National Taiwan University

Department of Electrical Engineering

Fault Tolerant Computing

Midterm Exam, Due Dec. 16, 2019

This is an open book exam. Feel free to consult any book, article, or notes. However, you cannot give or receive help from others during this examination period. All forms of calculating devices are permissible, so use them as you see fit. Please sign below, indicating that you agree with these terms. Return this signed page with your completed answers. Solve all problems. Show your work and clearly mark your final answer.

Student Name: _____

Signature:_____

1. (10 points) Definitions of reliability, availability, safety etc.

For the following systems (A and B), identify which attribute (reliability, availability etc.) is considered least important. Justify your answers.

A. An aircraft system has three computers voting on the results of every operation performed by the auto-pilot. If the auto-pilot fails, a warning alarm goes off in the cockpit to alert the pilot, who can then take over the manual controls of the aircraft and guide it to safety. However, the pilot does not interfere as long as the autopilot does not raise the alarm.

Availability is considered least important

由於飛機系統由三台電腦判斷是否有error而轉為手動控制，可以想像在系統出現問題時便會馬上修復，說明了飛機系統一直處於可用的狀態，因此可用性在本題中較為不重要，此時對系統比較有影響力的便是可靠性

B. An online trading website allows its customers to place bids on various items, and to track their bidding online. While it is acceptable for a user to not be able to place bids if the traffic is too high, it is not acceptable for a user who has placed bids to not track their bid's status and modify the bid. Also, as far as possible, the website should not display an incorrect value of the item's current bid, as this can cause users to over/under-bid for it.

Reliability is considered least important

本題中強調系統提供服務的即時性，如果系統沒有馬上提供正確的資訊會導致其他競標者出價錯誤，讓使用者困在錯誤狀態無法修改，因此可用性在本題較為重要，而可靠性相對而言較不重要

In each of the following descriptions (C and D), identify the fault, error and failure.

C. A program contains a rare race condition that is only triggered when the OS schedules threads in a certain order. Once triggered however, the race condition corrupts a value in the program, which in turn is used to make a branching decision. If the branching decision is incorrect, the program will go into an infinite loop and hang, thus failing to produce any output.

Fault : Once triggered however, the race condition corrupts a value in the program

Error : the branching decision is incorrect

Failure : the program will go into an infinite loop and hang, thus failing to produce any output

D. A radar system uses an array of processors to track its target in real-time. A soft error in a processor can lead to the processor computing an incorrect value for the target's location. However, the system can compensate for this effect by redundantly allocating the tasks to processors and comparing the results. But this compensation entails a performance overhead, which in some cases, can cause the system to miss the tasks' deadlines and lose the target.

Fault : A soft error in a processor can lead to the processor computing an incorrect value for the target's location

Error : this compensation entails a performance overhead

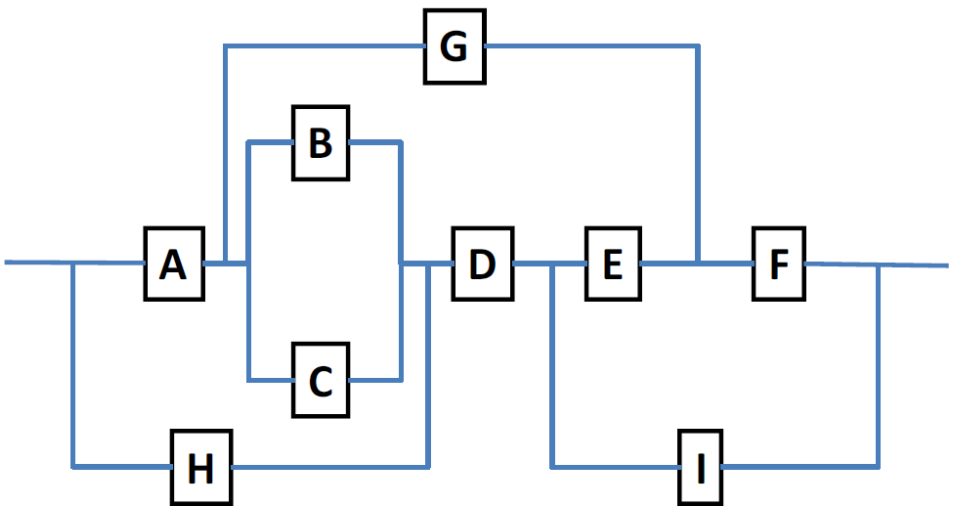
Failure : cause the system to miss the tasks' deadlines and lose the target

