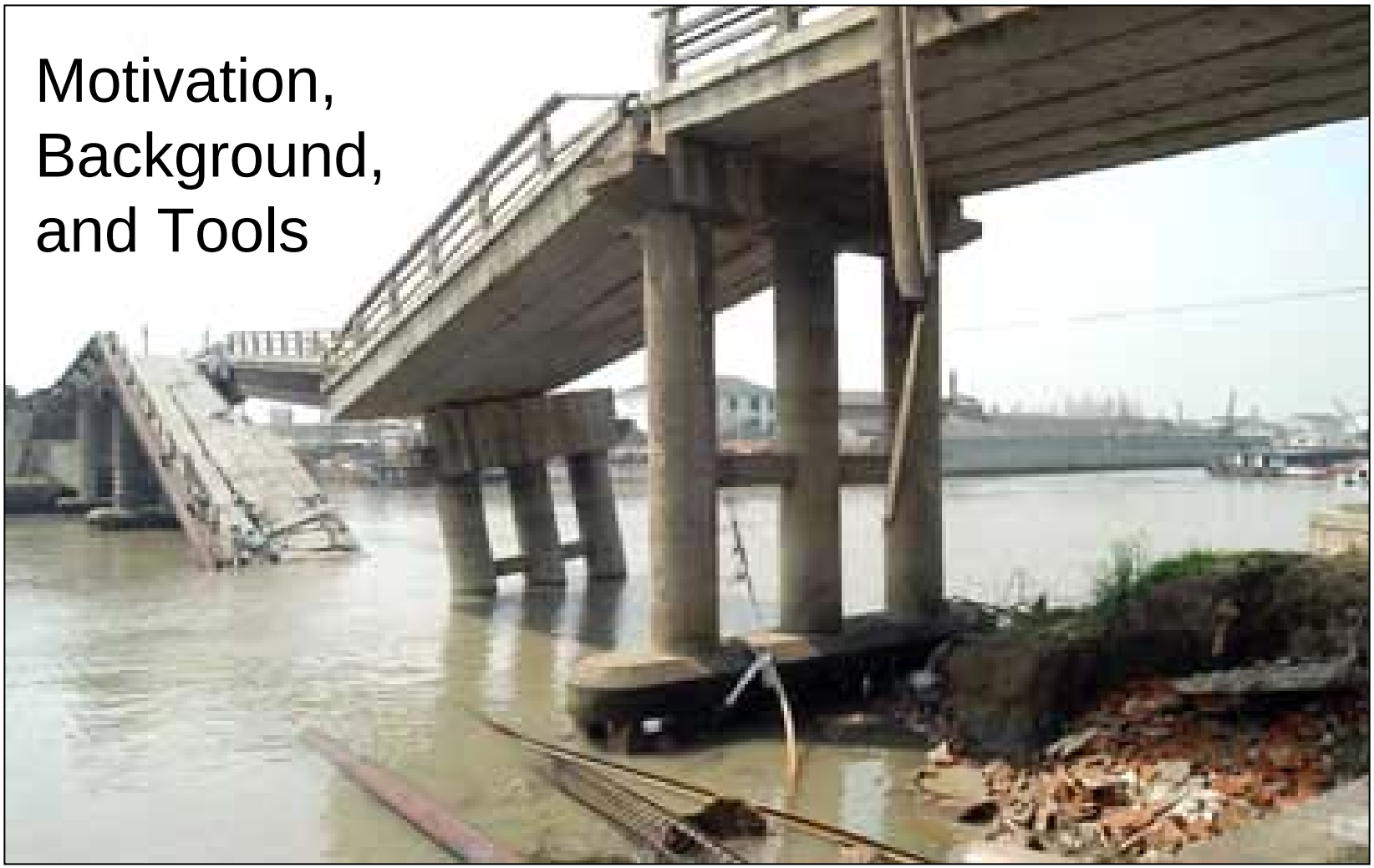
Fault-Tolerant Computing



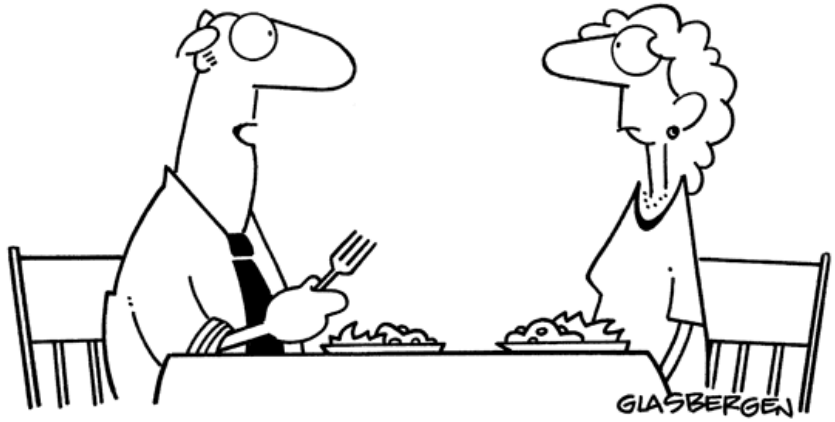
About This Presentation

This presentation has been prepared for the graduate course ECE 257A (Fault-Tolerant Computing) by Behrooz Parhami, Professor of Electrical and Computer Engineering at University of California, Santa Barbara. The material contained herein can be used freely in classroom teaching or any other educational setting. Unauthorized uses are prohibited. © Behrooz Parhami

Edition	Released	Revised	Revised
First	Oct. 2006		

State-Space Modeling

"It's the latest innovation in office safety.
When your computer crashes, an air bag is activated
so you won't bang your head in frustration."



