ACD 2010
Ferrara
Italy
18-19/11/2010

Design ***and Evaluation*** of Reconfiguration-based Fault Tolerance using the Lattice of System Configurations

Marcel Staroswiecki

SATIE, ENS Cachan, USTL, CNRS, UniverSud
61 avenue du Président Wilson
94235 Cachan Cedex, France

- **Introduction**
- **The lattice of system configurations**
- **Admissible configurations**
- **The design of FT strategies**
- ***<u>Evaluation issues</u>***
- **Example**

Introduction

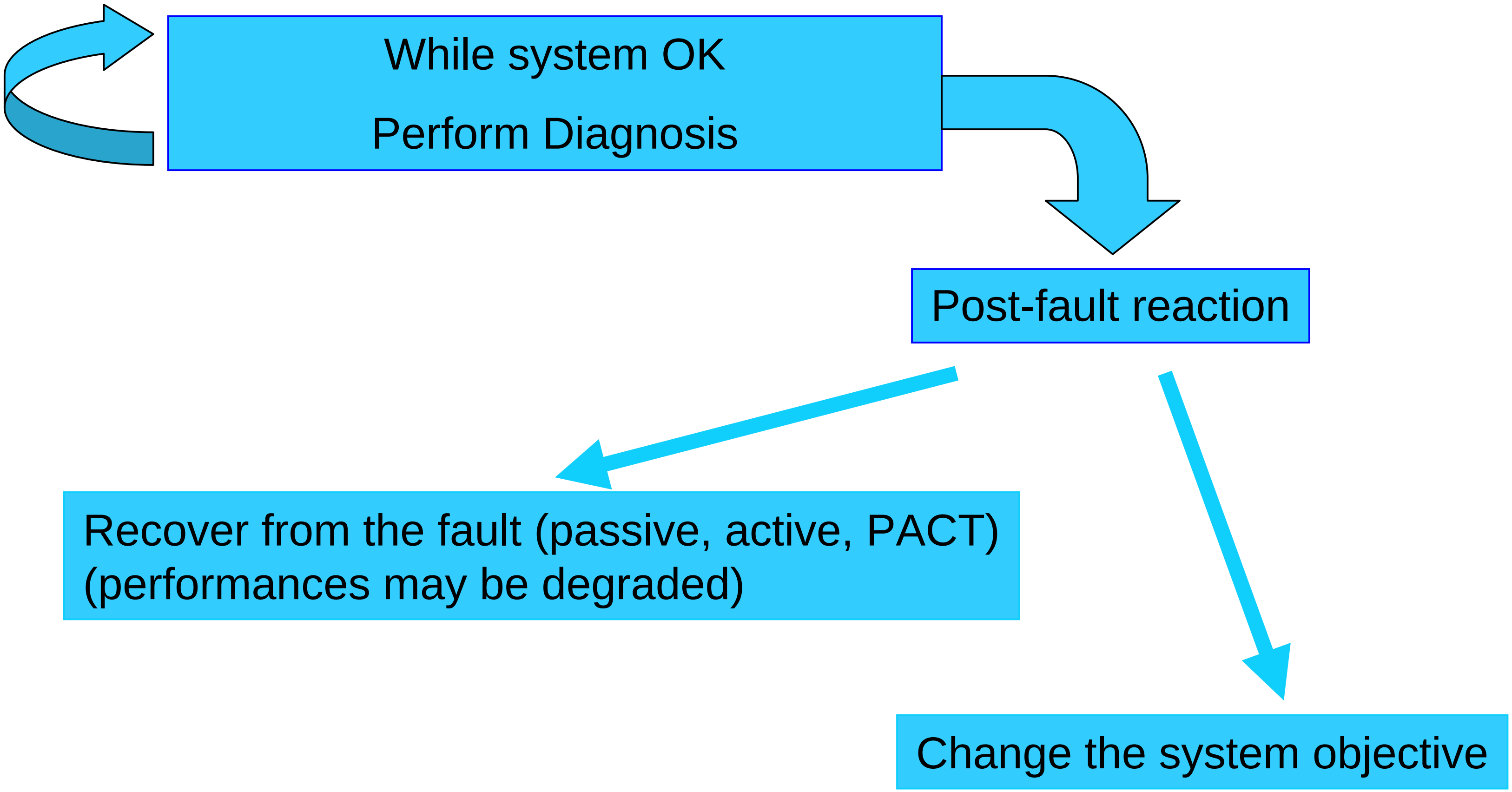
- Complex systems must be reliable
- On-line diagnosis and fault handling
- Accommodation and reconfiguration

Introduction : complex systems must be reliable

1. Sensors, actuators are prone to failure
2. Faults propagate (sometimes i ... prising way)
3. Some faults may be c
4. All applicati ... s are concerned
   1. Producti ... wer plants, chemical, petrochemical, mass production, ...
   2. ... : aerospace, printers, motors, cars, ...

Every one in this room is convinced

Introduction : on-line diagnosis and fault handling



Introduction : recovery by fault accommodation

Accommodation

adapt the control or estimation law
to the faulty components so as to achieve
the objective

- the model of faulty components is necessary
(isolation + estimation)

Introduction : recovery by system reconfiguration

Reconfiguration
switch-off faulty components,
achieve the objective (if possible)
by using only the healthy ones

- faulty components can indeed be switched-off
- does not need faulty components model, only isolation

Introduction : the lattice of system configurations

- SR-based Fault Tolerance : we are interested in all subsets of system components
- The lattice of system configurations is the underlying mathematical framework
- Key role played by this framework : useful concepts and tools for
  - the design (passive / active / reliable) control or estimation laws,
  - *the evaluation (fault recoverability, FT effectiveness, components usefulness)*

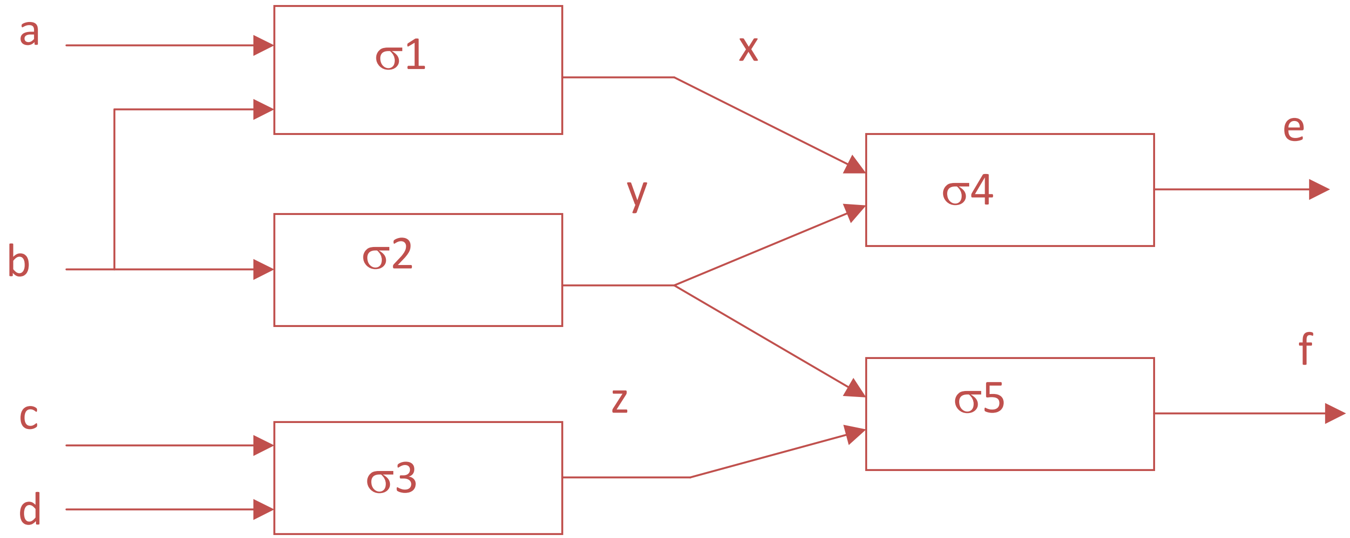
Introduction

Lattice of configurations

- System and configurations
- Interpretation
- The lattice of configurations
- Some definitions

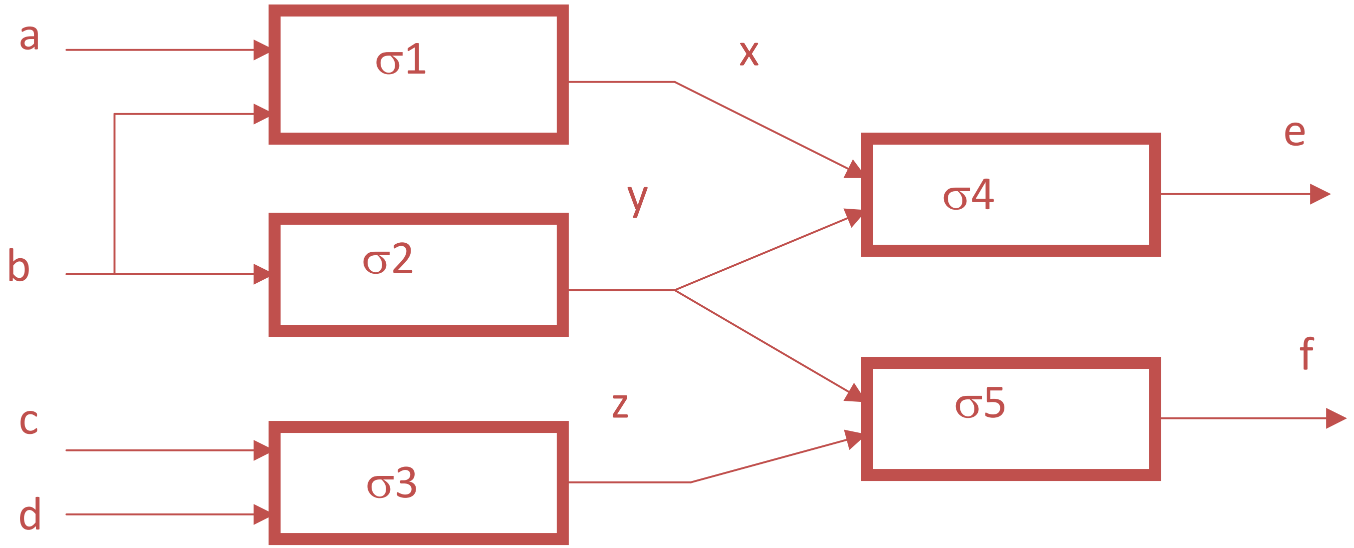
System

A system is a set of interconnected components



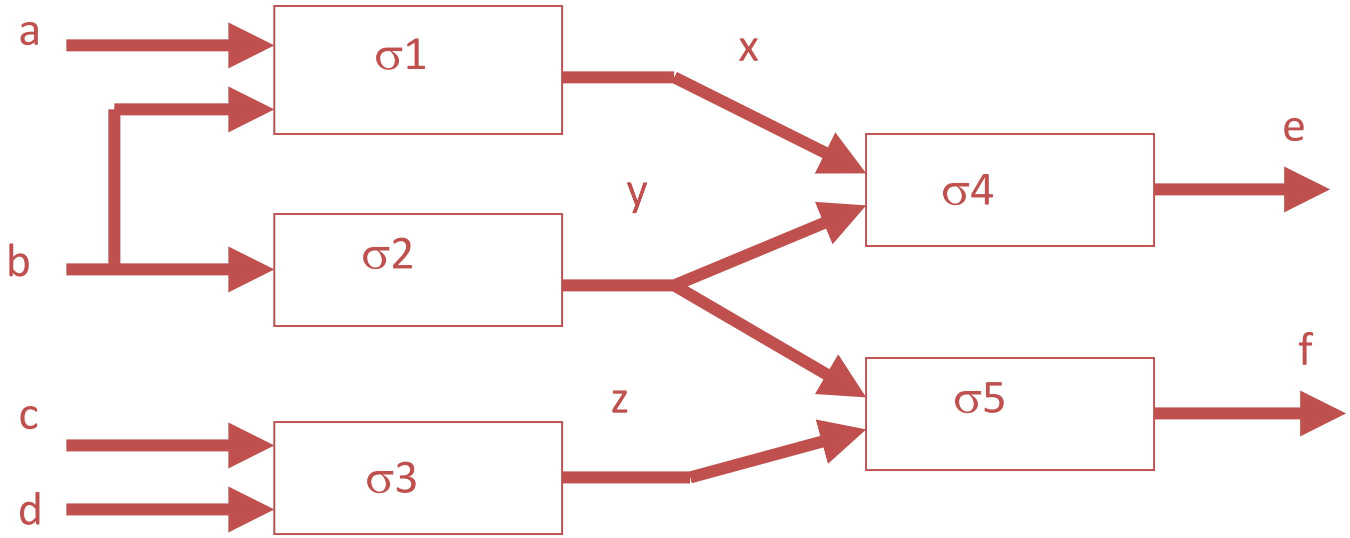
Components

s_0 = {σ1, σ2, σ3, σ4, σ5}



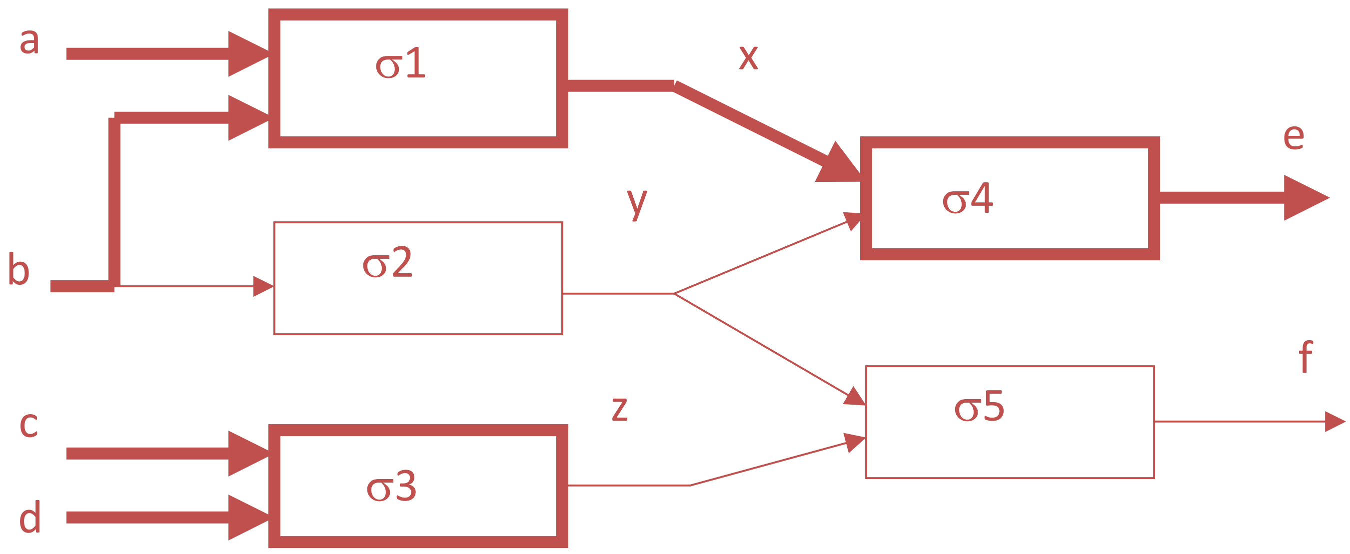
Interconnections

$I_0 = \{(a,\sigma1),(b,\sigma1),(b,\sigma2), (c,\sigma3), (d,\sigma3),(\sigma1, \sigma4), (\sigma2,\sigma4), (\sigma2,\sigma5), (\sigma3, \sigma5), (\sigma4,e), (\sigma5,f)\}$



Configuration

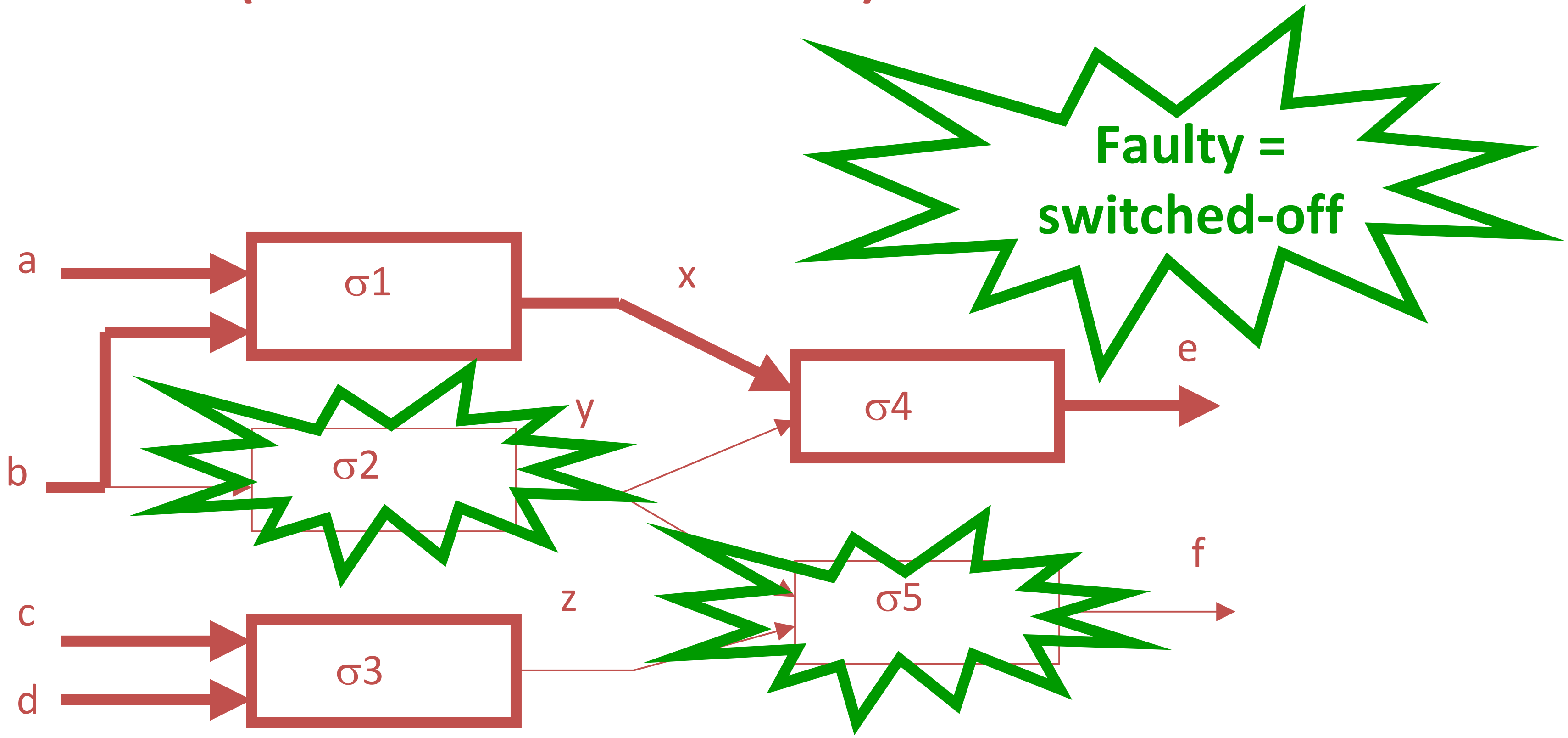
A configuration is a subset of those components along with their links