2. **(5 points)** Calculate the reliability of this system using the success diagram approach described in class. Derive the upper bound for the system reliability using the formula:

系統的working機率<=1-每條路徑都fail的機率

R_{sys} <= 1-((1-$R_A R_G R_F$)(1-$R_A R_B R_D R_E R_F$)(1-$R_A R_B R_D R_I$) (1-$R_A R_C R_D R_E R_F$)(1-$R_A R_C R_D R_I$) (1-$R_H R_D R_E R_F$)(1-$R_H R_D R_I$))

$$R_{sys} \leq 1 - \prod_{i=1}^{j} \left(1 - R_{path_i}\right)$$

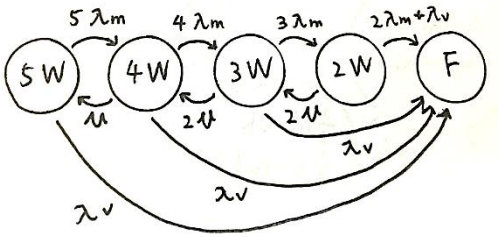


3. **(5 points)** Draw a Markov chain for reliability evaluation for self-purging redundancy with 5 modules. Assume that the voter can adopt to vote on less inputs. When only 2 modules are left, it works as a comparator.

When we say "voter fails", we mean that it starts producing an incorrect value on its output, so the system fails.

The failure rates of modules and the voter are λ_m and λ_v, respectively, and the repair rate is μ for each. There are two repair teams. Switches are perfect.

Label the state "XW" means "X modules working and the voter works".



4. (5 points) TMR Voting

Consider a simple TMR system with voting. Let the reliability of the voter be R_V and that of the module be R_m. Clearly, the lower the reliability of the voter, the lower the reliability of the system. However, there is a value of R_V beyond which the TMR system will have even lower reliability than that of the corresponding simplex system. Let's call this value $R_{V\text{---}min}$ owing questions:

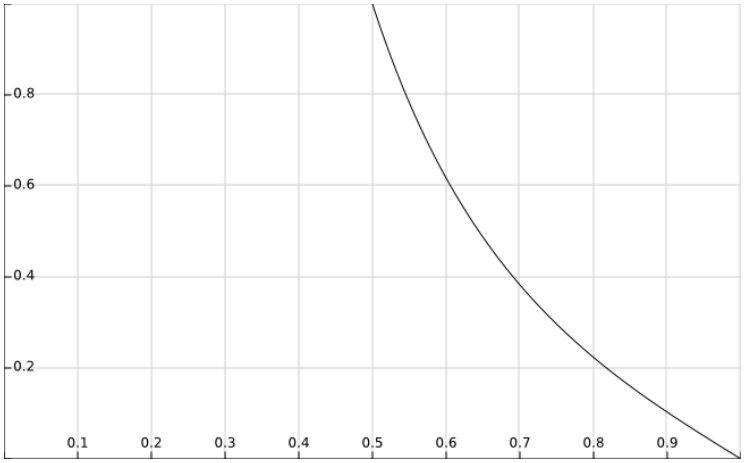
a. Derive an expression for Rv---min, as a function Rm, in order for the reliability of the TMR system to be greater than the reliability of the Simplex.

b. Draw a graph showing how Rv---min varies as a function of Rm.

c. Assume that the reliability of the voter is 0.95. What is the allowable range of Rm so that the reliability of the TMR system is higher than that of Simplex?

a. $R_{tmr} = R_v * \sum_{i=2}^{3} \binom{3}{i} R_m{}^i (1 - R_m)^{3-i} = R_v(3R_m\text{^}2\text{-}2R_m\text{^}3)$
$R_{simplx} = 1\text{-}R_m$
$R_{v\text{-}min} = (1\text{-}R_m)/(3R_m\text{^}2\text{-}2R_m\text{^}3)$

b.



c. For $R_v = 0.95$, $0.95*(3R_m\text{^}2\text{-}2R_m\text{^}3) > 1\text{-}R_m$
Solve the equation $38x\text{^}3\text{-}57x\text{^}2\text{-}20x+20<0$
We get $R_m>0.51031$

5. **(5 points)** A copy machines manufacturer estimates that the reliability of the machines he produces is 73% during the first 3 years of operation.

   i. How many copy machines will need a repair during the first year of operation?

