Cohérence faible byzantine appliquée au cloud

Présentation intermédiaire: "Practical Client-side Replication: Weak Consistency Semantics for Insecure Settings"

JOLY Amaury
Encadrants : GODARD Emmanuel, TRAVERS Corentin

LIS-LAB, Scille

9 juin 2023

Table des matières

Les processeurs multicœurs

Historique (1970)

- Besoin d'augmenter les performances des processeurs
  - Augmentation de la fréquence (limite physique)
  - Augmentation du nombre de processeurs (problèmes de cohérence)
- Lamport à défini des propriétés permettant de définir la notion de cohérence forte.
- L'approche de Lamport est de classer l'exécution et non pas l'algorithme.

> *"A correct execution is achieved if the results produced are the same as would be produced by executing the program steps in order."* [a]

a. Lamport, How to Make a Multiprocessor Computer That Correctly Executes Multiprocess Programs, 1979

La généralisation aux systèmes distribuée

Historique (1980)

- Lamport étend sa définition de la cohérence forte aux systèmes distribués. [a]
- Il définit trois propriétés :
  - **Sûreté**
  - **Régularité**
  - **Atomicité**
- Une exécution qui respecte ces 3 propriétés est dite linéarisable.

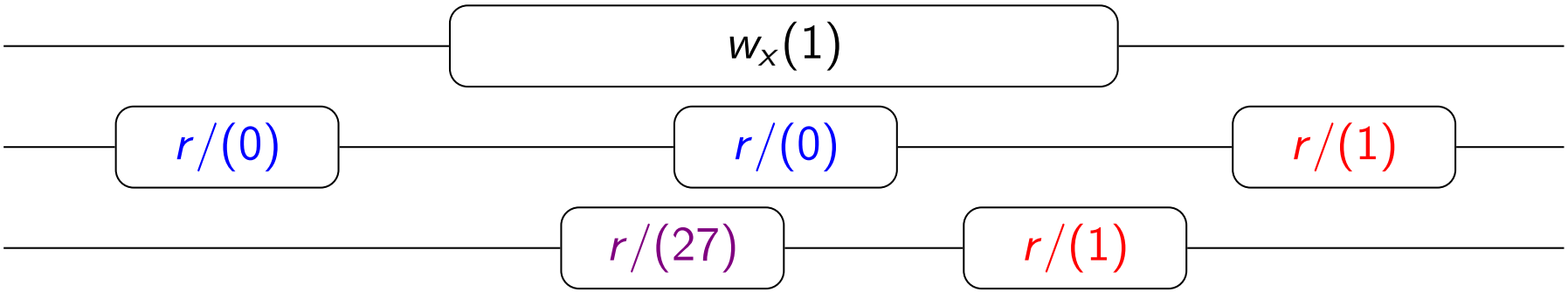
---

a. Lamport, On interprocess communication, 1986

Sûreté

Définition

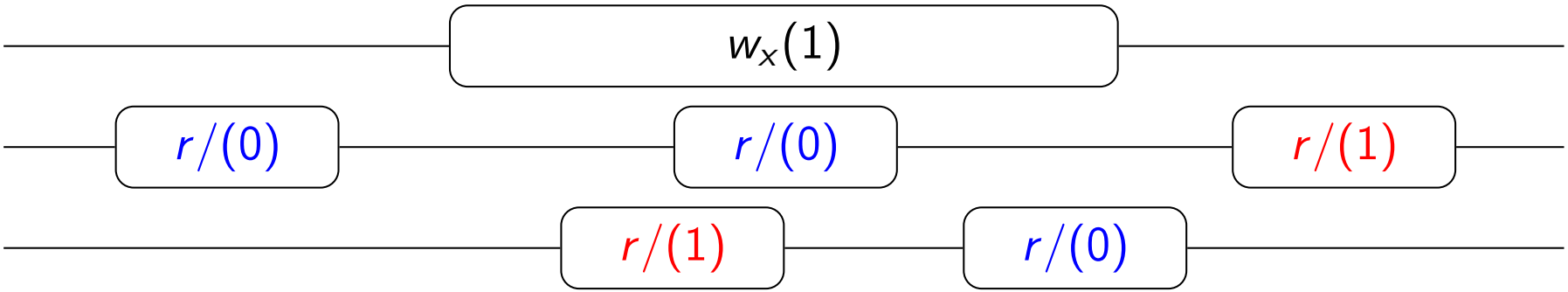
Toute lecture réalisée dans un même environnement non-concurrent est identique.



