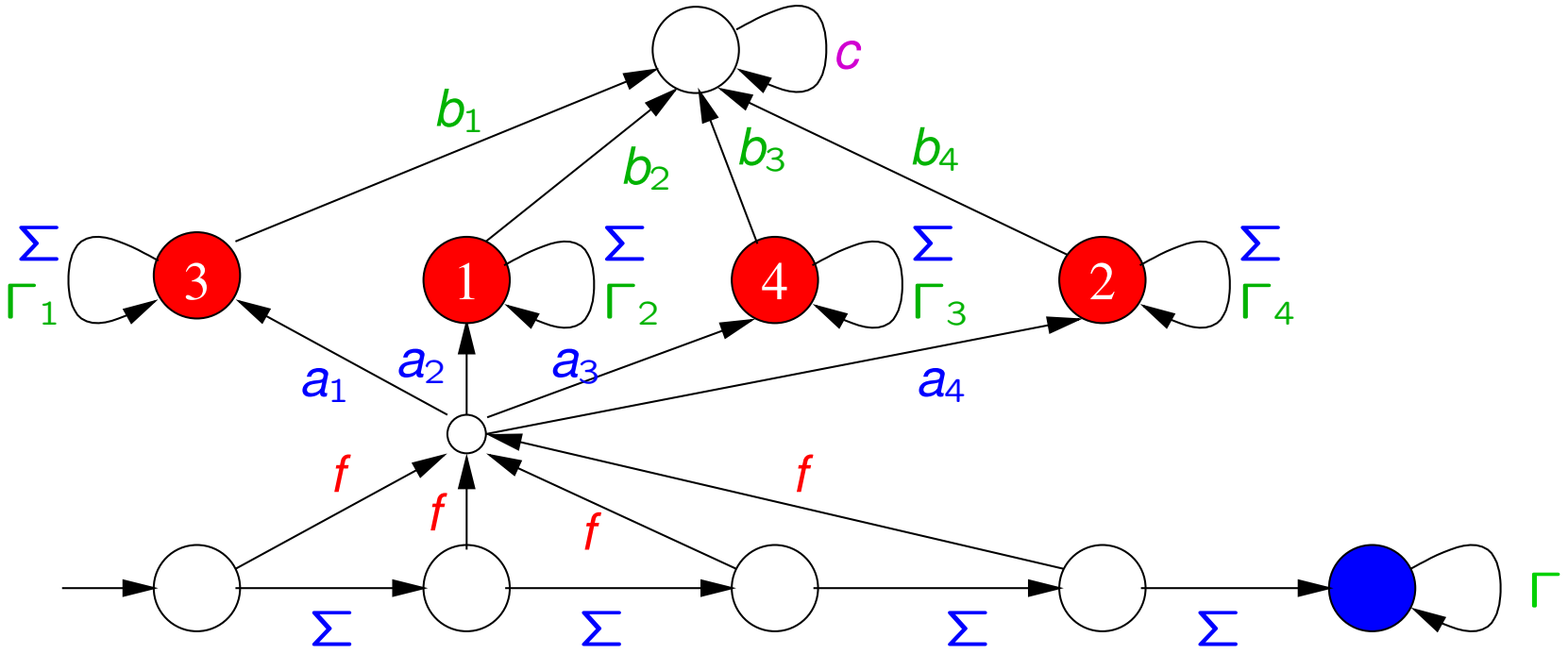
Definitions: $\Sigma := \{a_1, \ldots, a_4\}$, $\Gamma := \{b_1, \ldots, b_4\}$, $\Gamma_i := \Gamma \setminus \{b_i\}$




. . . and after $a_3 a_1 a_4 a_2$.

# Lower bound for minimal delay

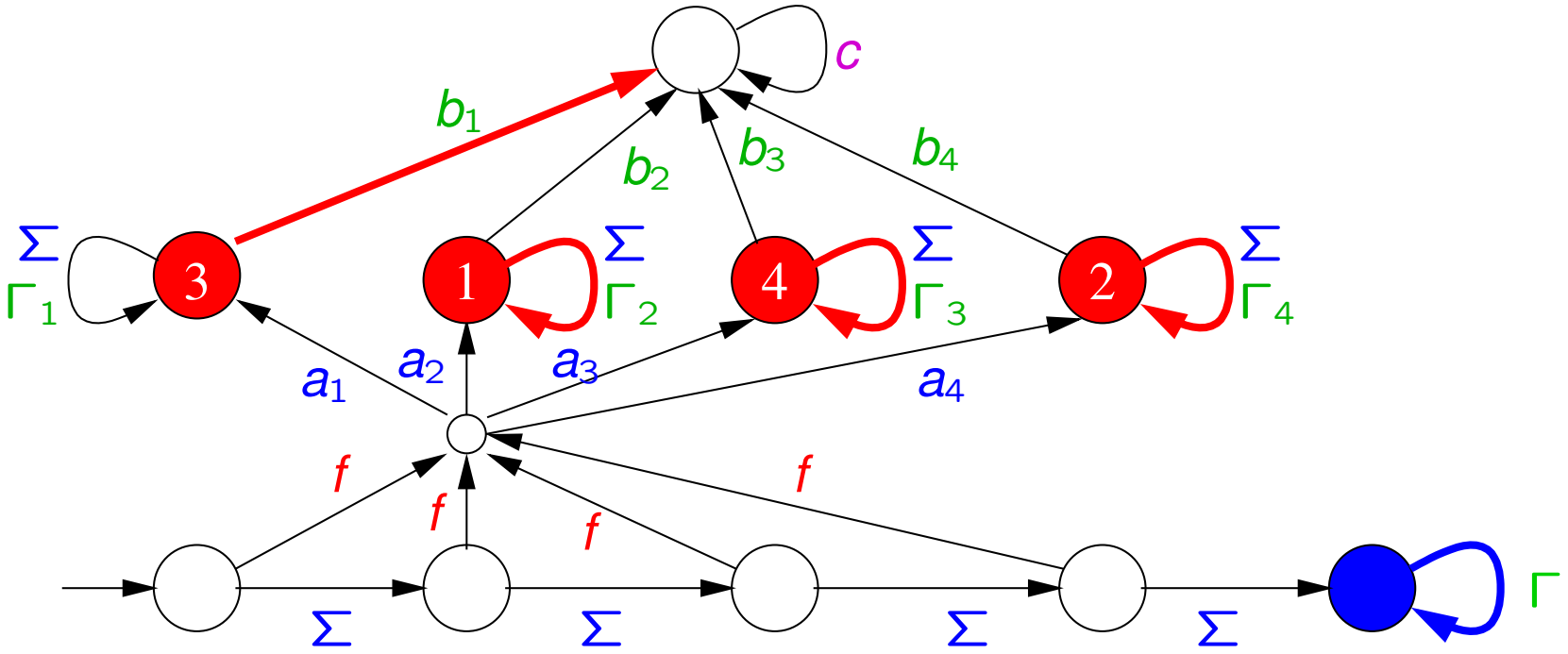
Definitions: $\Sigma := \{a_1, \ldots, a_4\}$, $\Gamma := \{b_1, \ldots, b_4\}$, $\Gamma_i := \Gamma \setminus \{b_i\}$