"An amazing thing happened at work today. For 8 minutes, my computer and I were both functional at the same time!"

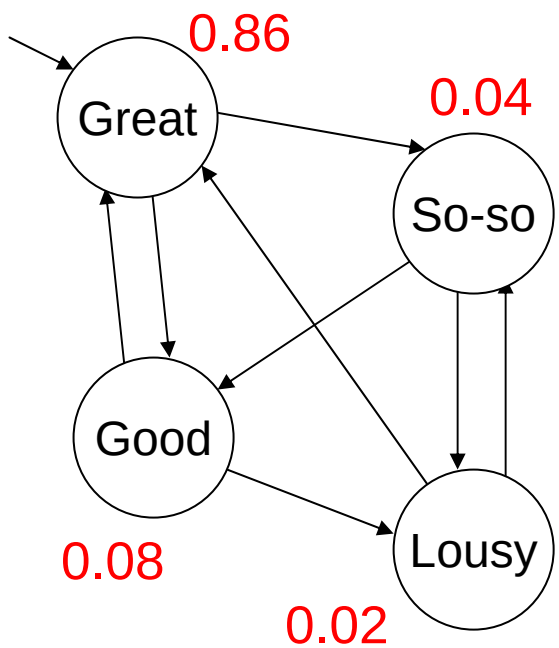
What Is State-Space Modeling?

With respect to availability of resources and computational capabilities, a system can be viewed as being in one of several possible states

The number of states can be large, if we want to make fine distinctions, or it can be relatively small if we lump similar states together

State transitions:
System moves from one state to another as resource availability and computational power change due to various events

State-space modeling entails quantifying transition probabilities so as to determine the probability of the system being in each state; from this, we derive reliability, availability, safety, and other desired parameters



Markov Chains

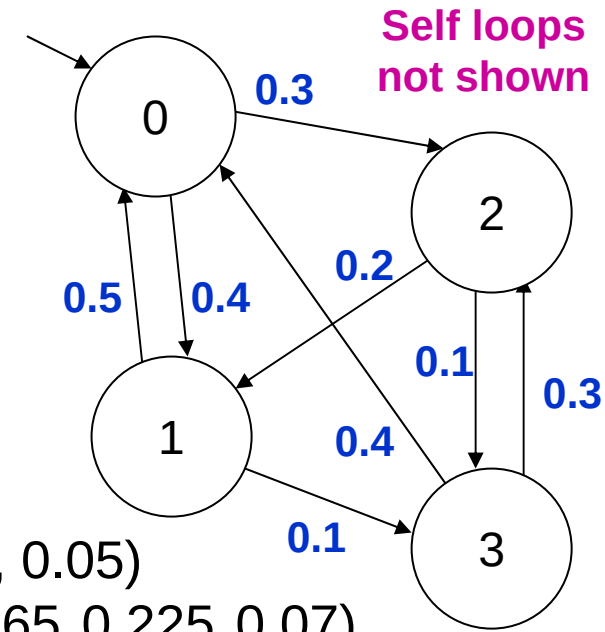
Represented by a state diagram with transition probabilities
Sum of all transition probabilities out of each state is 1

The state of the system is characterized by the vector (s_0, s_1, s_2, s_3)
(1, 0, 0, 0) means that the system is in state 0 Must sum to 1
(0.5, 0.5, 0, 0) means that the system is in state 0 or 1 with equal prob's
(0.25, 0.25, 0.25, 0.25) represents complete uncertainty

Transition matrix: $M =$

$$\begin{pmatrix} 0.3 & 0.4 & 0.3 & 0 \\ 0.5 & 0.4 & 0 & 0.1 \\ 0 & 0.2 & 0.7 & 0.1 \\ 0.4 & 0 & 0.3 & 0.3 \end{pmatrix}$$

Markov matrix
(rows sum to 1)



