Date ： 2019/12/01
Designer ： 陳麒宇(r07943034)

Dependable Systems and Networks

HW #2

Due Dec. 2, 2019

Each question is 10 points.

1. Devise an original example (different from the lecture examples) to illustrate the difference between faults, errors, and failures. As you illustrate these concepts, relate them to the three-universe model.

   假設紅綠燈有三個 state，紅燈持續 60 秒、綠燈 25 秒、黃燈 5 秒，可能的 design fault 是以 time counter 定義三種燈何時應該亮，以 90 秒為週期做一個循環，在 time counter 最後超出可計算範圍產生 overflow 的時候就會出現 error，此 error 可能導致像是由綠燈轉為紅燈或是黃燈轉為綠燈等 failure，如果修正 design fault 或在 error 發生時做 time shift 可避免 failure

2. Give three examples of applications in which a system failure can cost people's lives or environmental disaster.

   A. 電梯上下位移計算錯誤導致進出階距過大造成進出人員的傷亡

   B. 列車運行期間因剎車或轉彎等操作考量不周全導致列車出軌而造成人員的傷亡

   C. 飛機飛行期間機件發生錯誤行為導致人員的傷亡

3. Define the reliability of a system. What property of a system does the reliability characterize? In which situations is high reliability required?

   系統的 reliability 可定義為系統服務沒有 failure 的連續運行時間

   具有 reliability 的 system 可以長時間提供服務不中斷

   在自駕車或是飛機等攸關性命安全的場合需要較高的 reliability

4. What is the difference between the reliability and the availability of a system? How does the point availability compare to the system's reliability if the system cannot be repaired? What is the steady-state availability of a non-repairable system?

   Reliability 指的是一個系統能夠連續且無故障提供服務的時長，無故障運行時間越長則 reliability 越高，availability 指的是系統在固定時間內可提供服務的時長，通常使用百分比來衡量 availability 的高低

   對於 non-repairable system 我們只需計算系統開始運行至結束時間做為 availability 與 reliability 的依據

   Steady-state availability 指的是隨著時間趨近於無窮大，availability 會趨近於某個定值，我們稱之為 Ass，對於 non-repairable system，系統最終會收斂至 0

5. Compute the downtime per year for A(∞) = 90, 75, and 50%.
   A. A(∞) = 90%, downtime = 36.5days/year
   B. A(∞) = 75%, downtime = 91.25days/year
   C. A(∞) = 50%, downtime = 182.5days/year

6. A telephone system has less than 3min per year downtime. What is its steady state availability?

   A(∞) = 1-(3/60/24)/365 = 99.99943%

7. Explain the main differences between software and hardware faults.
   A. Software doesn't age or wear out.
   B. Software cannot be deformed or broken.
   C. Software cannot be affected by environmental factors.
   D. Software always performs the same way in the same circumstances if deterministic.

8. Why redundancy techniques used in hardware system cannot be used for software fault tolerance. If you are employed as a software quality engineer, what techniques you will prefer?

   Hardware redundancy 的手段類似於新增額外的硬體資源來做 fault tolerance，但對於 software 來說資源是有限的，因此 software redundancy 的作法可能是利用 pattern 去測試或檢查是否存在 fault

9. A combinational circuit is said to be *self dual* if and only if $f(X) = f'(X')$, where f is the output of the circuit and X is the input vector for the circuit.

   The dual of a function f_d is given by

   $$f_d = f'(x_1', x_2', \ldots, x_n')$$

   Show the function f_{sd} given by

   $$f_{sd} = x_{n+1} f + x'_{n+1} f_d$$

   is a self-dual function.

   Proof:

   $f_{sd}(X) = x_{n+1} f(x_1, x_2, \ldots, x_n) + x'_{n+1} f'(x_1', x_2', \ldots, x_n')$

   $f_{sd}'(X') = (x'_{n+1} f(x_1', x_2', \ldots, x_n') + x_{n+1} f'(x_1, x_2, \ldots, x_n)\ )'$

   $= (x_{n+1} + f'(x_1', x_2', \ldots, x_n'))(\ x'_{n+1} + f(x_1, x_2, \ldots, x_n))$

   $= 0 + x_{n+1} f(x_1, x_2, \ldots, x_n) + x'_{n+1} f'(x_1', x_2', \ldots, x_n') + 0 = f_{sd}(X)$

10. The inputs of a two input OR gate may be stuck-at-0 or stuck-at-1 with probabilities *P0* and *P1*, respectively. If the inputs are totally random, what is the reliability of the output?