A further occurrence from $\Sigma$ will betray the faulty states.

# Lower bound for minimal delay

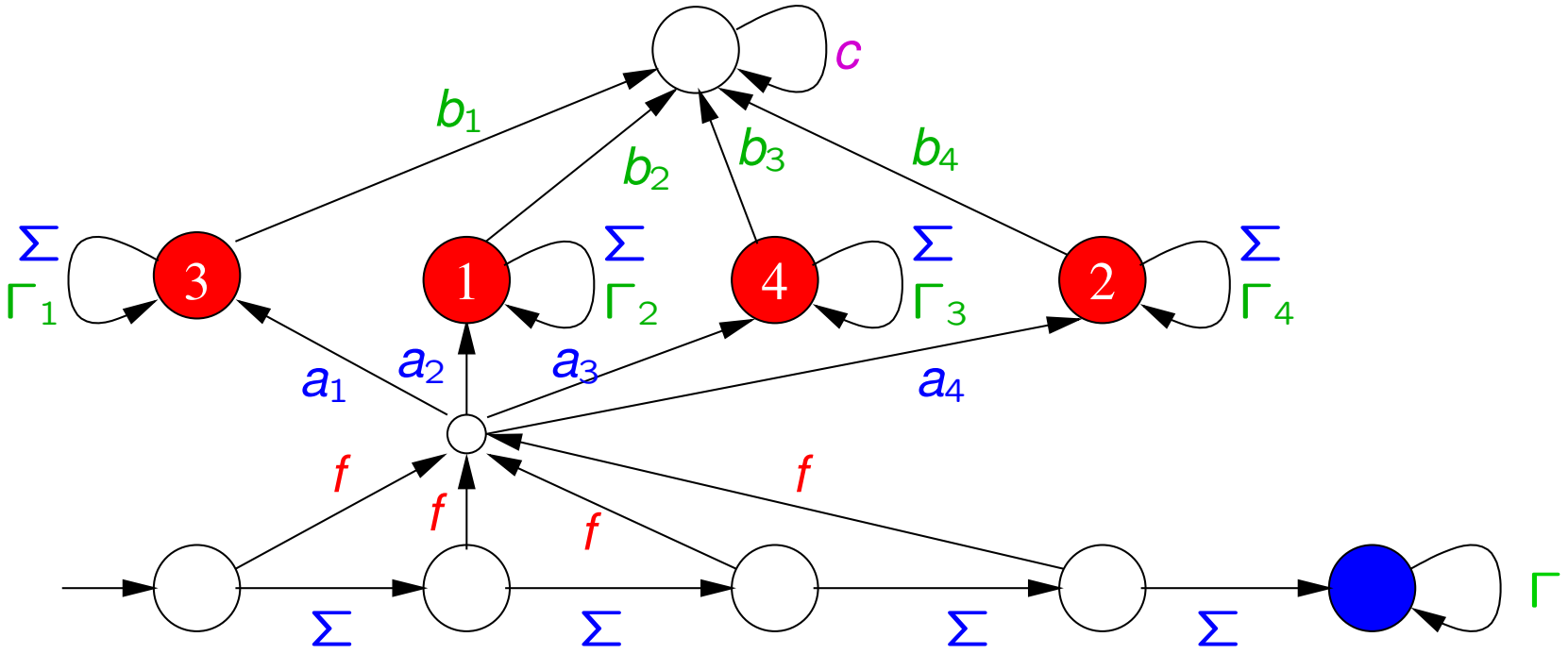
Definitions: $\Sigma := \{a_1, \ldots, a_4\}$, $\Gamma := \{b_1, \ldots, b_4\}$, $\Gamma_i := \Gamma \setminus \{b_i\}$




On the other hand, e.g., $b_1$ eliminates the leftmost state...

# Lower bound for minimal delay

Definitions: $\Sigma := \{a_1, \ldots, a_4\}$, $\Gamma := \{b_1, \ldots, b_4\}$, $\Gamma_i := \Gamma \setminus \{b_i\}$




Remember $\Gamma$ is controllable. Optimal-delay control: $b_3 b_1 b_4 b_2$.

# Perspectives

“Safe” control: avoid forcing the fault

Extension for multiple error types

Precise connection to game theory

Other types of systems, e.g. active diagnosis with concurrency