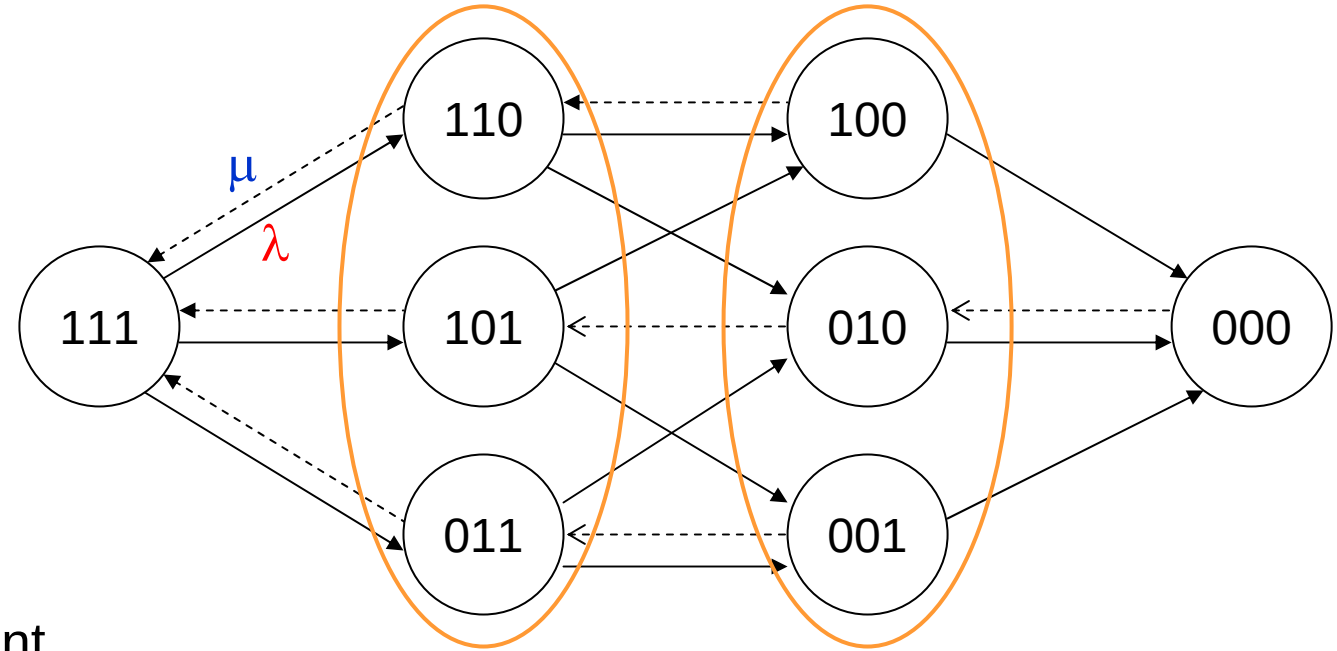
$s(t + 1) = s(t)\, M$
$s(t + h) = s(t)\, M^h$

Example:
$(s_0, s_1, s_2, s_3) = (0.5, 0.5, 0, 0)\, M = (0.4, 0.4, 0.15, 0.05)$
$(s_0, s_1, s_2, s_3) = (0.4, 0.4, 0.15, 0.05)\, M = (0.34, 0.365, 0.225, 0.07)$

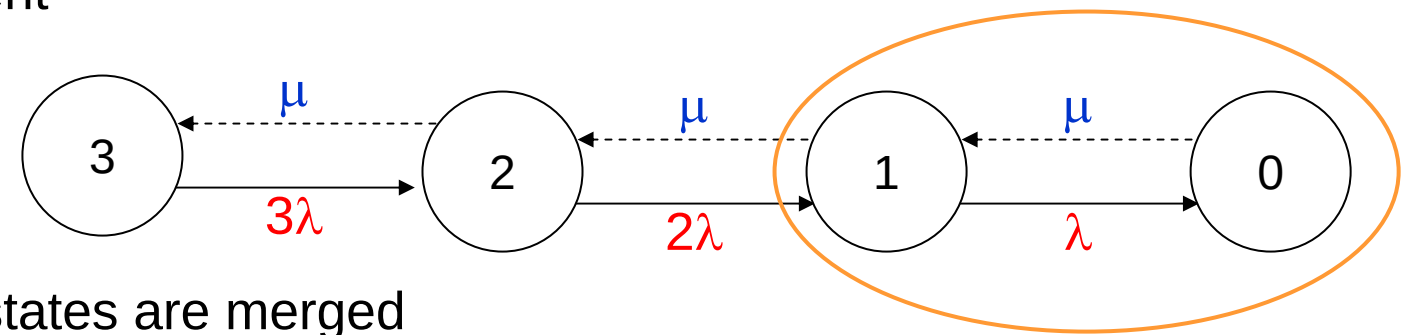
Merging States in a Markov Model

There are three identical units
1 = Unit is up
0 = Unit is down

All solid lines λ
Dashed lines μ



Simpler equivalent model for 3-unit fail-soft system



Failed state if TMR

Whether or not states are merged depends on the model's semantics

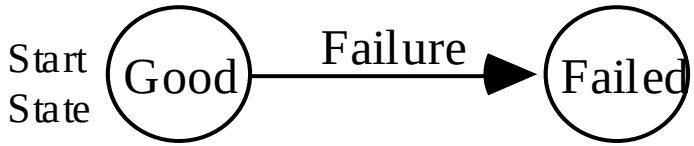
Two-State Nonrepairable Systems

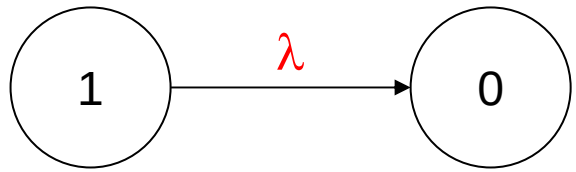
Rate of change for the probability of being in state 1 is $-\lambda$

