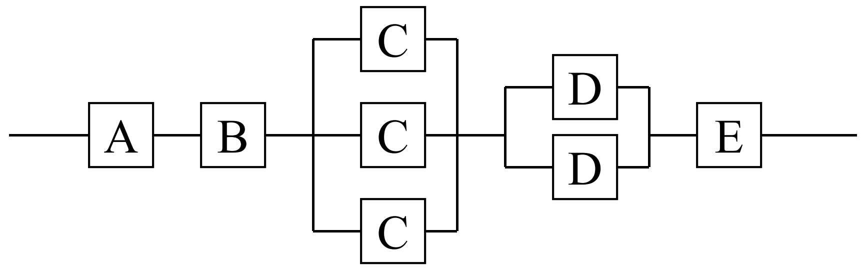
Chap 9: Reliability & Availability Modeling



Reliability Block Diagram using sharpe

P.358 Appendix B

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

can be one of the following:

1) comp name $\underbrace{\text{exponential-polynomial}}$

Referring to the cumulative distribution function (cdf) $F(t)$

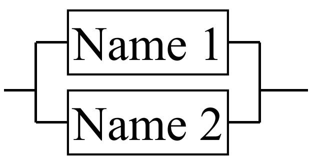
$$\begin{cases} F(t) = 1-e^{-\lambda t} \\ R(t) = e^{-\lambda t} \end{cases}$$

or
- exp (lambda) ← meaning
- cdf (component-name{,state}{;arg-list})
  which has been defined before
- gen triple 1, triple 2, ...
  in the form of (a_j, k_j, b_j)

See p. 352

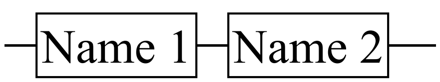
$$F(t) = \sum_j a_j \cdot t^{k_j} \cdot e^{b_j t}$$

2) parallel name name-1 name-2 {name-3 name-4 …}



The parallel system is assigned to the first name.

3) series name name-1 name-2 {name-3 name-4 …}



The series system is assigned to the first name.

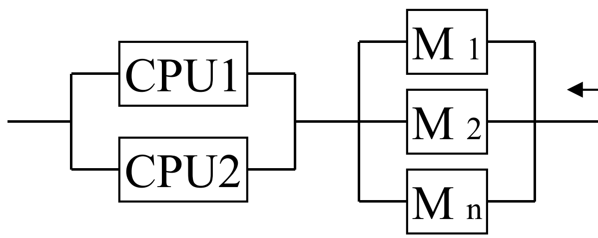
4) kofn name $\underbrace{\text{expression-1}}_{k}$, $\underbrace{\text{expression-2}}_{n}$, $\underbrace{\text{component-name}}_{\text{identical components}}$

5) <u>kofn</u> name k-expression, n-expression, name1 name2 {name3…}

representing a k-out-of-n system having possibly different components

Components do not have identical failure-time dist.

Ex:
Fig. 2.5 (p. 36)



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

<u>block</u> system (k, n, pfrate, mfrate)
<u>comp</u> CPU exp (pfrate)
<u>comp</u> mem exp (mfrate)
<u>parallel</u> CPUs CPU CPU
<u>kofn</u> mems k, n, mem
<u>series</u> top CPUs mems
<u>end</u>

Output

CDF for system (in semi symbolic form)
$1-6e^{-0.00903t}+3e^{-0.0104t}+\ldots$
(1-out-of-3)
k=1.00 mean(system;k,3,…) = $2.26*10^{2}$
rel (10,k,3…) = $9.9981*10^{-1}$
rel (365,k,3…) = $8.33*10^{-1}$
k=2.00

Comments: any line starting with the symbol “*”

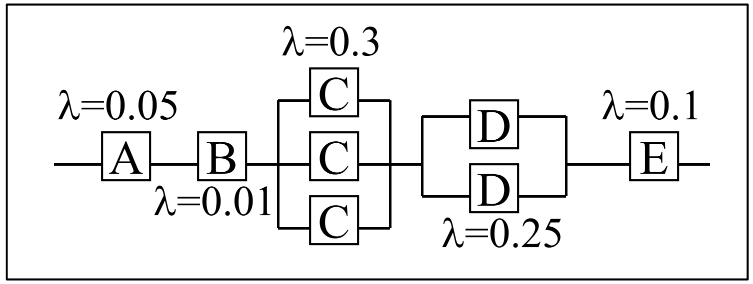
```
* printing output.
* printing F(t) in symbolic form
cdf (system;1, 3, 0.00139, 0.00764)
* define reliability function at time t
func  rel(t, k, n, pf, mf)\
      1-value (t; system; k, n, pf, mf)
```

