Model-based evaluation of dependability

State-based models

Availability

Availability - A(t)

the probability that the system is operating correctly and is available to perform its functions at the *instant* of time t

More general concept than reliability:

failure and repair of the system

Repair rate - which is the average number of repairs that occur per time period, generally number of repairs per hours. Analogous to failure rate, constant repair rate

$$\mu(t) = \mu$$

MTTR - The Mean Time To Repair is the average time required to repair the system. Analogous to MTTF, MTTR is expressed in terms of the repair rate:

$$MTTR = \frac{1}{\mu}$$

Failure events and repair events are not independent.

Model-based evaluation of dependability

State-based models: Markov models

Characterize the state of the system at time t:

- identification of system states
- identification of transitions that govern the changes of state within a system

Each state represents a distinct combination of failed and working modules

The system goes from state to state as modules fail and repair.

The state transitions are characterized by the probability of failure and the probability of repair

Model-based evaluation of dependability

Markov models (a special type of random process) :

Basic assumption: the system behavior at any time instant depends only on the current state (independent of past values)

Main points:

- systems with arbitrary structures and complex dependencies can be modeled

- assumption of independent failures no longer necessary

- can be used for both reliability and availability modeling

Random variable

Random variable

a random variable X *is a function from a sample space S to reals numbers*

Let X be a random variable representing the result of tossing a die

Sample space: 1, 2, 3, 4, 5, 6 X (1) = 1/6 X (2) = 1/6 ……

The probability assigned to each output of the experiment is 1/6

P[X=1]=1/6 P[X=2]=1/6 …………..

Random process

Random process

a collection of random variables $\{X_t\}$ *indexed by time*

The sequence of results of tossing a die can be expressed by a random process

$$\{X_t\} \text{ with } t = 0, 1, 2, 3. \ldots$$

$P[X_0 = 4] = 1/6$
$P[X_1 = 4] = 1/6$
$P[X_4 = 4 \mid X_3 = 2] = P[X_4 = 4] = 1/6$

In this case, the random variables are independent

$$P[X_i = j] = 1/6 \quad \text{for all } i \text{ and for all } j$$

Random processes

State space S of a random process $\{X_t\}$: the set of all possible values the process can take

$$S = \{y: X_t = y, \text{ for some } t\}$$

For example,

X_t number of faulty components at time t

Discrete-time random process

all state transitions occur at fixed intervals (probabilities assigned to each transition)

Continuous-time random process

state transitions occur at random intervals transition (rates assigned to each transition)

Random process

In a general random process $\{X_t\}$ the value of the random variable X_{t+1} may depend on the values of the previous random variables $X_{t0}\ X_{t1}\ \ldots\ldots\ldots\ldots X_t$.

Markov process

the state of a process at time t+1 depends only on the state at time t, and is independent *on any state before t.*

$$\mathcal{P}\{X_{t+1} = j | X_0 = k_0, \ldots, X_{t-1} = k_{t-1}, X_t = i\} = \mathcal{P}\{X_{t+1} = j | X_t = i\}$$

Markov property: "the current state is enough to determine in a stochastic sense the future state"

Markov process
steady-state transition probabilities

Let $\{X_t, t>=0\}$ be a Markov process. The Markov process X has *steady-state transition probabilities* if for any pair of states i, j:

$$\mathcal{P}\{X_{t+1} = j | X_t = i\} = \mathcal{P}\{X_1 = j | X_0 = i\} \ \forall t \geq 0$$

