National Taiwan University

Department of Electrical Engineering

Fault Tolerant Computing

Midterm Exam, Nov. 19, 2018

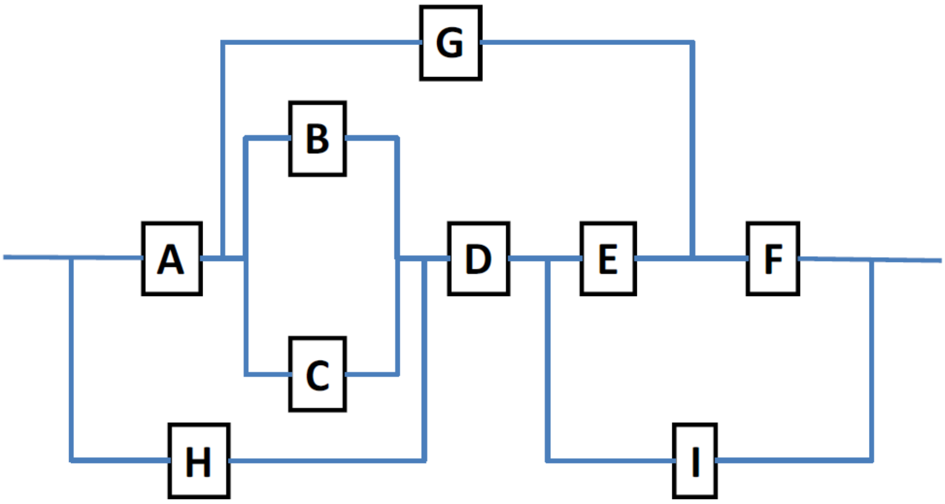
This is an open book exam. Feel free to consult any book, article, or notes. However, you cannot give or receive help from others during this examination period. All forms of calculating devices are permissible, so use them as you see fit. Please sign below, indicating that you agree with these terms.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

Student Name: 劉治硯 R07943098

Signature: 劉治硯

1. **(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:

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



$R_{System} \leq 1-(1-R_H R_D R_I)(1-R_H R_D R_E R_F)(1-R_A R_C R_D R_I)(1-R_A R_C R_D R_E R_F)(1-R_B R_C R_D R_I)(1-R_B R_C R_D R_E R_F)(1-R_A R_G R_F)$

假設所有的R_x=R

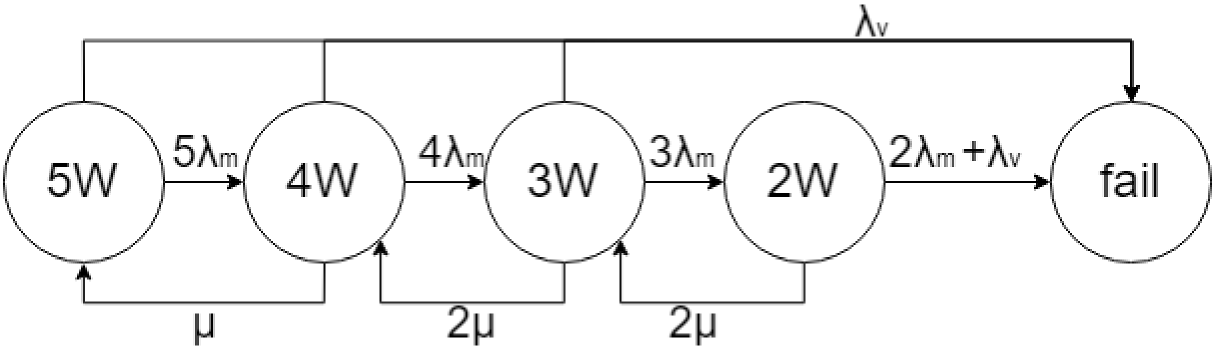
$R_{System} \leq$ R^28 - 2 R^25 - 3 R^24 - 2 R^23 + R^22 + 6 R^21 + 7 R^20 + 6 R^19 - 2 R^18 - 8 R^17 - 13 R^16 - 8 R^15 + 8 R^13 + 13 R^12 + 8 R^11 + 2 R^10 - 6 R^9 - 7 R^8 - 6 R^7 - R^6 + 2 R^5 + 3 R^4 + 2 R^3

2. **(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”.