\ means continuation to the next line

Returning F(t) at time t numerically

```
loop  k, 1, 3, 1
        expr    mean (system; k, 3, 0.00139, 0.00764)
        expr    rel (10, k, 3, 0.00139, 0.00764)
        expr    rel (365, k, 3, 0.00139, 0.00764)
end
end
```

Fig. 9.1 p. 156



block	block1a	
comp	A	exp(0.05)
comp	B	exp(0.01)
comp	C	exp(0.3)
comp	D	exp(0.25)
comp	E	exp(0.1)
parallel	threeC	C C C
parallel	twoD	D D
series	sys1	A B threeC twoD E
end		

- printing: 5 decimal places

  format 5
- cdf

  cdf (block1a)

  expr 1-value(10; block1a)

  end

Print 1-F(t)=R(t) at t=10

Availability Modeling

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

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

poly name(param-list) dist.

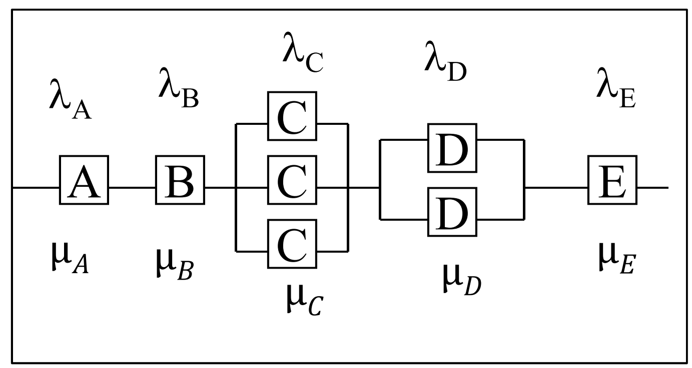
gen\
triple\
triple

of the form (a_j, k_j, b_j)

$$F(t) = \sum_j a_j \cdot t^{k_j} \cdot e^{b_j t}$$

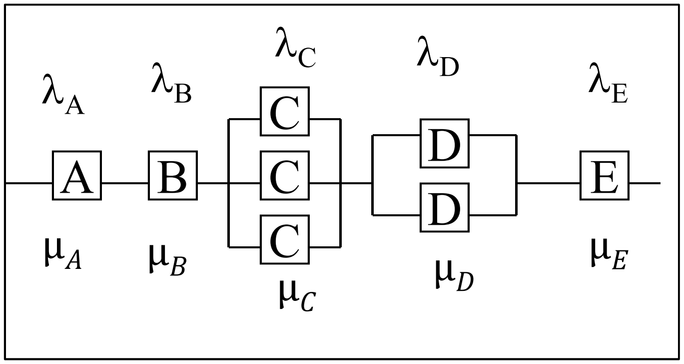
To define $1\text{-}A_i(t)$

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, $lambda_B$)	
comp	C unavail(mu_C, $lambda_C$)	
comp	D unavail(mu_D, $lambda_D$)	
comp	E unavail(mu_E, $lambda_E$)	
parallel	threeC	C C C
parallel	twoD	D D
series	sys1	A B threeC twoD E
end		



Availability Modeling

<u>bind</u>
mu$_A$ 1
mu$_B$ 2
mu$_C$ 3
mu$_D$ 4
mu$_E$ 5
lambda$_A$ 0.01
lambda$_B$ 0.02
lambda$_C$ 0.03
lambda$_D$ 0.04
lambda$_E$ 0.05
<u>end</u>
*
*print steady state
* availability A(∞)
expr <u>pinf</u>(block1a)
* print instantaneous
* availability at t=100
expr 1-value(100; block1a)
<u>end</u>