    假設兩 input x1, x2 各有機率產生 stuck-at-0 or stuck-at-1

    X1 stuck-at-0, x2 normally 0 : P0*(1-P1)

    X1 stuck-at-0, x2 stuck-at-0 : P0^2

    X1 normally 0, x2 stuck-at-0 : P0*(1-P1)

    X1 stuck-at-1, x2 normally 0 : P1*(1-P1)

    X1 stuck-at-1, x2 stuck-at-1 : P1^2

    X1 normally 0, x2 stuck-at-1 : P1*(1-P1)

    Output 出現 fault 的機率為 P0^2-P1^2+2P0+2P1-2P0*P1 = (P0-P1+2)(P0+P1)，output 的 reliability 為 1-(P0-P1+2)(P0+P1)

11. What is the difference between a permanent fault, an intermittent fault, and a transient fault (in terms of fault duration)? Is the following statement true or false? A single fault can cause multiple bit errors. Justify your answer

    Permanent fault 來自於不可逆的硬體錯誤，可能是製造不當或損壞等等，可透過修理或替歡故障零件來修復，持續最久

    transient fault 來自於環境的干擾，通常不會持續太久

    intermittent fault 通常是不規則的裝置或是系統的故障，會由幾個因素共同引起，有些因素可能是隨機的，涉及的系統越複雜則故障機率越大，持續時間介於前兩者之間

    True, 對於多個 bit 參考到單點 stuck-at-fault 便有可能產生 multiple bit errors

12. Answer the following and where ever possible, use an example to make your point.

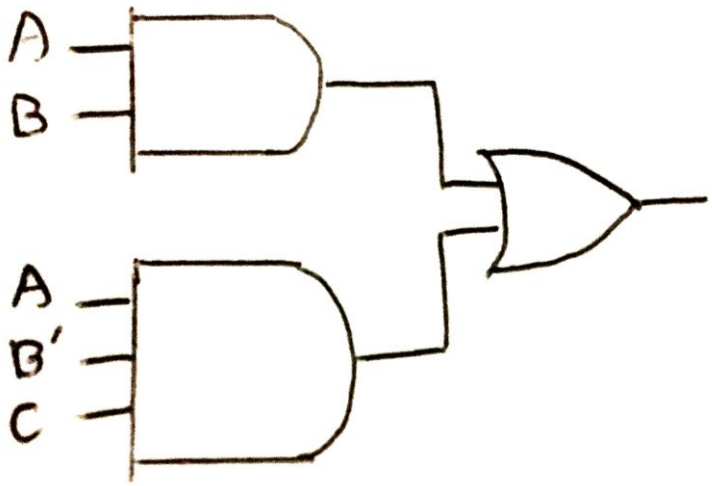
    (a) Bridging fault between a pair of lines in a circuit cannot be modeled by stuck-at fault model.

        No, 某些情況下我們能用 fault model 去表示 bridging fault，假設兩條線發生 bridging fault 後 stuck-at-0 or stuck-at-1，我們便可窮舉兩條線的可能組合

    (b) Circuit modification, i.e. adding more logic to the circuit, can be used to model a bridging fault between a pair of lines.

        Yes, 使用基本邏輯閘就可以判斷是否有 bridging fault 存在，可以將兩條線接到 AND 或 OR 等基本邏輯閘測試是否會產生不符合預期的訊號發生

13. Give an example of a combinational logic circuit in which a single stuck-at fault on a given line never causes an error on the output.



假設在 B’發生 stuck-at-fault 對於整個電路的結果不會產生影響，由 sum of product 的計算 AB+AB'C=AB+ABC+AB'C=AB+AC 可知 B’為 don’t care term

14. A heart pacemaker has a failure rate of $\lambda = 0.121 \times 10{-}8$ per hour. What is the probability that it fails during the first five years of operation? What is its MTTF?

MTBF = 1/λ = 826446281hour/1failure = 5years/(5.3*10^-5)failure

MTTF = 5years/1failure = 43800hours/1failure

15. At the end of the year of service, the reliability of a component is 0.96.

1. What is the failure rate of the component?

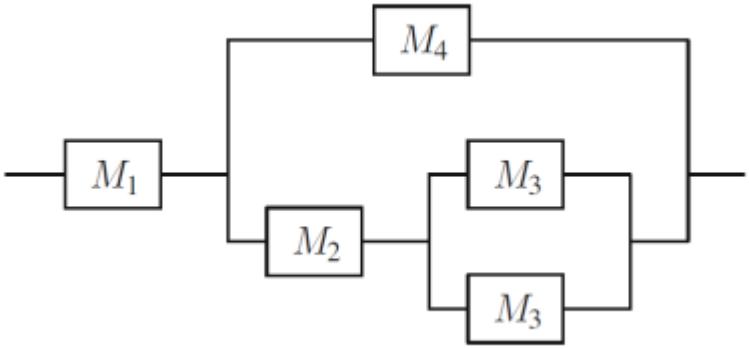
   R(t) = exp(-λt) = 0.96

   λ = -ln(0.96)/(365*24) = 4.66*10^-6/hours

2. If two components are connected in parallel, what will be the reliability of the resulting system during the first year of operation?