Interpretation

All possible configurations = all possible faults

(because SR is considered)



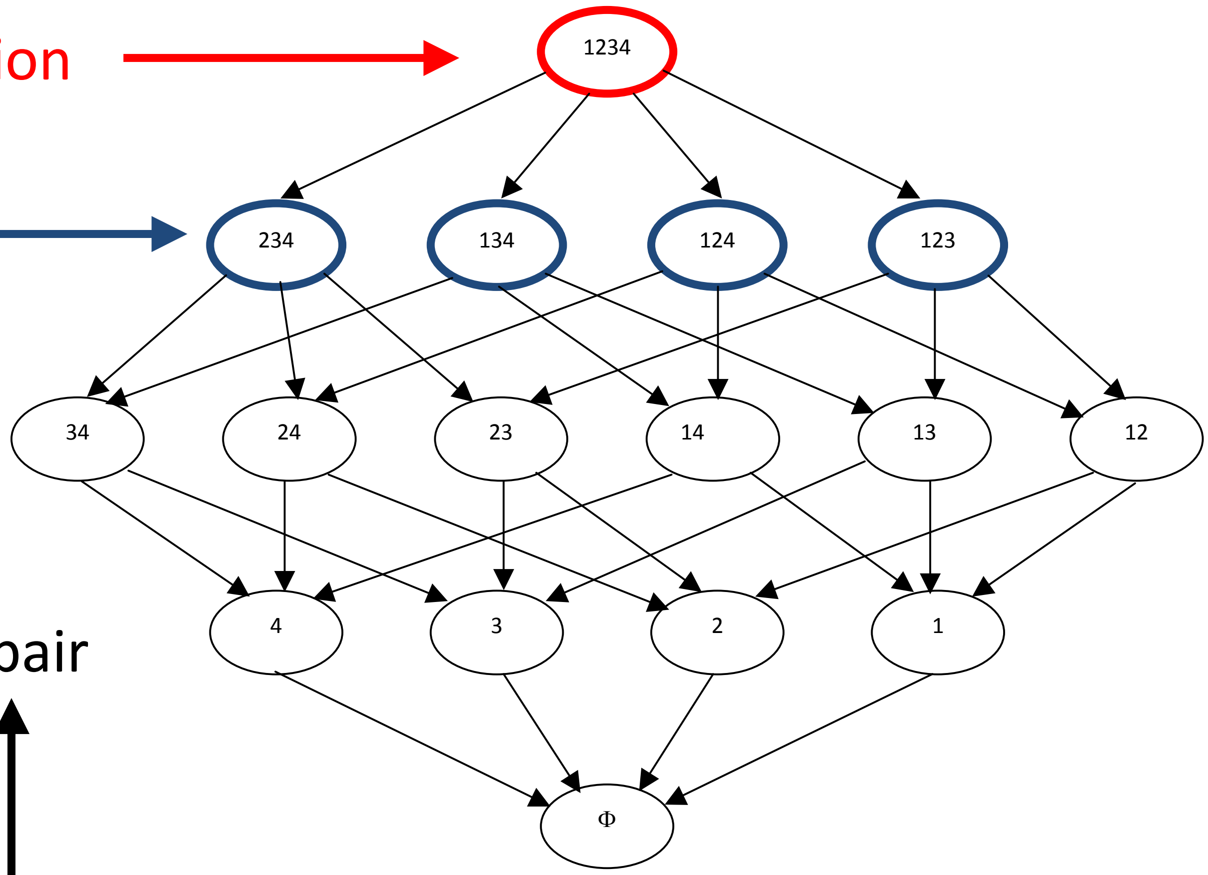
Lattice of configurations

A system with 4 components (e.g. sensors)

Nominal configuration

One sensor lost

etc.



fault

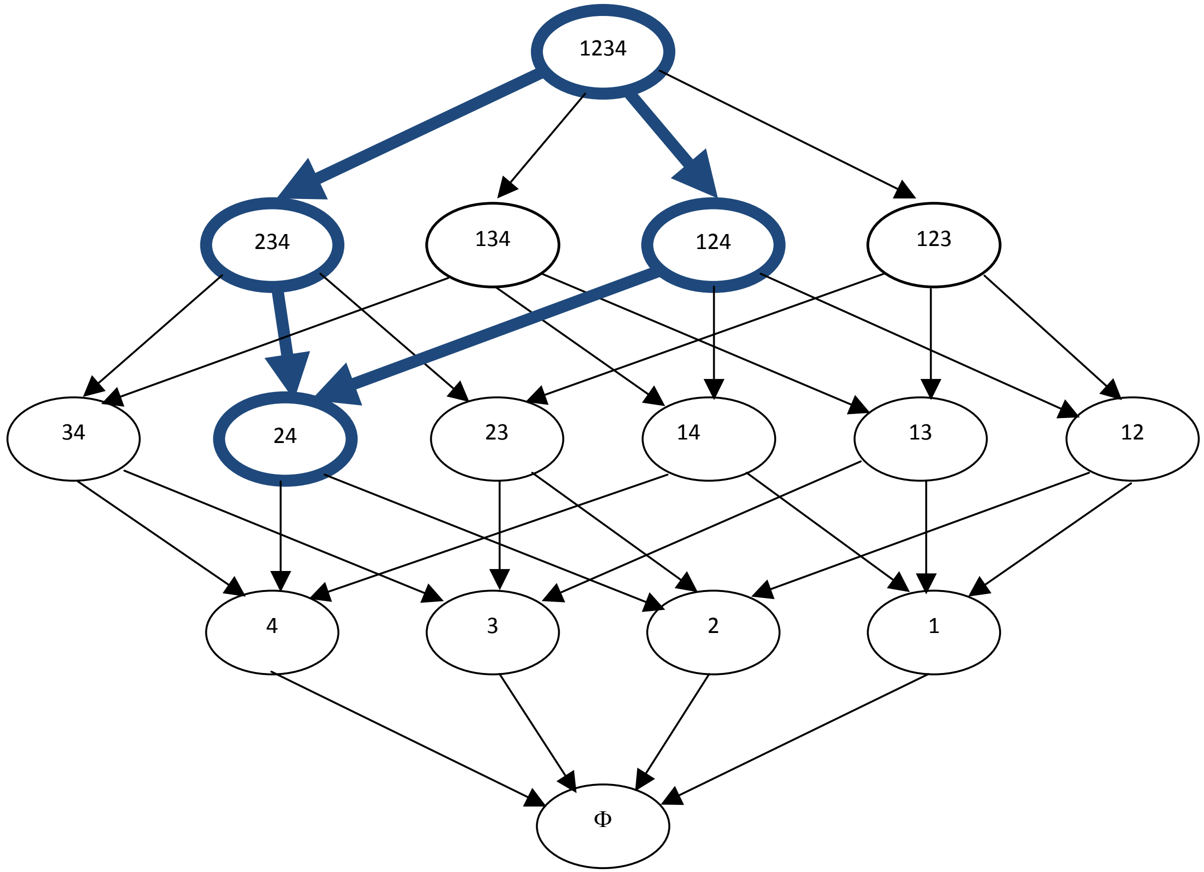
Autonomous system

repair

Maintenance

Some definitions : predecessors

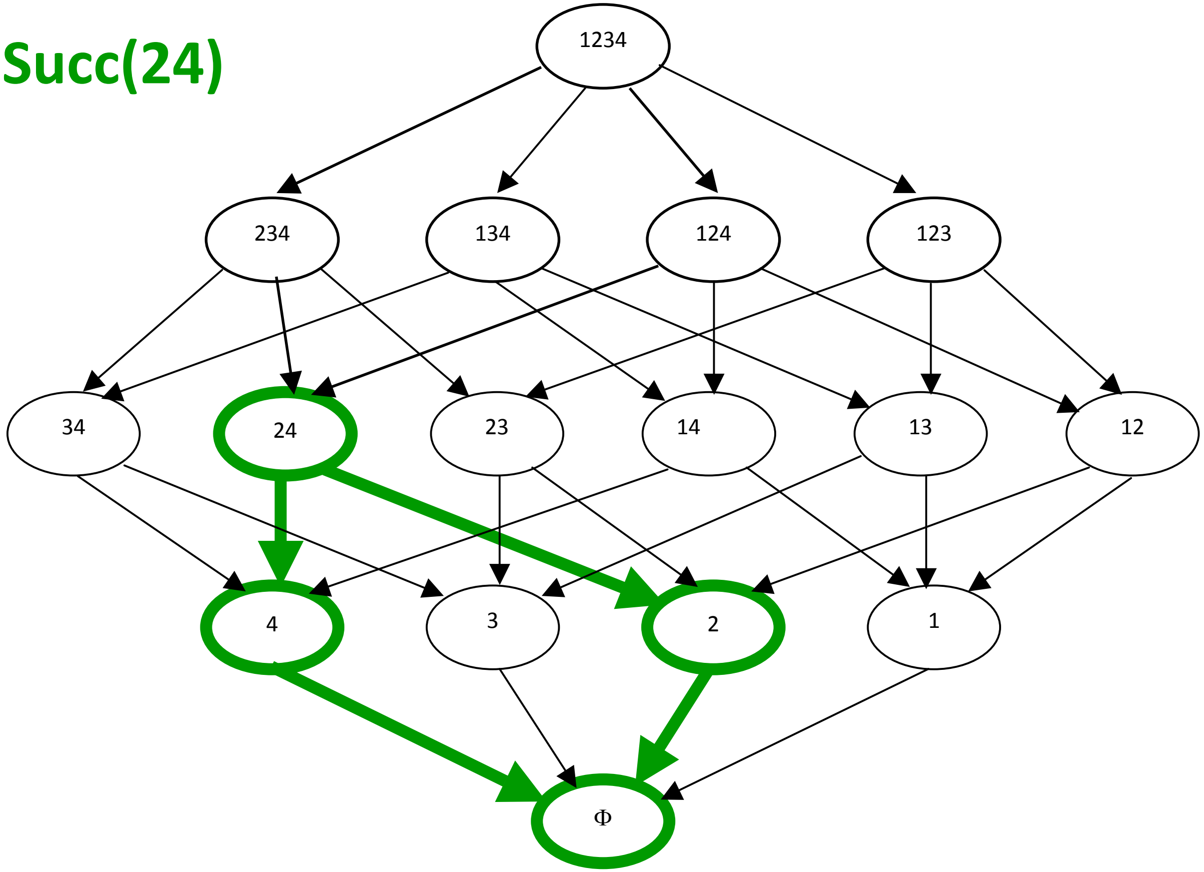
Predecessors of 24 : Pred(24)



Some definitions : successors

Predecessors of 24

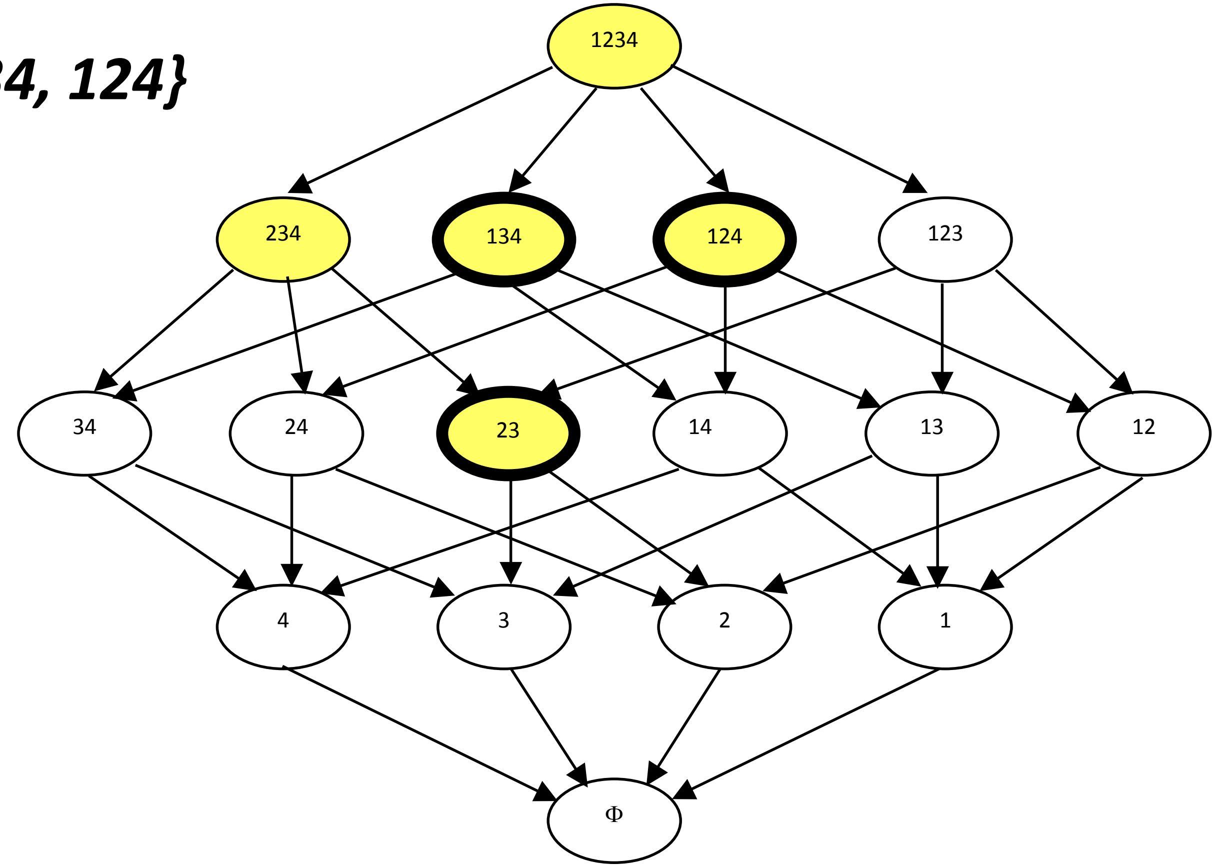
Successors of 24 : Succ(24)



Some definitions : minimal configurations

Minimal configurations in S

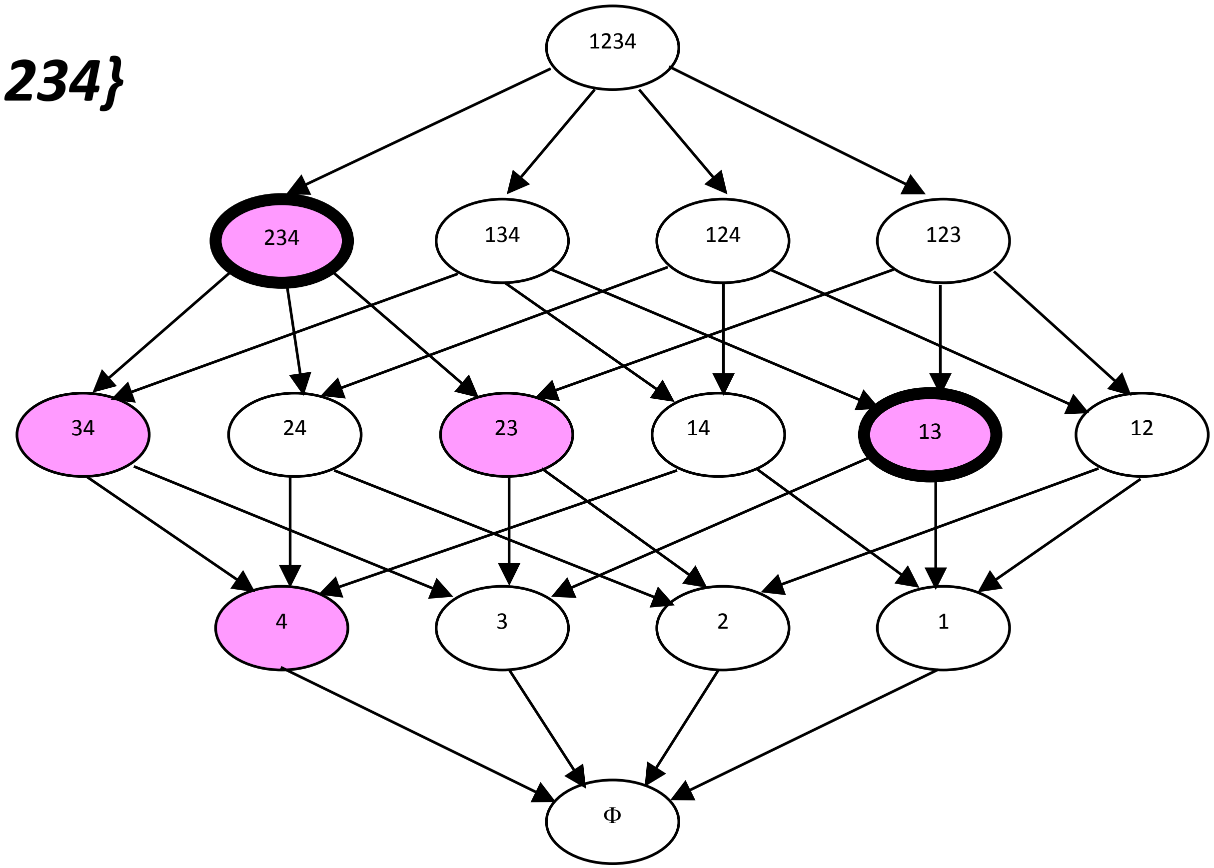
m(S) = {23, 134, 124}



Some definitions : maximal configurations

Maximal configurations in S

M(S) = {13, 234}



- Specifications
- Admissible configurations
  - Structural properties
  - Non structural properties

Specifications : Property

The specifications are expressed by some given property P that the system is wished to satisfy.