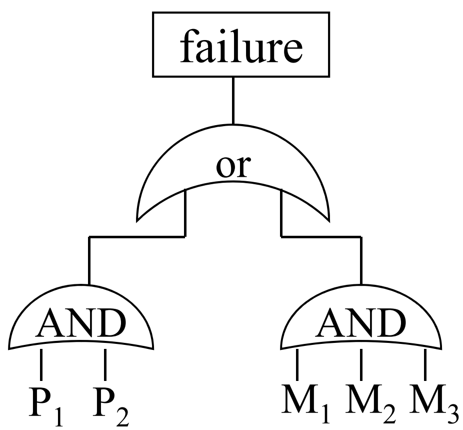


Fault Trees *P.39, chap.2*

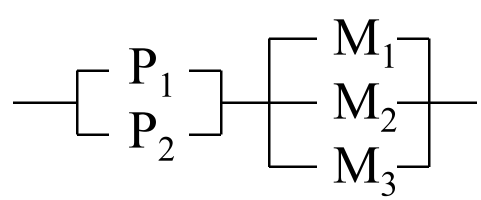
* A pictorial representation of events that can cause the occurrence of an undesirable event.
* An event at a high level is reduced to a combination of lower level events by means of logic gates

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.



$\equiv$



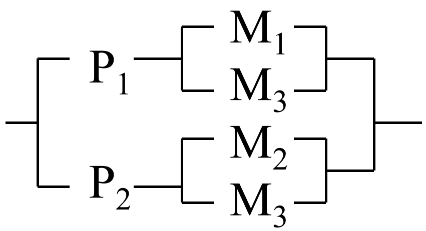
For a fault tree without repeated components:

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

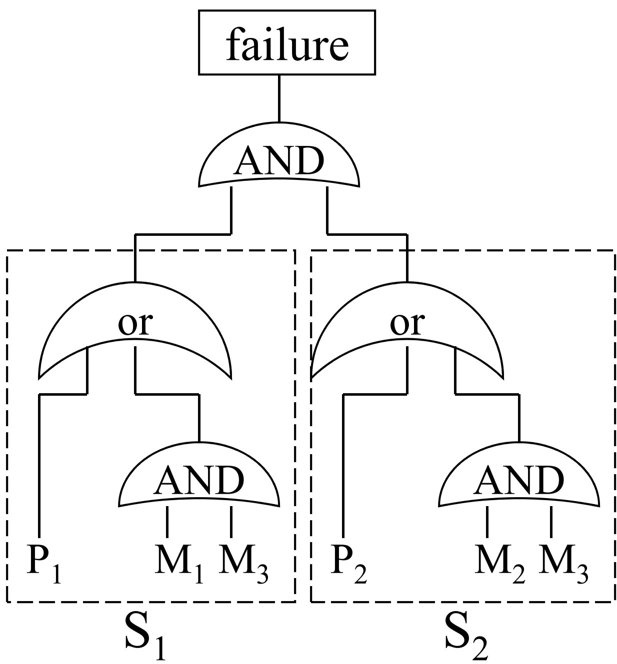
A set that contains
at least k failed components

The above equation cannot be used when there is a repeated component

e.g.



$\equiv$



2 processors: P_1 & P_2
3 memory modules: M_1, M_2 & M_3

M_3 is shared by P_1 & P_2
M_1 is private to P_1
M_2 is private to P_2

the system will operate as long as there is at least one operational processor with access to either a private or shared memory.

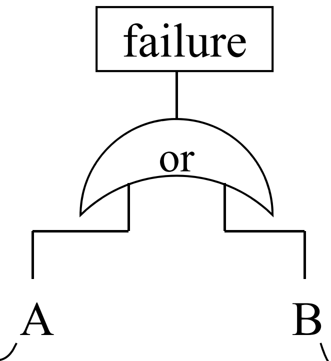
Fault Tree using Sharpe

P.172, chapter 9

e.g.