The probability of transition from state i to state j does not depend by the time. This probability is called p_{ij}

$$p_{ij} = \mathcal{P}\{X_1 = j | X_0 = i\}$$

Transition probability matrix

If a Markov process is finite-state, we can define the transition probability matrix P (nxn)

$$P = \begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \\ p_{n1} & \cdots & p_{nn} \end{bmatrix},$$

$$p_{ij} = \mathcal{P}\{X_1 = j | X_0 = i\}$$

pij = probability of moving from state i to state j in one step

row i of matrix P:

probability of make a transition starting from state i

column j of matrix P:

probability of making a transition from any state to state j

Transition probability after n-time steps

THEOREM: Generalization of the steady-state transition probabilities.
For any i, j in S, and for any n>0

$$\mathcal{P}\{X_{t+n} = j | X_t = i\} = \mathcal{P}\{X_n = j | X_0 = i\} \ \forall t \geq 0$$

Definition: steady-state transition probability after n-time steps

$$p_{ij}^{(n)} = \mathcal{P}\{X_n = j | X_0 = i\}, n \in \{0, 1, 2, ...\}$$

Definition: transition matrix after n-time steps

$$P^{(n)} = (p_{ij}^{(n)})$$

Transition probability after n-time steps

Definition:

$$p_{ij}^{(0)} = \mathcal{P}\{X_0 = j | X_0 = i\} = \begin{cases} 1 \text{ se } i = j \\ 0 \text{ se } i \neq j \end{cases}$$

$$p_{ij}^{(1)} = \mathcal{P}\{X_1 = j | X_0 = i\} = p_{ij}$$

$$p_{ij}^{(n)} = \mathcal{P}\{X_n = j | X_0 = i\}, \, n \in \{0, 1, 2, \ldots\}$$

Properties:

$$0 \leq p_{ij}^{(n)} \leq 1 \; \forall i, j \in \mathcal{S} \; \forall n \geq 0$$

$$P^{(0)} = I \qquad P^{(1)} = P.$$

$$\Sigma_{i=0,..,n} \, p_{ij} = 1$$

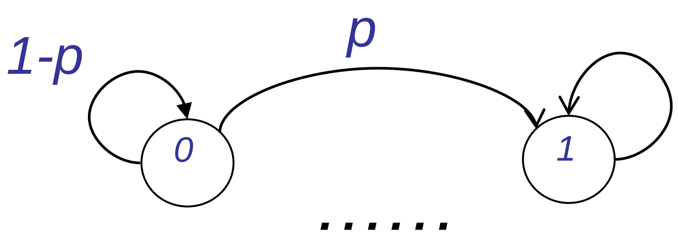
It can be proved that:

$P^{(n)} = P^n$ where $P^n = P \cdot P \cdot \ldots \cdot P$

the n-th power of P

Discrete-time Markov model

Markov model:
  graph where nodes are all the possible states and arcs are the possible transitions between states (labeled with a probability function)



Reliability/Availability modelling

Each state represents a distinct combination of working and failed components
  example: state 0: 0 faulty components   state 1: 1 faulty component

As time passes, the system goes from state to state as modules fails and are repaired

Discrete-time Markov model of a single system with repair

$\{X_t\}$ t=0, 1, 2, …. S={s0, s1}

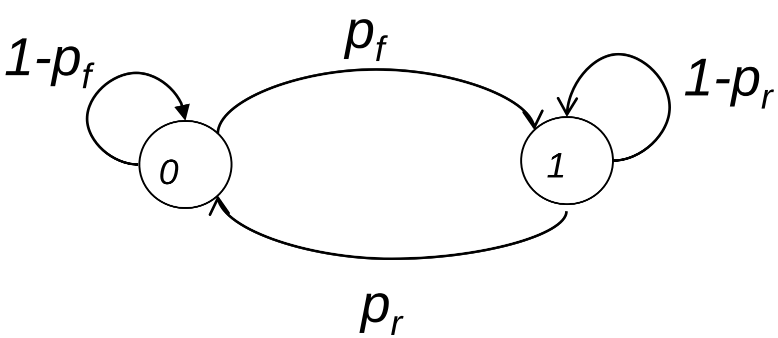
State s0 : working
State s1: failed

- all state transitions occur at fixed intervals
- probabilities assigned to each transition

p_f *Failure probability*

p_r *Repair probability*

The probability of state transition depends only on the current state



Graph model

new state

$$P = \begin{array}{c c} & \begin{array}{cc} \quad 0 \quad & \quad 1 \quad \end{array} \\ \begin{array}{c} 0 \\ 1 \end{array} & \begin{bmatrix} 1-p_f & p_f \\ p_r & 1-p_r \end{bmatrix} \end{array}$$

current state

Transition Probability Matrix

- *Pij = probability of a transition from state i to state j*
- *Pij >=0*
- *the sum of each row must be one*

