Chap 9: Reliability & Availability Modeling

Reliability Block Diagram using sharpe

```
block name {(( param-list ))}
[ < block line >
end
```

P.358 Appendix B

can be one of the following:
1) \textbf{comp} name exponential-polynomial
\[ F(t) = 1 - e^{-\lambda t} \]
Referring to the cumulative dist function (cdf)
\[ R(t) = e^{-\lambda t} \]
Referring to the cumulative dist function (cdf)

2) \textbf{parallel} name name-1 name-2 \{name3 name4 …\}
Name 1
Name 2
The parallel system is assigned to the first name.

3) \textbf{series} name name-1 name-2 \{name3 name4 …\}
Name 1
Name 2
The series system is assigned to the first name.

4) \textbf{kofn} name expression-1, expression-2, component-name
\[ F(t) = \sum_{j} a_j \cdot t^k \cdot e^{b_j t} \]
See p. 352

Referring to the cumulative dist function (cdf)
5) kofn name k-expression, n-expression, name1 name2 \{name3\ldots\}
representing a k-out-of-n system
having possibly different components

Components do not have identical failure-time dist.

Ex: CPU1
    M 1
    M 2
    M n
CPU2

Sharing memory: a k-out-of-n device

Output

in semi symbolic form

CDF for system
1-6e^{-0.00903t}+3e^{-0.0104t}+…

(1-out-of-3)
k=1.00 \quad \text{mean(system;k,3,\ldots) = 2.26*10^2}
\text{rel (10,k,3\ldots) = 9.9981*10^{-1}}
\text{rel (365,k,3\ldots) = 8.33*10^{-1}}
k=2.00

46
Comments: any line starting with the symbol “*”

* printing output.
* printing $F(t)$ in symbolic form

\[ \text{cdf} \ (\text{system};1, 3, 0.00139, 0.00764) \]

* define reliability function at time $t$

\[
\text{func} \ \text{rel}(t, k, n, pf, mf)\\
1-\text{value} \ (t; \text{system}; k, n, pf, mf)
\]

Returning $F(t)$ at time $t$ numerically

\[
\text{loop} \ k, 1, 3, 1
\]

\[
\begin{align*}
\text{expr} & \quad \text{mean} \ (\text{system}; k, 3, 0.00139, 0.00764) \\
\text{expr} & \quad \text{rel} \ (10, k, 3, 0.00139, 0.00764) \\
\text{expr} & \quad \text{rel} \ (365, k, 3, 0.00139, 0.00764)
\end{align*}
\]

\text{end}

\text{end}
* printing: 5 decimal places
  format 5
* cdf
  cdf (block1a)
  expr 1-value(10; block1a)
end
### Availability Modeling

\[
A_i(t) = \frac{\mu_i}{\lambda_i + \mu_i} + \frac{\lambda_i}{\lambda_i + \mu_i} e^{-(\lambda_i+\mu_i)t}
\]

To define \(1-A_i(t)\):

- **poly** `unavail(mu, lambda)`
- **gen** `1, 0, 0`
- `mu/(lambda+mu), 0, 0`
- `lambda/(lambda+mu), 0, -(lambda+mu)`

**block** `block1a`

**comp** `A unavail(mu_A, lambda_A)`

**comp** `B unavail(mu_B, lambda_B)`

...  

**end**

- **bind** `mu_A 1`
- `lambda_A 0.0001`

---

See p.354 text on a user-defined distribution syntax:

- poly `name(param-list) dist.`
- gen\`triple\` of the form `(a_j, k_j, b_j)`

\[
F(t) = \sum_{j} a_j \cdot t^{k_j} \cdot e^{b_j t}
\]

* print steady state
* availability \(A(\infty)\)
  
  `expr pinf(block1a)`

* print instantaneous
* availability at \(t=100\)
  
  `expr 1-value(100; block1a)`

**end**
Fault Trees

* A pictorial representation of events that can cause the occurrence of an undesirable event.
* An event at a high level is reduced to a combination of lower level events by means of logic gates

**AND:** when all fail, the failure event occurs.
**OR:** when one fails, the failure event occurs.
**K out of n:** when at least k out of n components fail, the failure event occurs.

E.g.

\[
\begin{align*}
failure \\
\text{or} \\
&\quad \text{AND} \\
&\quad P_1 P_2 \\
&\quad \text{AND} \\
&\quad M_1 M_2 M_3
\end{align*}
\]

\[
\equiv
\begin{align*}
P_1 & P_2 \\
M_1 & M_2 & M_3
\end{align*}
\]
For a fault tree without repeated components:

$$Q_{\text{f-tree}}(t) = \begin{cases} 
\prod_{i=1}^{n} Q_i(t) & \text{AND gate} \\
1 - \prod_{i=1}^{n} \left(1 - Q_i(t)\right) & \text{OR gate} \\
\sum_{i=k}^{n} \binom{n}{i} (Q(t))^i \left(1 - Q(t)\right)^{n-i} & \text{k-out-of-n gate: for n identically distributed components} \\
\sum_{|J| \geq k} \left( \prod_{j \in |J|} Q_j(t) \right) \left( \prod_{j \notin |J|} (1 - Q_j(t)) \right) & \text{k-out-of-n gate: for non-identically distributed components} 
\end{cases}$$

Unreliability or failure probability

A set that contains at least k failed components
The above equation cannot be used when there is a repeated component
e.g.

