

# Example Problems for Combinatorial Modeling

David Nicol

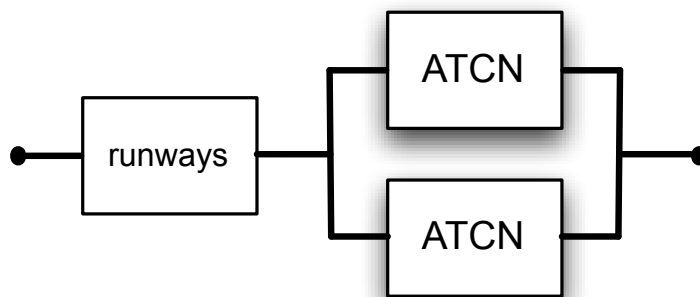
31 August 2009

1. Imagine an airport that has three runways and an air traffic control radio system with a (hot) back-up system. The airport is able to give “proper service” if at least two of the three runways are operational, and at least one of the radio control systems is operational.

The weather forecast for the next 24 hours call for the possibility of high winds. Depending on the severity, high wind might close one, two, or all of the runways. We suppose someone has mapped the forecast into an indicator random variable  $R$  which has value 1 if two or more of the runways stay open over the entire next 24 hours, and 0 if two or more of them are closed simultaneously at any point in the entire 24 hours. We assume a lifetime distribution function  $F_C(t)$  for the air traffic control radio system.

How can we model this with a reliability block diagram and come up with a distribution of the time of the first system failure?

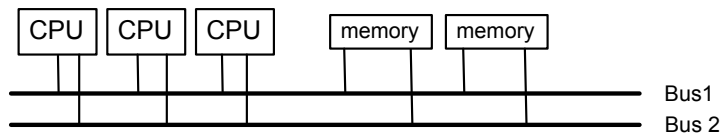
At the highest level, the system in RBD form is a series—it fails when either the runways fail or the air traffic control system fails. The air traffic control system is a parallel one. The RBD is



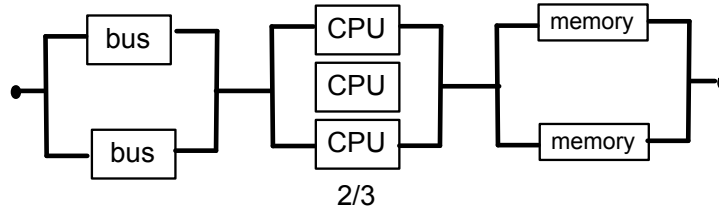
The CDF for the system’s time to failure is

$$\begin{aligned} \Pr\{\text{system fails by } t\} &= 1 - (\Pr\{R = 1\} \Pr\{\text{at least one ATC network up at } t\}) \\ &= 1 - (\Pr\{R = 1\}(1 - F_C(t)^2)) \end{aligned}$$

2. Consider the architecture below. Two buses connect 3 CPUs and 2 memory banks. The CDF of the lifetime distribution of a CPU is given by  $F_C(t)$ , of a memory bank by  $F_M(t)$ , and of a bus by  $F_B(t)$ . The system is considered to be operational if at least one of the buses has two or more live CPUs, and one or more live memory banks.



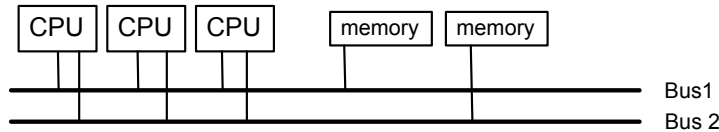
An RBD for this encodes the realization that the system is operational if either of the buses is, AND 2/3 of the CPUs are operational, AND either of the memories is operational.