Discrete-time Markov model

$[p_0(0), p_1(0)] = [1, 0]$ initial state: working

$$[1, 0] \begin{bmatrix} 0.9 & 0.1 \\ 0.5 & 0.5 \end{bmatrix} = [0.9, 0.1]$$

[p0(1), p1(1)]

State occupancy vector (state space distribution)

Initial state occupancy vector

[p0(0), p1(0)]

State occupancy vector after k time steps:

[p0(k), p1(k)]

State j can be made an trapping state with pjj = 1

Transient analysis

probability of being in a state after n time-steps

$$[p_0(n), p_1(n)] = [p_0(n-1), p1(n-1)] \begin{bmatrix} 1-p_f & p_f \\ p_r & 1-p_r \end{bmatrix}$$

$$[p_0(n), p_1(n)] = [p_0(0), p_1(0)] \begin{bmatrix} 1-p_f & p_f \\ p_r & 1-p_r \end{bmatrix}^n$$

Limiting behaviour

A Markov process can be specified in terms of the state occupancy probability vector $[p_0(n), p_1(n)]$ and a transition probability matrix P

Transitions at fixed time intervals:

$$[p_0(t), p_1(t)] = [p_0(0), p_1(0)] \; P^t$$

The limiting behaviour of a Markov process (steady-state behaviour):

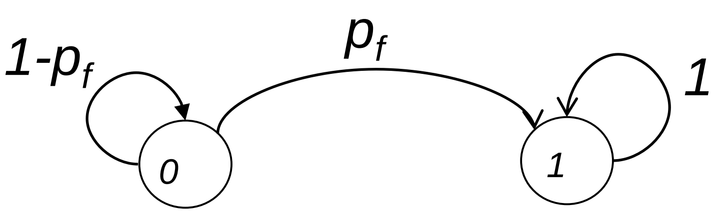
$$\lim_{t \to \infty} [p_0(t), p_1(t)]$$

The limiting behaviour depends on the characteristics of its states.

Sometimes the solution is simple.

Discrete-time Markov models: Reliability

failed state as trapping state



Graph model

new state

$$P = \begin{array}{c} \\ 0 \\ 1 \end{array} \begin{array}{c} \begin{array}{cc} 0 & \quad 1 \end{array} \\ \begin{bmatrix} 1-p_f & p_f \\ 0 & 1 \end{bmatrix} \end{array}$$

current state

Transition Probability Matrix

Continuous-time Markov models

Continuous-time models:

state transitions occur at random intervals

transition rates assigned to each transition

Markov property assumption:

the length of time already spent in a state does not influence either the probability distribution of the next state or the probability distribution of remaining time in the same state before the next transition

These very strong assumptions imply that the waiting time spent in any one state is exponentially distributed

Thus the Markov model naturally fits with the standard assumptions that failure rates are constant, leading to exponential distribution of inter-arrivals of failures

Continuous-time Markov models

Single system with repair

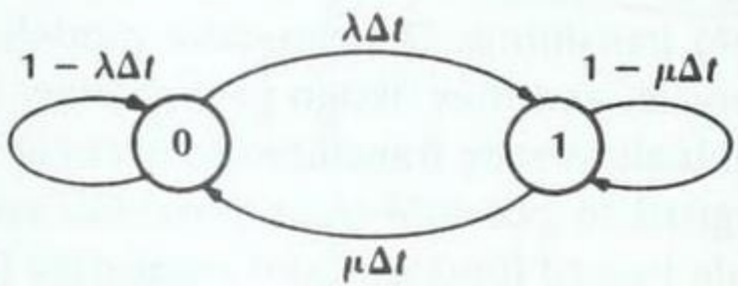
λ failure rate, μ repair rate

State occupancy vector

$p_0(t)$ probability of being in state 0 at time t (operational state)