Examples (estimation)

- a functional z of the state x is observable
- z remains observable in spite of the failure of q sensors
- estimation error remains less than a given bound in spite of such failures
- diagnosis remains possible in spite of such failures

Examples (control)

- stability, α stability, poles in some specified region
- guaranteed tracking performances
- optimal control (upper cost limit)
- guaranteed robustness and disturbance attenuation

Composed, structural, non structural properties

Composed properties

$$P = P_1 P_2 \ldots P_K$$

Example : generic observability of structured linear systems

P_1 : output-connection

P_2 : no-contraction

- **Structural properties** : are (or not) satisfied by a configuration

- **Non structural properties** are (or not) satisfied by a configuration according to the result of some external design process (e.g. a control or estimation law)

Examples

- **Structural properties**
  - observability by a sensor configuration
  - controllability by an actuator configuration
  - cost, weight, etc. of a sensor (an actuator) configuration

- **Non structural properties**
  - stability under a given control law
  - guaranteed estimation error under an estimation law
  - identifiability under a given sampling policy

Structural properties : span

Notation : $P(s)$: configuration s satisfies property P
$\neg P(s)$: configuration s does not satisfy property P

Admissibility : s admissible $\Leftrightarrow P(s)$
Composed property : $P(s) = P_1(s)P_2(s) \ldots P_K(s)$

Span of property P : $S(P) = \{s : P(s)\}$
Composed property : $S(P) = S(P_1) \cap S(P_2) \cap \ldots \cap S(P_K)$

Example : structural observability (linear structured systems)

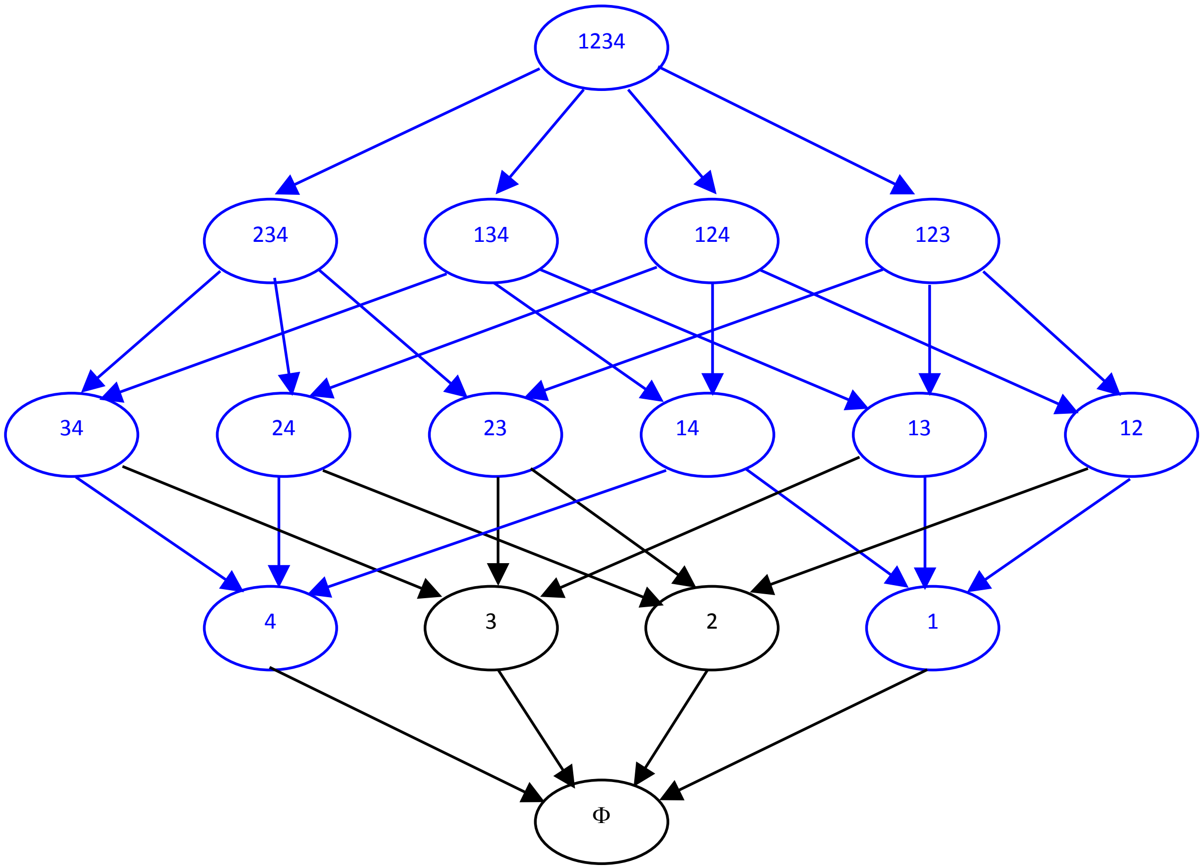
$$S(P) = S(P_1) \cap S(P_2)$$

Output connection → $S(P_1)$

No contraction → $S(P_2)$

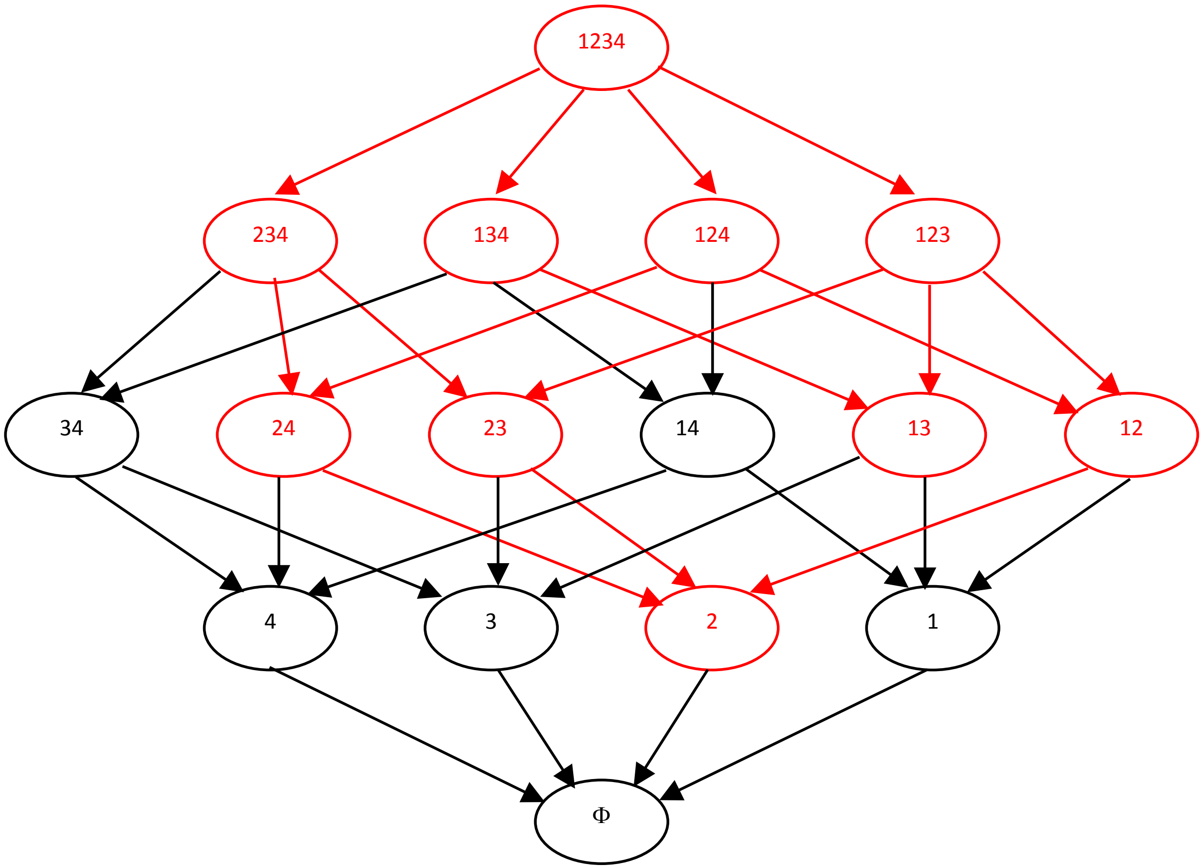
Structural properties : span (example 4 sensors)

$P_1(s)$: system is output connected by s



Structural properties : span (example 4 sensors)

$P_2(s)$: there is no contraction with s

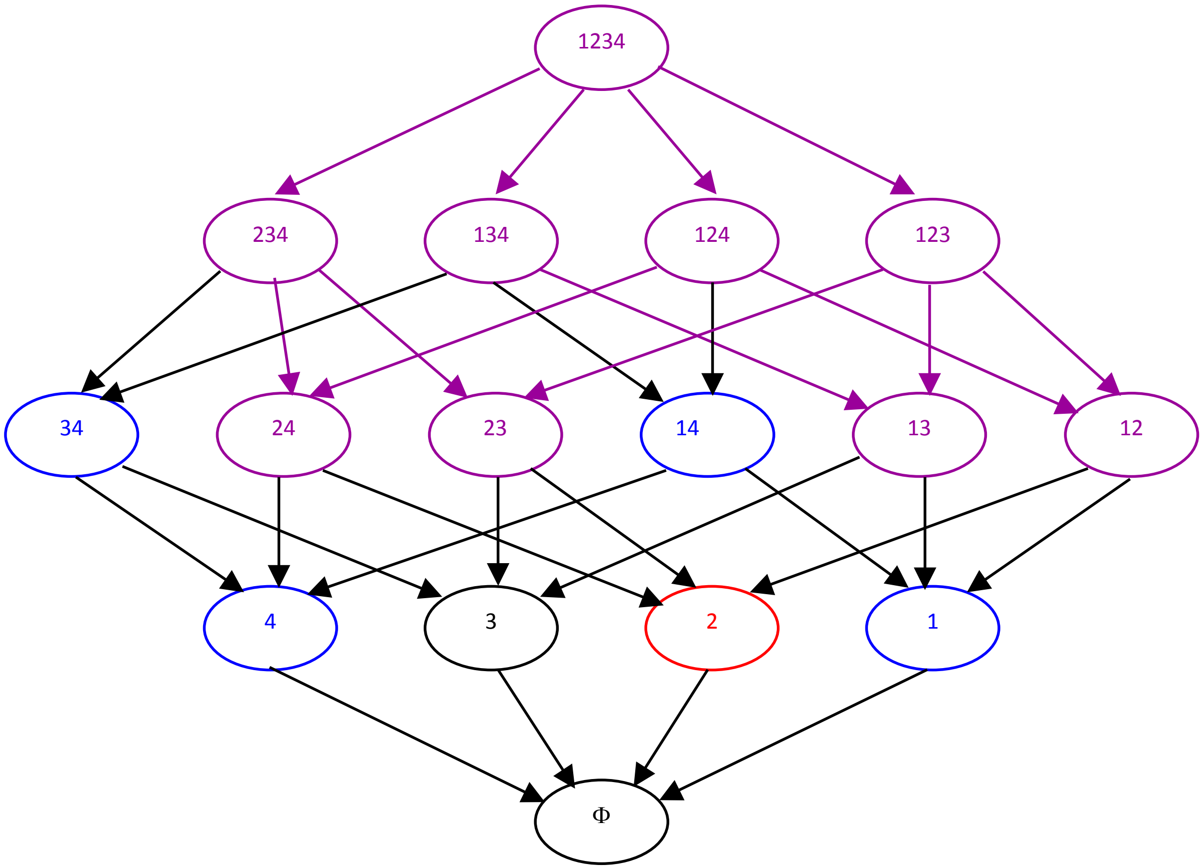


Structural properties : span (example 4 sensors)

P(s) : system is structurally observable by s

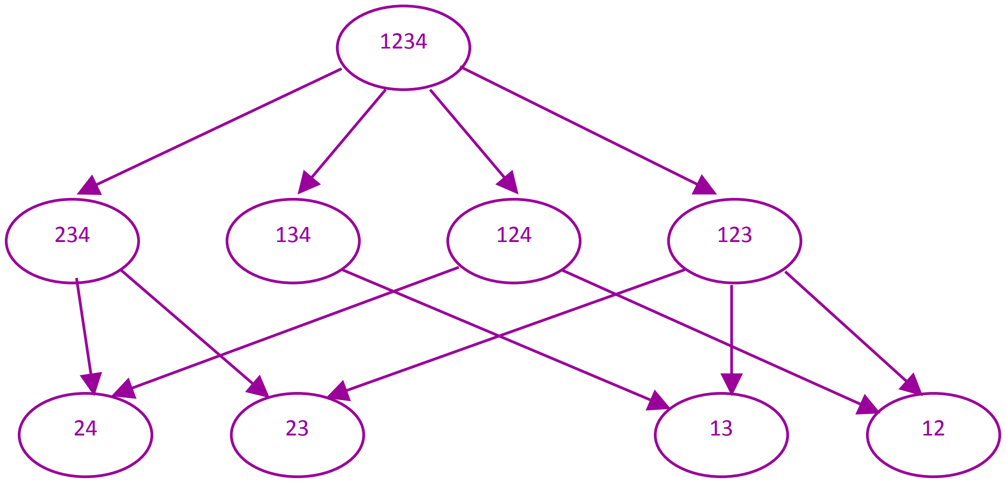
$P_1(s)$: system is output connected by s

$P_2(s)$: there is no contraction with s



Structural properties : span (example 4 sensors)

S(P) : span of P

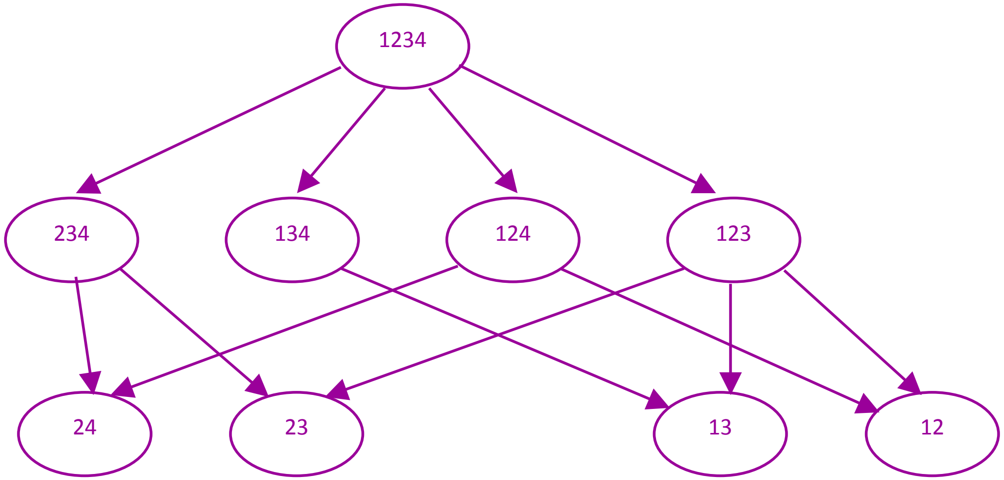


Structural properties : monotony

Monotony :

- P is bottom-up monotonous (bum) : $P(s) \Rightarrow P(s'), \forall s' \in Pred(s)$
- P is top-down monotonous (tdm) : $P(s) \Rightarrow P(s'), \forall s' \in Succ(s)$

Structural observability is bum

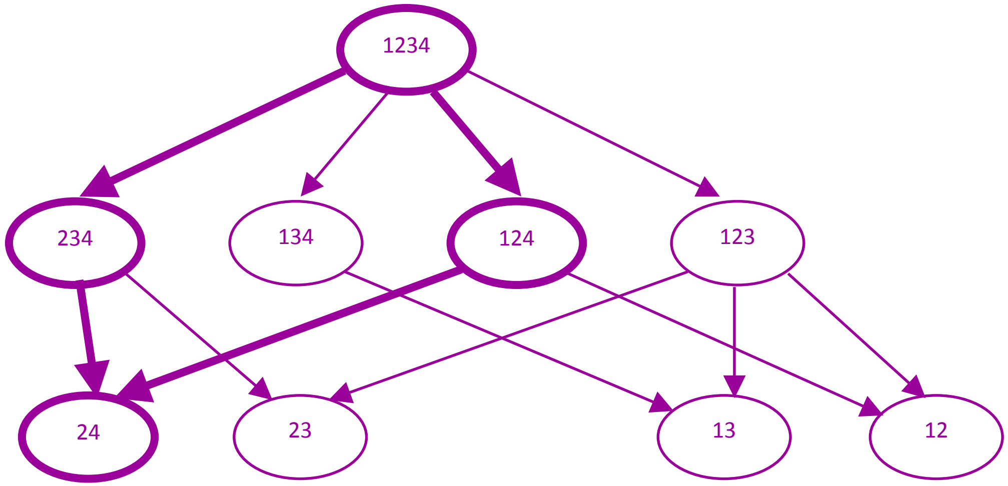


Structural properties : monotony

Monotony :

- P is bottom-up monotonous (bum) : $P(s) \Rightarrow P(s'), \forall s' \in Pred(s)$
- P is top-down monotonous (tdm) : $P(s) \Rightarrow P(s'), \forall s' \in Succ(s)$

Structural observability is bum

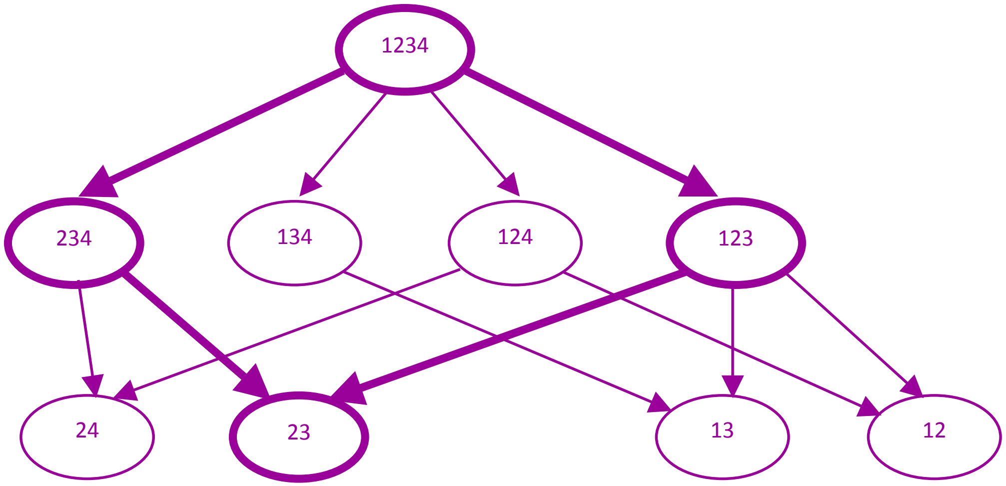


Structural properties : monotony

Monotony :

- P is bottom-up monotonous (bum) : $P(s) \Rightarrow P(s'), \forall s' \in Pred(s)$
- P is top-down monotonous (tdm) : $P(s) \Rightarrow P(s'), \forall s' \in Succ(s)$

Structural observability is bum

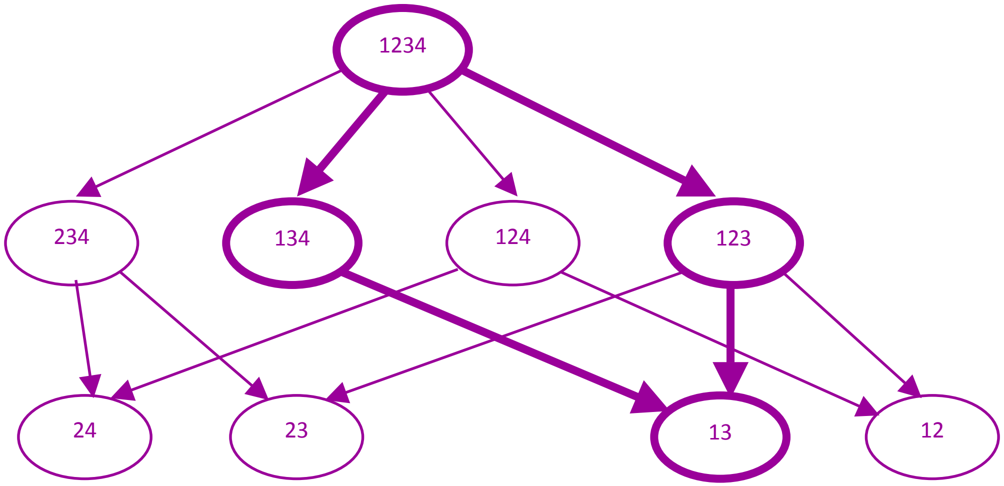


Structural properties : monotony

Monotony :