Régularité

Définition

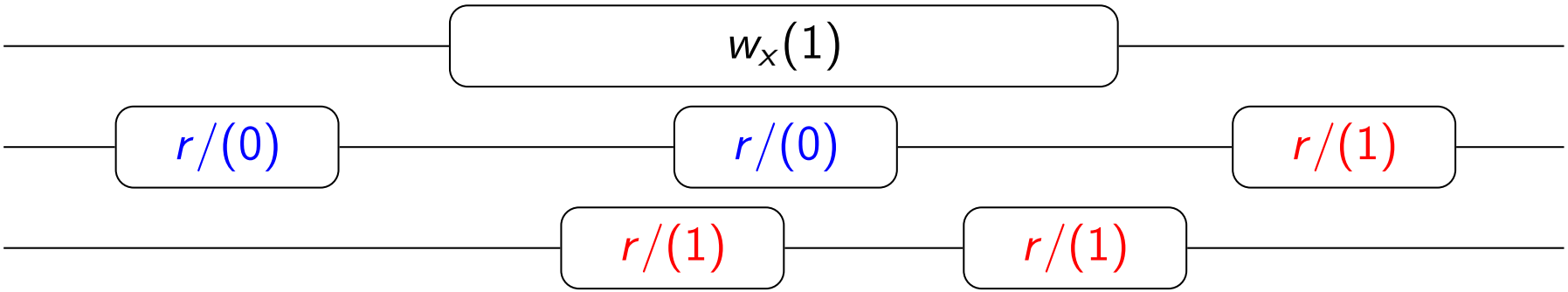
Une lecture concurrente à une écriture peut lire soit la valeur avant l'écriture, soit la valeur après l'écriture.



Atomicité

Définition

Si deux lectures ne sont pas concurrente la deuxième doit retourner une valeur au moins aussi récente que la première.



Cohérence Atomique ($C_\top$)

