Exercise 5

This exercise covers safety modeling and we will solve Problem 3.8, 3.9, and 5.3(c).

Problem 3.8

Derive an expression for the safety of a TMR system which is shut down after the second module failure. Assume that the shut-down is successful with a probability c. Also, assume that the modules in the system have a failure rate of λ. Calculate the steady-state safety.

Safety Probability that the system is either functioning properly or is in a safe state at time t.

Calculating the safety for this system requires two absorbing states in the Markov model (fail-safe and catastrophic failure).

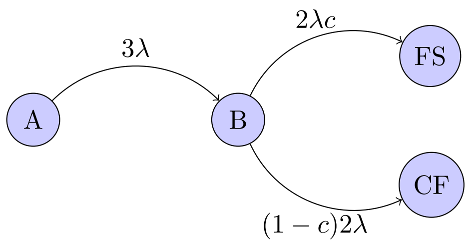

Figure 1: Markov chain

$$
\begin{aligned}
S(t) &= P_A(t) + P_B(t) + P_{FS}(t) \\
P(t) &= \begin{bmatrix} P_A(t) & P_B(t) & P_{FS}(t) & P_{CF} \end{bmatrix} \\
P'(t) &= P(t)Q \\
P(0) &= \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix} \\
Q &= \begin{bmatrix} -3\lambda & 3\lambda & 0 & 0 \\ 0 & -2\lambda & 2\lambda c & 2\lambda(1-c) \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}
\end{aligned}
$$

Laplace transform:

$$\mathcal{L}\{P'(t) = P(t)Q\} \Rightarrow sP(s) - P(0) = P(s)Q$$

$$
\begin{aligned}
sP_A - 1 &= -3\lambda P_A \\
sP_B &= 3\lambda P_A - 2\lambda P_B \\
sP_{FS} &= 2\lambda c P_B \\
sP_{CF} &= \ldots
\end{aligned}
$$

$$
\begin{aligned}
P_A &= \frac{1}{s+3\lambda} \\
P_B &= \frac{3\lambda}{s+2\lambda}P_A = \frac{3\lambda}{s+2\lambda}\frac{1}{s+3\lambda} = 3\lambda\frac{1}{\lambda}\left(\frac{1}{s+2\lambda} - \frac{1}{s+3\lambda}\right) \\
&= \frac{3}{s+2\lambda} - \frac{3}{s+3\lambda} \\
P_{FS} &= \frac{2\lambda c}{s}P_B = \frac{2\lambda c}{s}3\left(\frac{1}{s+2\lambda} - \frac{1}{s+3\lambda}\right) \\
&= 6\lambda c\left(\frac{1}{2\lambda}\left(\frac{1}{s} - \frac{1}{s+2\lambda}\right) - \frac{1}{3\lambda}\left(\frac{1}{s} - \frac{1}{s+3\lambda}\right)\right) \\
&= \frac{3c}{s} - \frac{3c}{s+2\lambda} - \frac{2c}{s} + \frac{2c}{s+3\lambda} \\
&= \frac{c}{s} - \frac{3c}{s+2\lambda} + \frac{2c}{s+3\lambda}
\end{aligned}
$$

$$\mathcal{L}^{-1}\left\{\frac{1}{s}\right\} = 1$$

$$
\begin{aligned}
P_A(t) &= e^{-3\lambda t} \\
P_B(t) &= 3e^{-2\lambda t} - 3e^{-3\lambda t} \\
P_{FS}(t) &= c - 3ce^{-2\lambda t} + 2ce^{-3\lambda t} \\
S(t) &= P_A(t) + P_B(t) + P_{FS}(t) \\
&= e^{-3\lambda t}(1 - 3 + 2c) + e^{-2\lambda t}(3 - 3c) + c \\
&= 2(c-1)\,e^{-3\lambda t} + 3(1-c)\,e^{-2\lambda t} + c
\end{aligned}
$$

Steady-state safety:

$$\lim_{t\to\infty} S(t) = c$$

This can be obtained directly from the Markov model!

$$\lim_{t\to\infty} S(t) = \frac{2\lambda c}{2\lambda c + 2\lambda(1-c)} = c$$

Problem 3.9

Derive an expression for the safety of a hot-standby system which is shut down after the first module failure. Assume that the shut-down time is exponentially distributed with the expected value $1/\mu$. The failure rate of the modules is $\lambda = 10^{-7}$ f/h.

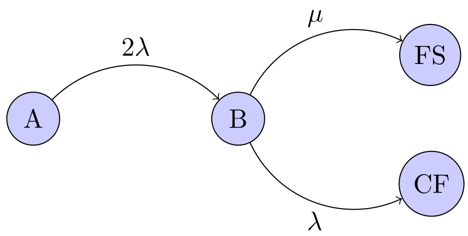

Figure 2: Markov chain

$$
\begin{aligned}
P(t) &= \begin{bmatrix} P_A(t) & P_B(t) & P_{FS}(t) & P_{CF} \end{bmatrix} \\
P'(t) &= P(t)Q \\
P(0) &= \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix} \\
Q &= \begin{bmatrix} -2\lambda & 2\lambda & 0 & 0 \\ 0 & -(\lambda+\mu) & \mu & \lambda \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}
\end{aligned}
$$