$Q(t) = 1 - Pe^{-a1t} - (1-P)e^{-a2t}$

hyperexponential



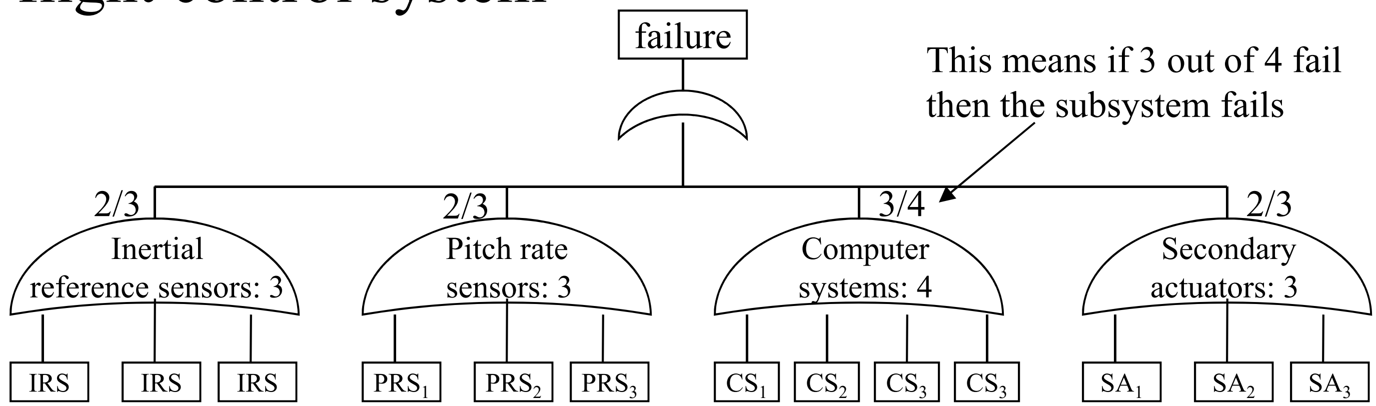
$Q(t) = 1 - e^{-\lambda t}$

exponential failure law

Failure rate

```
bind
    a1          0.028
    a2          0.25
    P           0.5
end
ftree       series (lambda)
basic       B               exp (lambda)
basic       A               gen \
            1, 0, 0  \                  * for 1
            -P, 0, -a1 \                * for -Pe^(-a1 t)
            -(1-P), 0, -a2              * for -(1-P)e^(-a2 t)
or          top  A  B
end
* print
  cdf (series; 0.05)
  eval (series; 0.05)  0.5  1.5  0.5
  end
```

e.g. Aircraft flight control system



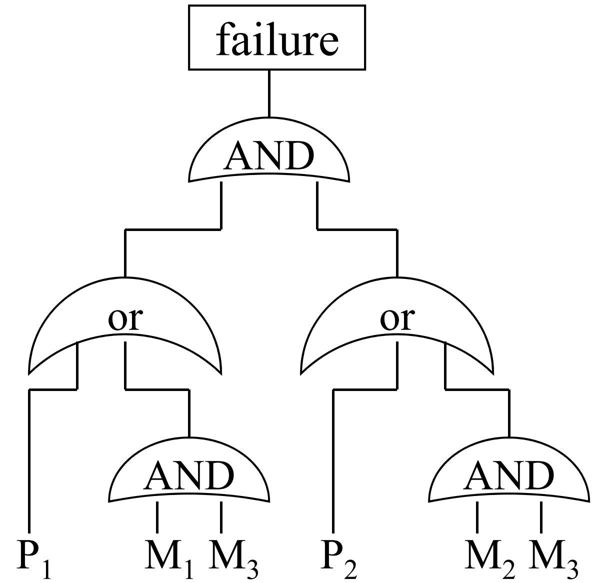

```
bind
mIRS    0.000015
mPRS    0.00099
mSA     0.000037
mCS     0.00048       * most susceptible to failure
end                   * ∴ use 4 CS components
ftree   aircraft
basic   IRS    exp (mIRS)
basic   PRS    exp (mPRS)
          :
kofn    IRS23    2, 3, IRS
kofn    PRS23    2, 3, PRS
        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

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

Fault Trees using SHARPE with repeated components

Ex: also see the example in *Fig. 9.22*

Ex:



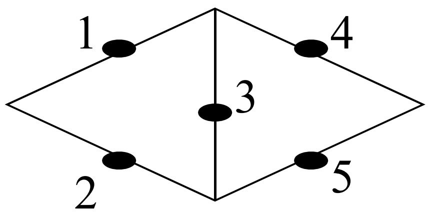