   $R(t) = \exp(-\lambda t) = 0.73$

   $\lambda = 1.197*10^{-5}$ failure/hour

   first year : R = 0.90045 = 90.045%, thus 9.955% need a repair

   ii. What is the MTTF of the copy machines?

   $MTTF = (1/\lambda) = 83542.19$ hour = 3479.38 day

   iii. The manufactures guarantee MTTR = 2 days. What is the MTBF of the copy machines?

   MTBF = MTTF+MTTR = 3481.38 day

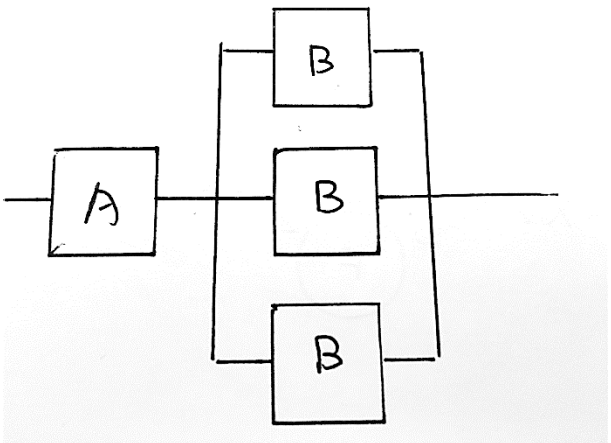
   iv. Suppose that two copy machines work in parallel and the failures are independent. What is the probability of failure during the first year of operation?

   兩台都fail才fail：$(1-R)^2 = 0.00991$

   一台fail就fail：$(1-R^2) = 0.189$

6. **(5 points)** You company produces a system which consists of two components, *A* and *B*, placed in series. The reliabilities of the components are R_A = 0.99 and R_B = 0.85. Their cost is approximately the same. The warranty for this system is 1 year. Your boss decides that too many items are returned for repair during the warranty period. He gives you a task of improving the reliability of the system so that no more than 2% of items are returned for repair during the first year of operation. This should be done by adding no more than two redundant components to the system. Find a reliability block diagram for the system which meets your boss's requirements.

   $R_{system} = R_A*(1-(1-R_B)^3) = 0.9867 > (1-2\%) = 0.98$, meet requirement

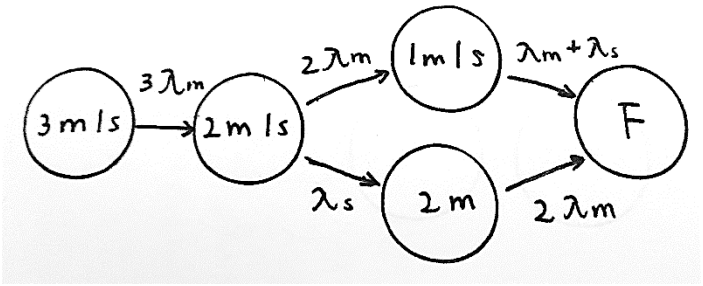


7. **(15 points)** Draw a Markov chain for 3-modular redundancy with one spare and the standard majority voter for the cases listed below.

(a) **(5 points)** Do reliability evaluation. Assume that:

- Each of the main modules has the failure rate λ_m. The spare has the failure rate λ_s.
- The spare cannot fail while in the spare mode.
- The voter, switch and disagreement detector units are perfect.

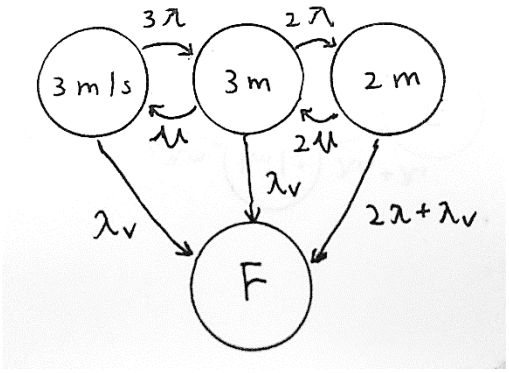
No repairs are allowed.



(b) **(5 points)** Do availability evaluation. Assume that:

- The modules and the spare have the same failure rate λ. The voter has the failure rate λ_v.
- The spare cannot fail while in the spare mode.
- The switch and disagreement detector units are perfect.
- Repairs are allowed. There are 2 repair teams. The repair rate of each module and the spare is μ.