Laplace transform:

$$\mathcal{L}\left\{P'(t) = P(t)Q\right\} \Rightarrow sP(s) - P(0) = P(s)Q$$

$$
\begin{aligned}
sP_A - 1 &= -2\lambda P_A \\
sP_B &= 2\lambda P_A - (\lambda+\mu)P_B \\
sP_{FS} &= \mu P_B \\
sP_{CF} &= \lambda P_B \\
P_A &= \frac{1}{s+2\lambda} \\
P_B &= \frac{2\lambda}{s+(\lambda+\mu)} P_A = \frac{2\lambda}{s+(\lambda+\mu)} \frac{1}{s+2\lambda} \\
&= \frac{2\lambda}{\lambda-\mu}\left(\frac{1}{s+(\lambda+\mu)} - \frac{1}{s+2\lambda}\right) \\
P_{FS} &= \frac{\mu}{s} P_B = \frac{\mu}{s} \frac{2\lambda}{\lambda-\mu}\left(\frac{1}{s+(\lambda+\mu)} - \frac{1}{s+2\lambda}\right) \\
&= \frac{2\lambda\mu}{\lambda-\mu}\left(\frac{1}{\lambda+\mu}\left(\frac{1}{s} - \frac{1}{s+(\lambda+\mu)}\right) - \frac{1}{2\lambda}\left(\frac{1}{s} - \frac{1}{s+2\lambda}\right)\right)
\end{aligned}
$$

Inverse Laplace transform:

$$\begin{aligned}
P_A(t) &= e^{-2\lambda t} \\
P_B(t) &= \frac{2\lambda}{\lambda-\mu}\left(e^{-(\lambda+\mu)t} - e^{-2\lambda t}\right) \\
P_{FS}(t) &= \frac{2\lambda\mu}{\lambda-\mu}\left(\frac{1}{\lambda+\mu}\left(1-e^{-(\lambda+\mu)t}\right) - \frac{1}{2\lambda}\left(1-e^{-2\lambda t}\right)\right) \\
S(t) &= e^{-2\lambda t}\left(1 - \frac{2\lambda}{\lambda-\mu} + \frac{\mu}{\lambda-\mu}\right) \\
&\quad + e^{-(\lambda+\mu)t}\left(\frac{2\lambda}{\lambda-\mu} - \frac{2\lambda\mu}{(\lambda-\mu)(\lambda+\mu)}\right) \\
&\quad + \underbrace{\frac{2\lambda\mu}{\lambda-\mu}\left(\frac{1}{\lambda+\mu} - \frac{1}{2\lambda}\right)}_{=\frac{2\lambda\mu}{\lambda-\mu}\frac{2\lambda-(\lambda+\mu)}{2\lambda(\lambda+\mu)}=\frac{\mu}{\lambda-\mu}\frac{\lambda-\mu}{\lambda+\mu}=\frac{\mu}{\lambda+\mu}} \\
&= \frac{\lambda-\mu-2\lambda+\mu}{\lambda-\mu}e^{-2\lambda t} \\
&\quad + \frac{2\lambda(\lambda+\mu)-2\lambda\mu}{\lambda^2-\mu^2}e^{-(\lambda+\mu)t} \\
&\quad + \frac{\mu}{\lambda+\mu} \\
&= \frac{\lambda}{\mu-\lambda}e^{-2\lambda t} + \frac{2\lambda^2}{\lambda^2-\mu^2}e^{-(\lambda+\mu)t} + \frac{\mu}{\lambda+\mu}
\end{aligned}$$

Steady-state safety:

$$\lim_{t\to\infty} S(t) = \frac{\mu}{\lambda+\mu}$$

Problem 5.3

A fault-tolerant computer system consist of two active modules and two cold standby spare modules. The spares can replace any of the active modules in case any of them fails. A working system requires at least two fault-free modules. The probability for correct activation of a spare in case of failure of an active module is c. If the activation fails it is assumed that the system crashes immediately. The life times of the active modules are exponentially distributed with a failure rate λ. The failure rates of the cold stand-by spares can be neglected.

5.3 c) Assume that a safe shutdown is initiated when two working modules remain. The shut-down time for the system is exponentially distributed with an average shut-down time of 2 hours. An unsafe shutdown occurs immediately if any of the two modules fails during the shut-down time. Calculate the steady-state safety of the system. *Hint: the steady-state safety can be derived directly from the transition rates in the Markov model.*

Solution

State	Working	Spares
A	2	2
B	2	1
C	2	0
FS	System failure: safe state	
CF	System failure: catastrophic failure	

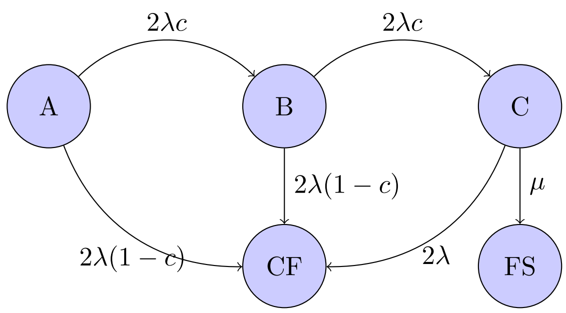

Figure 3: Markov chain

$$
\begin{aligned}
\lim_{t\to\infty} P_{FS}(t) &= P_{A\to B} \times P_{B\to C} \times P_{C\to FS} \\
P_{A\to B} &= \frac{2\lambda c}{2\lambda c + 2\lambda(1-c)} = c \\
P_{B\to C} &= \frac{2\lambda c}{2\lambda c + 2\lambda(1-c)} = c \\
P_{C\to FS} &= \frac{\mu}{2\lambda + \mu} \\
\Longrightarrow P_{FS} &= c \times c \times \frac{\mu}{2\lambda+\mu} = \frac{c^2\mu}{2\lambda+\mu}
\end{aligned}
$$