$$p'_1 = -\lambda p_1$$
$$p_1 + p_0 = 1$$

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

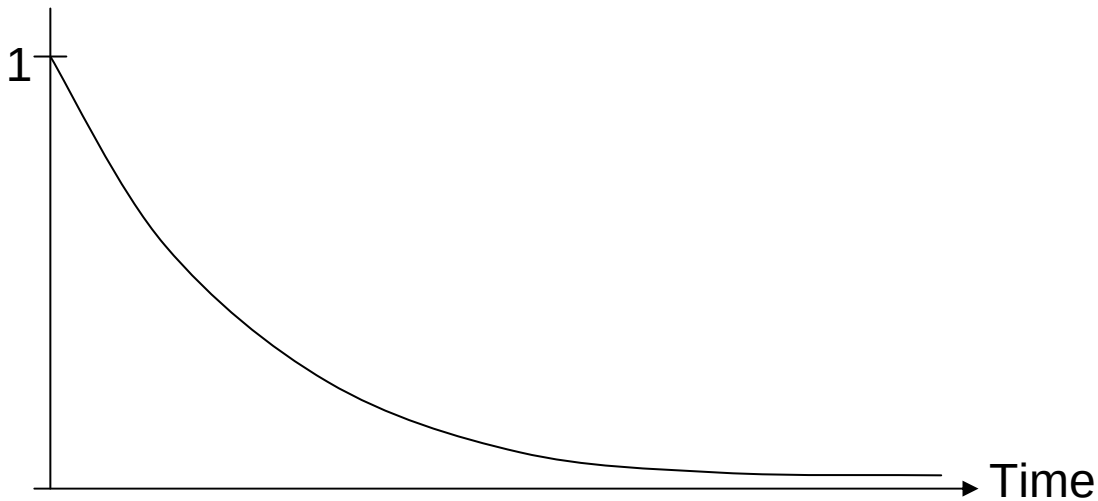
Initial condition: $p_1(0) = 1$





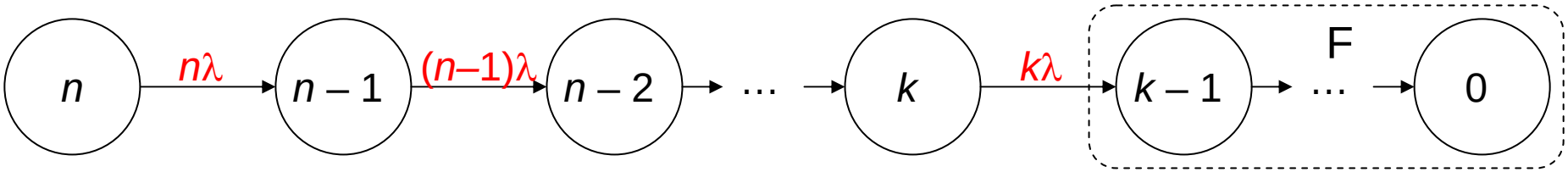
Reliability as a function of time:

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



The label λ on this transition means that over time dt, the transition will occur with probability λdt (we are dealing with a continuous-time Markov model)

k-out-of-*n* Nonrepairable Systems



$$p'_n = -n\lambda p_n$$
$$p'_{n-1} = n\lambda p_n - (n-1)\lambda p_{n-1}$$
$$\vdots$$
$$p'_k = (k+1)\lambda p_{k+1} - k\lambda p_k$$
$$p_n + p_{n-1} + \ldots + p_k + p_F = 1$$

$$p_n = e^{-n\lambda t} \qquad \text{Initial condition: } p_n(0) = 1$$
$$p_1 = ne^{-(n-1)\lambda t}(1 - e^{-\lambda t})$$
$$\vdots$$
$$p_k = \binom{n}{k} e^{-(n-k)\lambda t}(1 - e^{-\lambda t})^k$$
$$p_F = 1 - \sum_{j=k \text{ to } n} p_j$$

In this case, we do not need to resort to more general method of solving linear differential equations (LaPlace transform, to be introduced later)

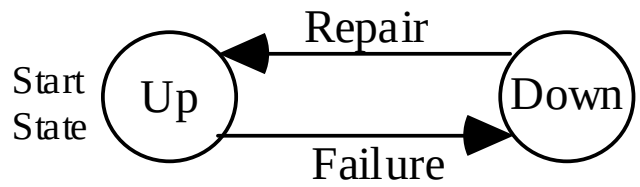
The first equation is solvable directly, and each additional equation introduces only one new variable