$p_1(t)$ probability of being instate 1 at time t (failed state)

Graph model



$\lambda\Delta t$, $\mu\Delta t$—State transition probabilities

λ, μ—State transition rates

Transition Matrix P

$$P = \begin{bmatrix} 1 - \lambda\Delta t & \lambda\Delta t \\ \mu\Delta t & 1 - \mu\Delta t \end{bmatrix}$$

Continuous-time Markov models

Probability of being in state 0 or 1 at time t+Δt:

$$[p_0(t+\Delta t),\ p_1(t+\Delta t)] = [p_0(t),\ p_1(t)]\begin{bmatrix} 1-\lambda\Delta t & \lambda\Delta t \\ \mu\Delta t & 1-\mu\Delta t \end{bmatrix}$$

↑

probability of being in state 0 at time t+Δt

Performing multiplication, rearranging and dividing by Δt, taking the limit as Δt approaches to 0:

$$\frac{dp_0(t)}{dt} = \dot{p}_0(t) = -\lambda p_0(t) + \mu p_1(t)$$

$$\frac{dp_1(t)}{dt} = \dot{p}_1(t) = \lambda p_0(t) - \mu p_1(t)$$

Chapman-Kolmogorov equations

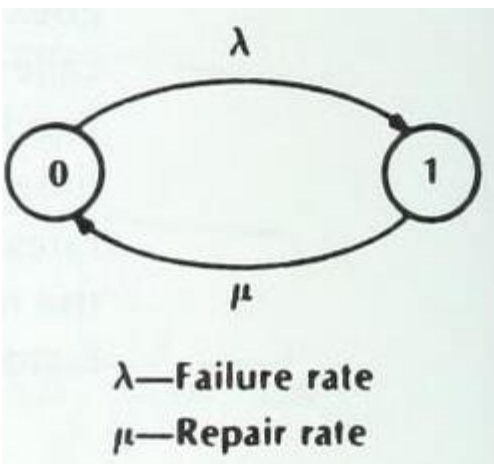
Continuous-time Markov models

Matrix form:

T matrix

$$[\dot{p}_0(t), \dot{p}_1(t)] = [p_0(t), p_1(t)] \begin{bmatrix} -\lambda & \lambda \\ \mu & -\mu \end{bmatrix}$$

The set of equations can be written by inspection of a transition diagram without self-loops and Δt's:



Continuous time Markov model graph

For each state: the sum of the flows out of the state plus the flow into the state must be 0

Continuous-time Markov models

$$p_0(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} e^{-(\lambda+\mu)t}$$

$$p_1(t) = \frac{\lambda}{\lambda + \mu} - \frac{\lambda}{\lambda + \mu} e^{-(\lambda+\mu)t}$$

A(t)

$p_0(t)$ probability that the system is in the operational state at time t, availability at time t

The availability consists of a steady-state term and an exponential decaying transient term