2 processors: P₁ & P₂
3 memory modules: M₁, M₂ & M₃

M₃ is shared by P₁ & P₂
M₁ is private to P₁
M₂ is private to P₂

the system will operate as long as there is at least one operational processor with access to either a private or shared memory.
Let \( P_i \) represent the failure of processor \( i \), \( M_i \) represent the failure of memory \( i \) & \( \phi \) be a boolean variable indicating system failure

\[
\begin{align*}
\text{i.e. } P_i &= 1 \text{ if Processor } i \text{ fails at time } t \\
\text{and } P_i &= 0 \text{ otherwise.} \\
\therefore F_{P_i} &= E[P_i] \\
(\therefore F_{P_i} &= 1 \cdot F_{P_i} + 0 \cdot R_{P_i}) \\
\text{Then } \phi &= X_{S_1}X_{S_2} = \left[1 - (1 - P_1)(1 - M_1M_3)\right]\left[1 - (1 - P_2)(1 - M_2M_3)\right]
\end{align*}
\]

The subsystem fails when either \( P_1 \) fails or both \( M_1M_3 \) fail

\[
\begin{align*}
\phi &= \left(P_1 + P_1M_1M_3\right)\left(P_2 + P_2M_2M_3\right) \\
&= P_1P_2 + P_1P_2M_2M_3 + P_1P_2M_1M_3 + P_1P_2M_1M_2M_3 \\
E[\phi] &= Q_{\text{system}} = Q_{P_1}Q_{P_2} + Q_{P_1}R_{P_2}Q_{M_2}Q_{M_3} + R_{P_1}Q_{P_2}Q_{M_1}Q_{M_3} \\
&\quad + R_{P_1}R_{P_2}Q_{M_1}Q_{M_2}Q_{M_3}
\end{align*}
\]
Fault Tree using Sharpe

e.g.\[
Q(t) = 1 - Pe^{-a_1 t} - (1-P)e^{-a_2 t}
\]

Hyperexponential

\[
Q(t) = 1 - e^{-\lambda t}
\]

Exponential failure law

```plaintext
bind
  a_1  0.028
  a_2  0.25
  P    0.5
end

ftree series (lambda)
  basic B exp (lambda)
  basic A gen \n    1, 0, 0 \ * for 1
    -P, 0, -a_1 \ * for -Pe^{-a_1 t}
    -(1-P), 0, -a_2 \ * for -(1-P)e^{-a_2 t}
or top A B
end
* print
cdf (series; 0.05)
eval (series; 0.05) 0.5 1.5 0.5
end
```

P.172, chapter 9
e.g. Aircraft flight control system

This means if 3 out of 4 fail then the subsystem fails

```
bind
mIRS 0.000015
mPRS 0.00099
mSA 0.000037
mCS 0.00048  * most susceptible to failure
end  * ∴ use 4 CS components
f{tree} aircraft
basic IRS exp (mIRS)
basic PRS exp (mPRS)
  kofn IRS23  2, 3, IRS
kofn PRS23  2, 3, PRS
  or top IRS23 PRS23 CS34 SAS23
end

* print
  format 8
  expr mean(aircraft)
  eval (aircraft) 1000 10000 1000
  expr value(10; aircraft) * unreliability
end
```

Inertial reference sensors: 3

- IRS
- IRS
- IRS

Pitch rate sensors: 3

- PRS
- PRS
- PRS

Computer systems: 4

- CS1
- CS2
- CS3
- CS3

Secondary actuators: 3

- SA1
- SA2
- SA3
Fault Trees using SHARPE with repeated components

Ex: also see the example in Fig. 9.22

Ex:

\[
\text{ftree system}
\]
\[
\begin{align*}
\text{basic} & \quad P_1 & \text{exp} \ (\text{lambda} \ P_1) \\
\text{basic} & \quad P_2 & \text{exp} \ (\text{lambda} \ P_2) \\
\text{basic} & \quad M_1 & \text{exp} \ (\text{lambda} \ M_1) \\
\text{basic} & \quad M_2 & \text{exp} \ (\text{lambda} \ M_2) \\
\text{repeat} & \quad M_3 & \text{exp} \ (\text{lambda} \ M_3) \\
\text{AND} & \quad M_1M_3 & M_1 \ M_3 \\
\text{AND} & \quad M_2M_3 & M_2 \ M_3 \\
\text{OR} & \quad \text{system}_1 & P_1 \ M_1M_3 \\
\text{OR} & \quad \text{system}_2 & P_2 \ M_2M_3 \\
\text{AND} & \quad \text{top} \ \text{system}_1 \ \text{system}_2 \\
\end{align*}
\]

\[\equiv \text{kofn system}_1 \ 1, \ 2, \ P_1 \ M_1M_3\]

\[\equiv \text{kofn top} \ 2, \ 2, \ \text{system}_1 \ \text{system}_2\]