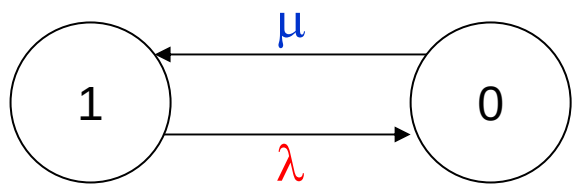
Two-State Repairable Systems

In steady state (equilibrium), transitions into/out-of each state must "balance out"

$$-\lambda p_1 + \mu p_0 = 0$$
$$p_1 + p_0 = 1$$

$$\Rightarrow \quad p_1 = \mu/(\lambda + \mu)$$
$$p_0 = \lambda/(\lambda + \mu)$$

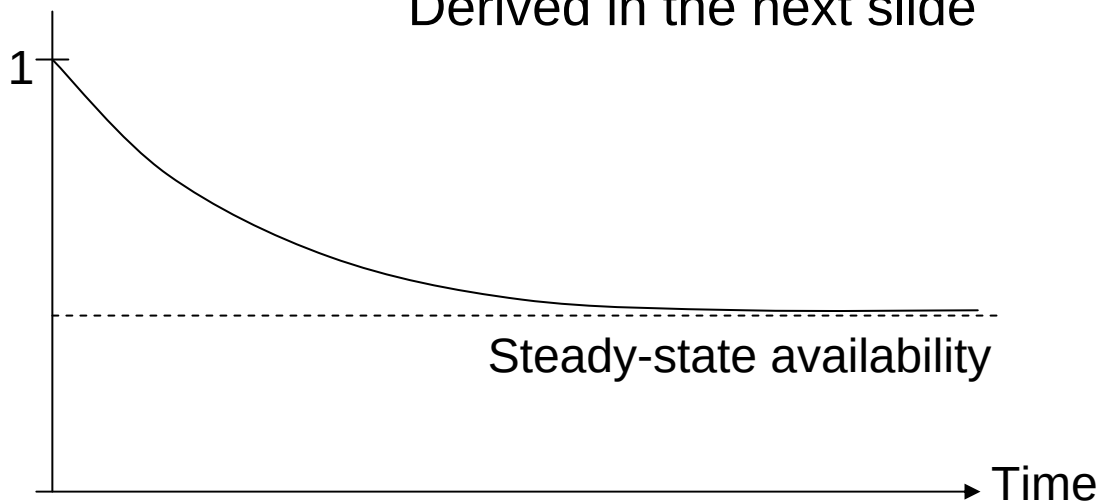




Availability as a function of time:

$A(t) = p_1(t) = \mu/(\lambda + \mu) + \lambda/(\lambda + \mu)\, e^{-(\lambda+\mu)t}$

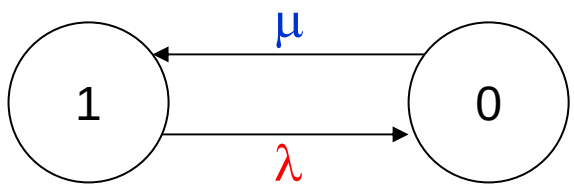
Derived in the next slide



The label μ on this transition means that over time dt, repair will occur with probability μdt (constant repair rate as well as constant failure rate)

Solving the State Differential Equations

$$p'_1(t) = -\lambda p_1(t) + \mu p_0(t)$$
$$p'_0(t) = -\mu p_0(t) + \lambda p_1(t)$$



To solve linear differential equations with constant coefficients:
1. Convert to algebraic equations using LaPlace transform
2. Solve the algebraic equations
3. Use inverse LaPlace transform to find original solutions

$$sP_1(s) - \cancel{p_1(0)}^{1} = -\lambda P_1(s) + \mu P_0(s)$$
$$sP_0(s) - \cancel{p_0(0)}_{0} = -\mu P_0(s) + \lambda P_1(s)$$

$$P_1(s) = (s + \mu) / [s^2 + (\lambda + \mu)s]$$
$$P_0(s) = \lambda / [s^2 + (\lambda + \mu)s]$$

$$p_1(t) = \mu/(\lambda + \mu) + \lambda/(\lambda + \mu)\, e^{-(\lambda+\mu)t}$$
$$p_0(t) = \lambda/(\lambda + \mu) - \lambda/(\lambda + \mu)\, e^{-(\lambda+\mu)t}$$

LaPlace Transform Table

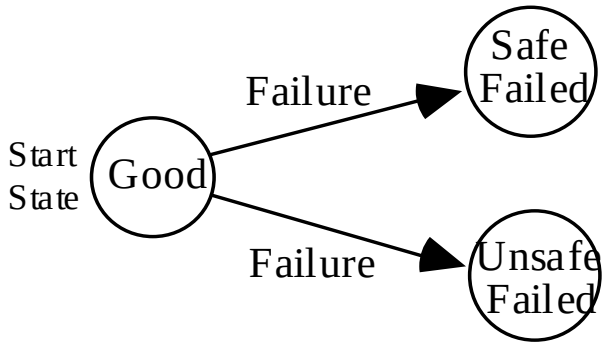
$h(t)$	$H(s)$
k	k/s
e^{-at}	$1/(s + a)$
$t^{n-1}e^{-at}/(n-1)!$	$1/(s + a)^n$
$k\,h(t)$	$k\,H(s)$
$h(t) + g(t)$	$H(s) + G(s)$
$h'(t)$	$sH(s) - h(0)$