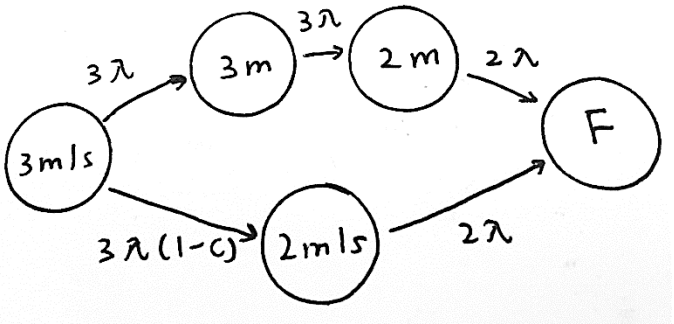
When the system fails, it shuts itself down.



(c) **(5 points)** Do safety evaluation. Assume that:

- The modules and the spare have the same failure rate λ.
- The spare cannot fail while in the spare mode.
- The voter and switch are perfect.
- The disagreement detector unit detects the disagreement with the probability C.

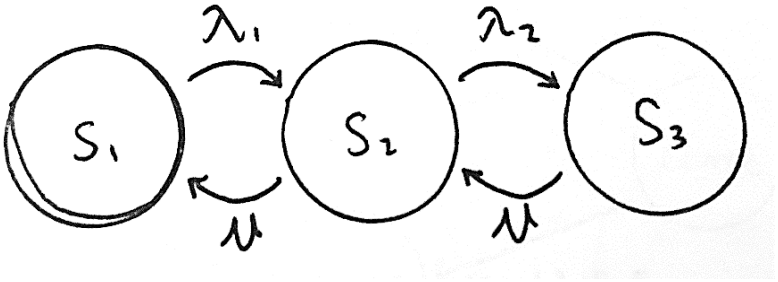
No repairs are allowed.



8. **(5 points)** Suppose that a system was modeled using a Markov chain with 3 states: S_1, S_2 and S_3, and the following set of differential equations (in matrix form) were obtained from this chain:

$$\frac{d}{dt}\begin{bmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \end{bmatrix} = \begin{bmatrix} -\lambda_1 & \mu & 0 \\ \lambda_1 & -\lambda_2 - \mu & \mu \\ 0 & \lambda_2 & -\mu \end{bmatrix} \cdot \begin{bmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \end{bmatrix}.$$

Draw the Markov chain corresponding to this set of equations.



9. **(5 points)** Check whether the function $f(a,b,c) = abc$ is self-dual.
f'(a', b', c') = (a'b'c')' = a+b+c != f(a, b, c), f is not self-dual
truth table :

a	b	c	f
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

a'	b'	c'	f'
1	1	1	0
1	1	0	1
1	0	1	1
1	0	0	1
0	1	1	1
0	1	0	1
0	0	1	1
0	0	0	1

10. **(10 points)** A standby redundant system composed of three components connected in parallel, each with a constant failure rate of and it's time to failure exponentially distributed. Only one component is required to be operative for the system to function properly. Initially the power is applied to only one component and the other two components are kept in a powered-off state (de-energized). When the energized component fails, it is de-energized and removed from operation, and the second component is energized and connected in the second's place, while the third component is still kept in powered-off state. When the second component fails, it is replaced by the third component.

- Derive the reliability function of this standby redundant system.
- Name the distribution that best describes the time to failure of the system?
- Name the distribution that best describes the time to failure of the system if the failure rate of the three components were **not** identical?

(**Hint:** Reliability of a single component with a hazard/failure rate , $R(t) = e^{-\lambda}$
(a) **R_{sys} = 1-(1-exp(-λ))^3 = exp(-3λ)-3exp(-2λ)+3exp(-λ)**
(b) Exponential distribution
(c) Poisson distribution

11. (10 points)