- P is bottom-up monotonous (bum) : $P(s) \Rightarrow P(s'), \forall s' \in Pred(s)$
- P is top-down monotonous (tdm) : $P(s) \Rightarrow P(s'), \forall s' \in Succ(s)$

Structural observability is bum

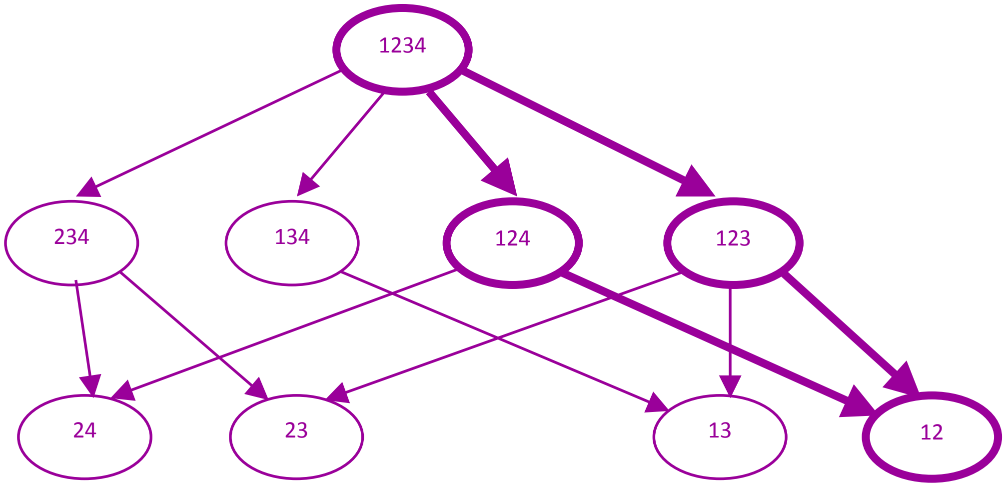


Structural properties : monotony

Monotony :

- P is bottom-up monotonous (bum) : $P(s) \Rightarrow P(s'), \forall s' \in Pred(s)$
- P is top-down monotonous (tdm) : $P(s) \Rightarrow P(s'), \forall s' \in Succ(s)$

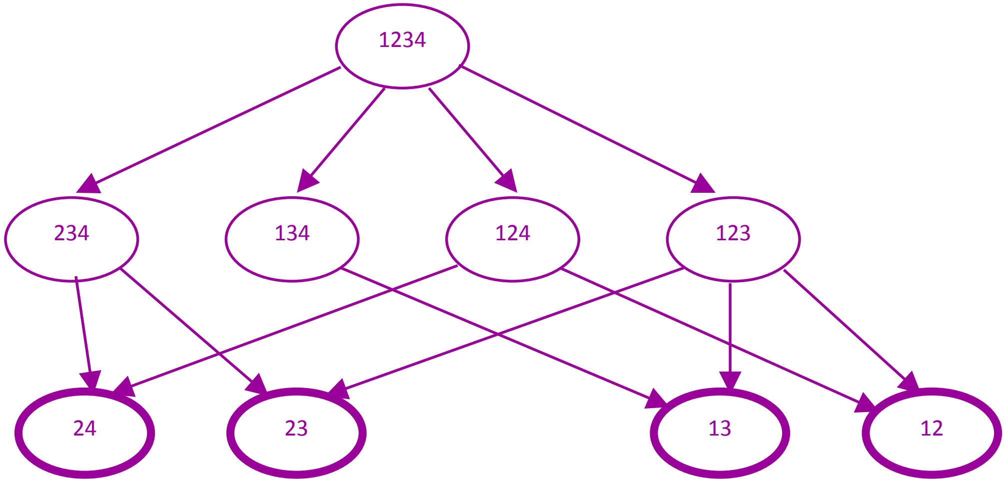
Structural observability is bum



Structural properties : minimality / maximality

Minimal admissible configurations of a bum property
$m(P) = \{s : P(s) \text{ and } \neg P(s'), \forall s' \in Succ(s)\}$

Maximal admissible configurations of a tdm property
$M(P) = \{s : P(s) \text{ and } \neg P(s'), \forall s' \in Pred(s)\}$



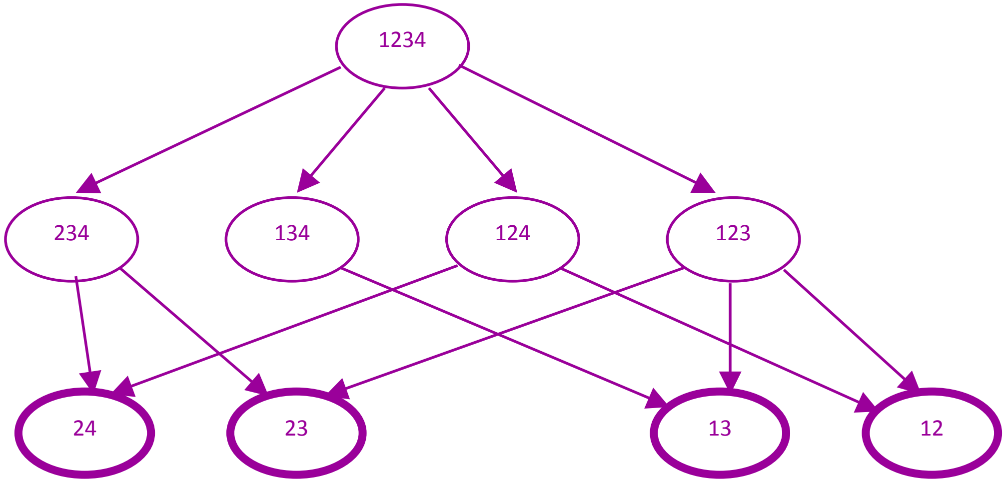
m(structural observability)

Span and extremal configurations

The span can be characterised using only the minimal (maximal) admissible configurations

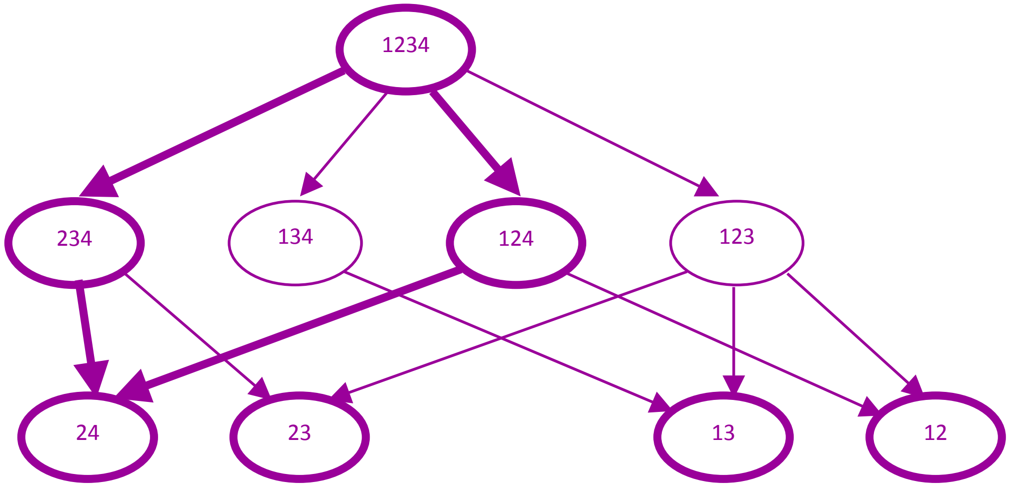
P is bum $\Rightarrow$ $S(P) = \cup_{\{s \in m(P)\}} Pred(s)$

Minimal configurations



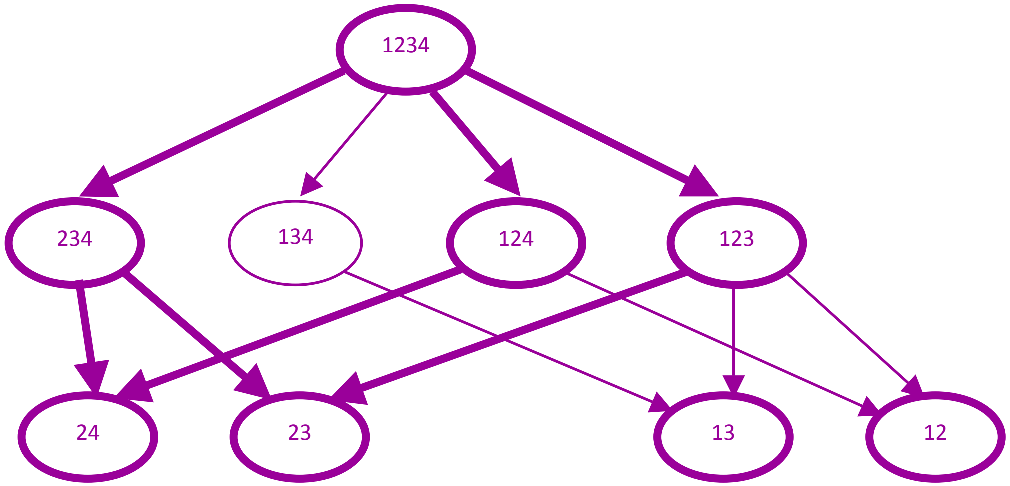
m(structural observability)

Span and extremal configurations



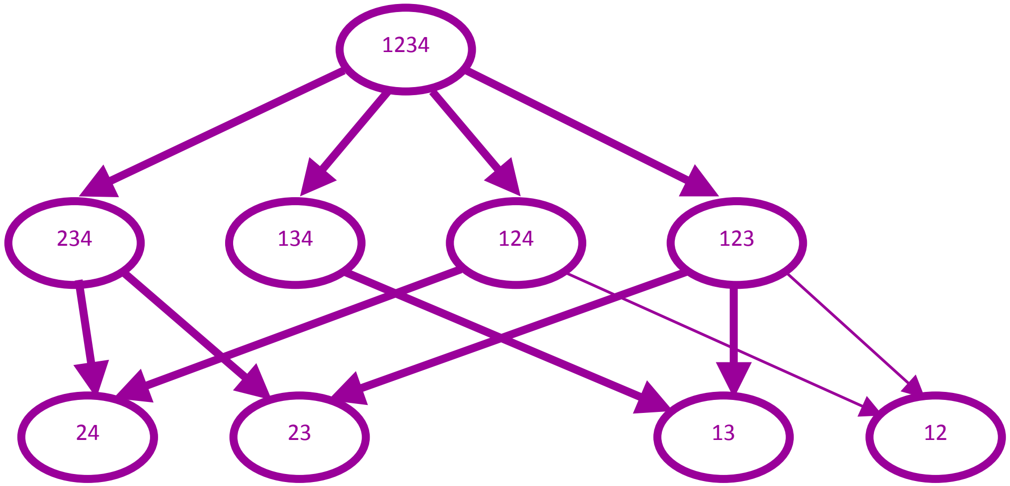
m(structural observability)

Span and extremal configurations



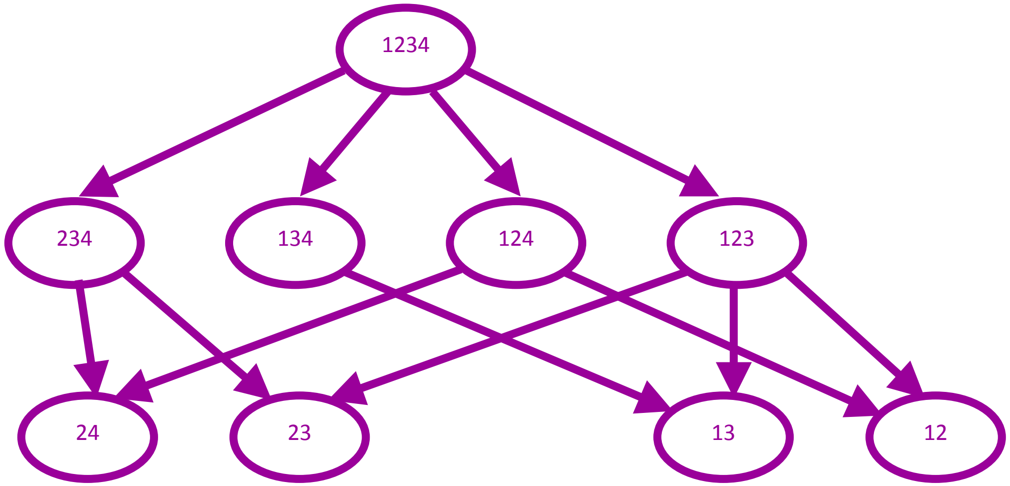
m(structural observability)

Span and extremal configurations



m(structural observability)

Span and extremal configurations



m(structural observability)

Non structural properties : definitions

The fulfilment of a non-structural property depends both on the configuration that is considered and on the result *u* of some design process (e.g. the control/estimation law)

Admissibility : (*u,s)* is admissible for property *P* if *P*(*s,u*)

Span : *S*(*P,u*) is the set of all configurations that satisfy *P* when *u* is used.

Non structural properties : definitions

Monotony : P is bum using u if $\forall s \in S : \forall \sigma \in \text{Pred}(s)$
$$P(s,u) \Rightarrow P(\sigma,u)$$

(remark that a non-structural property may be monotonous for some law u, and non-monotonous for another one).

Minimal admissible configurations : Let P be bum using u, the set $m(P,u)$ of minimal admissible configuration is

$$m(P,u) = \{s \in S : P(s,u) \text{ and } \rceil P(s,u)\ ;\ \forall \sigma \in \text{Succ}(s)\}$$

Non structural properties : definitions

Recoverability : A fault $s_f \subseteq s_0$ is recoverable if there exists a law u such that $P(s_0 \backslash s_f, u)$.

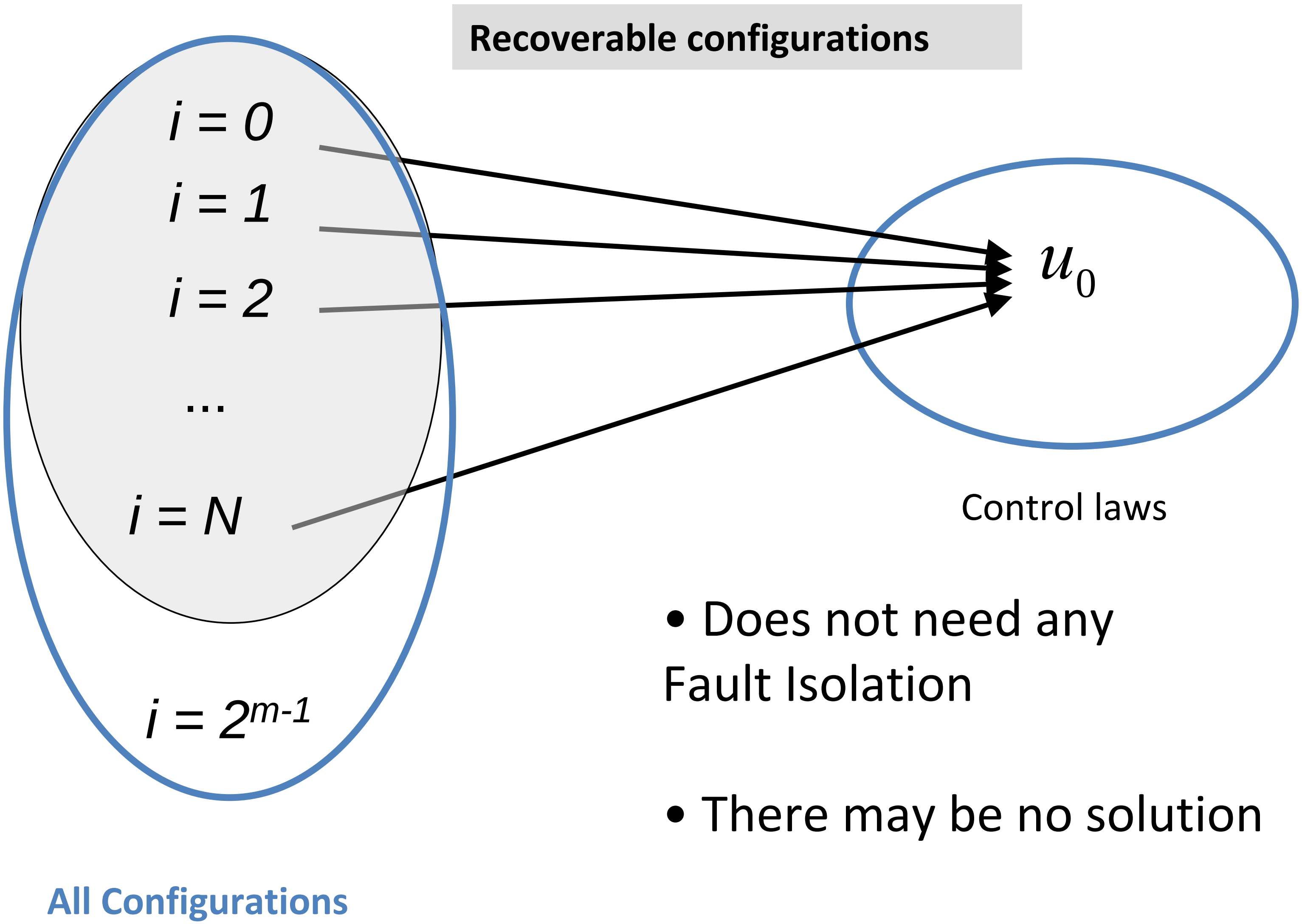
Remark : Let s_f be recoverable and let u be a law that recovers from s_f. If P is bum using u then u also recovers from faults that are "smaller" than s_f *because*

$$P(s_0 \backslash s_f, u) \Rightarrow P(s_0 \backslash \sigma, u), \forall \sigma \subseteq s_f$$

Extensivity : The law u is bum-extensive for property P if it is such that P is bum using u. It is bum-extensive over s_m if $s_m \in m(P,u)$