Steady-state solution

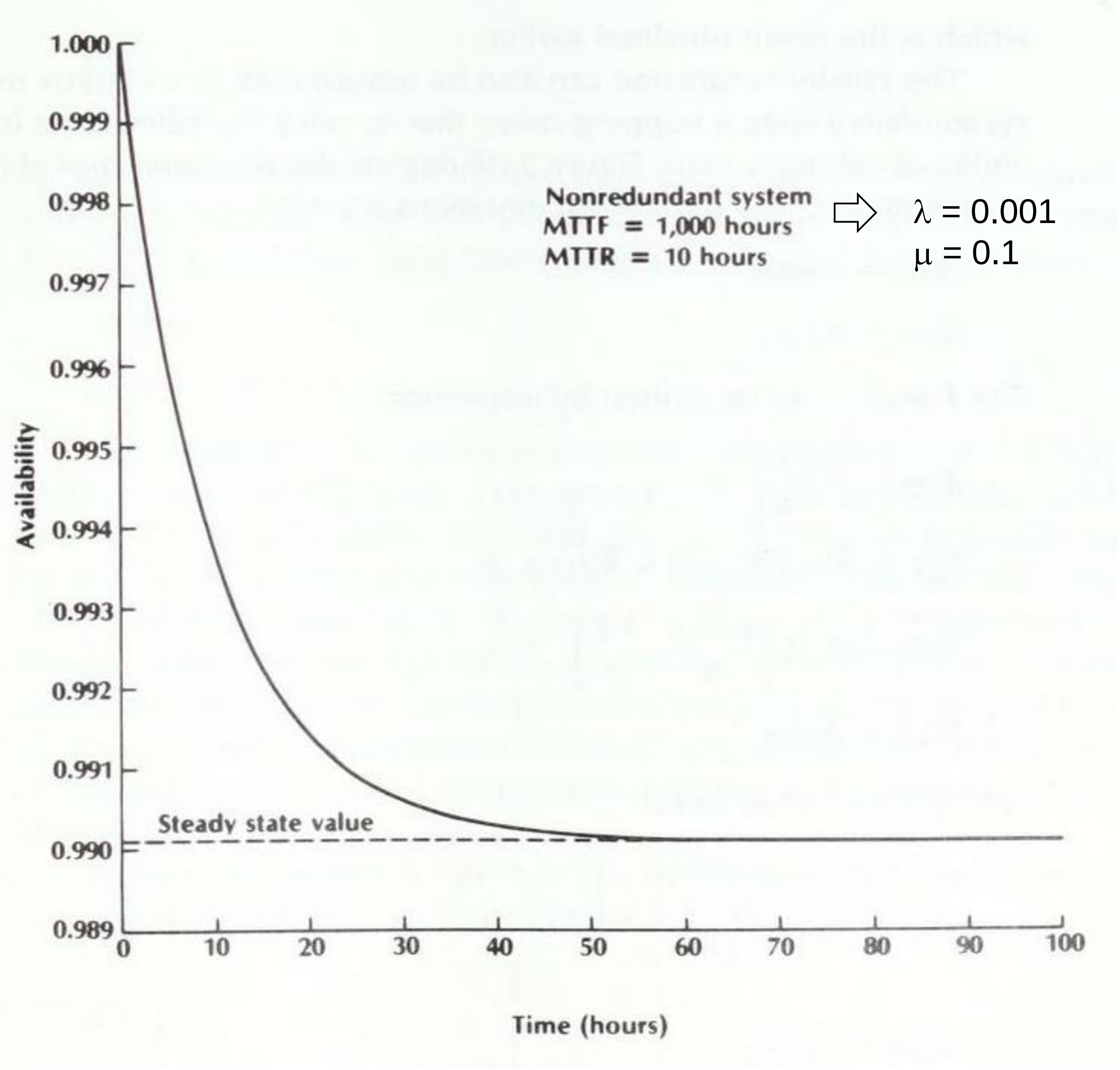
Chapman-Kolmogorov equations: derivative replaced by 0; p0(t) replaced by p0(0) and p1(t) replaced by p1(0)

$$0 = -\lambda p_0 + \mu p_1$$

$$0 = \lambda p_0 - \mu p_1$$

$$\Rightarrow \quad p_0 = \frac{1}{1 + \frac{\lambda}{\mu}} = \frac{\mu}{\lambda + \mu}$$