```
ftree   system
basic   P1   exp (lambda P1)
basic   P2   exp (lambda P2)
basic   M1   exp (lambda M1)
basic   M2   exp (lambda M2)
repeat  M3   exp (lambda M3)
AND     M1M3   M1   M3
AND     M2M3   M2   M3
OR      system1   P1   M1M3
OR      system2   P2   M2M3
AND     top   system1   system2
end
* print reliability at time t
  expr 1-value ( t; system)
```

≡ kofn $system_1$ 1, 2, P_1 M_1M_3

≡ kofn top 2, 2, $system_1$ $system_2$

Series-Parallel Block Diagrams with Components in common
(Also called Network Reliability Models)

e.g.



Can be arranged as

A parallel connection of series structures

A series connection of parallel structures

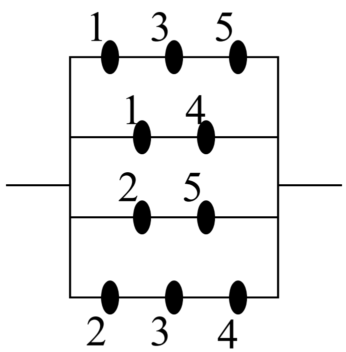
Definition: a minimal path (set) is a minimal set of components whose functioning ensures the functioning of the system.

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

Q: how many minimal path sets?

A: 4: {1,3,5},{1,4},{2,5},{2,3,4}

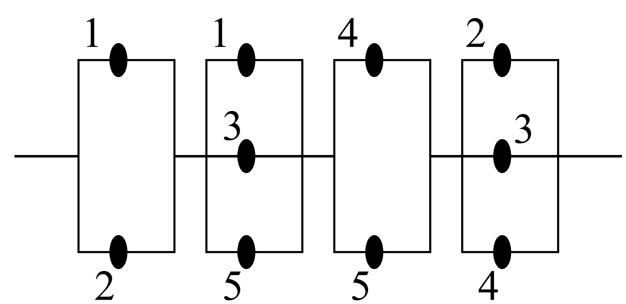
Use parallel connection



Q: how many minimal cut sets?

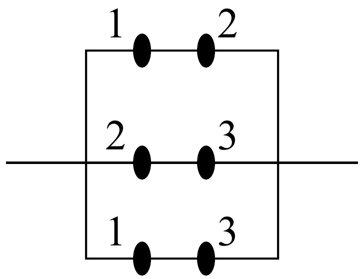
A: 4: {1,2},{4,5},{1,3,5},{2,3,4}

Connect them in series



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

$$\begin{cases} \varphi(t) = 1 & \text{if alive} \\ \varphi(t) = 0 & \text{if dead} \end{cases}$$

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

$$\begin{cases} \mathrm{X}i(t) = 1 & \text{if alive} \\ \mathrm{X}i(t) = 0 & \text{if dead} \end{cases}$$

$$\begin{aligned} \varphi(t) &= 1 - [(1 - X1X2)(1 - X2X3)(1 - X1X3)] \\ &= 1 - (1 - X1X2 - X2X3 - X1X3 + X1X_2^2X3 + X1X2X_3^2 + X_1^2X2X3 - X_1^2X_2^2X_3^2) \\ &= 1 - (1 - X1X2 - X2X3 - X1X3 + 2X1X2X3) \end{aligned}$$

Due to $X_i^2 = X_i$ from X_i's definition

Now

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

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

