Combinatorial Modeling Methods
Introduction to Combinatorial Methods

• Combinatorial validation methods are the simplest kind of analytical/numerical techniques and can be used for reliability and availability modeling under certain assumptions.

• Assumptions are that component failures are independent, and for availability, repairs are independent.

• When these assumptions hold, simple formulas for reliability and availability exist.
Lecture Outline

• Review definition of reliability
• Failure rate
• System reliability
  – Maximum
  – Minimum
  – $k$ of $N$
• Reliability formalisms
  – Reliability block diagrams
  – Fault trees
  – Reliability graphs
• Reliability modeling process
Reliability

- One key to building highly available systems is the use of reliable components and systems.
- Reliability: The *reliability* of a system at time $t$ ($R(t)$) is the probability that the system operation is proper throughout the interval $[0,t]$.
- Probability theory and combinatorics can be directly applied to reliability models.
- Let $X$ be a random variable representing the time to failure of a component. The *reliability* of the component at time $t$ is given by
  \[ R_X(t) = P[X > t] = 1 - P[X \leq t] = 1 - F_X(t). \]
  Also called the *survivor* function.
- Similarly, we can define *unreliability* at time $t$ by
  \[ U_X(t) = P[X \leq t] = F_X(t). \]
Failure Rate

What is the rate that a component fails at time $t$? This is the probability that a component that has not yet failed fails in the interval $(t, t + \Delta t)$ divided by $\Delta t$, as $\Delta t \to 0$.

Note that we are not looking at $P[X \in (t, t + \Delta t)] = f_X(t)$. Rather, we are seeking $P[X \in (t, t + \Delta t) | X > t]$.

$$P[X \in (t, t + \Delta t) | X > t] = \frac{P[X \in (t, t + \Delta t), X > t]}{P[X > t]} = \frac{P[X \in (t, t + \Delta t)]}{1 - F_X(t)}$$

Thinking in terms of rate

$$r_X(t) = \lim_{\Delta t \to 0} \frac{P[\in (t, t + \Delta t)]}{\Delta t} = \frac{f_X(t)}{1 - F_X(t)}$$

$r_X(t)$ is called the failure rate or hazard rate.
Typical Failure Rate

Break in  Normal operation  Wear out

$r_X(t)$

time $t$
**System Reliability**

While $F_X$ can give the reliability of a component, how do you compute the reliability of a system?

System failure can occur when one, all, or some of the components fail. If one makes the *independent failure assumption*, system failure can be computed quite simply. The independent failure assumption states that all component failures of a system are independent, i.e., the failure of one component does not cause another component to be more or less likely to fail.

Given this assumption, one can determine:

1) Minimum failure time of a set of components
2) Maximum failure time of a set of components
3) Probability that $k$ of $N$ components have failed at a particular time $t$. 
Example: Weibull Distribution

Weibull Distribution
- Often used to model lifetime data
- $\beta$ called the shape parameter
- $\eta$ is the scale parameter
- $\gamma$ is the location parameter

$$f(t) = \frac{\beta}{\eta} \left( \frac{t - \gamma}{\eta} \right)^{\beta-1} e^{-\left( \frac{t-\gamma}{\eta} \right)^{\beta}}$$
Example: Weibull Distribution

Weibull Distribution
• Impact of $\beta$
• Bathtub function constructed by piece-wise definition of Weibulls with different $\beta$
Example: Weibull Distribution

Weibull Distribution

- *Early Life*: (failure rate decreases with time)
- *Useful Life*: (failure rate approx. constant)
- *Wearout Life*: (failure rate increases with time)

*Time (hours, miles, cycles, etc.)*

*Failure Rate (failures per unit time)*
Example: Weibull Distribution

Weibull Distribution

\[
f(t) = \frac{\beta}{\eta} \left( \frac{t - \gamma}{\eta} \right)^{\beta-1} e^{-\left( \frac{t-\gamma}{\eta} \right)^\beta}
\]

\[
F(t) = e^{-\left( \frac{t-\gamma}{\eta} \right)^\beta}
\]

\[
r_X(t) = \frac{f_X(t)}{F(t)} = \frac{\beta}{\eta} \left( \frac{t - \gamma}{\eta} \right)^{\beta-1}
\]

Observe special case of \( \gamma = 0, \ \ \beta = 1 \) \( r_X(t) = \frac{1}{\eta} \)
Maximum of \( n \) Independent Failure Times

Let \( X_1, \ldots, X_n \) be independent component failure times. Suppose the system fails at time \( S \) if \( S \) is the earliest time at which all components are in the failed state.

Thus, \( S = \max\{X_1, \ldots, X_n\} \)

What is \( F_s(t) \)?

\[
F_s(t) = P[S \leq t] = P[X_1 \leq t \text{ AND } X_2 \leq t \text{ AND } \ldots \text{ AND } X_n \leq t]
= P[X_1 \leq t] P[X_2 \leq t] \ldots P[X_n \leq t] \quad \text{By independence}
= F_{X_1}(t) F_{X_2}(t) \ldots F_{X_n}(t) \quad \text{By definition}
= \prod_{i=1}^{n} F_{X_i}(t)
\]
Minimum of $n$ Independent Component Failure Times

Let $X_1, \ldots, X_n$ be independent component failure times. A system fails at time $S$ if $S$ is the earliest time at which any component is in the failed state.
Thus, $S = \min\{X_1, \ldots, X_n\}$.

