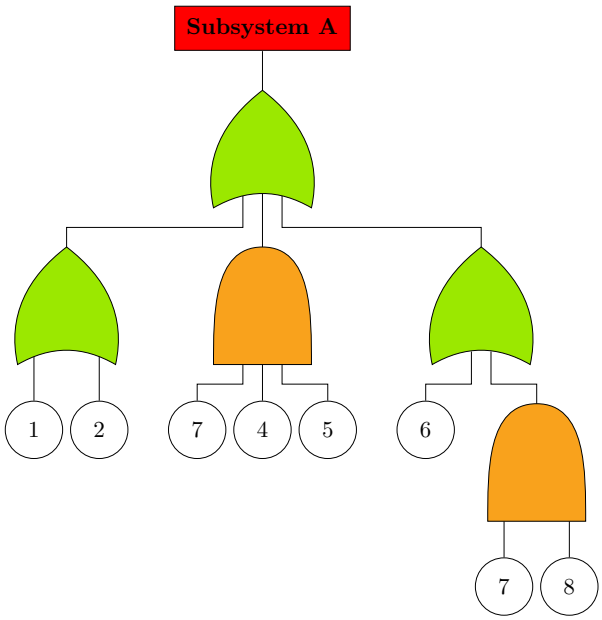
Model Checking: exercise set 11 - Static fault trees

Due date: May 22

1. Consider the following fault tree:



   (a) Derive two BDDs for the fault tree in the figure above: one where the number of nodes in minimal, and one where the number of nodes is much larger.

   (b) Use the BDD to compute the failure probability that the top level event occurs, if we assume that the probability for BE i to fail is $\frac{1}{i+1}$.

   (c) Approximate the probability the failure probability that the top level event occurs via the cut set method.

   (d) Compare your answers at (b) and (c)

2. Suppose that we introduce a XOR-gate in fault trees. The XOR (eXclusive OR) gate has at least 2 children, and fails if either of exactly one of its children fails. Consider a XOR gate with independent children A and B.

   (a) Assume that A and B fail with probability p_A and p_B respectively. What is the probability for the XOR gate to fail?

   (b) Suppose the probability for A to fail within time t is given by $p_A(t) = 1 - e^{-\lambda t}$ and probability for B to fail within time t is given by $p_B(t) = 1 - e^{-\mu t}$. What is the probability for the XOR gate to fail within time t?

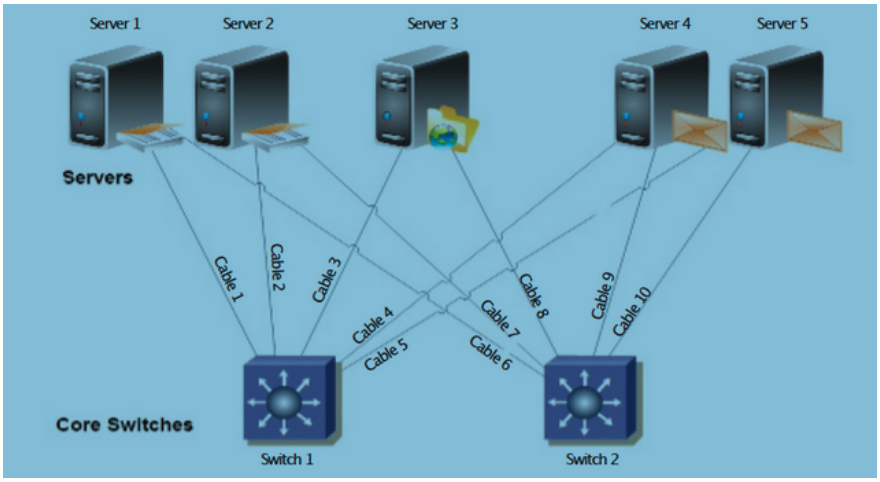
3. Which of the following computation methods for computing the failure probability for the top level event still work for fault trees with XOR gates? Explain your answers.

   (a) The bottom up method.

   (b) The BDD method.

   (c) The cut set method for overapproximating probabilities.

4. You are the reliability engineer of the company CoolCloudSolutions. Your boss has promised your customers a reliability of 99%. The architecture is depicted in the figure below.



(a) Model the system as a fault tree. Assume that all servers have the same functionality. So for the system to be operational, at least one of the 5 servers must be operational, together with its network cable and one switch.

(b) Determine:

i. all minimal cut sets of order 1, 2, 3, and 4.

ii. the maximal order. List one minimal cut set of this order.

(c) What are the most vulnerable elements?

(d) Assuming the following failure probabilities:

i. p_1 = server failure = 0.2

ii. p_2 = network cable failure = 0.2

iii. p_3 = switch failure = 0.2

Does your architecture meet the reliability requirements?

(e) Now we assume that the 5 servers serve 3 different purposes: two file servers, one network server and two email servers. All 3 groups must work in order for the system to be operational. Model the new architecture as a fault tree.