Availability as a function of time

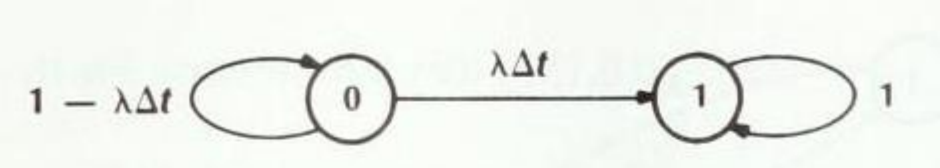


$\lambda = 0.001$
$\mu = 0.1$

The steady-state value is reached in a very short time

Continuous-time Markov models: Reliability
failed state as trapping state

Single system without repair



$\lambda \Delta t$ = *state transition probability*

Differential equations:

$$\dot{p}_0(t) = -\lambda p_0(t)$$
$$\dot{p}_1(t) = \lambda p_0(t)$$

T matrix

$$\begin{bmatrix} -\lambda & \lambda \\ 0 & 0 \end{bmatrix}$$

Continuous time Markov model graph

λ = *failure rate*

We can prove that:

$$p_0(t) = e^{-\lambda t}$$
$$p_1(t) = 1 - e^{-\lambda t}$$

Markov chain

A **Markov chain** is a Markov process X with *discrete state space S*.

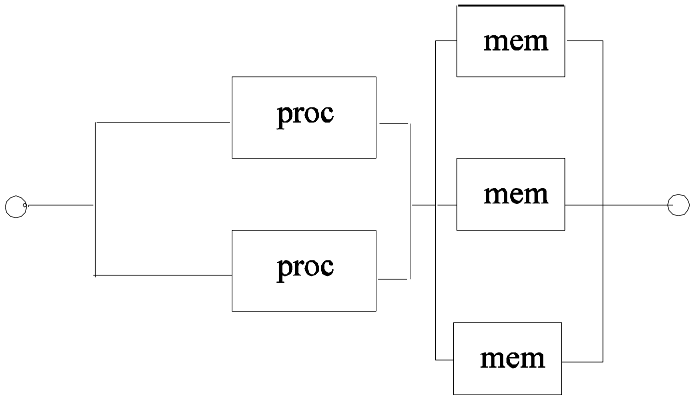
A Markov chain is h*omogeneous* if X has steady-state transition probabilities

We consider only *homogeneous* Markov chains

Discrete-time Markov chains (DTMC)
Continuous-time Markov chains (CTMC)

An example of modeling (CTMC)

Multiprocessor system with 2 processors and 3 shared memories system. System is operational if at least one processor and one memory are operational.



λ_m failure rate for memory

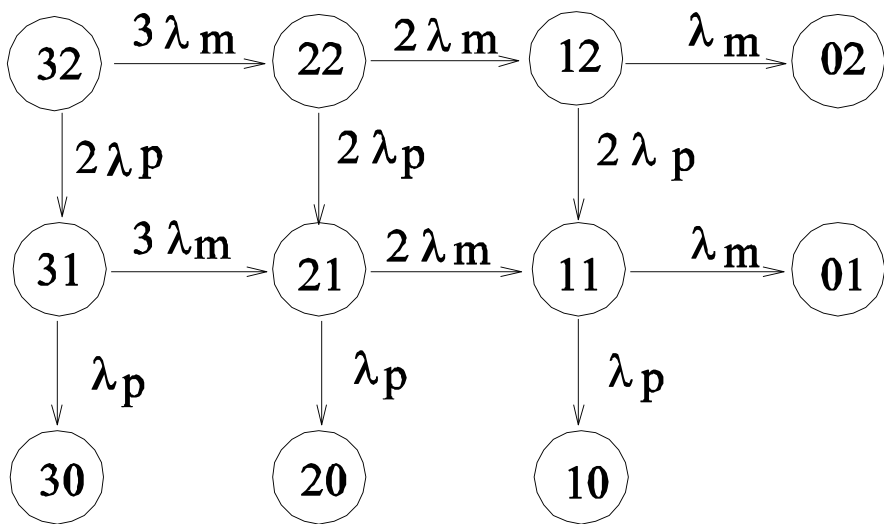
λ_p failure rate for processor

X random process that represents the number of operational memories and the number of operational processors at time t

