Lecture 08

Software Repairability and Availability

Software Repairability

- Two kind of software
  - Reairable
    - i.e. Batch fortran program
  - Unrepairable
    - i.e. Computer controlled air traffic control system
- Repair of software
  - Debugging
  - Error correction
  - Reinitialization
- Down Time
- Up Time

Software Repairability

- Repairability and Availability of repairable software (any systems) is based on the concept of error correction and software reinitialization

- Repair rate : is average rate measured in corrections per hour for a complete repair

- Complete repair time : (i) recognition of the problem
  (ii) diagnosis of the problem
  (iii) correction of the error
  (iv) testing
  (v) reinitialization

Software Repairability

- Effect of repair on system reliability :

- Ex. Let, two computer with independent redundant program and also let, they have no repair capabilities

  In case of system failure requires the simultaneous occurrence of 3 events, (i) failure of prog1 (ii) failure of prog2 and (iii) inability to repair prog1 before prog2 fails.

Availability

- Definition :is the probability that the program is performing successfully, according to specifications, at a given point in time.

- Reliability means no failures in the interval 0 to t

- Availability means only that the system is up at time t

- Example of availability,
  - 100 identical computers, all with same operating systems (i.e. same release, configuration, h/w, s/w corrections etc.) and similar or equivalent input streams (regardless of variety, load, feature used etc.)
  - Same instant we inspect all the installations, find 97 are up and 3 are down

Availability

- So, Availability = 97/100

- By repeating the same process, in a life testing of a software, we get correct estimation of availability

- From life testing of a software (repairable)

- Suppose we get downtime such as $t_{d_{1}}, t_{d_{2}}, \ldots, t_{d_{n}}$

  and uptime such as $t_{u_{1}}, t_{u_{2}}, \ldots, t_{u_{n}}$

- Availability, $A_{ss} = T_{up} / T_{up} + T_{down}$ where $T_{up} = \sum t_{u_i}$ and $T_{down} = \sum t_{d_i}$

- So, two way availability can be defined,
  1) the ratio of systems up at some instant to the size of the population studied
  2) the ratio of observed uptime to the sum of the uptime and downtime

Availability

- Useful needs of availability,
  - to quantify the present level of availability and compare it with other systems or stated goal.
  - to track the availability over a time period to see if it is increases as errors are removed or possibly decreases as more and more complex input streams are applied and excite lurking residual errors.
  - planning for adequate repair personnel, facilities (mainly test time for software and replacement parts or units for h/w) and alternative services if necessary during downtime.
- So, availability is actual time function, it has the value of unity at time zero and decreases to some steady-state value after several failure repair cycles.
- To estimates the system availability during design

$$A_{SS} = MTTF / MTTF + MTTR$$

Availability Model (Markov Model)

- Mathematical technique generally used to model system availability
- Measure the performance of any system
- Properties :
  - 4 kind of Markov probability models
  - M(x,t) where x is state and t is time of obsrvation ; both are random variable
- 4 kind of combination possible
  - Discrete state –discrete time (Markov chain) model
  - Discrete state –continuous time (Markov process) model

Availability Model (Markov Model)

- Any Markov model is defined by a set of probabilities, Pij (probability of transition from any state i to any state j)

- Markov process (Poisson process) model
  - is a stochastic process in which events occur continuously and independently of one another

- Basic assumptions(which are necessary in deriving a poisson process model :
  1. The probability that a transition occurs from the state of n occurrences to the state of n+1 occurrences in time Δt as $\lambda \Delta t$. The parameter λ is a constant and has dimensions of occurrences per unit time. The occurrences are irreversible.
  2. Each occurrence is independent of all other occurrences.
  3. The transition probability of two or more occurrences in interval Δt is negligible. $(\lambda \Delta t)(\lambda \Delta t)$

Availability Model (Markov Model)

- To solve the probability of n occurrences in time t,

$$P(X = n, t) \equiv P_n(t)$$

- Case I : Zero occurrences at time $t + \Delta t$

$$P_0(t + \Delta t) = (1 - \lambda \Delta t) P_0(t)$$

Probability that zero occurrences at time $t + \Delta t$

Prob. No. of occurrences in interval Δt

Prob. Of zero occurrences at time t

- Case II : One occurrences at time $t + \Delta t$

$$P_1(t + \Delta t) = (\lambda \Delta t) P_0(t) + (1 - \lambda \Delta t) P_1(t)$$