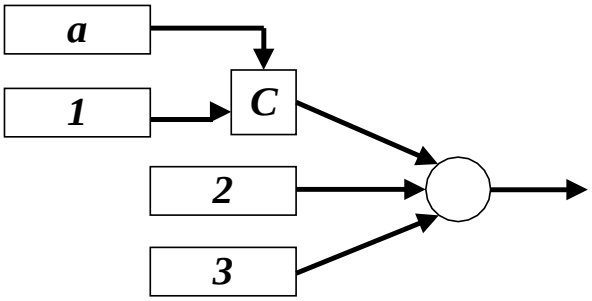
(a) **(5 points)** The system shown consists of a TMR core with a single spare *a* which can serve as a spare only for module 1. Assume that modules 1 and *a* are active. When either of the two module 1 or *a* fails, the failure is detected by the perfect comparator *C* and then the single operational module is used to provide an input to the voter. Assuming that the voter is perfect as well, which one of the following expressions for the system reliability is correct (where each module has a reliability *R* and the modules are independent). Explain your answer. A correct answer with either no explanation or an incorrect one is worth only 2 point.

i. $R_{system}=R^4+4R^3(1-R)+3R^2(1-R)^2$

ii. $R_{system}=R^4+4R^3(1-R)+4R^2(1-R)^2$

iii. $R_{system}=R^4+4R^3(1-R)+5R^2(1-R)^2$

iv. $R_{system}=R^4+4R^3(1-R)+6R^2(1-R)^2$



(iii.) $R_{system}=R^4+4R^3(1-R)+5R^2(1-R)^2$，本題中第一項為全部working的reliability(C4取0)，第二項為壞掉一個(C4取1)，第三項為壞掉兩個(C4取2)，排列組合原本有6種可能，但並非壞兩個module都能夠working，要扣除module2與module3同時壞掉的狀況

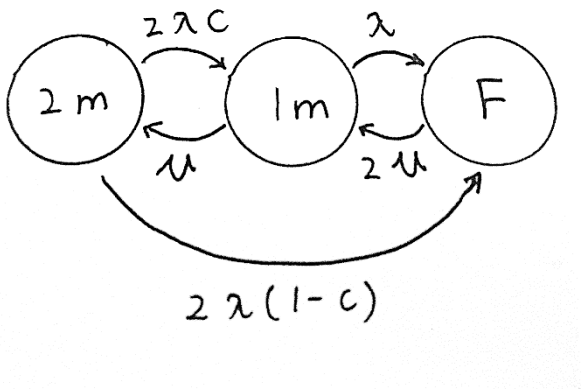
(b) **(5 points)** Write an expression for the readability of the system if instead of a perfect comparator for modules 1 and *a* there is a coverage factor *c*, i.e., *c* is the probability that a failure in one module is detected, the faulty module is correctly identified and the operational module is successfully connected to the voter (which is still perfect).

$R_{system}=R^4+4R^3(1-R)+(4c+1)R^2(1-R)^2$，本題中需要乘上coverage factor的地方是兩個module壞掉，且module1或module a其中一個壞掉的狀況總共有4種，module1與module a同時壞掉不需要乘

12. (10 points)

(a) **(5 points)** A duplex system consists of two active units and a comparator. Assume that each unit has a failure rate of λ and a repair rate of μ. The outputs of the two active units are compared and when a mismatch is detected, a procedure to locate the faulty unit is performed. The probability that upon a failure, the faulty unit is correctly identified and the fault-free unit (and consequently, the system) continues to run properly is denoted by *c* and is called the coverage factor. Note that when a coverage failure occurs, the entire system fails and then both units have to be repaired (at a rate μ each). When one unit is repaired, the system become operational and the repair of the second unit continues allowing the system to return its original state.

Show the Markov model for the duplex system.



(b) **(5 points)** Derive an expression for the steady-state availability of the system assuming that $\mu=2\lambda$.

$2\lambda P_2 = \mu P_1 \Rightarrow P_2 = P_1$

$2\lambda(1-c)P_2+\lambda P_1 = 2\mu P_F \Rightarrow P_F = P_1*((3-2c)/4)$

$P_1+P_2+P_F = 1 \Rightarrow P_1*((3-2c)/4+2) = 1 \Rightarrow P_1 = P_2 = 4/(11-2c)$

$P_1+P_2 = 8/(11-2c)$

13. (10 points)

To answer this problem, you will need to read (and understand) the paper "Sender-Based Message Logging" by D. B. Johnson and W. Zwaenepoel. The paper is provided at Ceiba.

In providing the answer, please use the following notation (from Section 4 of the paper). For process Pi, the following protocol variables are introduced:

- SSNi – the next sender sequence number to use;
- RSNi – the next receive sequence number to use;
- LOGi – a set containing logged message. Note that elements of this set are triples of the form (m, Pj, ssn);
- Ti' – a table associating to each process the highest SSN value received in a message sent by that process;
- Ti" – a table associating to each received message m, the RSN value returned by Pi when m was received.