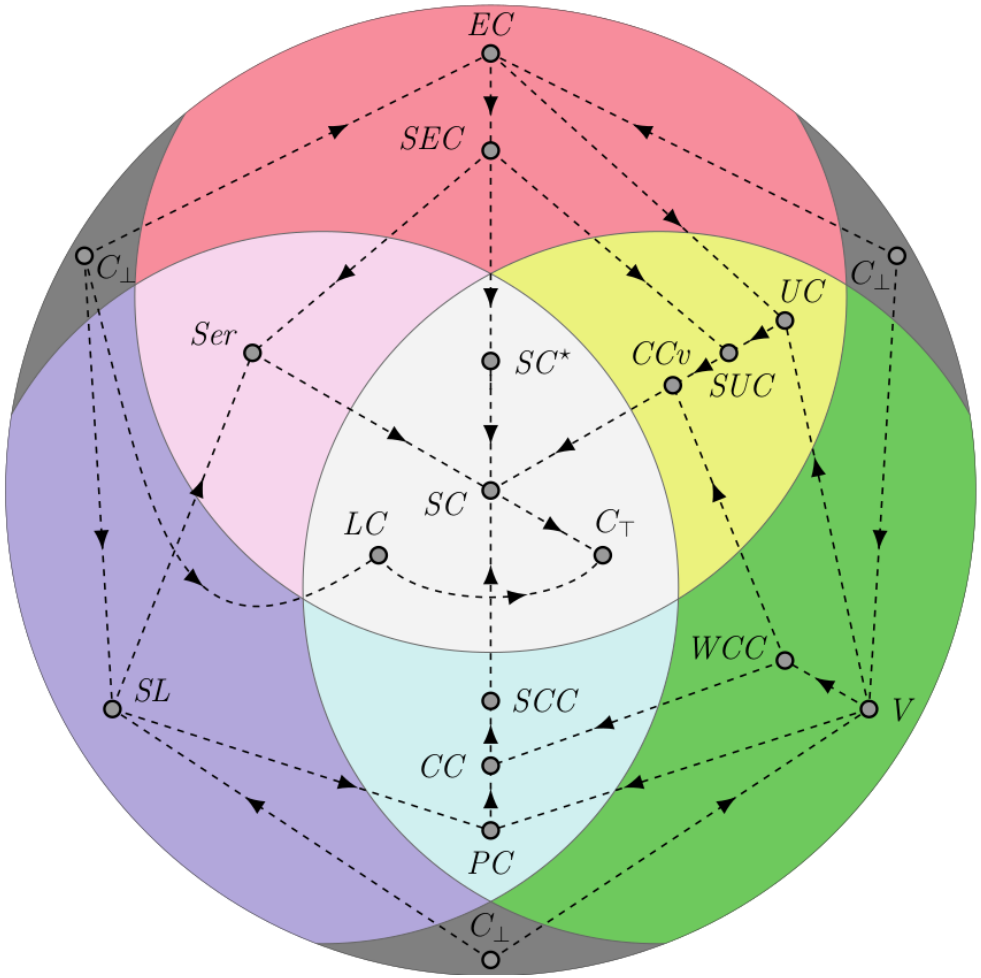
Définition

La cohérence atomique est le critère de cohérence le plus fort existant.

- Il est le moins efficace en terme d'interactivité.
- Il demande une synchronisation entre les opérations
  - Chaque opération d'écriture ou de lecture est bloquante et doit attendre la fin de la précédente.
- Il est utilisé en tant que référence.

Les modèles de cohérences

a



Les classes de cohérences

2 Grandes familles :

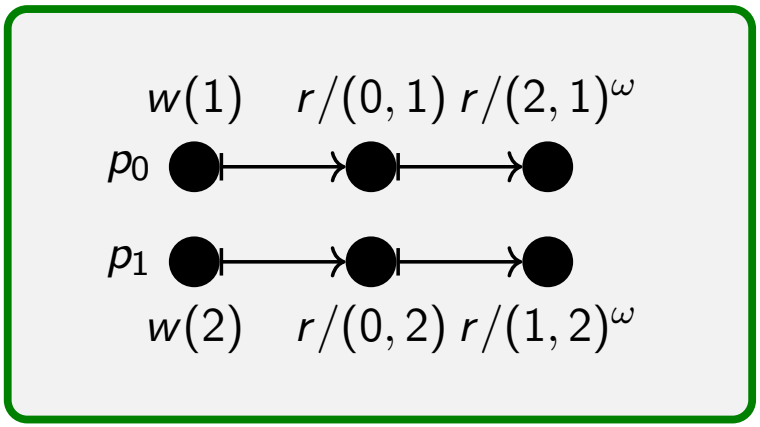
- Cohérence Forte
- Cohérence Faible :
  - Localité d'état (SL)
  - Convergence (EC)
  - Validité (V)

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

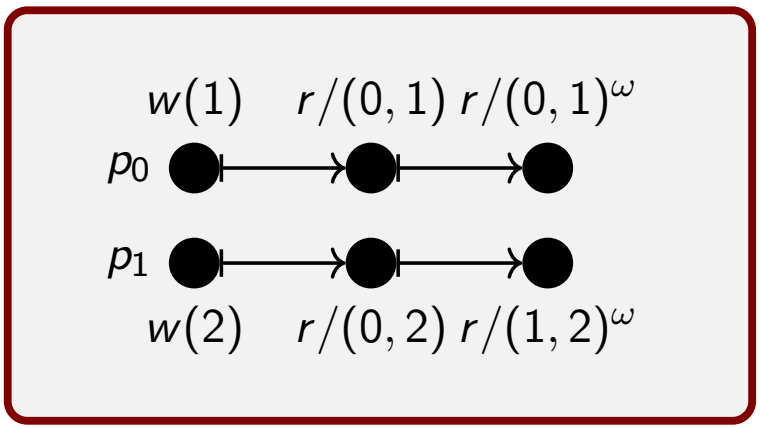
Validité (V)

Définition

Il existe, un ensemble cofini d'événement tel que pour chacun d'entre eux une linéarisation de toutes les opérations d'écriture les justifient.