   R(t) = 1-((1-0.96)*(1-0.96)) = 0.9984

16. Write an expression for the reliability of the system shown by the RBD in the figure below. Assume that Ri (t) is the reliability of the module Mi, for i ∈ {1, 2, 3, 4}.

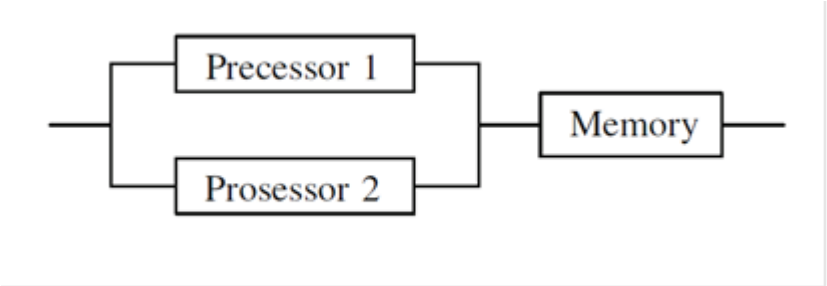


R = R1*(1-(1-R2*(1-(1-R3)^2))*(1-R4))

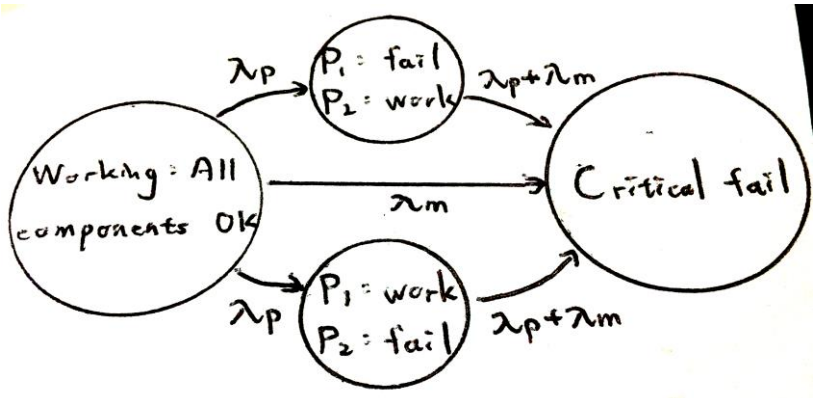
= R1*(1-(1-2*R2*R3+R2*R3^2)*(1-R4))

= $2R_1R_2R_3-R_1R_2R_3^2+R_1R_4-2R_1R_2R_3R_4+R_1R_2R_3^2R_4$

17. Draw a Markov chain for reliability evaluation of the system shown below. The failure rate of the processors 1 and 2 is λp. The failure rates of the memory is λm. No repairs are allowed.



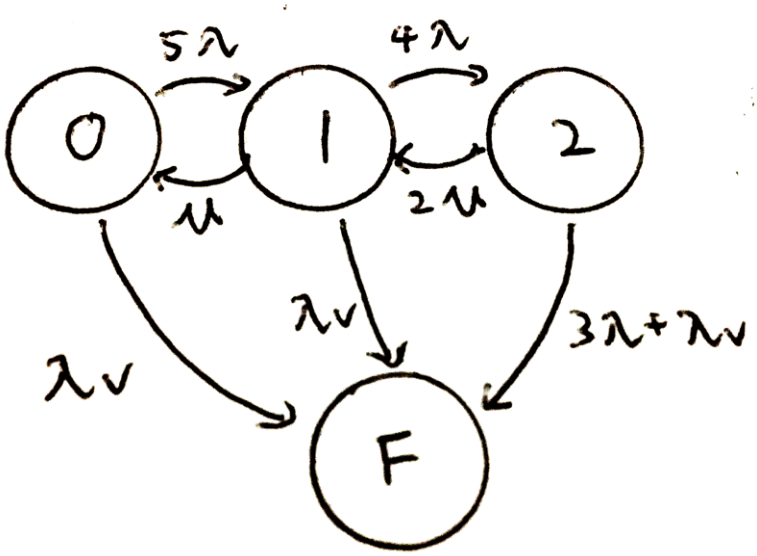
RBD of a three component system consisting of two duplicated processors and a memory