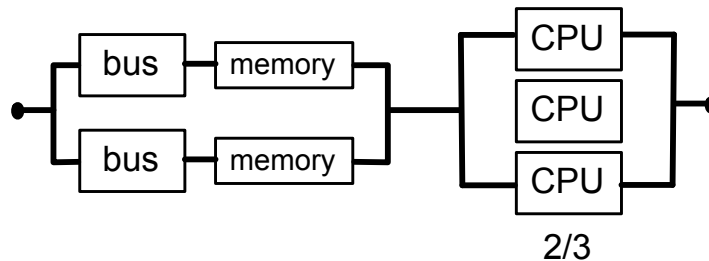
The distribution of  $S$  the time to failure is then

$$\begin{aligned}
 F_S(t) &= \Pr\{\text{bus system failed by } t \vee \text{CPU system failed by } t \vee \text{memory system failed by } t\} \\
 &= 1 - \Pr\{\text{bus system survives to } t \wedge \text{CPU system survives to } t \wedge \text{memory system survives to } t\} \\
 &= 1 - \Pr\{\text{At least 1 bus survives to } t\} \times \Pr\{\text{At least 2 CPUs survive to } t\} \\
 &\quad \times \Pr\{\text{At least one memory survives to } t\} \\
 &= 1 - (1 - \Pr\{\text{Both buses fail by } t\}) \times \Pr\{\text{At least 2 CPUs survive to } t\} \\
 &\quad \times (1 - \Pr\{\text{both memories fail by } t\}) \\
 &= 1 - (1 - F_B(t)^2) \times \left( \sum_{n=2}^3 \binom{3}{n} \bar{F}_C(t)^n F_C(t)^{3-n} \right) \times (1 - F_M(t)^2)
 \end{aligned}$$

But now consider a slight modification to the architecture



If a bus goes out, the associated memory may as well be considered to be out. If a memory goes out, then the other memory has to be accessible to the CPUs for the system to be operational, which implies that the other bus has to be operational as well. The net effect is that we can lump a memory and its bus together as a subsystem, denote failure of that subsystem if either component fails, and require that at least one of the subsystems be operational for the system to be operational. This gives us the RBD

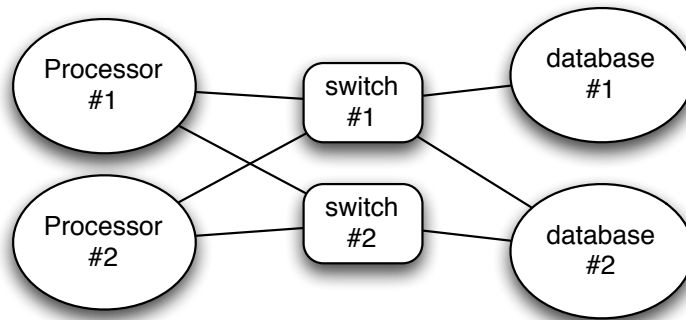


And a different derivation of  $S$  the time to failure

$$\begin{aligned}
 F_S(t) &= \Pr\{\text{memory/bus system failed by } t \vee \text{CPU system failed by } t\} \\
 &= 1 - \Pr\{\text{memory/bus system survives to } t \wedge \text{CPU system survives to } t\} \\
 &= 1 - \Pr\{\text{At least 1 memory/bus survives to } t\} \times \Pr\{\text{At least 2 CPUs survive to } t\} \\
 &= 1 - (1 - \Pr\{\text{Both memory/buses fail by } t\}) \times \Pr\{\text{At least 2 CPUs survive to } t\}
 \end{aligned}$$

