Étude de la cohérence dans les systèmes distribués

Journée DALGO

JOLY Amaury

Encadrants : GODARD Emmanuel, TRAVERS Corentin

LIS-LAB, Scille

6 juillet 2023

Table des matières

1 Introduction
- Introduction
- My internship

Présentation

- Amaury JOLY
- Master Informatique
  - Option Fiabilité Sécurité Informatique (FSI)

My Internship

- Begin in april
- Collaboration between Parsec and LIS-LAB
  - Parsec is a for-profit organization working on an open-source software named Parsec
  - It's a software architecture to file sharing with E2EE in a zero-trust approach
- Parsec want to add Collaborative Editing on their products :
  - With a zero-trust approach (so probably decentralized)
  - With a high avaibility and low latency approach
- Subject is *Weak Consistency Byzantin Fault Tolerent*

2 Distributed systems and consistency

- Définition

A distributed system

Definition

A distributed system is a group of **actors** able to comunicate **each-other** working together to **complete a common task**.

The system we consider on this presentation is a **asynchronous message-passing** system.

A distributed system is a living system

A distributed system changes over time.
There's some way to study these changes :

- focus on the **churn** (node addition and removal).
- focus on the **messages**.
- focus on the **connectedness**.
- focus on the **states**. $\Leftarrow$
- probably more... ?

The study of the state changes is also called the study of **consistency**.
A small exemple : A peer-to-peer discussion

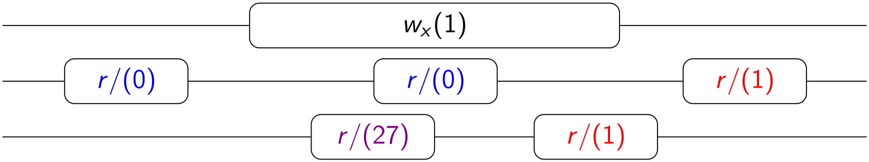
3 The compromises of consistency

- Strong consistency
- The compromises of the strong consistency
- In a malicious context ?

Safety

Definition

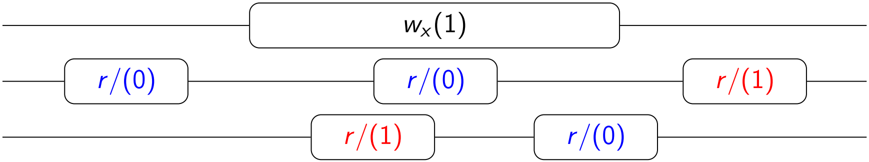
Each **read** operation made in the same **non-competitor** context provide the same result.



Regularity

Definition

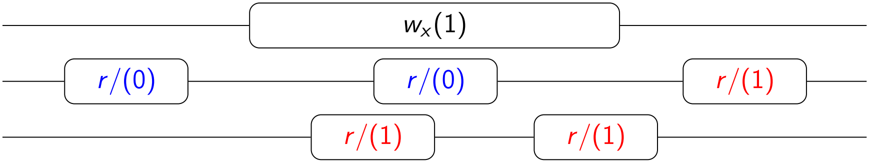
An **reading operation concurrent with a writing operation** must provide the value **before or after the write**.



Atomicity

Definition

If **two reading are non-competitor**, the second one must provide a value **at least as recent as** the previous one.



Atomic Consistency ($C_\top$)

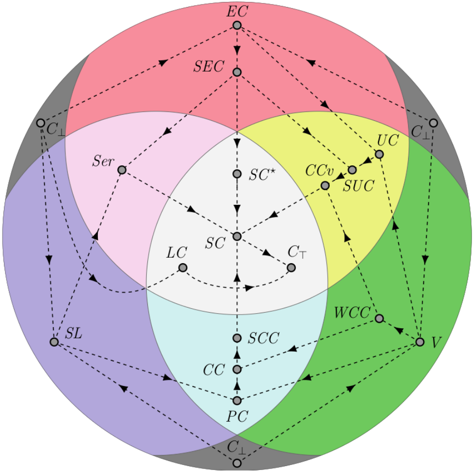
Définition

Atomic consistency is the stronger consistency class.

- Provide an awful interactivity.
- Need a strong synchronization between each operation.
  - Each read or write operation lock the others and need to wait the realease from the previous one.
- He's used as a reference for the other consistency class.