Given a state (i, j):
- i is the number of operational memories;
- j is the number of operational processors

S = {(3,2), (3,1), (3,0), (2,2), (2,1), (2,0), (1,2), (1,1), (1,0), (0,2), (0,1)}

Reliability modeling



λ_m failure rate for memory

λ_p failure rate for processor

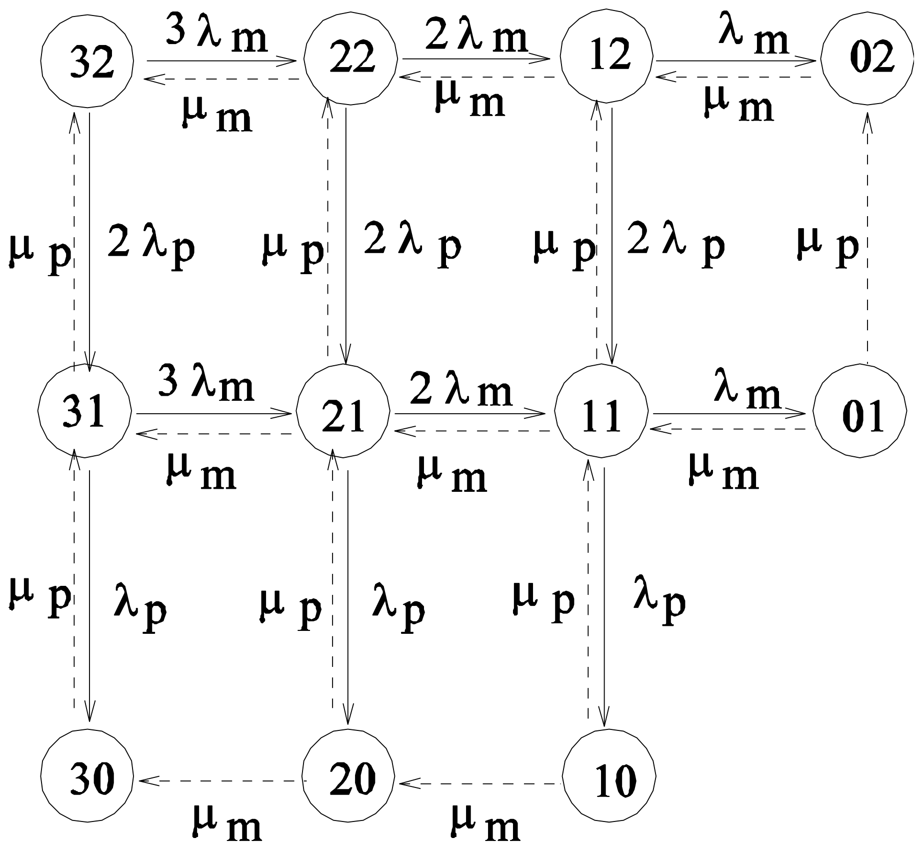
(3, 2) -> (2,2) failure of one memory

(3,0), (2,0), (1,0), (0,2), (0,1) are absorbent states

Availability modeling

- Assume that faulty components are replaced and we evaluate the probability that the system is operational at time t
- Constant repair rate μ (number of expected repairs in a unit of time)
- Strategy of repair:
  only one processor or one memory at a time can be substituted
- The behaviour of components (with respect of being operational or failed) is not independent: it depends on whether or not other components are in a failure state.

- Strategy of repair:
  only one component can be substituted at a time



λm failure rate for memory

λp failure rate for processor

μm repair rate for memory

μp repair rate for processor

- An alternative strategy of repair:
  only one component can be substituted at a time and processors have higher priority
- exclude the lines μm representing memory repair in the case where there has been a process failure