3. **(5 points)** How many faulty modules can you tolerate in:

i. 5-modular passive redundancy?

正常>壞掉即可運作→2個

ii. Standby sparing redundancy with 5 modules?

有一個沒壞掉即可運作→4個

iii. Pair-and-a-spare redundancy with 5 modules?

至少存在兩個能用的→3個

4. **(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?

利用R(t)=$e^{-\lambda t}$求解$e^{-\lambda *3*365*24}$=0.73

λ = 0.00001197529(failures/per hour)

代入一年時間量0.1049035404(failure/per year)

ii. What is the MTTF of the copy machines?

MTTF=(1/λ)= 3479.38 (day)

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

MTBF=MTTF+MTTR=3481.38(day)

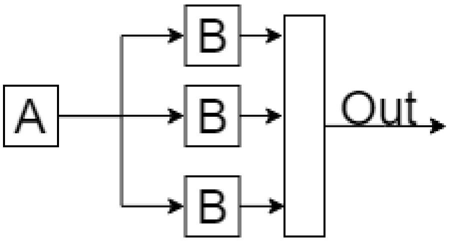
iv. Suppose that two copy machines work in parallel and the failures are independent. What is the probability of failure during the first year of operation?

利用R(t)=$e^{-\lambda t}$求解$e^{-\lambda *3*365*24}$=0.9

第一年時有10%機率壞掉，又因兩台為分開運作，因此兩台皆壞的機率為 10%*10%=1%

5. **(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.

多加兩個B的spare，則Reliability為1-(0.99*(1-0.15^3))= 0.01334125 < 2%

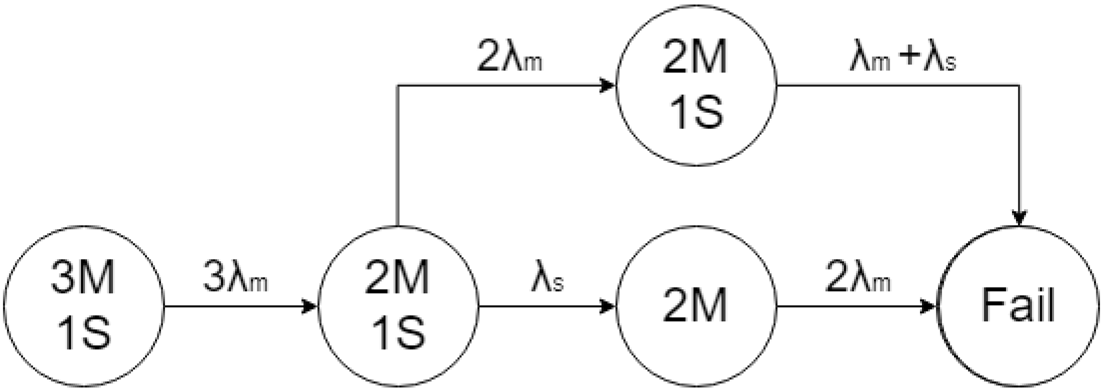


6. **(15 points)** Draw a Markov chain for 3-modular redundancy with one spare and the standard majority voter for the cases listed below.

(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.

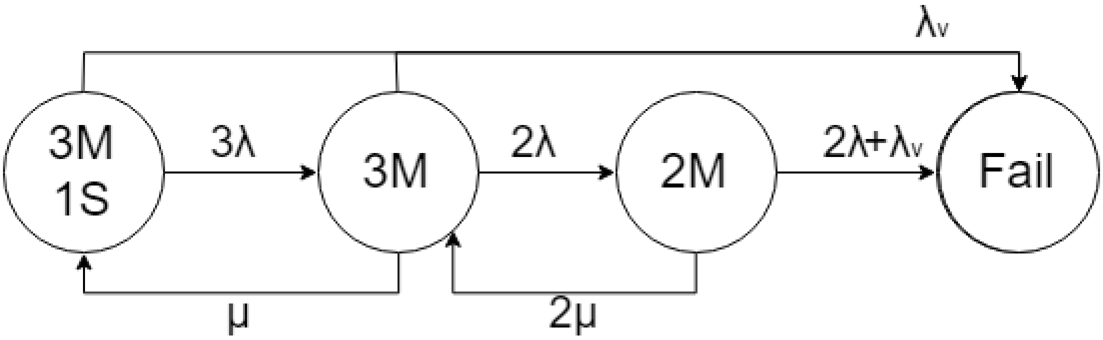
No repairs are allowed.