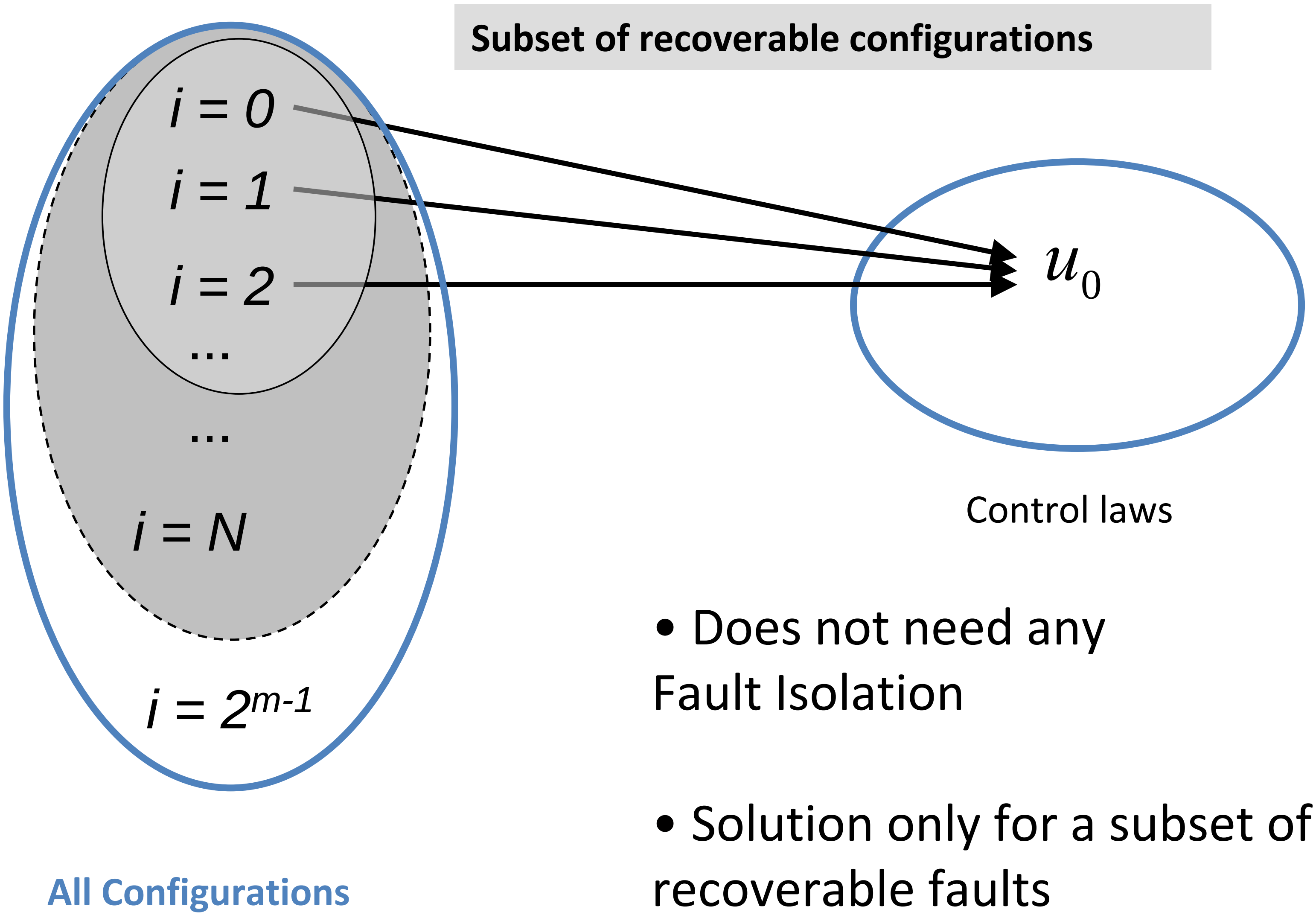
- Different FTC approaches
- The PACT strategy
  - Definition
  - Design of a PACT

Different FTC approaches : passive FTC



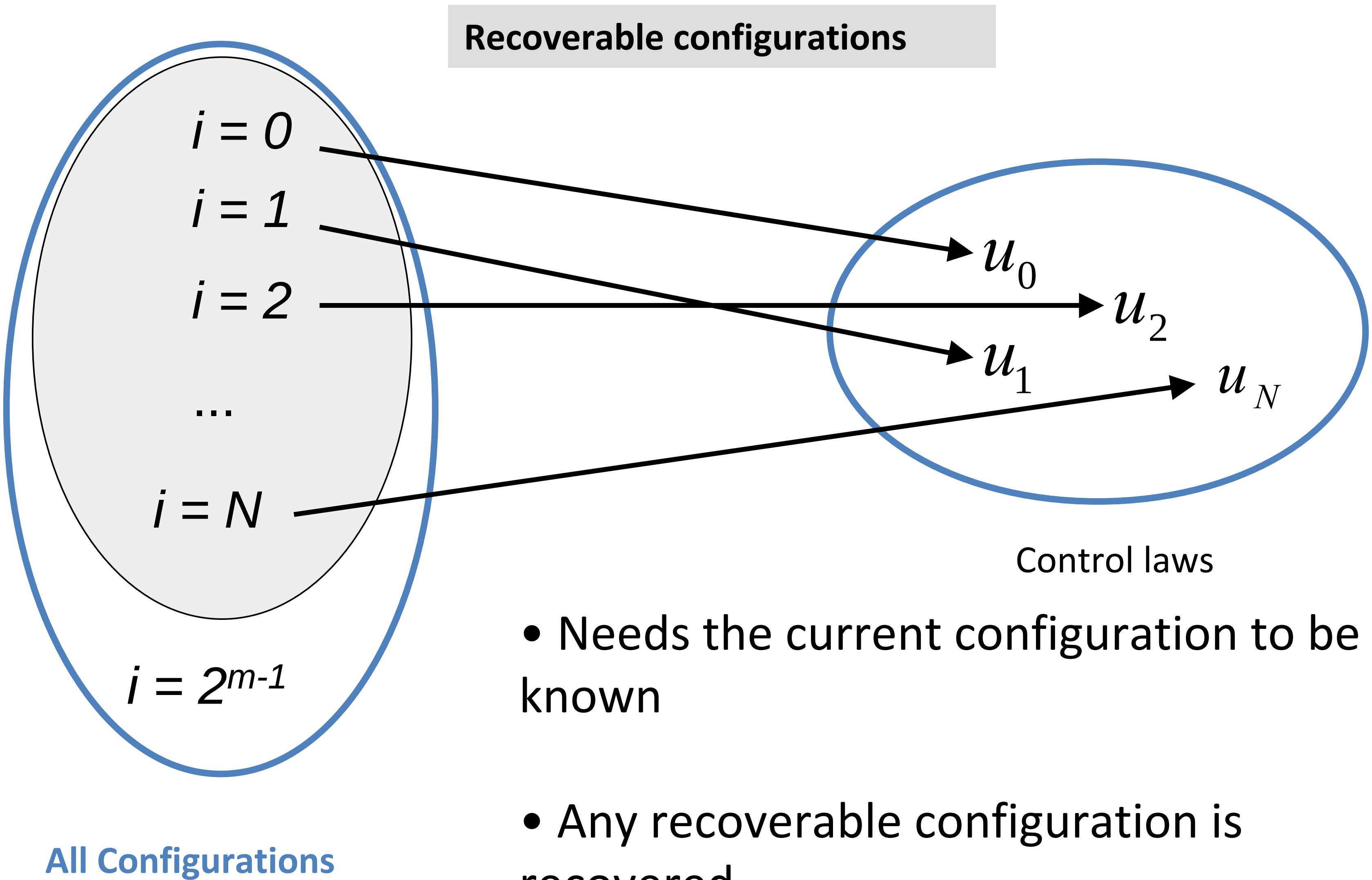
- Does not need any Fault Isolation
- There may be no solution

Different FTC approaches : reliable control



- Does not need any Fault Isolation
- Solution only for a subset of recoverable faults

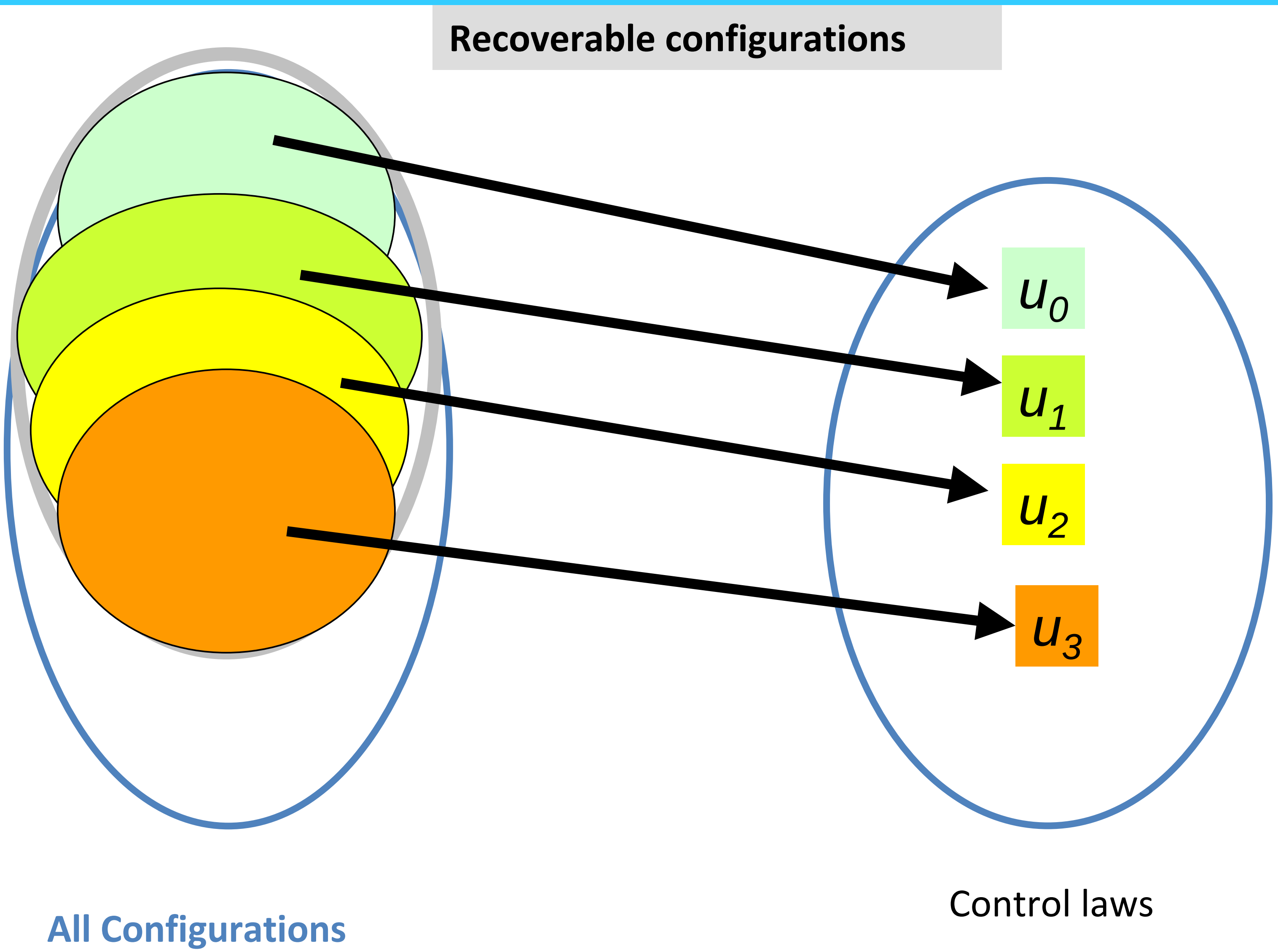
Different FTC approaches : active FTC



- Needs the current configuration to be known

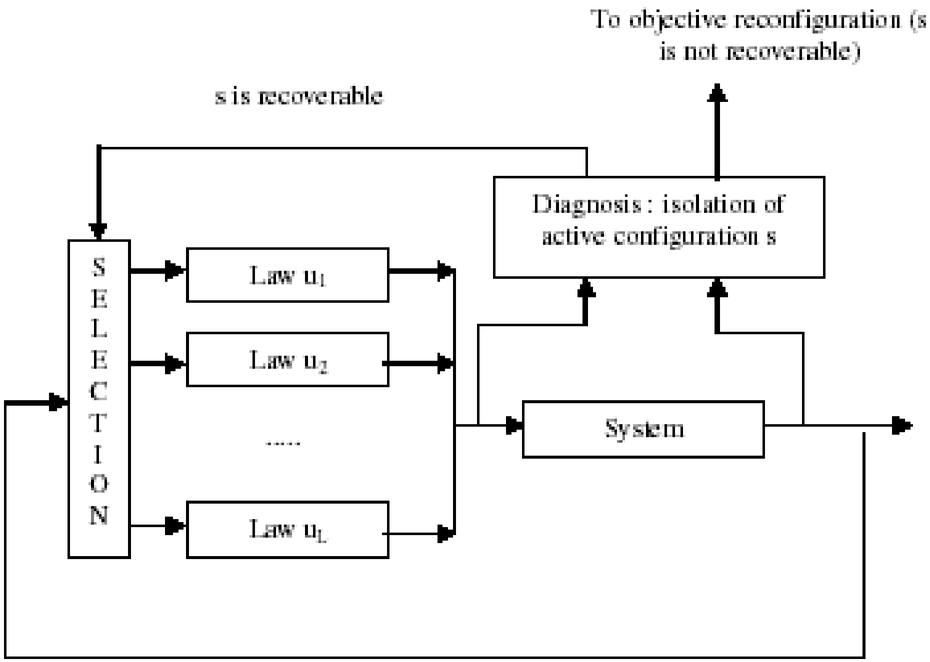
- Any recoverable configuration is recovered

Different FTC approaches : PACT control



Different FTC approaches : PACT control

Definition: A PACT (PAssive / ACTive) scheme is a pair (U, d) where U is a bank of laws such that for any recoverable configuration s, $\exists$ U(s) $\subseteq$ U : u $\in$ U (s) $\Rightarrow$ P(s,u) and *d* is a decision procedure that associates one single control law *u* $\in$ *U* (*s*) with each recoverable configuration s.



Design of a PACT

Interest of a PACT : trades-off the efficiency of AFT (by allowing to cover the set of all recoverable faults) and the simplicity of PFT (by finding a bank with a low number of laws.

Design of a PACT involves two steps :

- find a bank of laws that covers all recoverable configurations,

- for each recoverable configuration define a decision procedure that selects only one law.

Design of a PACT

Proposition: Let U be a bank of bum-extensive laws.
A necessary and sufficient condition for *U to be a PACT bank* is that for each Minimal Recoverable Configuration s_m, U contains a bum-extensive law over s_m.

The PACT bank problem is therefore to design, for each MRC, a bum-extensive law. Design approaches depend on the component models and on the property to be satisfied.

Example : LTI system under actuator outages (reconfiguration) with a quadratic cost constraint.

Design of a PACT (example)

$$\dot{x} = Ax + Bu$$

$$I = \{0, 1, \ldots 2^{m-1}\}$$

Faults = actuator outages $\Rightarrow B \in \{B_i, i \in I\}$

Nominal configuration
(all actuators available)

Faulty situations
(a subset of actuators switched-off)

Configuration n°i (A, B_i) $\quad B_i = B_0 \Sigma_i \quad \Sigma_\text{i} = diag\{\sigma_i(k), k = 1, \ldots m\}$

Set of configurations
=
lattice

Design of a PACT (example)

(A,B,Q,R), $B = B_0\Sigma$, $Q = C^T C \geq 0$, $R > 0$

(C,A) detectable, (A,B) stabilizable

Performance of $u=Kx$

$$J = \int_0^\infty \left(x^T Q x + u^T \Sigma R \Sigma u\right) dt$$

under $\dot{x}=(A+BK)x$ and $x(0)=x_0$

The control law

The configuration

cost : $J(x_0,K)=x_0^T W x_0$

$W \geq 0$ satisfies the Lyapunov equation

$$Q+K^T \Sigma R \Sigma K+W(A+BK)+(A+BK)^T W=0$$

$u=Kx$ is admissible $\Leftrightarrow J(x_0,K) \leq x_0^T N x_0 \Leftrightarrow W\text{-}N \leq 0$

where $N=N^T > 0$ is given.

Design of a PACT (example)

Theorem 1 (Veillette 1995). Let W_s^* be the unique symmetric positive definite stabilizing solution of the Riccati equation associated with a configuration *s*. Then, the control law

$$u_s(t) = -R^{-1} B^T{}_0 W_s^* x(t)$$

stabilizes all configurations $\sigma \in$ Pred(*s*) and the associated cost satisfies

$$J(x_0, \sigma, u_s) \leq x^T{}_0 W^*{}_s x_0$$

Consequence : for each minimal recoverable configuration s, $u_s(t) = -R^{-1} B^T{}_0 W_s^* x(t)$ is bum-extensive

Design of a PACT (example)

Theorem 2 (extension). For any configuration s, if there exists two symmetric positive definite matrices H_s and W_s such that

$$Q + H_s B_s R^{-1} B_s^T H_s + W_s(A - B_s R^{-1} B^T{}_0 H_s) + (A - B_s R^{-1} B^T{}_0 H_s)^T W_s \leq 0$$

$$W_s - N \leq 0$$

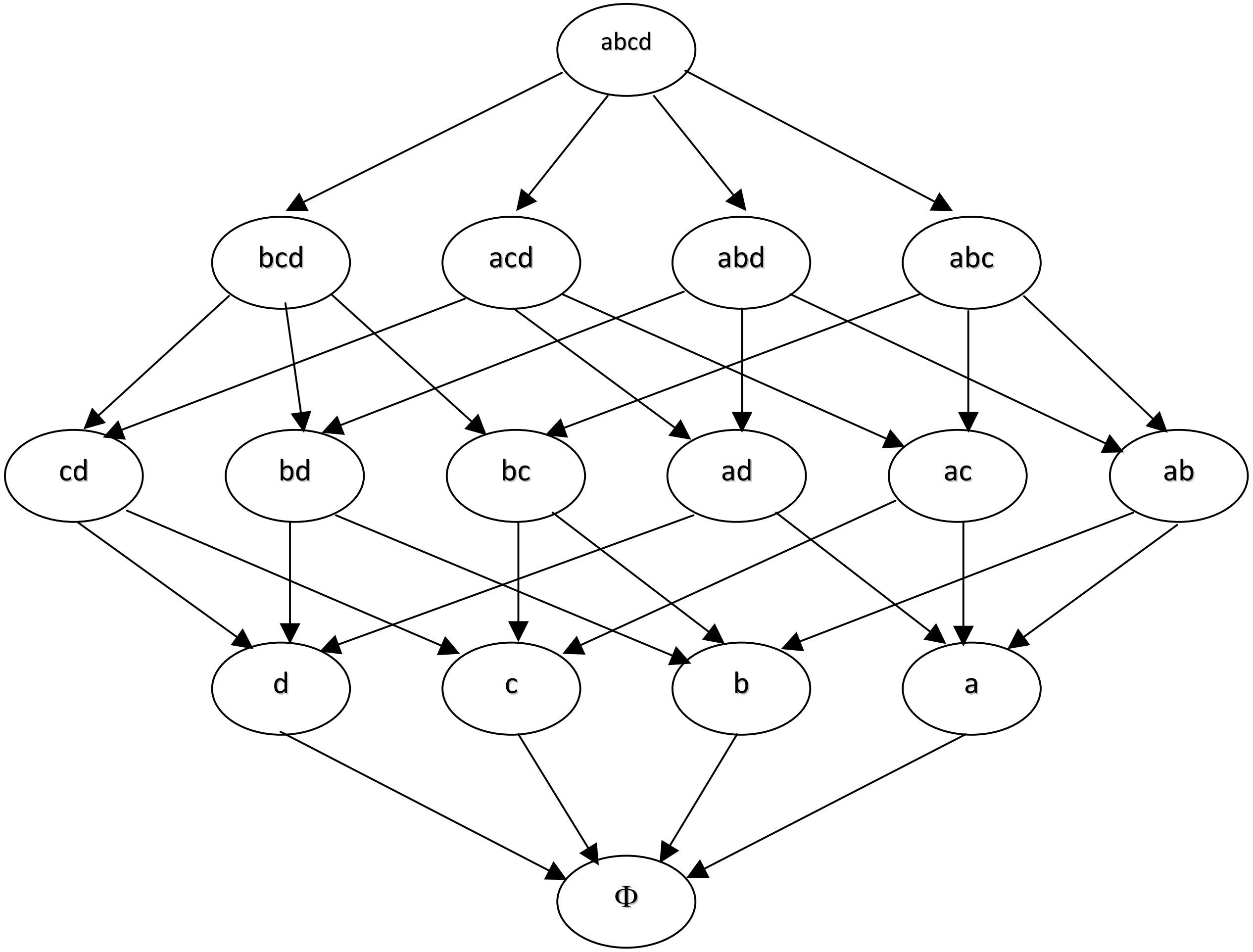
then, the control law $u_s(t) =- R^{-1} B^T{}_0 H_s x(t)$ stabilizes all configurations $\sigma \in$ Pred(s) and the associated cost satisfies

$$J(x_0, \sigma, u_s) \leq x^T{}_0 N x_0$$

Consequence : for each minimal recoverable configuration s, $u_s(t) = - R^{-1} B^T{}_0 H_s x(t)$ is bum-extensive