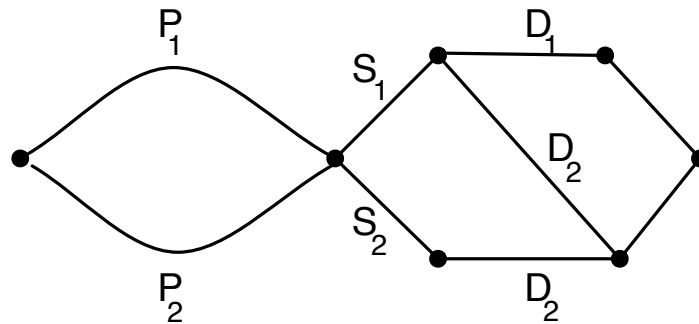
$$\begin{aligned}
&= 1 - (1 - \Pr\{\text{A memory/bus fails by } t\}^2) \times \Pr\{\text{At least 2 CPUs survive to } t\} \\
&= 1 - (1 - \Pr\{\text{A memory fails by } t \vee \text{ a bus fails by } t\}^2) \times \Pr\{\text{At least 2 CPUs survive to } t\} \\
&= 1 - (1 - (1 - \Pr\{\text{A memory survives to } t \wedge \text{ a bus survives to } t\})^2) \times \Pr\{\text{At least 2 CPUs survive to } t\} \\
&= 1 - (1 - (1 - \bar{F}_M(t)\bar{F}_B(t))^2) \times \left(\sum_{n=2}^3 \binom{3}{n} \bar{F}_C(t)^n F_C(t)^{3-n}\right)
\end{aligned}$$

3. Consider the system below

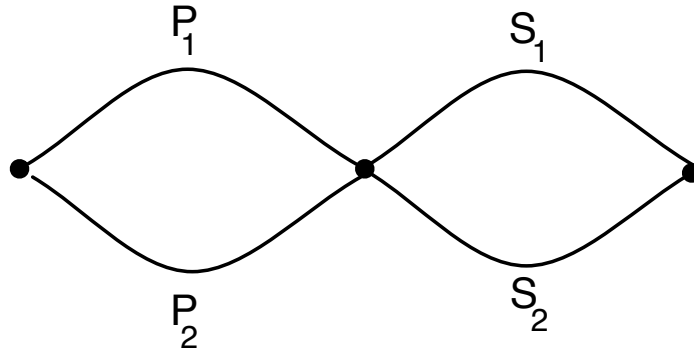


The system is considered to be operational so long as one of the servers can reach one of the databases. A processor has a lifetime CDF distribution  $F_P(t)$ , a switch has CDF lifetime distribution  $F_W(t)$ , and a database has CDF lifetime distribution of  $F_D(t)$ .

This being a “path” oriented statement of proper service, we model this with a reliability graph. But we can’t seem to do it without duplicating a label.



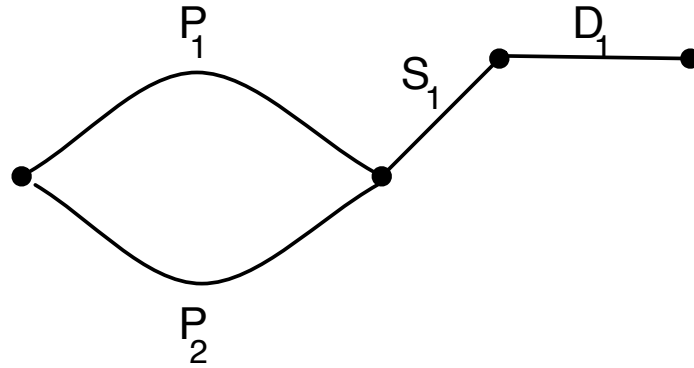
This is not series parallel....But suppose we condition on the state of  $D_2$ . When it is up, then any path to either switch will give an operational system (because both switches connect to database 2.) That gives the graph



with lifetime  $S$  distribution function that is a series of two parallel systems.

$$\begin{aligned}
\Pr\{S \leq t \mid D_2 \text{ is up at } t\} &= \Pr\{\text{Both processors failed by } t \vee \text{Both switches failed by } t\} \\
&= 1 - \Pr\{\text{At least one processor is up at } t \wedge \text{At least one switch is up at } t\} \\
&= 1 - \Pr\{\text{At least one processor is up at } t\} \times \Pr\{\text{At least one switch is up at } t\} \\
&= 1 - (1 - \Pr\{\text{both processors are down at } t\}) \times (1 - \Pr\{\text{both switches are down at } t\}) \\
&= 1 - (1 - F_P(t)^2) \times (1 - F_W(t)^2).
\end{aligned}$$