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

- The modules and the spare have the same failure rate λ. The voter has the failure rat 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.

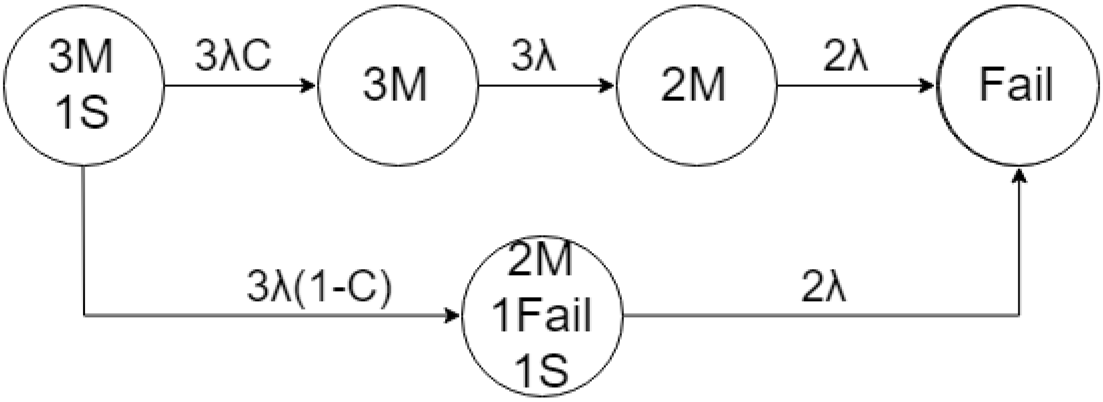
When the system fails, it shuts itself down.



(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.

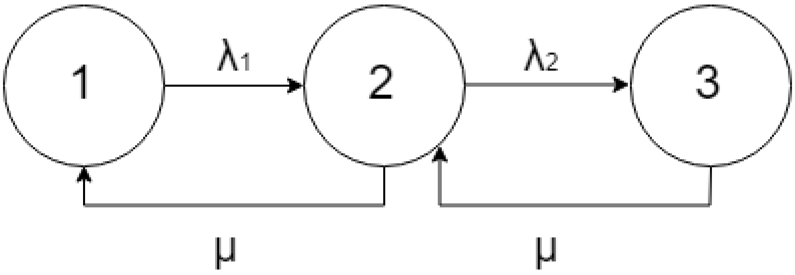
No repairs are allowed.



7. **(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.



8. **(5 points)** Check whether the function $f(a,b,c) = abc$ is self-dual.

不是。因其不滿足 f(a,b,c)=f’(a’,b’,c’)→真值表無從中間相反值對稱

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

9. **(10 points)** A standby redundant system composed of three components connected in parallel, each with a constant failure rate of λ 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.

R=1-(1- $e^{-\lambda}$)^3= $e^{-3\lambda}$-3$e^{-2\lambda}$+3$e^{-\lambda}$

- Name the distribution that best describes the time to failure of the system?

Exponential distribution

- Name the distribution that best describes the time to failure of the system if the failure rate of the three components were **not** identical?