Design of a PACT (example)

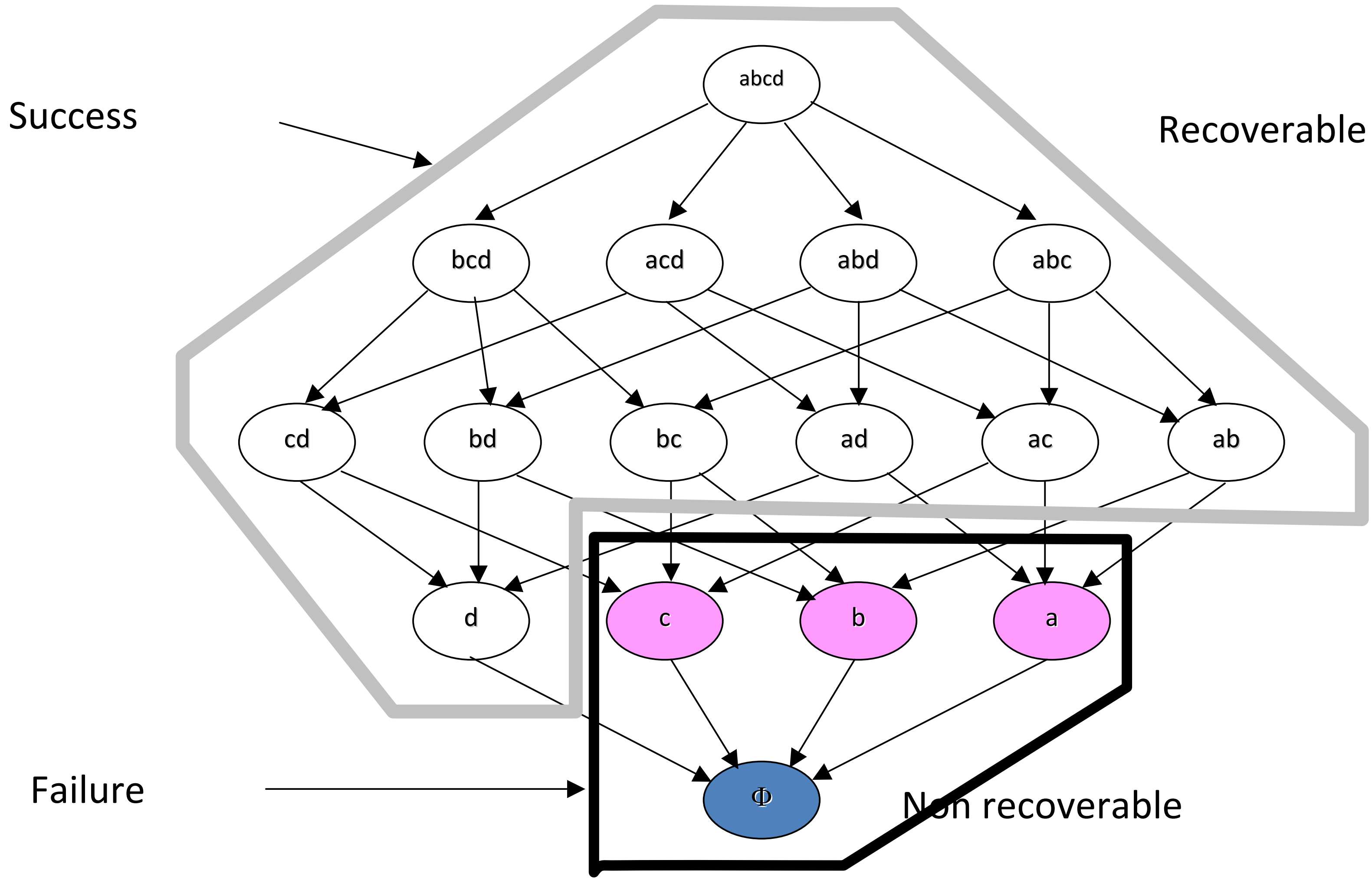
1 : the lattice of configurations



Design of a PACT (example)

1 : the lattice of configurations

2 : the recoverable configurations

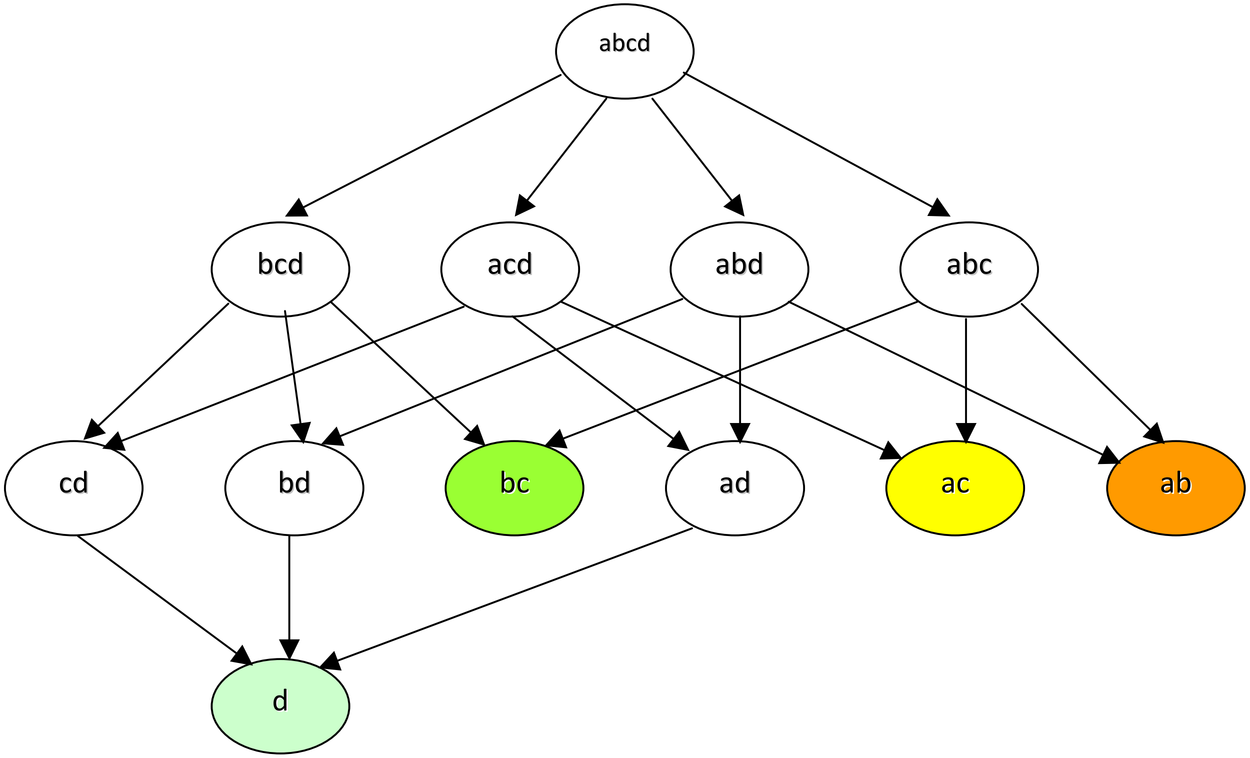


Design of a PACT (example)

1 : the lattice of configurations

2 : the recoverable configurations

3 : the minimal recoverable ones



Design of a PACT (example)

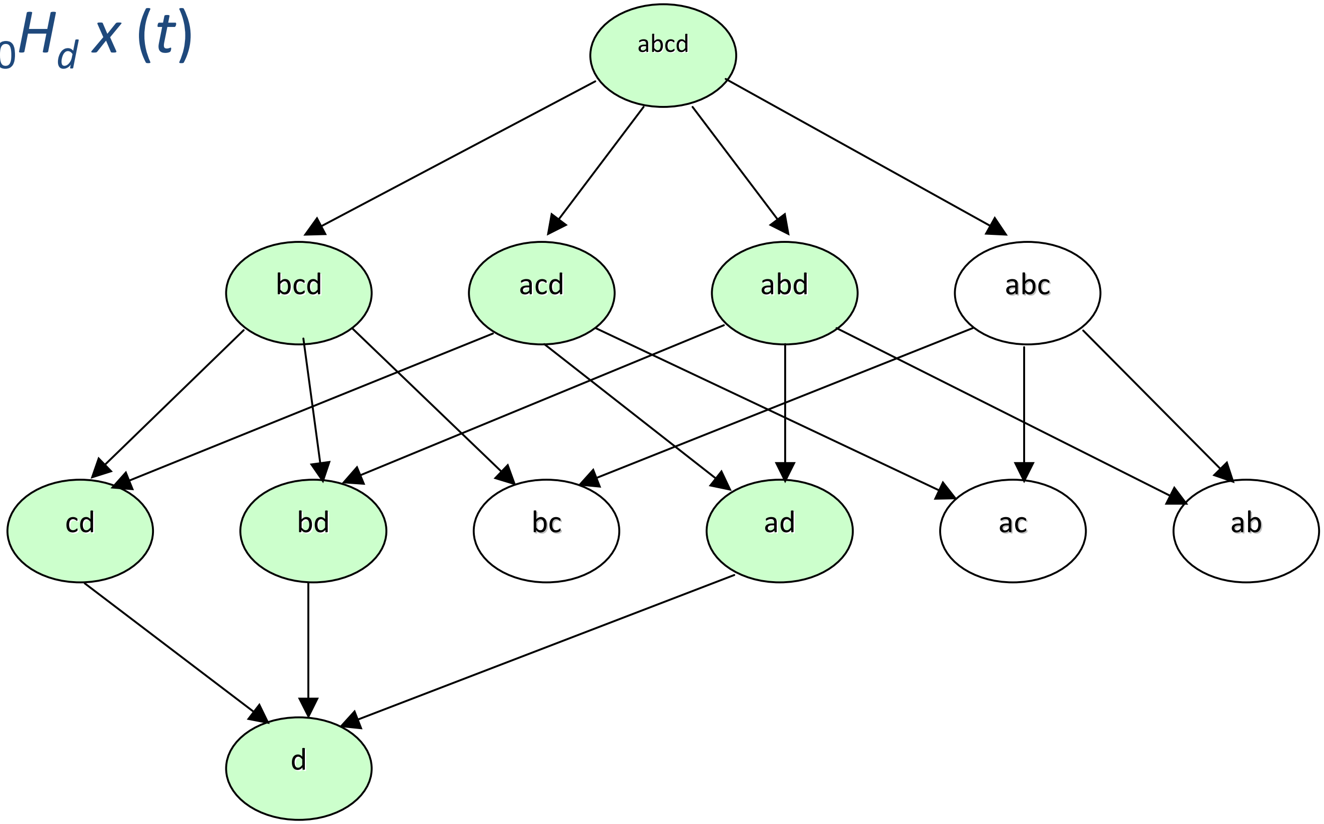
1 : the lattice of configurations

2 : the recoverable ones

3 : the minimal recoverable ones

4 : the bum-extensive control over d

$$u_d(t) = -R^{-1} B^T{}_0 H_d\, x(t)$$



Design of a PACT (example)

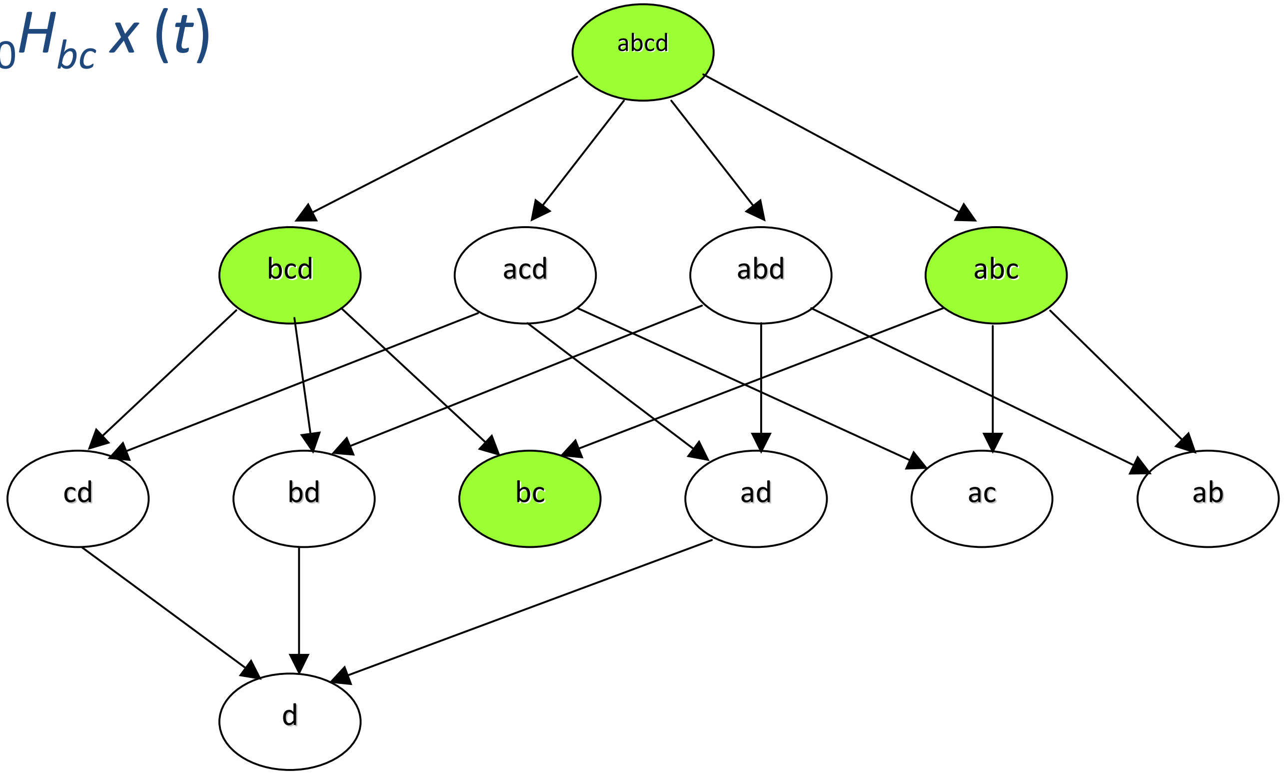
1 : the lattice of configurations

2 : the recoverable ones

3 : the minimal recoverable ones

4 : the bum-extensive control over bc

$$u_{bc}(t) = - R^{-1} B^{T}{}_{0} H_{bc}\, x(t)$$



Design of a PACT (example)

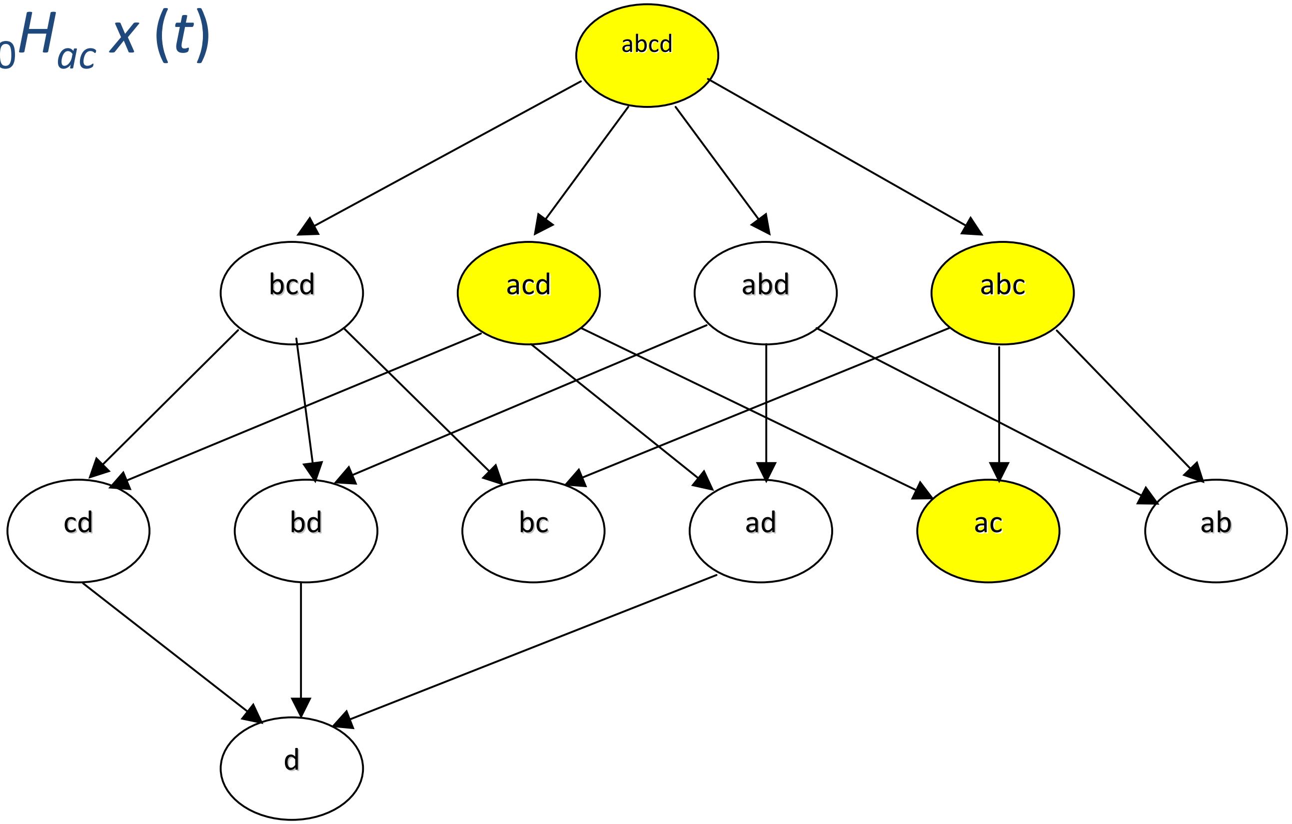
1 : the lattice of configurations

2 : the recoverable ones

3 : the minimal recoverable ones

4 : the bum-extensive control over ac

$$u_{ac}(t) = - R^{-1} B^T{}_0 H_{ac}\, x(t)$$



Design of a PACT (example)