If now we condition on  $D_2$  being down then the only paths that led to the system being operational go through switch 1 and onto database 1



with a lifetime distribution function that is a series of 3 subsystems : the two processors (itself a parallel system),  $S_1$ , and  $D_1$ .

$$\begin{aligned}
\Pr\{S \leq t \mid D_2 \text{ is down at } t\} &= \Pr\{\text{Both processors failed by } t \vee \text{Both switches failed by } t\} \\
&= 1 - \Pr\{\text{At least one processor is up at } t \wedge S_1 \text{ is up at } t \wedge D_1 \text{ is up at } t\} \\
&= 1 - \Pr\{\text{At least one processor is up at } t\} \times \Pr\{S_1 \text{ is up at } t\} \times \Pr\{D_1 \text{ is up at } t\} \\
&= 1 - (1 - \Pr\{\text{Both processors failed by } t\}) \times \bar{F}_W(t) \times \bar{F}_D(t) \\
&= 1 - (1 - F_P(t)^2) \times \bar{F}_W(t) \times \bar{F}_D(t)
\end{aligned}$$

Piecing these results together we obtain

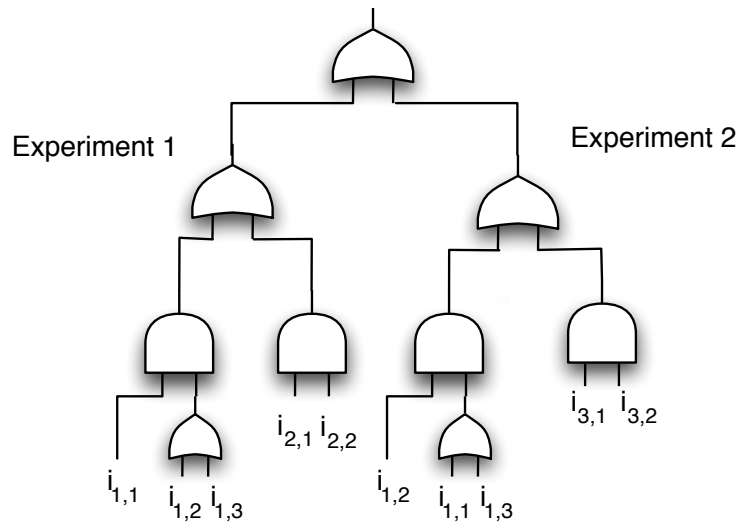
$$\begin{aligned}
\Pr\{S \leq t\} &= \Pr\{D_2 \text{ is up at } t\} \Pr\{S \leq t \mid D_2 \text{ is up at } t\} + \Pr\{D_2 \text{ is down at } t\} \Pr\{S \leq t \mid D_2 \text{ is down at } t\} \\
&= \bar{F}_D(t) (1 - (1 - F_P(t)^2) \times (1 - F_W(t)^2)) + F_D(t) (1 - (1 - F_P(t)^2) \times \bar{F}_W(t) \times \bar{F}_D(t)).
\end{aligned}$$

4. A laboratory runs two different kinds of experiments. Experiment 1 needs one each of instruments  $I_1$  and  $I_2$ , experiment 2 needs one each of  $I_1$ , and  $I_3$ . There is one spare for each instrument type—so there are three instances of  $I_1$ , and two instances of the others. we use notation  $i_{1,1}$  to denote instrument 1 of type 1,  $i_{1,2}$  to denote instrument 2 of type 1, and so on.

The CDF of the lifetime distribution for instrument  $I_j$  is denoted  $F_j(t)$ .

The lab is operational if it can simultaneously perform both kinds of experiments. If an instrument fails and the spare is available, the spare is used.

