EDA122/DIT061 Fault-Tolerant Computer Systems
DAT270 Dependable Computer Systems

Welcome to Lecture 4

Markov chain models

Markov chain models

- Basic theory
- Hot stand-by system
- Cold stand-by system
- Coverage factor
- Dormancy factor

Markov property

Let ***X*** denote the lifetime for a component.

The Markov property is defined as follows:

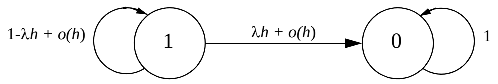
$$P(X \leq t + h | X > t) = \lambda \cdot h + o(h)$$

The probability that a component fails in the small interval *h* is proportional to the length of the interval.

λ is the proportional constant.

The probability above does not depend on the time *t*.

State diagram for one component



The reliability for one component

(reliability = function probability)

The probability that the component *is working* at the time *t+h* is

$$P_1(t+h) = (1 - \lambda \cdot h + o(h)) \cdot P_1(t)$$

We divide with *h*

$$\frac{P_1(t+h) - P_1(t)}{h} = -\frac{\lambda \cdot h}{h} \cdot P_1(t) + \frac{o(h)}{h}$$

Let $h \to 0$, and we get

$$P'_1(t) = -\lambda \cdot P_1(t)$$

Reliability for one component (cont'd)

$$P'_1(t) = -\lambda \cdot P_1(t)$$

The solution to this differential equation is

$$P_1(t) = C_1 \cdot e^{-\lambda t} \text{ , where } C_1 = 1, \text{ since } P_1(0) = 1$$

Assuming that the component works at the time *t = 0*, we get

$$P_1(0) = 1$$

The reliability of the component is:

$$P_1(t) = e^{-\lambda t}$$

The failure probability for one component

The probability that the component is faulty at the time *t+h* is

$$P_0(t+h) = (\lambda h + o(h))P_1(t) + P_0(t)$$

Rearranging the expression yields

$$\frac{P_0(t+h) - P_0(t)}{h} = \lambda \cdot P_1(t) + \frac{o(h)}{h} \cdot P_1(t)$$

If we let $h \to 0$, we get

$$P'_0(t) = \lambda \cdot P_1(t)$$

Failure probability for one component (cont'd.)

Solving the differential equation yields

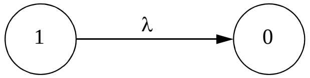
$$P'_0(t) = \lambda \cdot P_1(t)$$

$$P_0(t) = \int \lambda e^{-\lambda t} dt + C_0$$

$$P_0(t) = -e^{-\lambda t} + C_0 \text{ , } C_0 = 1 \text{ since } P_0(0) = 0$$

$$P_0(t) = 1 - e^{-\lambda t}$$

State diagram with simplified notation



Markov chain model

The Markov chain model is defined by the following equation system

$$\begin{cases} P'_1(t) = -\lambda \cdot P_1(t) \\ P'_0(t) = \lambda \cdot P_1(t) \end{cases}$$

Markov chain model (cont'd.)

The equation system can be written using matrices:

$$\mathbf{P}'(\mathbf{t}) = \mathbf{P}(\mathbf{t}) \cdot \mathbf{Q}(\mathbf{t})$$

where

$$\mathbf{P}(\mathbf{t}) = \begin{bmatrix} P_1(t) & P_0(t) \end{bmatrix}$$

$$\mathbf{P}'(\mathbf{t}) = \begin{bmatrix} P'_1(t) & P'_0(t) \end{bmatrix}$$

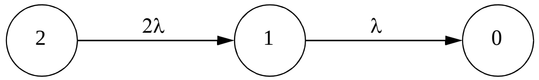
and

$$\mathbf{Q} = \begin{bmatrix} -\lambda & \lambda \\ 0 & 0 \end{bmatrix}$$

Q is called the transition rate matrix.

Hot stand-by system with one spare

State diagram



State labelling:

2 Both modules work

1 One module works

0 No module works, system failure

We calculate the reliability on the blackboard!

The Laplace transform

But first we need to introduce the Laplace transform, which is defined as

$$L[f(t)] = \tilde{f}(s) = \int_0^{\infty} e^{-st} f(t)dt, \quad \text{for } s > 0$$

Using the Laplace transform, we can transform the system of ordinary differential equations into a system of algebraic equations.