Consider the scenario in which application processes P1, P2, and P3 exchange messages as described in Figure 1. Assume that sending a message from one process to another takes one unit of time. (Time units are represented by vertical dotted lines in the figure.)

(A) (5 points) Suppose that processes use the protocol described in Section 5.1 of the paper (do not consider the optimistic protocol of Section 5.4) for implementing message-logging based checkpointing.

Complete Figure 1 by showing:

a. The additional messages that the processes must exchange to support the message logging protocol.

b. Any information piggybacked on any message.

c. How protocol variables change as messages are exchanged. Assume that all processes start with SSN = 1, RSN = 1, Log = , T' = , T" = and no process takes a checkpoint. Show this in the form of a table with the columns representing the above 5 variables for each process and the rows representing the time intervals (from *t0* to *t11*) as the three processes execute.

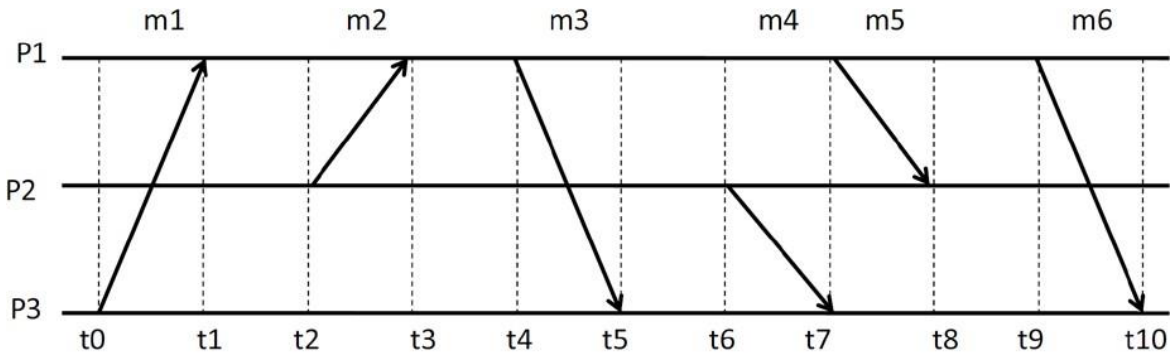


Figure 1: Process communication diagram

(B) (5 points) The paper proposes a recovery strategy without providing sufficient details for an actual implementation (see Section 5.2). Suggest and describe your own recovery protocol, based on that of Section 5.2, and show how it would work if, in Figure 1, process P3 crashes immediately after receiving message m6 (i.e., P3 does not send any message between receipt of m6 and the time it crashes). You can use the diagram in Figure 2 to show the messages exchanged by your recovery protocol and be precise in your answer.

Assume that P3 took its last checkpoint at time t0.

Be precise in your answer and do not write more than half a page.

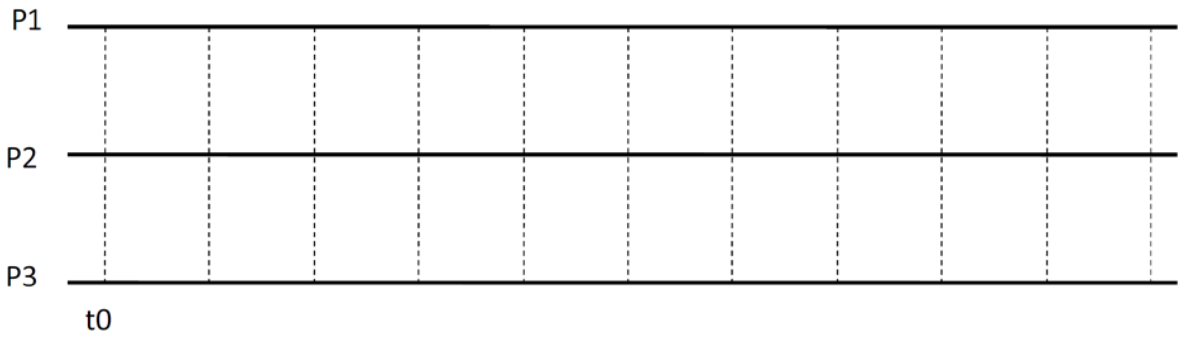


Figure 2: Diagram to depict messages exchanged