We develop a fault tree model by considering at a high level the conditions for failure : experiment 1 cannot be performed, or experiment 2 cannot be performed. Experiment 1 cannot be performed if its primary type 1 instrument has failed and the spare is unavailable (either by its own failure, or by using in Experiment 2), or both of the type 2 instruments have failed. Experiment 2 cannot be performed if its primary type 1 instrument has failed and the spare is unavailable, or both of the type 3 instruments have failed. This gives us the fault tree below



The branches of this tree are not independent, because each of the type 1 instruments appears more than once. The most straightforward approach is to condition on the states of the three type 1 instruments. For any assignment of 0 and 1 to each of the components of the vector  $(i_{1,1}, i_{1,2}, i_{1,3})$  we get a different simplified fault tree. Figure 1 shows all the possibilities.

This verifies what I originally showed in class, that the key thing to condition on is whether 2 or more of the instrument 1 devices failed—in which case the system does, or not, in which case there is a common resulting fault tree. The overall lifetime distribution is then

$$\Pr\{S \leq t\} = \Pr\{\text{At least 2 of 3 type 1 instruments fail by } t\} \times 1 + (1 - \Pr\{\text{At least 2 of 3 type 1 instruments fail by } t\}) \times (1 - (1 - F_2(t)^2)(1 - F_3(t)^2)).$$

The coefficients can be looked up in the tables.

5. Service demands arrive at a service center where there are five servers  $S_1, S_2, S_3, S_4,$  and  $S_5$ . Each demand is one of four types, characterized by the sequence of servers applied to the demand :