Useful Laplace transforms

$$L[e^{-at}] = \tilde{f}(s) = \int_0^{\infty} e^{-st} e^{-at} dt = \int_0^{\infty} e^{-(s+a)t} dt$$

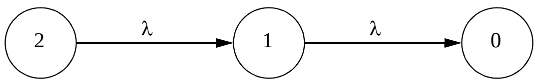
$$= \left[-\frac{1}{(s+a)} e^{-(s+a)t}\right]_0^{\infty} = \frac{1}{s+a}, \; s > a$$

$$L[f'(t)] = \int_0^{\infty} e^{-st} f'(t)dt = [e^{-st} f(t)]_0^{\infty} + \int_0^{\infty} s e^{-st} f(t)\, dt$$

$$= -f(0) + s\tilde{f}(s) = s\tilde{f}(s) - f(0)$$

Cold stand-by system with one spare

State diagram



State labelling:

2 Both modules work

1 One module works

0 No module works, system failure

Assumption: The failure rate for the spare is zero.

Cold stand-by system with one spare (cont'd.)

We calculate the reliability of the system by solving the equation system:

$$\mathbf{P}'(\mathbf{t}) = \mathbf{P}(\mathbf{t}) \cdot \mathbf{Q}(\mathbf{t})$$

where

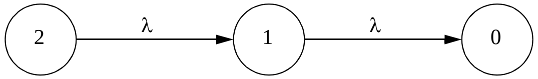
$$\mathbf{P}(\mathbf{t}) = \begin{bmatrix} P_2(t) & P_1(t) & P_0(t) \end{bmatrix}$$

$$\mathbf{P}'(\mathbf{t}) = \begin{bmatrix} P'_2(t) & P'_1(t) & P'_0(t) \end{bmatrix}$$

$$\mathbf{Q} = \begin{bmatrix} -\lambda & \lambda & 0 \\ 0 & -\lambda & \lambda \\ 0 & 0 & 0 \end{bmatrix}$$

Identifying the Q-matrix

The state diagram



The Q-matrix

$$\mathbf{Q} = \begin{bmatrix} -\lambda & \lambda & 0 \\ 0 & -\lambda & \lambda \\ 0 & 0 & 0 \end{bmatrix}$$

The equation system

$$\begin{cases} P'_2(t) = -\lambda \cdot P_2(t) \\ P'_1(t) = \lambda \cdot P_2(t) - \lambda \cdot P_1(t) \\ P'_0(t) = \lambda \cdot P_1(t) \end{cases}$$

We solve this by applying the Laplace transform using the following relation

$$f'(t) = s\tilde{f}(s) - f(0)$$

Solving the equation system

The Laplace transform get

$$s \cdot \tilde{\mathbf{P}}(\mathbf{s}) - \mathbf{P}(\mathbf{0}) = \tilde{\mathbf{P}}(\mathbf{s}) \cdot \mathbf{Q}$$

where

$$\mathbf{P}(\mathbf{0}) = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$$

which give us

$$s \cdot \tilde{P}_2(s) - 1 = -\lambda \cdot \tilde{P}_2(s)$$
$$s \cdot \tilde{P}_1(s) - 0 = \lambda \cdot \tilde{P}_2(s) - \lambda \cdot \tilde{P}_1(s)$$
$$s \cdot \tilde{P}_0(s) - 0 = \lambda \cdot \tilde{P}_1(s)$$

Laplace transforms

Time function	Laplace transform
$e^{-\lambda \cdot t}$	$\dfrac{1}{s+\lambda}$
$t \cdot e^{-\lambda \cdot t}$	$\dfrac{1}{(s+\lambda)^2}$

Solving the equation system (cont'd.)

We first solve $\tilde{P}_2(s)$

$$\tilde{P}_2(s) = \frac{1}{s+\lambda}$$

which gives the following time function

$$P_2(t) = e^{-\lambda \cdot t}$$

Solving the equation system (cont'd.)

We the compute $\tilde{P}_1(s)$

$$\tilde{P}_1(s) = \frac{\lambda \cdot \tilde{P}_2(s)}{(s+\lambda)} = \frac{\lambda}{(s+\lambda)^2}$$

$$P_1(t) = \lambda t e^{-\lambda \cdot t}$$

The reliability of the system can be written as

$$R(t) = P_2(t) + P_1(t) = e^{-\lambda \cdot t} + \lambda t e^{-\lambda \cdot t} = (1 + \lambda t) \cdot e^{-\lambda \cdot t}$$

Calculating the MTTF

Let X_2 and X_1 denote the time spent in state 2 and state 1, respectively.