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

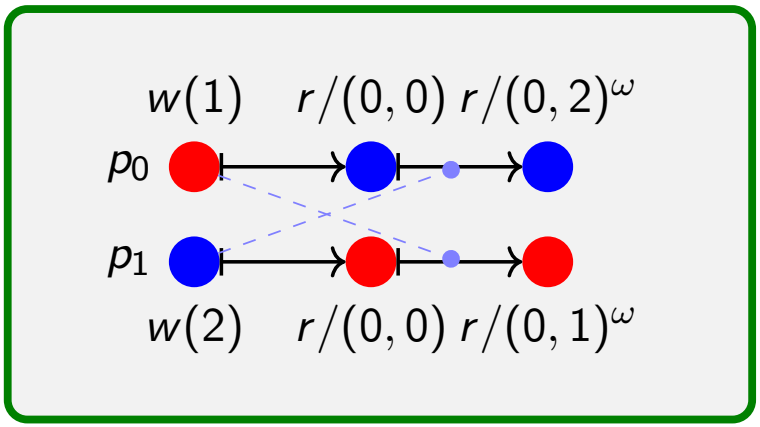


$E' = \{r/(0,1)^\omega, r/(1,2)^\omega\}$.
Il n'existe pas de linéarisation des opérations d'écritures qui justifie $r/(0,1)^\omega$.

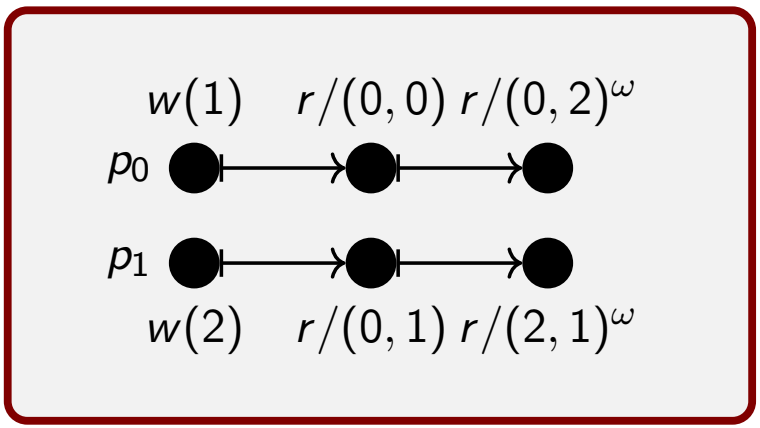
Localité d'état

Définition

Pour tout processus p, il existe une linéarisation contenant toutes les lectures pures de p. Respectant l'ordre local de ces lectures.



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

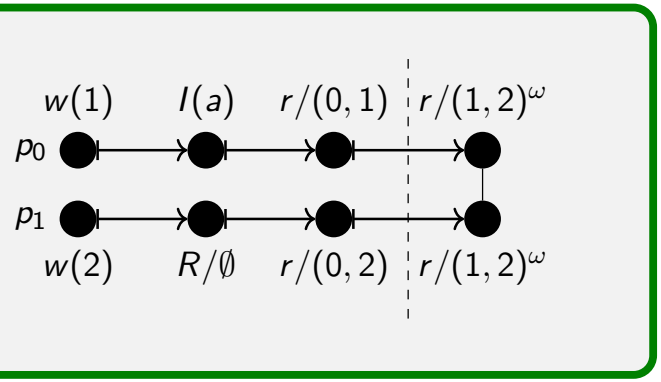


$E'_{p_0} = \{r/(0,0), r/(2,1)^\omega\}$,
$r/(0,0) \bullet w(2) \bullet w(1) \bullet r/(2,1)^\omega$
$E'_{p_1} = \{r/(0,1), r/(2,1)^\omega\}$.
Il n'existe pas de linéarisation de p_1 respectant la localité d'état.