18. Suppose that a system was modeled using the Markov chain model and the following transition matrix was obtained from the resulting chain:

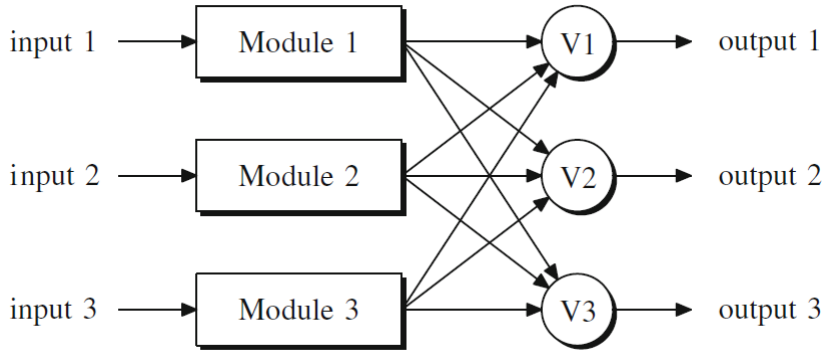
$$\begin{bmatrix} -(5\lambda+\lambda_v) & \mu & 0 & 0 \\ 5\lambda & -(\mu+4\lambda+\lambda_v) & 2\mu & 0 \\ 0 & 4\lambda & -(2\mu+3\lambda+\lambda_v) & 0 \\ \lambda_v & \lambda_v & 3\lambda+\lambda_v & 0 \end{bmatrix}$$

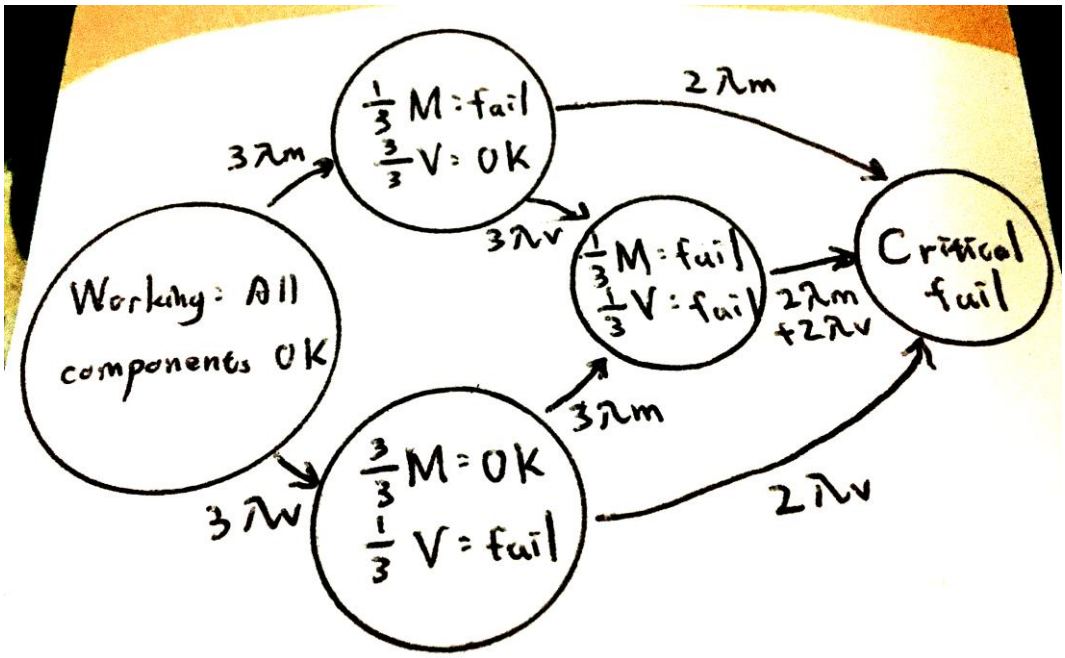
Draw the Markov chain corresponding to this transition matrix. Was the Markov chain intended for reliability or availability evaluation?



State	description
0	All components work
1	One module fails
2	Two module fail
F	System failure

19. Draw a Markov chain for reliability evaluation of the TMR with three voters shown below. Assume that the failure rate of each module is λm, and the failure rate of each voter is λv. No repairs are allowed.





20. Compare watchdog times and heartbeats. What are the advantages and disadvantages of each technique?

A watchdog timer looks over something and if it hasn't observed a change within in set time it performs an action.

A heartbeat is a changing signal that implies that something is alive.

A heartbeat signal supplies the data that a watchdog timer consumes in order to decide whether to perform its action.