* print reliability at time t
  \[\text{expr} \ 1\text{-value} \ (t; \ \text{system})\]
2.6 Series-Parallel Block Diagrams with Components in common
(Also called Network Reliability Models)

Can be arranged as

A parallel connection of series structures

Definition: a minimal path (set) is a minimal set of components whose functioning ensures the functioning of the system.

A series connection of parallel structures

Definition: a minimal cut (set) is a minimal set of components whose failure ensures the failure of the system.

e.g.
Q: how many minimal path sets?  A: 4: \{1,3,5\}, \{1,4\}, \{2,5\}, \{2,3,4\}

Q: how many minimal cut sets?  A: 4: \{1,2\}, \{4,5\}, \{1,3,5\}, \{2,3,4\}

There are series-parallel diagrams with common components
Another example: TMR is a 2-out-of-3 system

3 minimal path sets: \{1,2\} \{2,3\} & \{1,3\}

Let \(\phi(t)\) be a boolean variable indicating if the system is alive at time \(t\), i.e.,

\[
\begin{align*}
\phi(t) &= 1 & \text{if alive} \\
\phi(t) &= 0 & \text{if dead}
\end{align*}
\]

Let \(X_i(t)\) be a boolean variable indicating if component \(i\) is alive at time \(t\), i.e.,

\[
\begin{align*}
X_i(t) &= 1 & \text{if alive} \\
X_i(t) &= 0 & \text{if dead}
\end{align*}
\]

\[
\phi(t) = 1 - \left[ (1 - X_1X_2)(1 - X_2X_3)(1 - X_1X_3) \right]
= 1 - \left( 1 - X_1X_2 - X_2X_3 - X_1X_3 + X_1X_2X_3 + X_1X_2X_3^2 + X_1^2X_2X_3 - X_1^2X_2^2X_3^2 \right)
= 1 - \left( 1 - X_1X_2 - X_2X_3 - X_1X_3 + 2X_1X_2X_3 \right)
\]

Due to \(X_i^2 = X_i\) from \(X_i\)'s definition
Now

\[ E[\phi(t)] = R(t) \]

\[ \therefore E[\phi(t)] = 1 \cdot \{\text{prob. it is alive at } t\} + 0 \cdot \{\text{prob. it fails at } t\} = R(t) \]

\[ \Rightarrow E[\phi(t)] = E\left[ X_1X_2 + X_2X_3 + X_1X_3 - 2X_1X_2X_3 \right] \]

Terms each contain only independent components

\[ = E[ X_1X_2 ] + E[ X_2X_3 ] + E[ X_1X_3 ] - 2E[ X_1X_2X_3 ] \]

\[ \therefore R_{\text{system}} = R_1R_2 + R_2R_3 + R_1R_3 - 2R_1R_2R_3 \]

For identical components, \( R_1=R_2=R_3 \), \( R_{\text{system}} = 3R^2 - 2R^3 \)
Modeling with a Reliability Graph

* A reliability graph consists of nodes & directed arcs.
  - source node — no arcs enter it
  - target (sink) node — no arcs leave it

* A system represented by a reliability graph fails when there is no path from the source to the sink.

* arcs are associated with failure time distribution (in cdf)
relgraph bridge(v1, v2, v3, v4, v5)
    a  b  exp(v1)
    a  c  exp(v4)
    b  d  exp(v2)
    c  d  exp(v5)
    bidirect
    b  c  exp(v3)
end
* print
cdf (bridge;\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5)
pqcdf (bridge;\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5)
end

The underlying technique for solving the model is minimal path set & minimal cut set.
What is the reliability graph corresponding to the fault tree model on the left?

Ans:

Sharpe code:

```
relgraph P 2M3shared
src 1 exp(lambda_P1)
src 2 exp(lambda_P2)
1 sink exp(lambda_M1)
2 sink exp(lambda_M2)
share sink exp(lambda_M3)
1 share inf
2 share inf
end
```

Specifying for P1

\[ F(t) = 1 - e^{-\lambda_p t} \]

See p.353 Appendix B specifying a component having all its mass at \( \infty \), i.e., \( F(t)=0 \) except at \( F(\infty)=1 \)

This means

1 \( \rightarrow \) share &
2 \( \rightarrow \) share
links never fail

* print reliability at time t
expr 1-value(t; P2M3shared)
end