Availability Model (Markov Model)

- Generalized,

$$P_n(t+\Delta t) = (\lambda\Delta t)P_{n-1}(t) + (1-\lambda\Delta t)P_n(t) \qquad for \quad n = 0,1,2,.....$$

$$\left\lfloor P_n(t+\Delta t) - P_n(t) \right\rfloor / \Delta t = \left\lfloor \lambda P_{n-1}(t) - \lambda P_n(t) \right\rfloor$$

$$dP_n(t)/dt = \lambda P_{n-1}(t) - \lambda P_n(t)$$

- Initial condition, t=0; n=0

$$P_0(0) = 1 \qquad P_1(0) = P_2(0) = \quad = P_n(0) = 0$$

Markov Reliability and Availability Models:

- Failure and repair complicates the direct calculation of elements reliability and availability

- There is three approach,

  1. Failure hazards (z(t)) and repair hazards (w(t)) are constant
  2. Using joint density function
  3. Using integration

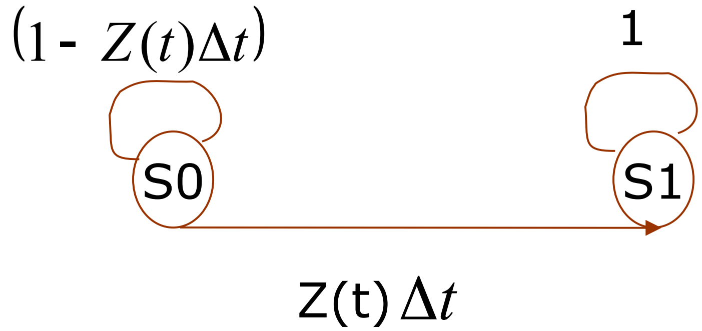
Markov Reliability Model:

- Continuous time and discrete state model
- All mutually exclusive state
- The system composed of

non-repairable element X1

- Two possible states :
  - S0=X1, when elements are good
  - S1=X1′, when elements are bad
- At t=0; initial state

equilibrium is final state



Initial State	Final State	
	S0	S1
S0	1-Z(t) Δt	Z(t) Δt
S1	0	1

State transition table

Markov Reliability Model:

- The transition probability must obey the rules :
  1. $Z(t)\Delta t$ is the transition probability at Δt ,If Z(t)=λ constant then model is called homogeneous. Otherwise non-homogeneous (if time function)
  2. Probability of more than one is neglected due to higher order of Δt

Probability of being in state S0 at time $t + \Delta t$

$$P_{S0}(t+\Delta t) = \left[1 - Z(t)\Delta t\right] P_{S0}(t) + 0.P_{S1}(t)$$

No failure in time Δt

Probability that the system is in state S0, at time t

Probability of repair in time Δt

Probability of being in state S1 at time t

Markov Reliability Model:

- Similarly, Probability of being in state S0 at time $t+\Delta t$

$$P_{S1}(t+\Delta t) = \left[Z(t)\Delta t\right] P_{S0}(t) + 1.P_{S1}(t)$$

- From the first equation we get,

$$\left[P_{S0}(t+\Delta t) - P_{S0}(t)\right] / \Delta t = -Z(t) P_{S0}(t)$$

$$dP_{S0}(t) / dt = -Z(t) P_{S0}(t)$$

$$dP_{S0}(t) / P_{S0}(t) = -Z(t) dt$$

$$\ln P_{S0}(t) = -\int Z(t) dt + k$$

$$P_{S0}(t) = k1 \exp\left[-\int Z(t) dt\right]$$

$$R(t) = P_{S0}(t) = \exp\left[-\int_0^t Z(t) dt\right]$$

Markov Reliability Model:

- Similarly,

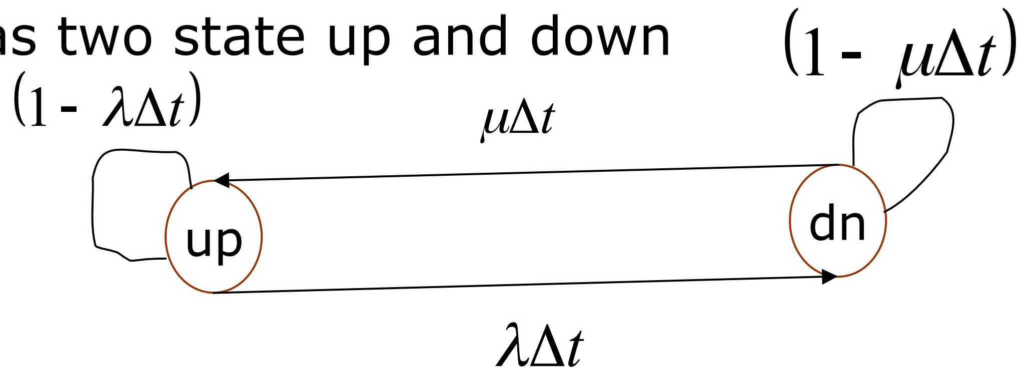
$$P_{S1}(t) = 1 - e^{-\int_0^t z(t)dt}$$

- So at any time, $P_{S0}(t) + P_{S1}(t) = 1$

Markov Availability Model:

- Availability, A(t)= Probability that the system is remain successful at a given time t / software is up at time t, regardless up or down at time t=0

- Consider the system has two state up and down



1. Failure rate = λ
2. Repair rate = μ

(i) $\lambda\Delta t \equiv$ Transition probability from up→down at Δt

(ii) $\mu\Delta t \equiv$ Transition probability from down→up at Δt

assume, $\Delta t \rightarrow 0$

Markov Availability Model:

$P_u(t) =$ Probability that the system is up at time t

$P_d(t) =$ Probability that the system is down at time t

$P_u(t+\Delta t) =$ Probability that the system is up at time $t+\Delta t$

$P_d(t+\Delta t) =$ Probability that the system is down at time $t+\Delta t$

- At any point of time, $P_u(t) + P_d(t) = 1$

$$P_u(t+\Delta t) = P_u(t)(1 - \lambda\Delta t) + P_d(t)\mu\Delta t \qquad (1)$$

$$P_d(t+\Delta t) = P_d(t)(1 - \mu\Delta t) + P_u(t)\lambda\Delta t \qquad (2)$$

Markov Availability Model:

- From equation (1),

$$\left\{ P_d(t+\Delta t) - P_u(t) \right\} / \Delta t = \mu - P_u(t)(\mu + \lambda)$$

$$dP_u(t)/dt + P_u(t)(\mu + \lambda) = \mu \qquad \left[\text{Taking} \overset{\text{Multiply}}{} \; \overset{e^{(\mu+\lambda)t}}{\text{Limit}} / \Delta t -> 0 \right]$$

$$\int d\left[P_u(t)\, e^{(\mu+\lambda)t} \right] = \int \mu e^{(\mu+\lambda)t} dt \qquad \left[\text{Integrating} \right]$$

$$P_u(t)\, e^{(\mu+\lambda)t} = \mu e^{(\mu+\lambda)t} / (\mu + \lambda) + k$$

$$at\ t \to 0: \ P_u(0) \to 1 \qquad k = \lambda / (\mu + \lambda)$$

Markov Availability Model

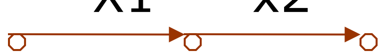
$$A(t) = P_u(t) = \mu/(\mu+\lambda) + \lambda e^{-(\mu+\lambda)t}/(\mu+\lambda)$$

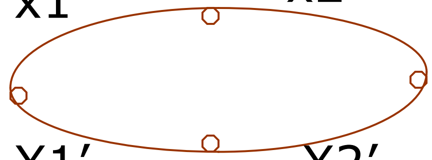
At Steady state, $t \to \infty$: $e^{-(\mu+\lambda)t} \to 0$

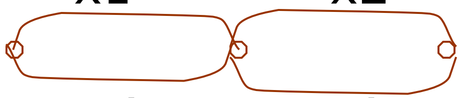
$$A_{SS}(t) = \mu/(\mu+\lambda)$$

Redundancy

- To improve the system reliability, creation of new parallel paths
- Connect a duplicate in parallel
- Ex. Automatic break system- install a duplicate set of break shoes
  1. Unit redundancy
  2. Component redundancy







$$R_a(P) = P(x_1)P(x_2) = P^2$$

$$R_b(P) = P(x_1x_2 + x_1'x_2') = 2R_a - R_a{}^2 = P^2(2 - P^2)$$

$$R_c(P) = P(x_1 + x_1')P(x_2 + x_2')$$

$$= P^2(2 - P^2)$$

$$R_c \geq R_b \geq R_a$$