Systems with Multiple Failure States

In steady state (equilibrium), transitions into/out-of each state must "balance out"

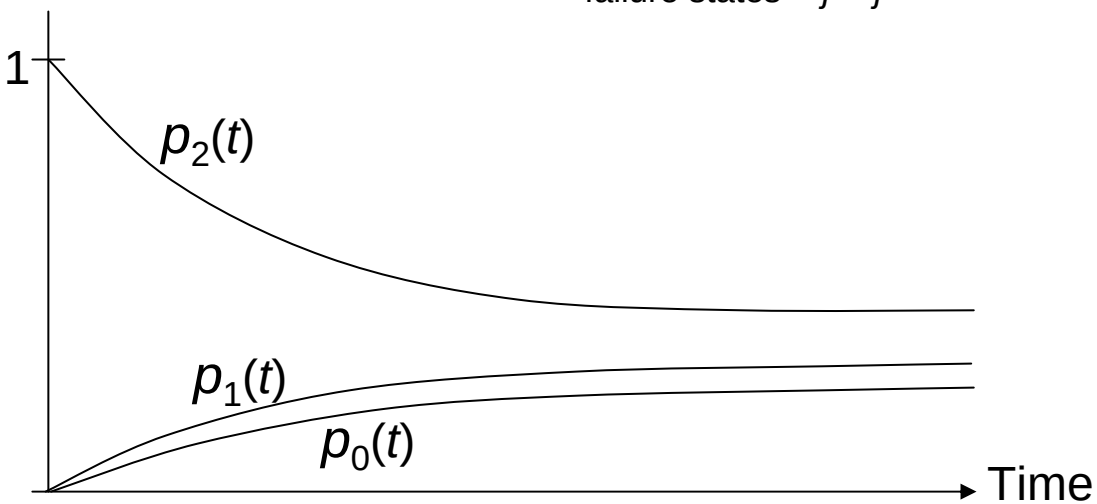
$$-\lambda p_2 + \mu p_1 + \mu p_0 = 0$$
$$-\mu p_1 + \lambda_1 p_2 = 0$$
$$p_2 + p_1 + p_0 = 1$$

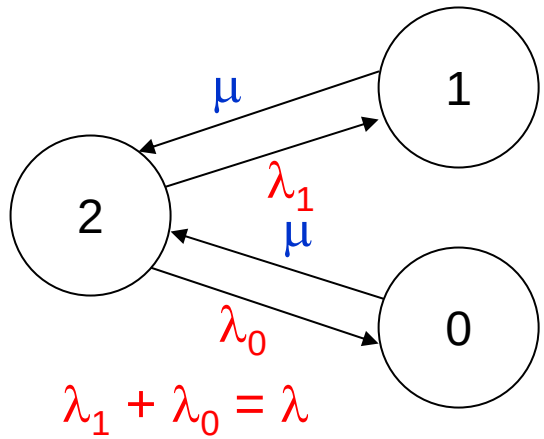
$$p_2 = \mu/(\lambda + \mu)$$
$$p_1 = \lambda_1/(\lambda + \mu)$$
$$p_0 = \lambda_0/(\lambda + \mu)$$



Safety evaluation:

Total risk of system is $\Sigma_{\text{failure states}}\ c_j\ p_j$



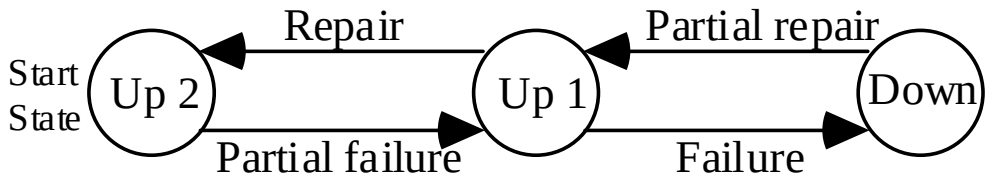


$\lambda_1 + \lambda_0 = \lambda$

Failure state j has a cost (penalty) c_j associated with it

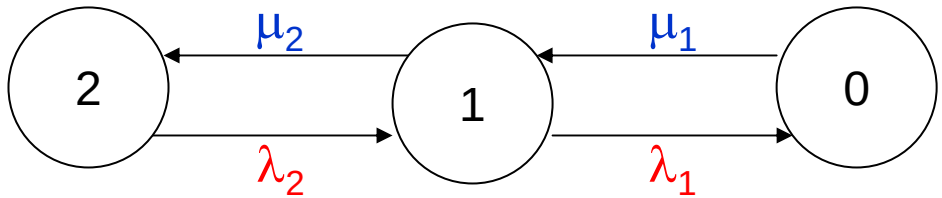
Systems with Multiple Operational States