Poisson distribution

(**Hint:** Reliability of a single component with a hazard/failure rate λ, R(t) = $e^{-\lambda}$

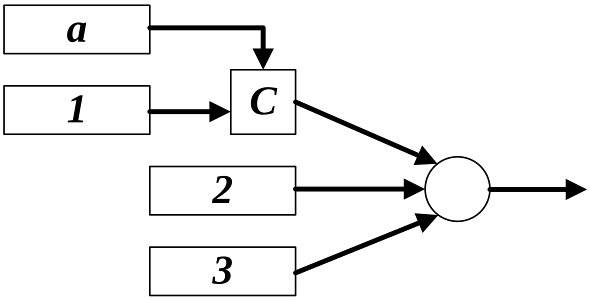
10. (a) **(5 points)** The system shown consists of a TMR core with a single spare *a* which can serve as a spare only for module 1. Assume that modules 1 and *a* are active. When either of the two module 1 or *a* fails, the failure is detected by the perfect comparator *C* and then the single operational 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. $R_{system}=R^4+4R^3(1-R)+6R^2(1-R)^2$



對 spare 那組而言，正常的機率為 $1-(1-R)^2$

所有的可能性為$(1-(1-R)^2)*R^2+(1-[1-(1-R)^2])R^2+(1-(1-R)^2)*2R(1-R)$

透過計算 R^2 可得答案為 iii. $R_{system}=R^4+4R^3(1-R)+5R^2(1-R)^2$

(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).

對 spare 那組而言，正常的機率變為 $R^2+2cR(1-R)$

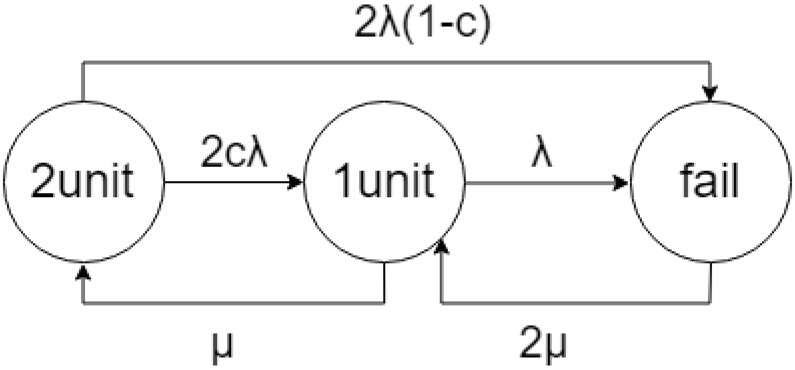
$R=(R^2+2cR(1-R))*R^2+(1-(R^2+2cR(1-R)))R^2+(R^2+2cR(1-R))*2R(1-R)$

$=R^4+2cR^3-2cR^4+R^2-R^4-2cR^3+2cR^4+2R^3-2R^4+4cR^2-4cR^3-4cR^3+4cR^4$

$=(4c-2)R^4+(2-8c)R^3+(4c+1)R^2$

11. (a) **(5 points)** A duplex system consists of two active units and a comparator. Assume that each unit has a failure rate of $\lambda$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 $\mu=2\lambda$.

$2\lambda P_2=\mu P_1$

$2\lambda(1\text{-}c)P_2+\lambda P_1=2\mu P_f$

$P_2+P_1+P_F=1$

$P_2= P_1$

$2(1\text{-}c)\ P_2+ P_1=4P_f \rightarrow (3\text{-}c)\ P_2=4P_f$

$P_2+P_1+P_F=1 \rightarrow P_2+P_2+(0.75\text{-}0.25c)\ P_2=1 \rightarrow (2.75+0.75c)P_2 =1 \rightarrow P_2=1/(2.75+0.75c)$

$P_1=1/(2.75+0.75c)$

Availability = $P_1+P_2=2/(\ 2.75+0.75c)$

12. **(20 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) (10 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.