MTTF for the system can then be written as

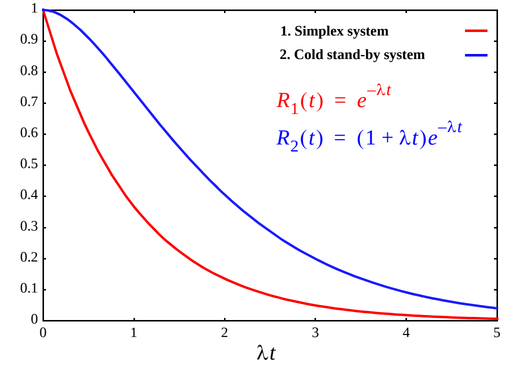
$$MTTF = E[X_2 + X_1] = E[X_2] + E[X_1] = \frac{1}{\lambda} + \frac{1}{\lambda} = \frac{2}{\lambda}$$

Alternatively, the MTTF can be computed as

$$MTTF = \int_0^\infty R(t)dt = \int_0^\infty (1+\lambda t)e^{-\lambda \cdot t}dt = \int_0^\infty e^{-\lambda \cdot t}dt + \int_0^\infty \lambda t e^{-\lambda \cdot t}dt$$

$$= \frac{1}{\lambda} + \frac{1}{\lambda} = \frac{2}{\lambda}$$

The reliability



Coverage

Designing a fault-tolerant system that will correctly detect, mask or recover from every conceivable fault, or error, is not possible in practice.

Even if a system can be designed to tolerate a very large number of faults, or errors, there are for most systems *a* non-zero probability that a single fault will cause the system to fail.

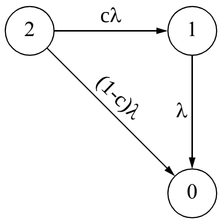
Such faults are known as “*non-covered*” faults.

The probability that a fault is *covered* (i.e., correctly handled by the fault-tolerance mechanisms) is known as the ***coverage factor***, and denoted ***c***.

The probability that a fault is *non-covered* can then be written as ***1 - c***.

Cold stand-by system with coverage factor

State diagram



We can write-up the Q-matrix directly by inspecting the state diagram.

$$\mathbf{Q} = \begin{bmatrix} -\lambda & c \cdot \lambda & (1-c) \cdot \lambda \\ 0 & -\lambda & \lambda \\ 0 & 0 & 0 \end{bmatrix}$$

Solving the equation system (cont’d.)

We have the following equation system

$$P'_2(t) = -\lambda \cdot P_2(t)$$
$$P'_1(t) = c\lambda \cdot P_2(t) - \lambda \cdot P_1(t)$$
$$P'_0(t) = (1-c)\lambda \cdot P_2(t) + \lambda \cdot P_1(t)$$

After applying the Laplace transform, we get

$$s \cdot \tilde{P}_2(s) - 1 = -\lambda \cdot \tilde{P}_2(s)$$
$$s \cdot \tilde{P}_1(s) - 0 = c\lambda \cdot \tilde{P}_2(s) - \lambda \cdot \tilde{P}_1(s)$$
$$s \cdot \tilde{P}_0(s) - 0 = (1-c)\lambda \cdot \tilde{P}_2(s) + \lambda \cdot \tilde{P}_1(s)$$

Solving the equation system (cont’d.)

$\tilde{P}_2(s)$ can we compute directly from the first equation

$$\tilde{P}_2(s) = \frac{1}{s+\lambda} \Rightarrow P_2(t) = e^{-\lambda \cdot t}$$

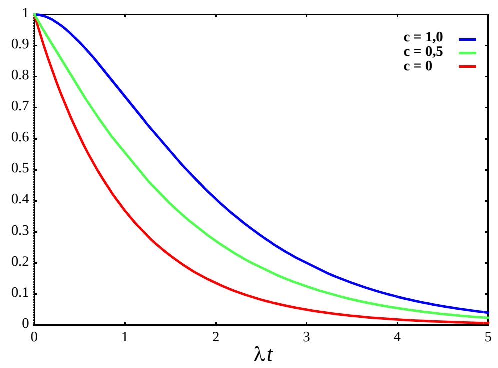
We then compute $\tilde{P}_1(s)$

$$\tilde{P}_1(s) = \frac{c\lambda \cdot \tilde{P}_2(s)}{(s+\lambda)} = \frac{c\lambda}{(s+\lambda)^2} \Rightarrow P_1(t) = c\lambda t e^{-\lambda \cdot t}$$

Reliability for the system is

$$R(t) = P_2(t) + P_1(t) = e^{-\lambda \cdot t} + c\lambda t e^{-\lambda \cdot t} = (1 + c\lambda t) \cdot e^{-\lambda \cdot t}$$