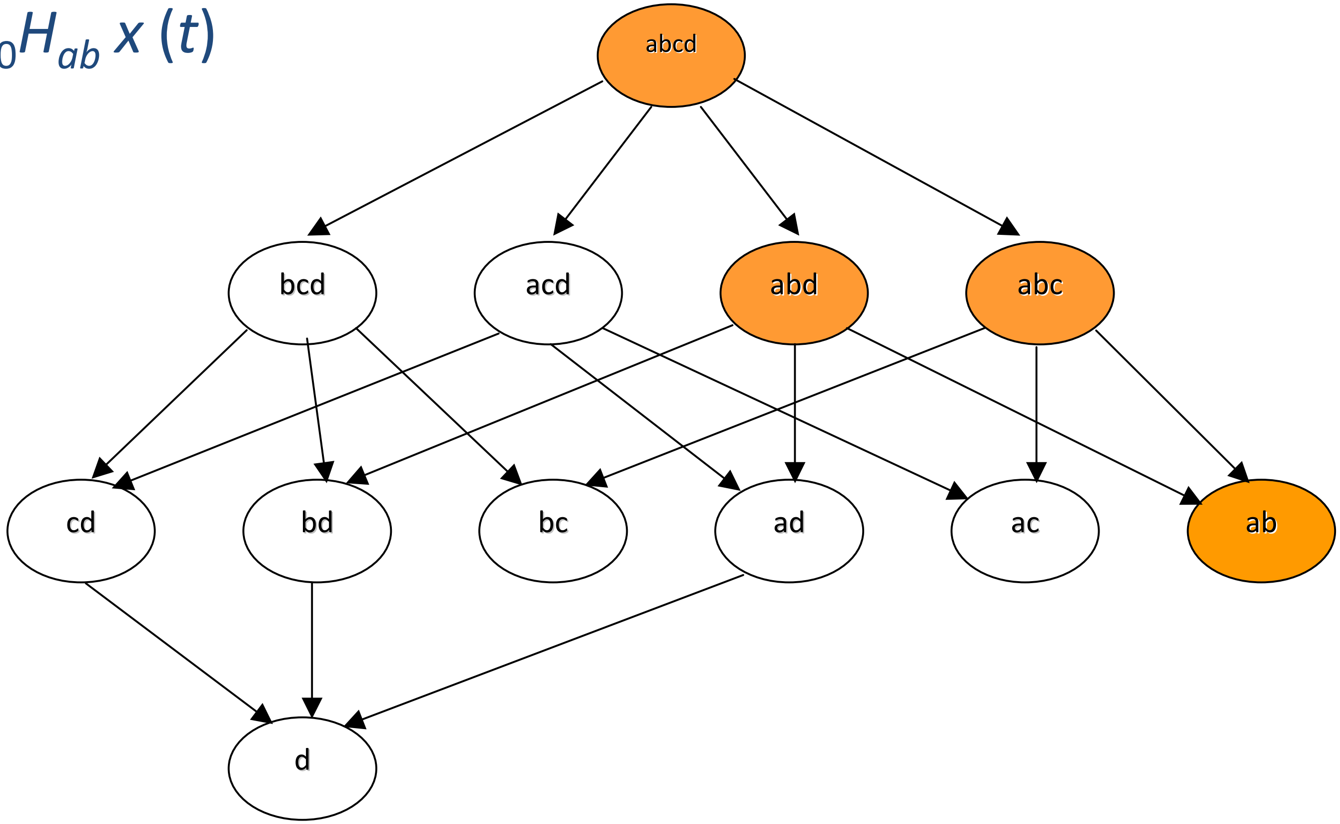
1 : the lattice of configurations

2 : the recoverable ones

3 : the minimal recoverable ones

4 : the bum-extensive control over ab

$$u_{ab}\,(t) = -\,R^{-1}\,B^{T}{}_{0}H_{ab}\,x\,(t)$$



Design of a PACT (example)

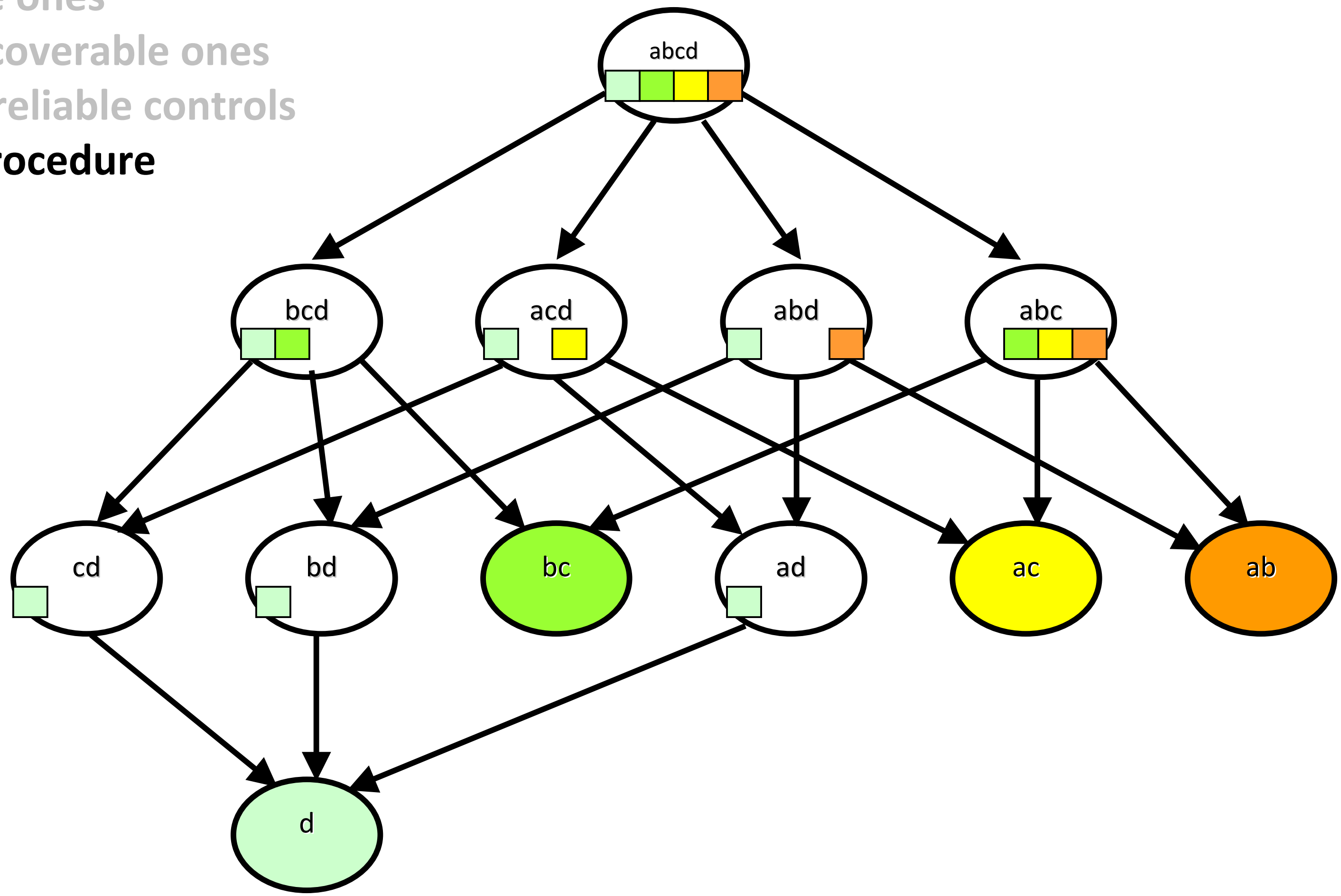
1 : the lattice of configurations

2 : the recoverable ones

3 : the minimal recoverable ones

4 : the associated reliable controls

5 : the selection procedure



- What is to be evaluated ?
- Components and laws
- Span of the property
  - Deterministic measures
  - Probabilistic measures
- FT sensitivity

What is to be evaluated ?

Architecture design (AD)

Given

- possible components $s_{possible}$
- s

Sol

- *s*
- *S*

Fault tolerance (FT)

Given

- nominal components s_0

In both cases, a solution is evaluated by two criteria, namely :

(1) the cost of the components s_0 - resp. the cost of the bank of laws *U*

(2) the fault tolerance of *P*, that results from the span *S*(*P*) - resp. of the span *S*(*P*,*U*).

Components and laws

Let *v* be a component (AD problem) or a law (FT problem)

• cost associated with v is g(*v*) (purchase cost, maintenance cost, complexity, memory requirement, etc.).

• cost associated with the whole set of components (laws) is G(*V*) assumed to be known.

Example

$$g(u) = 1 \text{ for any law } u \in U$$

$$G(V) = \sum_{u \in U} g(u) \text{ is the number of laws in the bank } U.$$

Span of *P*

Structural property : $2^{s0} = S(P) \cup S(\neg P)$

Non structural property : $2^{s0} = S(P,U) \cup S(\neg P,U)$

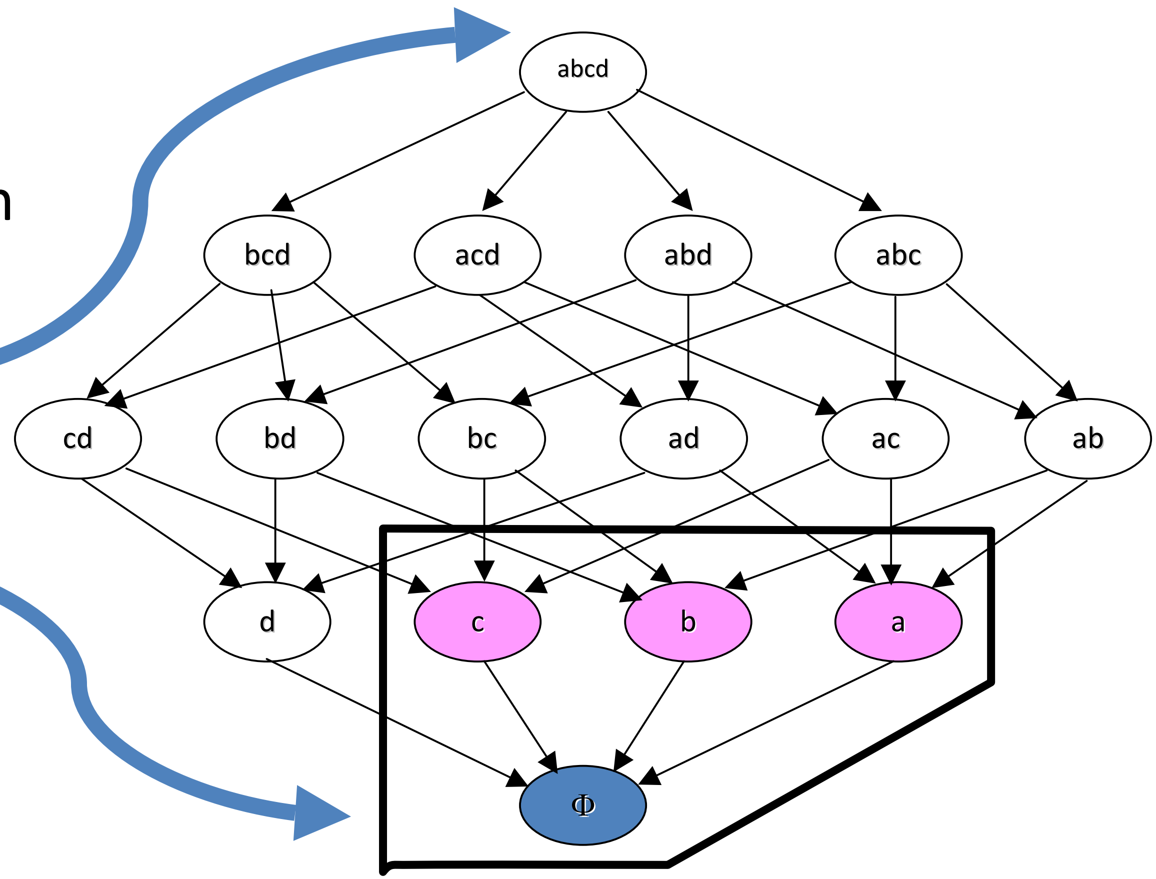
Fault tolerant configurations : measure of this set

Span of P : deterministic measures

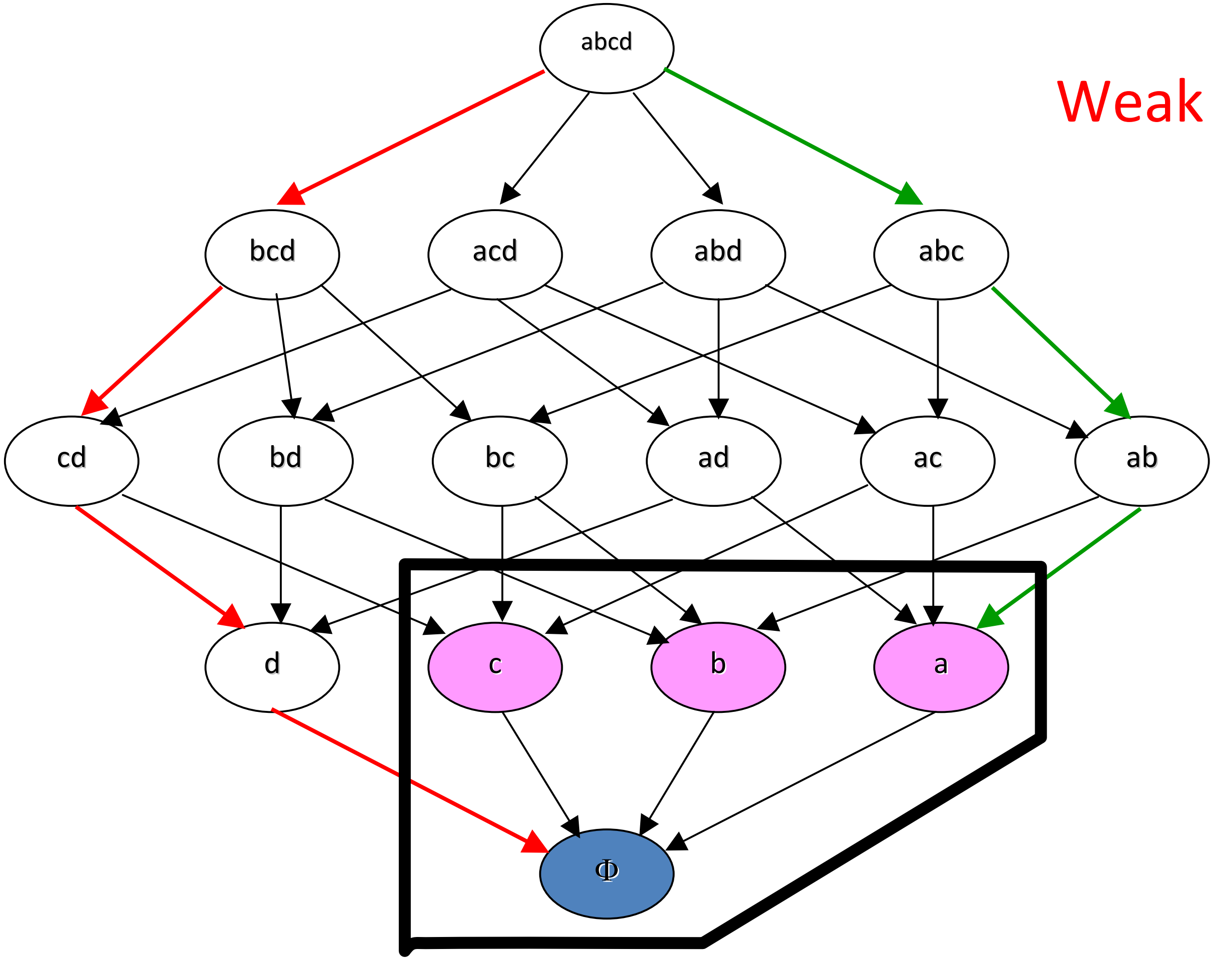
Deterministic measures do not need any model that governs the transitions from one configuration to another one.

Redundancy degrees
measure the shortest
(resp. the longest)
path from a configuration
in S(P)

to the set S(⌉P)
or S(⌉P,U)



Span of *P* : deterministic measures



Weak RDD = 4

Strong RDD = 3

As long as number of faults < strong RDD : system can work

Span of *P* : probabilistic measures

Probabilistic measures use a model that governs the transitions from one configuration to another one

Actuator reliabilities are assumed to be known : $r_i\left(t_1, t_2\right) = \Pr\left\{i(t_2) / i(t_1)\right\}$

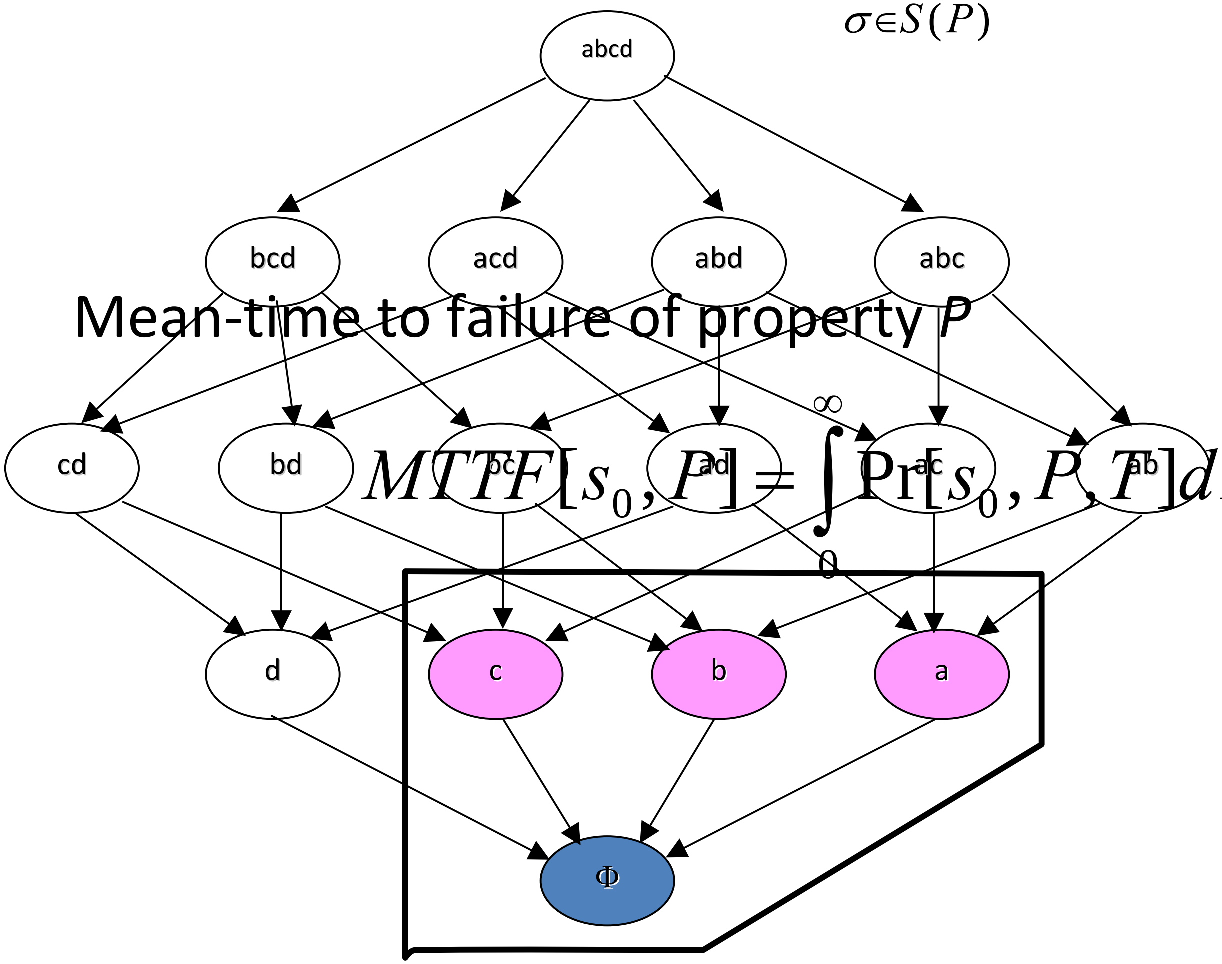
Probability for configuration *s* to be active at time t / nominal active at *0* :

$$P\{s,t\} = \prod_{\sigma \in s} r_\sigma(t,0) \prod_{\sigma \notin s} \left[1 - r_\sigma(t,0)\right]$$