What is $F_S(t)$?

$$F_S(t) = P[S \leq t] = P[X_1 \leq t \text{ OR } X_2 \leq t \text{ OR } \ldots \text{ OR } X_n \leq t]$$

Trick: If $A_i$ is an event, and $\overline{A_i}$ is the set complement such that $A_i \cup \overline{A_i} = \Omega$ and $A_i \cap \overline{A_i} = \emptyset$, then

$$P[A_1 \text{ OR } A_2 \text{ OR } \ldots \text{ OR } A_n]$$

$$= 1 - P[\overline{A_1} \text{ AND } \overline{A_2} \text{ AND } \ldots \text{ AND } \overline{A_n}]$$

This is an application of the law of total probability (LOTP).
Minimum cont.

\[ F_s(t) = P[X_1 \leq t \text{ OR } X_2 \leq t \text{ OR } \ldots \text{ OR } X_n \leq t] \]

\[ = 1 - P[X_1 > t \text{ AND } X_2 > t \text{ AND } \ldots \text{ AND } X_n > t] \quad \text{By trick} \]

\[ = 1 - P[X_1 > t] P[X_2 > t] \ldots P[X_n > t] \quad \text{By independence} \]

\[ = 1 - (1 - P[X_1 \leq t])(1 - P[X_2 \leq t]) \ldots (1 - P[X_n \leq t]) \quad \text{By LOTP} \]

\[ = 1 - \prod_{i=1}^{n} (1 - F_{X_i}(t)) \]
k of N

Let $X_1, \ldots, X_n$ be component failure times that have identical distributions (i.e., $F_{X_1}(t) = F_{X_2}(t) = \ldots$). The system fails at time $S$ if $S$ is the earliest time at which any $k$ of the $N$ components are in the failed state.

$$F_S(t) = P[\text{at least } k \text{ components failed by time } t]$$

$$= P[\text{ exactly } k \text{ failed OR exactly } k + 1 \text{ failed OR } \ldots \text{ OR exactly } N \text{ failed}]$$

$$= P[\text{ exactly } k \text{ failed}] + P[\text{ exactly } k + 1 \text{ failed}] + \ldots + P[\text{ exactly } N \text{ failed}]$$

What is $P[\text{ exactly } k \text{ failed}]$?

$$= P[k \text{ failed and } (N - k) \text{ have not}]$$

$$= \binom{N}{k} F_X(t)^k (1 - F_X(t))^{N-k}$$

where $F_X(t)$ is the failure distribution of each component.

Thus, $F_S(t) = \sum_{i=k}^{N} \binom{N}{i} F_X(t)^i (1 - F_X(t))^{N-i}$

- by independence and axiom of probability.
k of N in General

For non-identical failure distributions, we must sum over all combinations of at least $k$ failures.

Let $G_k$ be the set of all subsets of $\{X_1, \ldots, X_N\}$ such that each element in $G_k$ is a set of size at least $k$, i.e.,

$$G_k = \{g_i \subseteq \{X_1, \ldots, X_N\} : |g_i| \geq k\}.$$

The set $G_k$ represents all the possible failure scenarios.

Now $F_S$ is given by

$$F_S(t) = \sum_{g \in G_k} \left( \prod_{X \in g} F_X(t) \right) \left( \prod_{X \notin g} (1 - F_X(t)) \right)$$
Component Building Blocks

Complex systems can be analyzed hierarchically.

Example: A computer fails if both power supplies fail or both memories fail or the CPU fails.

System problem is one of a minimum: the system fails when the first of three subsystems fails…proper formulation is

- **Power supply subsystem** is a maximum: both must fail
- **Memory subsystem** is a maximum: both must fail

\[
F_S(t) = 1 - (1 - F_{P1}(t)F_{P2}(t)) (1 - F_{M1}(t)F_{M2}(t)) (1 - F_C(t))
\]

Probability at least 1 power source is up at \( t \)

Probability all 3 subsystems are up at \( t \)
## Summary

A system comprises $N$ components, where the component failure times are given by the random variables $X_1, \ldots, X_N$. The system fails at time $S$ with distribution $F_S$ if:

<table>
<thead>
<tr>
<th>Condition:</th>
<th>Distribution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>all components fail</td>
<td>$F_S(t) = \prod_{i=1}^{N} F_{X_i}(t)$</td>
</tr>
<tr>
<td>one component fails</td>
<td>$F_S(t) = 1 - \prod_{i=1}^{N} \left(1 - F_{X_i}(t)\right)$</td>
</tr>
<tr>
<td>$k$ components fail, identical distributions</td>
<td>$F_S(t) = \sum_{i=k}^{N} \binom{N}{i} F_{X_i}(t)^i \left(1 - F_{X_i}(t)\right)^{N-i}$</td>
</tr>
<tr>
<td>$k$ components fail, general case</td>
<td>$F_S(t) = \sum_{g \in G_k} \left(\prod_{X \in g} F_{X}(t)\right) \left(\prod_{X \notin g} \left(1 - F_{X}(t)\right)\right)$</td>
</tr>
</tbody>
</table>