$-\lambda_2 p_2 + \mu_2 p_1 = 0$
$\lambda_1 p_1 - \mu_1 p_0 = 0$
$p_2 + p_1 + p_0 = 1$



Let $\delta = 1/[1 + \lambda_2/\mu_2 + \lambda_1\lambda_2/(\mu_1\mu_2)]$

$p_2 = \delta$
$p_1 = \delta\lambda_2/\mu_2$
$p_0 = \delta\lambda_1\lambda_2/(\mu_1\mu_2)$



Operational state j has a benefit b_j associated with it

Performability evaluation:

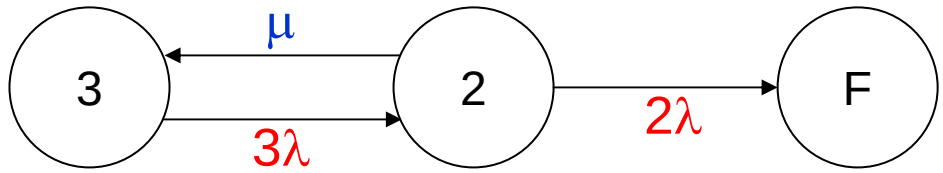
Performability = $\sum_{\text{operational states}} b_j\, p_j$

Example: $\lambda_2 = 2\lambda$, $\lambda_1 = \lambda$, $\mu_1 = \mu_2 = \mu$ (single repairperson or facility), $b_2 = 2$, $b_1 = 1$, $b_0 = 0$

$P = 2p_2 + p_1 = 2\delta + 2\delta\lambda/\mu = 2(1 + \lambda/\mu)/(1 + 2\lambda/\mu + 2\lambda^2/\mu^2)$

TMR System with Repair

$-3\lambda p_3 + \mu p_2 = 0$
$-(\mu + 2\lambda)p_2 + 3\lambda p_3 = 0$
$p_3 + p_2 + p_F = 1$



Steady-state analysis of no use
$p_3 = p_2 = 0$, $p_F = 1$

Assume the voter is perfect
Upon first module malfunction, we switch to duplex operation with comparison

Mean time to failure evaluation:

See [Siew92], pp. 335-336, for derivation

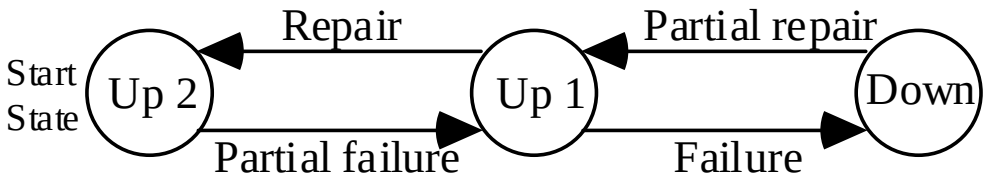
$$\text{MTTF} = 5/(6\lambda) + \mu/(6\lambda^2) = [5/(6\lambda)](1 + 0.2\mu/\lambda)$$

MTTF for TMR | Improvement due to repair | Improvement factor

MTTF Comparisons	($\lambda = 10^{-6}$/hr, $\mu = 0.1$/hr)	
Nonredundant	$1/\lambda$	1 M hr
TMR	$5/(6\lambda)$	0.833 M hr
TMR with repair	$[5/(6\lambda)](1 + 0.2\mu/\lambda)$	16,668 M hr

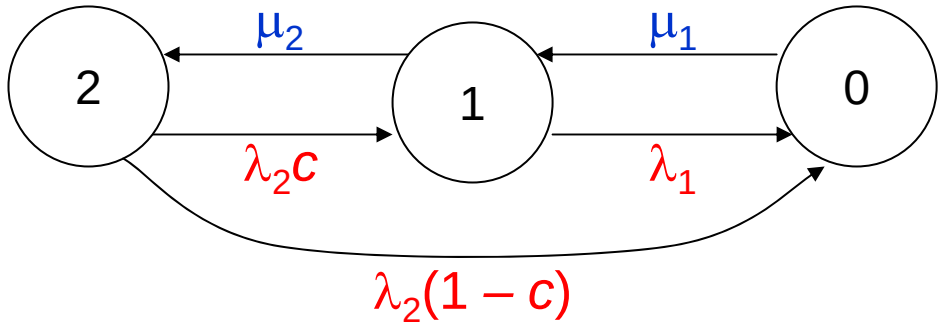
Fail-Soft System with Imperfect Coverage

$-\lambda_2 p_2 + \mu_2 p_1 = 0$
$\lambda_2(1-c)p_2 + \lambda_1 p_1 - \mu_1 p_0 = 0$
$p_2 + p_1 + p_0 = 1$



We solve this in the special case of $\lambda_2 = 2\lambda$, $\lambda_1 = \lambda$, $\mu_2 = \mu_1 = \mu$