The models of consistency

a



Les classes de cohérences

2 big family :

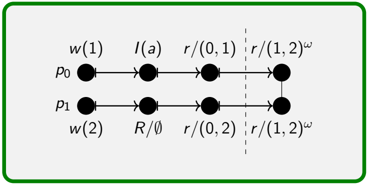
- Strong Consistency
- Weak Consistency :
  - Eventual Consistency (EC)
  - State Locality (SL)
  - Validity (V)

a. Perrin, Concurrence et cohérence dans les systèmes répartis, 2017

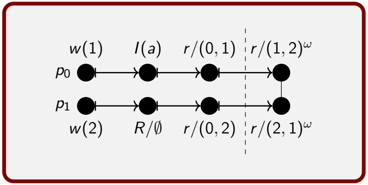
Eventual Consistency (EC)

Definition

There exist a set of confinite operations where each one must be justify with the same state.



$E' = \{r/(1,2)^\omega, r/(1,2)^\omega\}$
$\delta = ((1,2), \emptyset)$ is a valid state justifying E'.

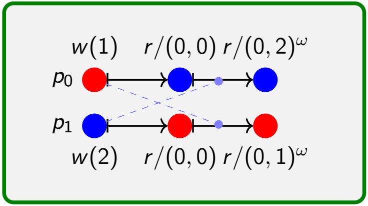


$E' = \{r/(1,2)^\omega, r/(2,1)^\omega\}$.
There exist no state able to justify E' because the two infinite read are not consistent.

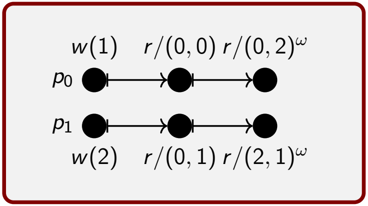
State Locality

Definition

For all p, there exist one linearization who include all the read operations of p. According to the local order of these reads.



$C_{p_0} = \{r/(0,0), r/(0,2)^\omega, w(2)\}$,
$C_{p_1} = \{r/(0,0), r/(0,1)^\omega, w(1)\}$,
$r/(0,0) \bullet w(2) \bullet r/(0,2)^\omega$
$r/(0,0) \bullet w(1) \bullet r/(0,1)^\omega$

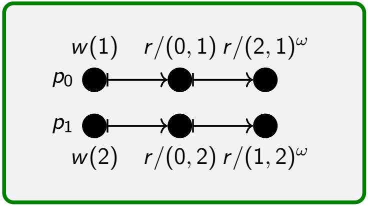


$E'_{p_0} = \{r/(0,0), r/(2,1)^\omega\}$,
$r/(0,0) \bullet w(2) \bullet w(1) \bullet r/(2,1)^\omega$
$E'_{p_1} = \{r/(0,1), r/(2,1)^\omega\}$.
There exist no linearization of p_1 satisfying the definition of state locality

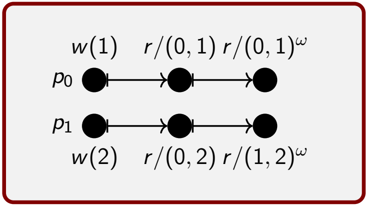
Validity (V)

Definition

There exist a cofinite set of operations such as for each of them must be justified by a linearization of all the write operation.



$$E' = \{r/(2,1)^\omega, r/(1,2)^\omega\}$$
$$w(2) \bullet w(1) \bullet r/(2,1)^\omega$$
$$w(1) \bullet w(2) \bullet r/(1,2)^\omega$$



$E' = \{r/(0,1)^\omega, r/(1,2)^\omega\}$.
There is no linearization of the write operation able to justify $r/(0,1)^\omega$.

The Byzantin context associate to the weak consistency

Some questions about :

- is the weak consistency introduce new possibility of malicious behaviours.
- is the weak consistency reduce by design the field of milicious behaviours.

The state of the art is poor about these questions and few formalized algoritms are avaible.

4 What's next ?

Conclusion

What's next ?

- Study and formalize some "in-prod" algoritms using weak consistency in byzantin contexts.
- Continue the colaboration with Parsec :
  - formalize a list of properties
  - provide a proof of concept of a colaborative editor