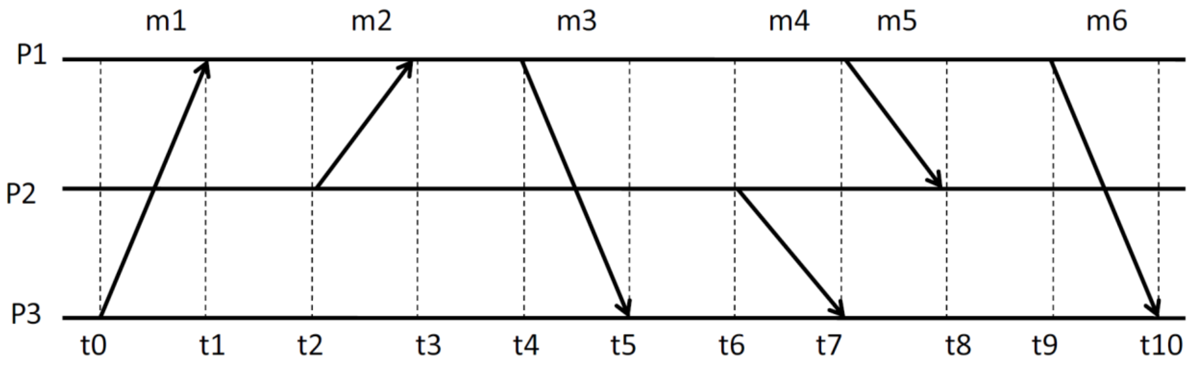
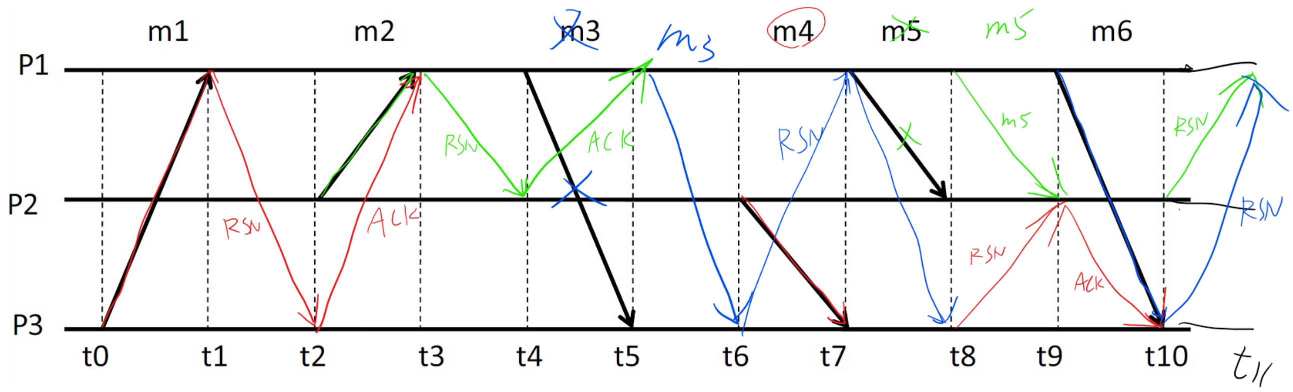


Figure 1: Process communication diagram



(B) (10 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.

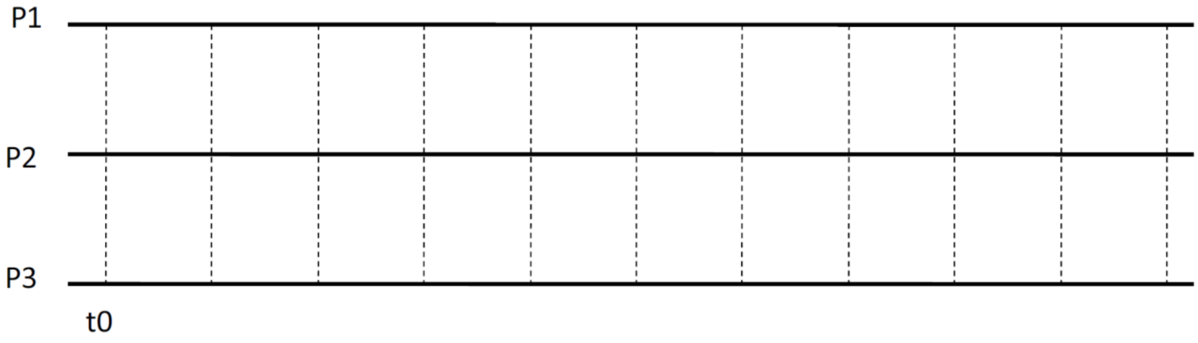


Figure 2: Diagram to depict messages exchanged