**Demand type 1**  $S_1 \rightarrow S_4$

**Demand type 2**  $S_1 \rightarrow S_3 \rightarrow S_5$

**Demand type 3**  $S_2 \rightarrow S_5$

**Demand type 4**  $S_2 \rightarrow S_3 \rightarrow S_4$

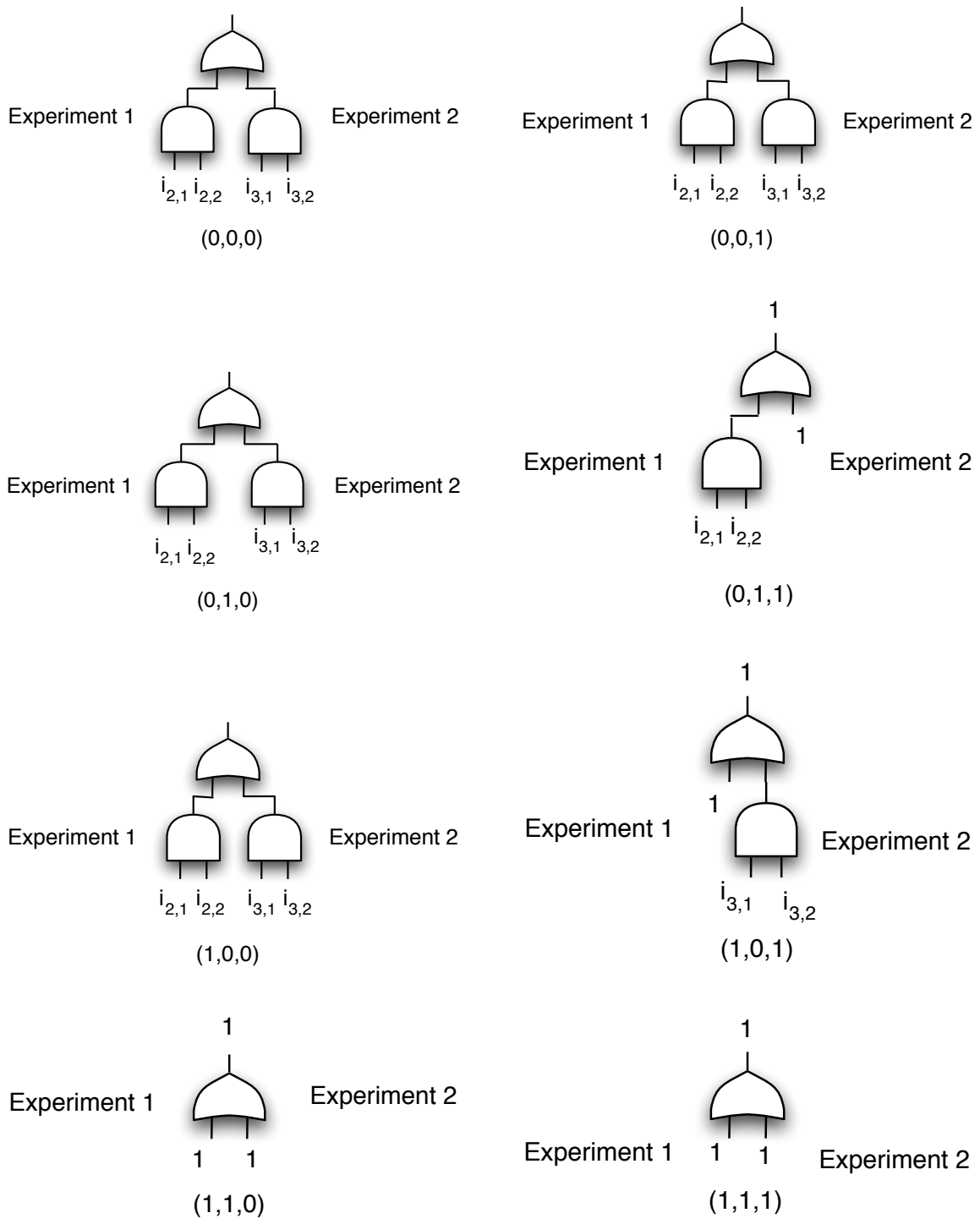


Figure 1: Fault trees from conditioning on  $(i_{1,1}, i_{1,2}, i_{1,3})$

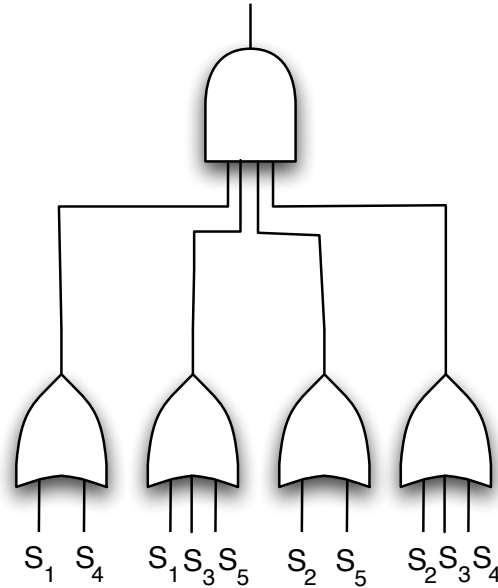
The CDF of the time to failure of server  $S_i$  is denoted  $F_i(t)$ . The system is considered to have failed only if no demand of any type can be processed.

Let  $b_i$  be the Boolean variable with value “true” if server  $S_i$  has failed. To say that a demand of the first type cannot be processed is to say that  $(b_1 \vee b_4)$  is true. Likewise, to say that a demand of type 2 cannot be processed is to say that  $(b_1 \vee b_3 \vee b_5)$  is true.

In this way we can derive a Boolean expression which is true if and only if the system has failed, by

$$(b_1 \vee b_4) \wedge (b_1 \vee b_3 \vee b_5) \wedge (b_2 \vee b_5) \wedge (b_2 \vee b_3 \vee b_4)$$

We can describe this with a fault tree as shown below



In this diagram every component appears twice! It appears that solution by frontal assault may be the only answer. For every assignment of true or false to all component states, (i) the equation above tells us whether the system is failed in that state, and (ii) we can compute the probability of being in that state at time  $t$ .

For instance

$$\Pr\{b_1 \wedge \bar{b}_2 \wedge \bar{b}_3 \wedge b_4 \wedge \bar{b}_5\} = F_1(t)\bar{F}_2(t)\bar{F}_3(t)F_4(t)\bar{F}_5(t).$$

The probability that the system has failed by  $t$  is the sum over all system states the reflected system failure of being in that state at time  $t$ .