Let $\rho = \lambda/\mu$ and
$\theta = 1/(1 + 4\rho - 2c\rho + 2\rho^2)$



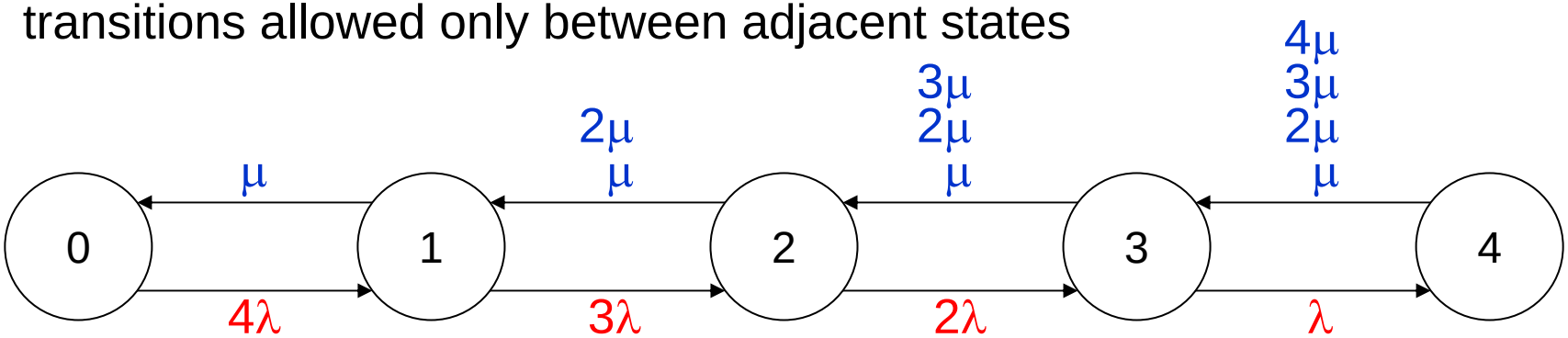
If malfunction of one unit goes undetected, the system fails

$p_2 = \theta$
$p_1 = 2\rho\theta$
$p_0 = 2\rho(1 - c + \rho)\theta$

We can also consider coverage for the repair direction

Birth-and-Death Processes

Special case of Markov model with states appearing in a chain and transitions allowed only between adjacent states



This model is used in queuing theory, where the customers' arrival rate and provider's service rate determine the queue size and waiting time

Closed-form expression for state probabilities can be found, assuming $n + 1$ states and s service providers (repair persons): M/M/s/n/n queue

$$p_j = (n - j + 1)(\lambda/\mu)p_{j-1}/j \quad \text{for } j = 1, 2, \ldots, r$$

$$p_j = (n - j + 1)(\lambda/\mu)p_{j-1}/r \quad \text{for } j = r + 1, r + 2, \ldots, n$$

Equation for p_0 [Siew92], p. 347

The Dependability Modeling Process

Choose modeling approach
- Combinational
- State-space

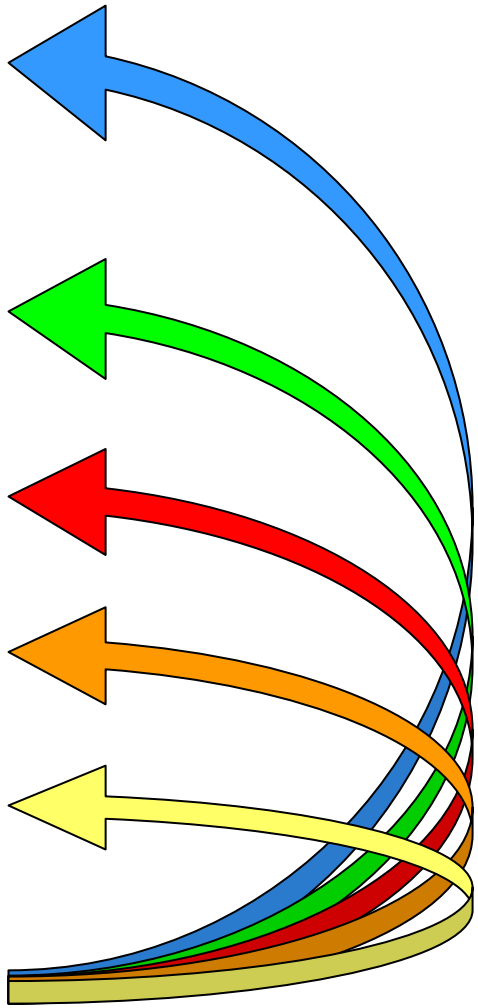
Construct model

Derive model parameters

Solve model

Interpret results

Validate model and results



Iterate until results are satisfactory

Software Aids for Reliability Modeling

Relex (company specializing in reliability engineering)
- Reliability block diagram: http://www.relex.com/products/rbd.asp
- Markov: http://www.relex.com/products/markov.asp

University of Virginia
- Galileo: http://www.cs.virginia.edu/~ftree/2003-redesign/pages/Software/index.html

Iowa State University
- HIMAP:

See Appendix D, pp. 504-518, of [Shoo02] for more programs

Dept. of Mechanical Engineering, Univ. of Maryland:
- List of reliability engineering tools: http://www.enre.umd.edu/tools.htm