The reliability with coverage factor



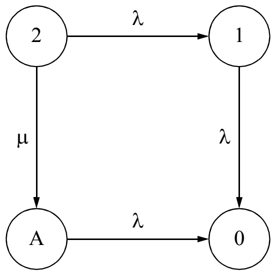
MTTF for cold stand-by system with coverage factor

$$MTTF = \int_0^\infty R(t)dt = \int_0^\infty (1 + c\lambda t)e^{-\lambda \cdot t}dt = \int_0^\infty e^{-\lambda \cdot t}dt + c\int_0^\infty \lambda t e^{-\lambda \cdot t}dt$$

$$= \frac{1}{\lambda} + \frac{c}{\lambda} = \frac{1+c}{\lambda}$$

Cold stand-by system with dormancy factor

State diagram

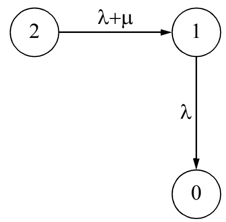


Dormancy factor

$$\lambda = k \cdot \mu$$

Cold stand-by system with dormancy factor (cont'd)

Simplified state diagram



$$\mathbf{Q} = \begin{bmatrix} -(\lambda+\mu) & (\lambda+\mu) & 0 \\ 0 & -\lambda & \lambda \\ 0 & 0 & 0 \end{bmatrix}$$

Cold stand-by system with dormancy factor (cont'd)

We have the following equations

$$P'_2(t) = -(\lambda + \mu) \cdot P_2(t)$$
$$P'_1(t) = (\lambda + \mu) \cdot P_2(t) - \lambda \cdot P_1(t)$$
$$P'_0(t) = \lambda \cdot P_1(t)$$

Applying the Laplace transform, we get

$$s \cdot \tilde{P}_2(s) - 1 = -(\lambda + \mu) \cdot \tilde{P}_2(s)$$
$$s \cdot \tilde{P}_1(s) - 0 = (\lambda + \mu) \cdot \tilde{P}_2(s) - \lambda \cdot \tilde{P}_1(s)$$
$$s \cdot \tilde{P}_0(s) - 0 = \lambda \cdot \tilde{P}_1(s)$$

Cold stand-by system with dormancy factor (cont'd)

We get

$$\tilde{P}_2(s) = \frac{1}{s + (\lambda + \mu)} \Rightarrow P_2(t) = e^{-(\lambda + \mu) \cdot t}$$

$$\tilde{P}_1(s) = \frac{(\lambda + \mu)}{(s + \lambda)} \cdot \tilde{P}_2(s) = \frac{(\lambda + \mu)}{(s + \lambda)(s + (\lambda + \mu))}$$

Decomposition into partial fractions give us

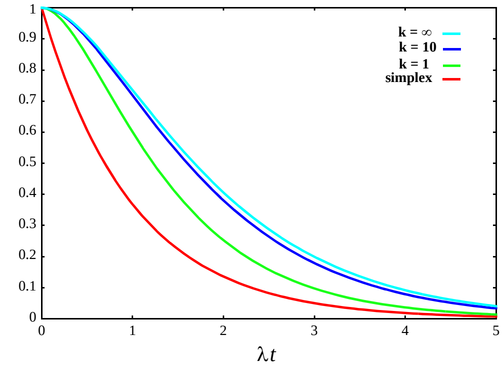
$$\tilde{P}_1(s) = \frac{(\lambda + \mu)}{\mu(s + \lambda)} - \frac{(\lambda + \mu)}{\mu(s + (\lambda + \mu))} \Rightarrow P_1(t) = \frac{\lambda + \mu}{\mu}(e^{-\lambda \cdot t} - e^{-(\lambda + \mu) \cdot t})$$

Cold stand-by system with dormancy factor (cont'd)

The reliability is

$$R(t) = P_2(t) + P_1(t) = e^{-(\lambda + u) \cdot t} + \frac{\lambda + \mu}{\mu}(e^{-\lambda \cdot t} - e^{-(\lambda + \mu) \cdot t})$$
$$= \frac{\lambda + \mu}{\mu} e^{-\lambda \cdot t} - \frac{\lambda}{\mu} e^{-(\lambda + \mu) \cdot t}$$

Reliability with dormancy factor



Overview of Lecture 5

- Availability modeling
- Safety modeling

Preparations:

- Course book:
  - Availability (pages 20, 21, 25,167),
  - Safety (Section 1.1 - 1.3, pages 1 - 14)
  - Section 5.6 Maintainability (pages 101-103)
  - Section 7.2 Markov models (pages 183 – 186)
- Lecture slides