$$\Rightarrow E[\phi(t)] = E[X_1 \underbrace{X_2 + X_2 X_3 + X_1 X_3 - 2 X_1 X_2 X_3]}_{\text{Terms each contain only independent components}}$$

$$= E[X_1 X_2] + E[X_2 X_3] + E[X_1 X_3] - 2E[X_1 X_2 X_3]$$

$$\therefore \boxed{R_{system} = R_1 R_2 + R_2 R_3 + R_1 R_3 - 2 R_1 R_2 R_3}$$

For identical components, $R_1=R_2=R_3$, $R_{system}=3R^2-2R^3$

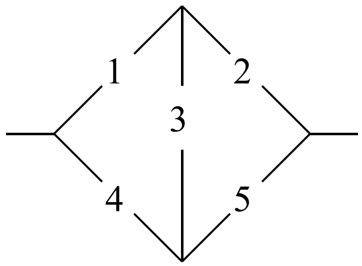
Modeling with a Reliability Graph

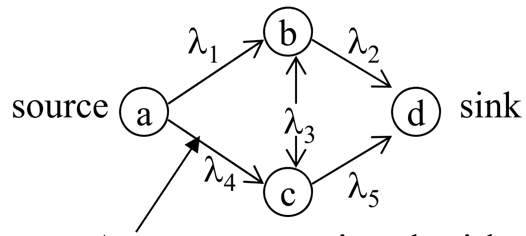
* A reliability graph consists of nodes & directed arcs.
  - source node — no arcs enter it
  - target (sink) node — no arcs leave it

* 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)

e.g.,





Arcs are associated with exponential distributions with rates λ_i's

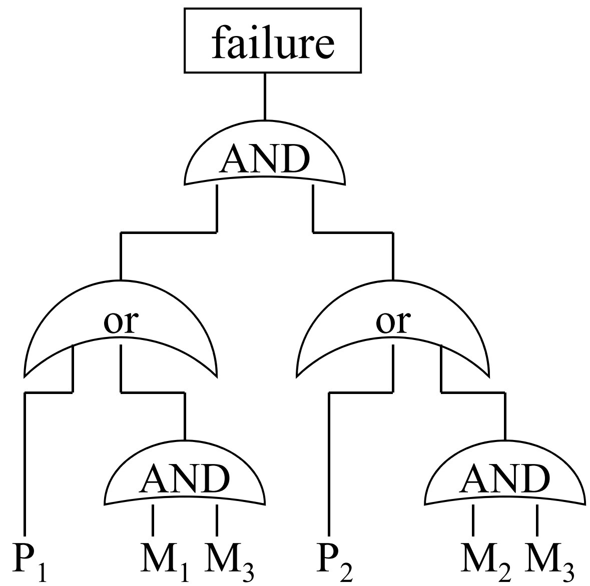
relgraph bridge(v1, v2, v3, v4, v5)
a b exp(v1)
a c exp(v4)
b d exp(v2)
c d exp(v5)
bidirect
b c exp(v3)
end
* print
cdf (bridge; $\lambda_1,\lambda_2,\lambda_3,\lambda_4,\lambda_5$)
pqcdf (bridge; $\lambda_1,\lambda_2,\lambda_3,\lambda_4,\lambda_5$)
end

output for pqcdf (bridge; $\lambda_1,\lambda_2,\lambda_3,\lambda_4,\lambda_5$):

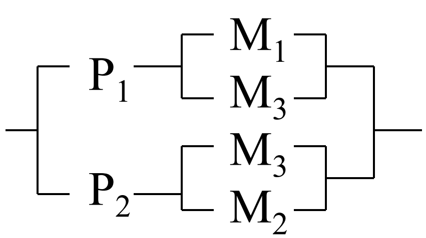
1-([P(0:a,b)*P(1:b,d)]
meaning $1 - e^{-\lambda_1 t} e^{-\lambda_2 t}$
+[P(2:a,c)*P(3:c,d)*(1-P(0:a,b)*P(1:b,d))]
+[P(0;a,b)*Q(1:b,d)*Q(2:a,c)*P(3:c,d)*P(4:b,c)]
+[Q(0:a,b)*P(1:b,d)*P(2:a,c)*Q(3:c,d)*P(4:b,c)]
meaning $(1-e^{-\lambda_1 t})$

The underlying technique for solving the model is minimal path set & minimal cut set.

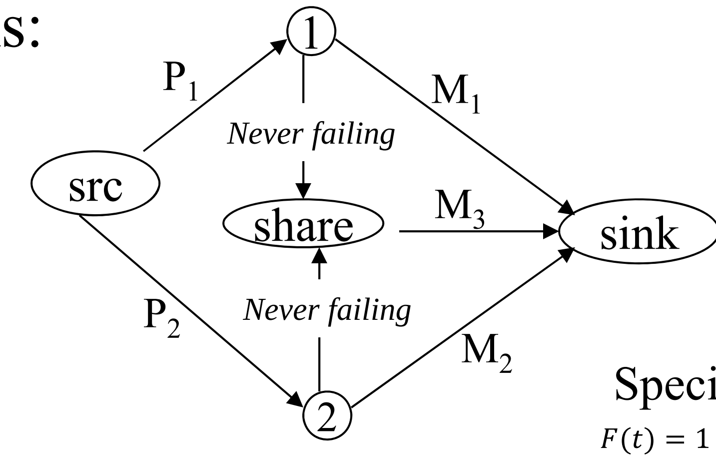
What is the reliability graph corresponding to the fault tree model on the left?



$\equiv$



Ans:



Specifying $F(t) = 1 - e^{-\lambda P1t}$ for P_1

Sharpe code:

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

This means $1 \rightarrow$ share & $2 \rightarrow$ share links never fail

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