Span of P : probabilistic measures

Success probability for property P on $[0,T]$ (reliability of P)

$$\Pr[s_0, P, T] = \sum_{\sigma \in S(P)} \Pr(\sigma, T)$$



Mean-time to failure of property P

$$MTTF[s_0, P] = \int_0^{\infty} \Pr[s_0, P, T]\, dT$$

Span of *P* : sensitivity w.r.t. the specification

Consider (s_0, P_1, P_2) where P_1 and P_2 are two properties then

$$P_1 \Rightarrow P_2 \Rightarrow S(P_1) \subseteq S(P_2)$$

(P_2 is weaker than or is a degraded specification w.r.t. P_1)

$$\text{Sensitivity} = \frac{\text{measure of } S(P_2) \text{ - measure of } S(P_1)}{\text{measure of the delta specification}}$$

Example : P_1 the system is observable and the cost of sensors is less than 1000, P_2 the system is observable and the cost of sensors is less than 1200.

$$\text{Sensitivity} = \frac{\text{Delta Mean Time To Non Observability}}{200}$$

Span of *P* : sensitivity w.r.t. the components

Consider (s_1, s_2, P) where s_1 and s_2 are two sets of components then

$$s_1 \subseteq s_2 \Rightarrow S_1(P) \subseteq S_2(P)$$

$$\text{Sensitivity} = \frac{\text{measure of } S_2(P) \text{ - measure of } S_1(P)}{\text{delta components set}}$$

Example : $s_2 = s_0$ and $s_1 = s_0 \backslash s_c$

$$s^{\text{useless}} = \{s_c \subseteq s_0 : \text{Measure } S_2(P) = \text{Measure } S_{s1}(P)\}$$

$$s^{\text{cut-set}} = \{s_c \subseteq s_0 : S_1(P) = \varnothing\}$$

- System and specifications
- Recoverable configurations
- Design of the bank of control laws
- The PACT
- Domination relation
- FT performances
- Simplicity/performance trade-off

Example : system and specifications

LTI system

$$A=\begin{pmatrix} 0 & 1 & 1 & 2 & 0 & 0 \\ -1 & 1 & 1 & 0 & 0 & 0 \\ 2 & 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix} \qquad B=\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

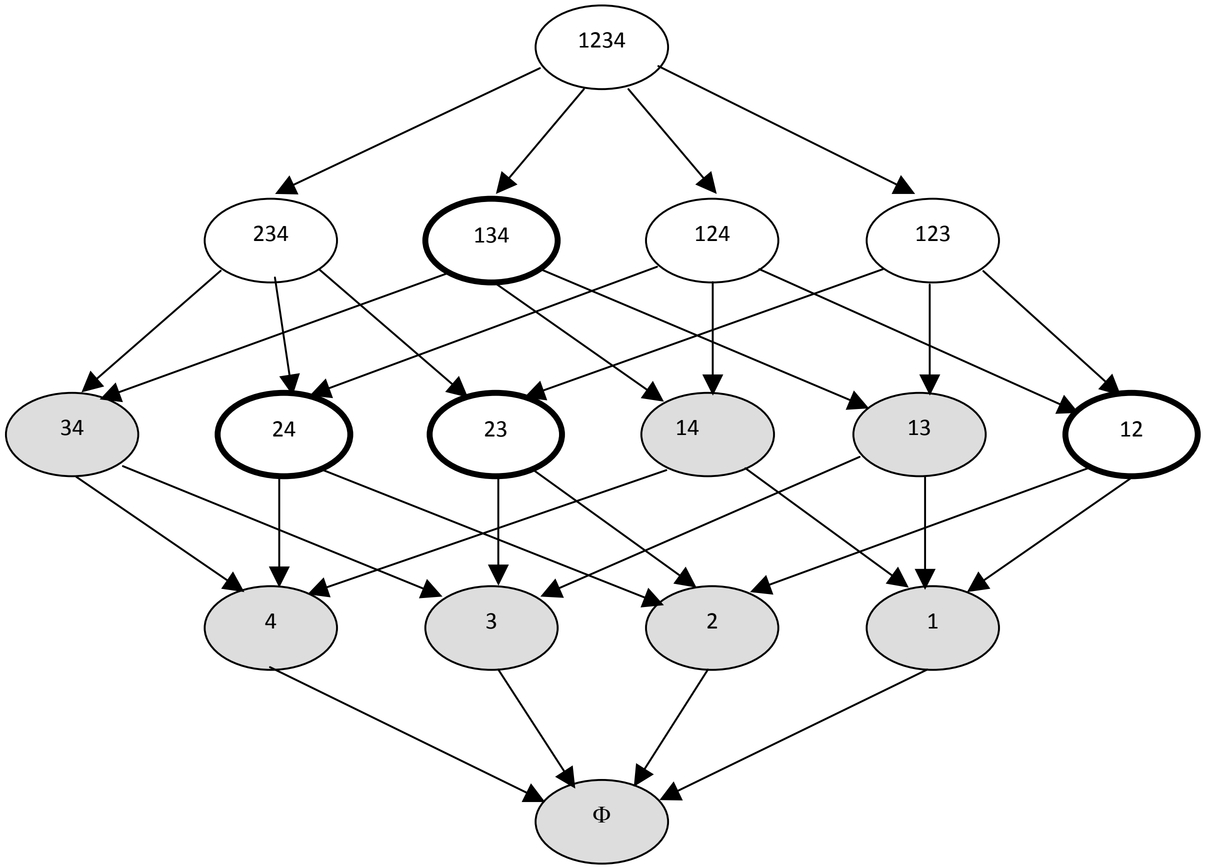
$$\lambda_{\max}(W_{1234}^{*}) = 7.3554$$

Specification $\int_0^\infty (x^T Q x + u^T R u)dt \le \tau[x_0^T W_{1234}^{*} x_0]$

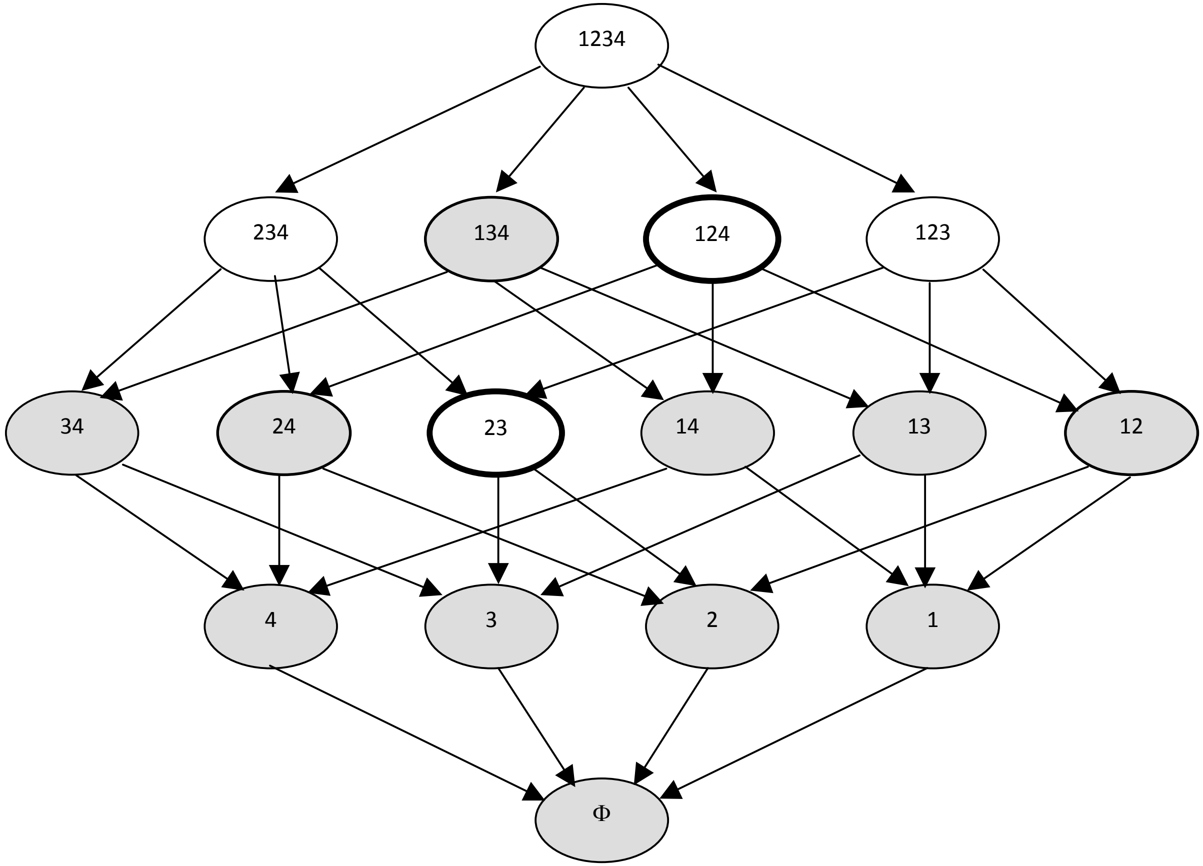
Admissible degradation factor

Optimal cost of the nominal system

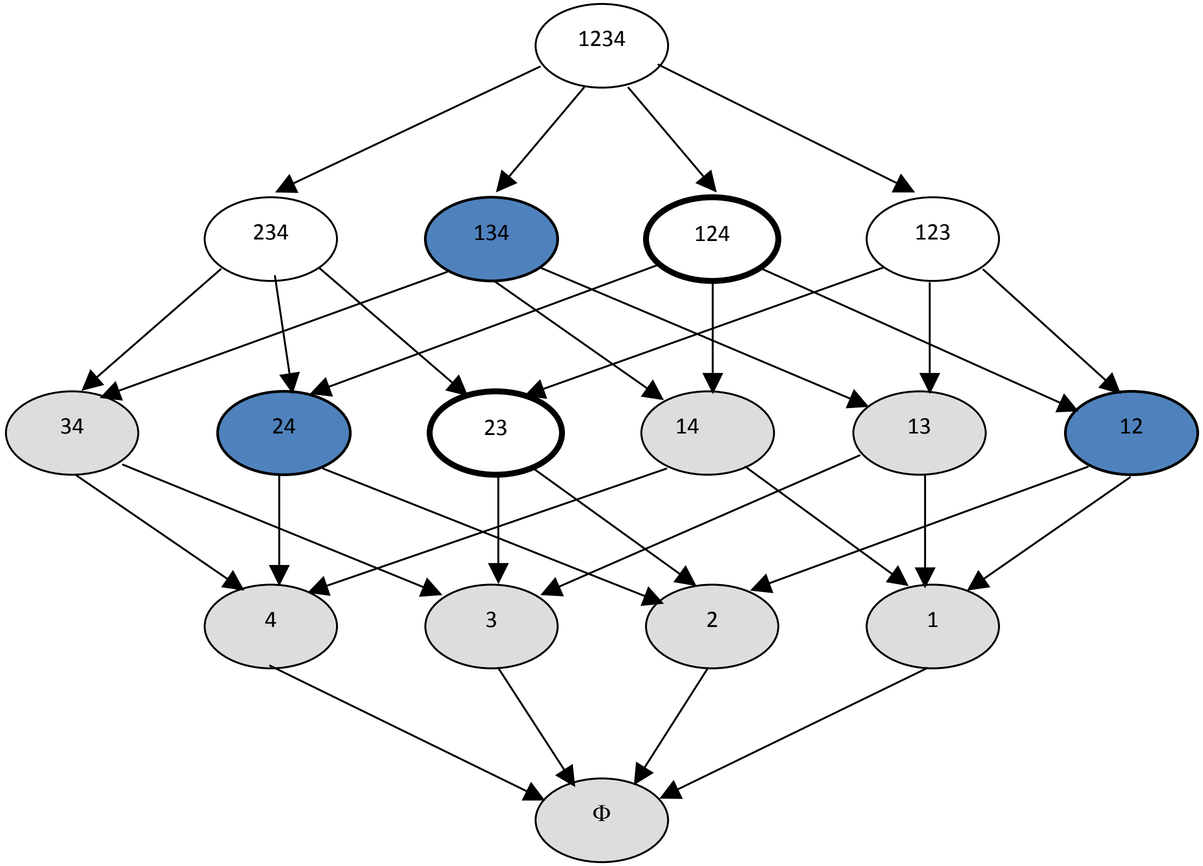
Example : recoverable configurations τ = 15



Example : recoverable configurations $\tau = 5$



Example : recoverable configurations $\tau = 5$



Example : design of the bank of control laws

Theorem 1 (Veillette 1995). Let W_s^* be the unique symmetric positive definite stabilizing solution of the Riccati equation associated with a configuration *s*. Then, the control law

$$u_s(t) = -R^{-1} B^T_0 W_s^* x(t)$$

stabilizes all configurations $\sigma \in \text{Pred}(s)$ and the associated cost satisfies

$$J(x_0, \sigma, u_s) \leq x^T_0 W^*_s x_0$$

$\tau = 15$

Application

$U_4 = \{u_s(t) = -R^{-1} B^T_{1234} W^*_s x(t) \; ; \; s \in \{12,134,23,24\}$

$\lambda_{max}(W^*_{12}) = 17.4285$ $\lambda_{max}(W^*_{134}) = 32.9450$

$\lambda_{max}(W^*_{23}) = 16.5649$ $\lambda_{max}(W^*_{24}) = 18.6938$

Example : the PACT

$$S(\mathscr{P}_{15}, u_{12}) = \{1234, 123, 124, 12, \underline{234}, \underline{23}\}$$

$$S(\mathscr{P}_{15}, u_{134}) = \{1234, \underline{123}, 134, \underline{234}\}$$

$$S(\mathscr{P}_{15}, u_{23}) = \{1234, 123, 234, 23\}$$

$$S(\mathscr{P}_{15}, u_{24}) = \{1234, 124, 234, 24\}$$

TABLE I

THE RC-BASED PACT $\mathscr{U}_4$

1234	123	124	12	134	234	23	24
u_{12} u_{134} $\underline{u_{23}}$ u_{24}	u_{12} u_{134} $\underline{u_{23}}$	$\underline{u_{12}}$ u_{24}	$\underline{u_{12}}$	$\underline{u_{134}}$	u_{12} u_{134} $\underline{u_{23}}$ u_{24}	u_{12} $\underline{u_{23}}$	$\underline{u_{24}}$

Example : domination relation

TABLE II

DOMINATION RELATION

$\mathscr{D}$ ↗	u_{12}	u_{134}	u_{23}	u_{24}
u_{12}	1	0	1	0
u_{134}	0	1	0	0
u_{23}	0	0	1	0
u_{24}	0	0	0	1

A control law dominates another one if it recovers all its configurations (and possibly more)

TABLE III

THE RC-BASED PACT $\mathscr{U}_3$

1234	123	124	12	134	234	23	24
$\underline{u_{12}}$ u_{134} u_{24}	$\underline{u_{12}}$ u_{134}	$\underline{u_{12}}$ u_{24}	$\underline{u_{12}}$	$\underline{u_{134}}$	$\underline{u_{12}}$ u_{134} u_{24}	$\underline{u_{12}}$	$\underline{u_{24}}$

Example : FT performances

The system is expected to operate on the time interval $[0,10^5\ h]$

The actuator reliabilities are

$r_1(t,0) = r_2(t,0) = \exp\text{-}4.10^{-6t}$

$r_3(t,0) = r_4(t,0) = \exp\text{-}4.10^{-7t}$

At time t_0 initial configuration is 1234

Using U_4 or U_3 one has

Weak RDD = 3

Strong RDD = 2 → Fail operational wrt the first fault

Success probability = 0.8740

Example : the simplicity/performance trade-off

Remark : in U_3 the law u_{24} is used only for one configuration

Deleting u_{24} may be of interest : the performances of
$U_2 = \{u_{12} , u_{134}\}$ become

Weak RDD = 3
Strong RDD = 2 → Fail operational wrt the first fault

Success probability = 0.8657 (0.8740)

Example : reliability overcost

Remark : u_{12} is used when configuration 1234 occurs

u_{1234} would be optimal (but u_{1234} is not tdm extensive !)

Reliability overcost : $J(x_0, 1234, u_{12}) - J(x_0, 1234, u_{1234})$

Idea : instead of using Theorem 1 (Veillette)

$$u_{12}(t) = -R^{-1} B^T_{1234} W^*_{12} x(t)$$

.... use its extension

$$\underline{u}_{12}(t) = -R^{-1} B^T_{1234} H_{12} x(t)$$

Example : reliability overcost

H_{12} such that :

(1) $\underline{u}_{12}(t)$ is bum extensive and

(2) it minimizes the reliability overcost

Newton-Kleinman algorithm

	Algorithm 1	Algorithm 4	Improvement
$\lambda_{max}[W_{03}(2)]$	12.2667	10.1592	17,18%
$\lambda_{max}[W_{04}(2)]$	19.3397	15.8924	17.83%
$\lambda_{max}[W_{09}(3)]$	12.7427	7.8729	38.22%
$\lambda_{max}[W_{0,10}(2)]$	10.8692	9.1817	15.53%

- The lattice frame
- Design
- Evaluation
- Fault avoidance

Conclusion : the lattice frame

Lattice of system configurations : general mathematical frame that underlies the AD and the reconfiguration based FT problems.

It can be used to analyze any set of system components, or specific subsets like sensors or actuators.

Plays a key role for the :
- design of PFT / AFT / RC laws, and
- evaluation (fault recoverability, FT effectiveness, components usefulness).

Conclusion : design

• parallel combination of PFT and AFT = PACT
• implements several controllers (AFT)
• each is dedicated to a subset of recoverable faults (PFT).

Research still to be done :
• efficient algorithms to design the PACT bank (including robustness and optimisation issues),
• development of decision procedures to select an optimal law among those that allow to recover from a given fault.

Conclusion : evaluation

Evaluation conditions the acceptability of the solution in practical applications.

- Success probabilities (or mean time to failure)
- Redundancy degrees
- Classification of components into critical or noncritical subsets,
- Evaluation of components usefulness

The event that a critical subset of components fails is a feared event, whose probability must be minimized (ideally, whose impossibility must be proven).

Conclusion : fault avoidance

- Only autonomous systems have been considered ---> fault tolerance

- For systems that can be repaired in operation, fault avoidance
is a direct complement to fault tolerance ----> maintenance policies.

Thank you for your attention