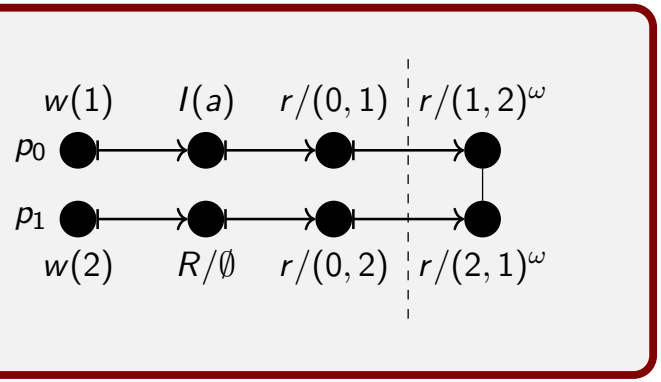
Convergence (EC)

Définition

Il existe un ensemble cofini d'événements dont chacun peut être justifié par un seul et même état.

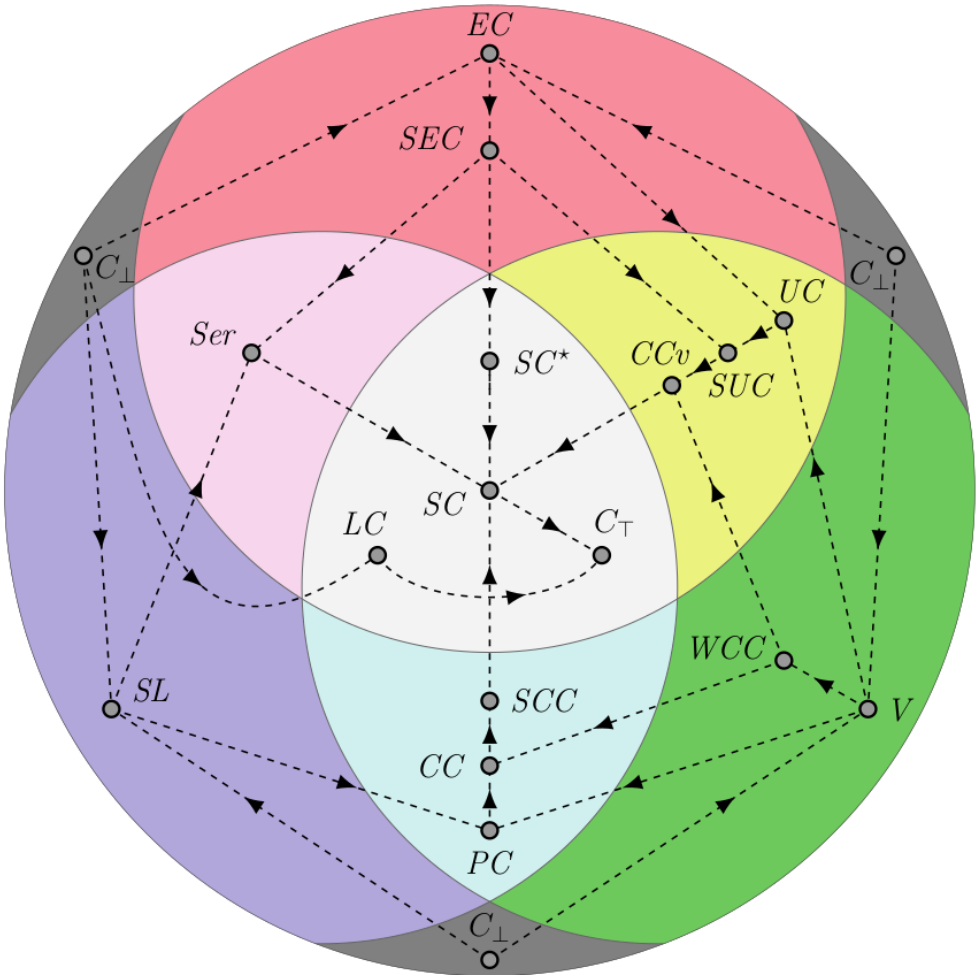


$E' = \{r/(1,2)^\omega, r/(1,2)^\omega\}$
$\delta = ((1,2), \emptyset)$ est un état possible justifiant E'.



$E' = \{r/(1,2)^\omega, r/(2,1)^\omega\}$.
Il n'existe aucun état possible justifiant E' puisque deux lectures infinies sont incohérentes.

Cohérence Causale



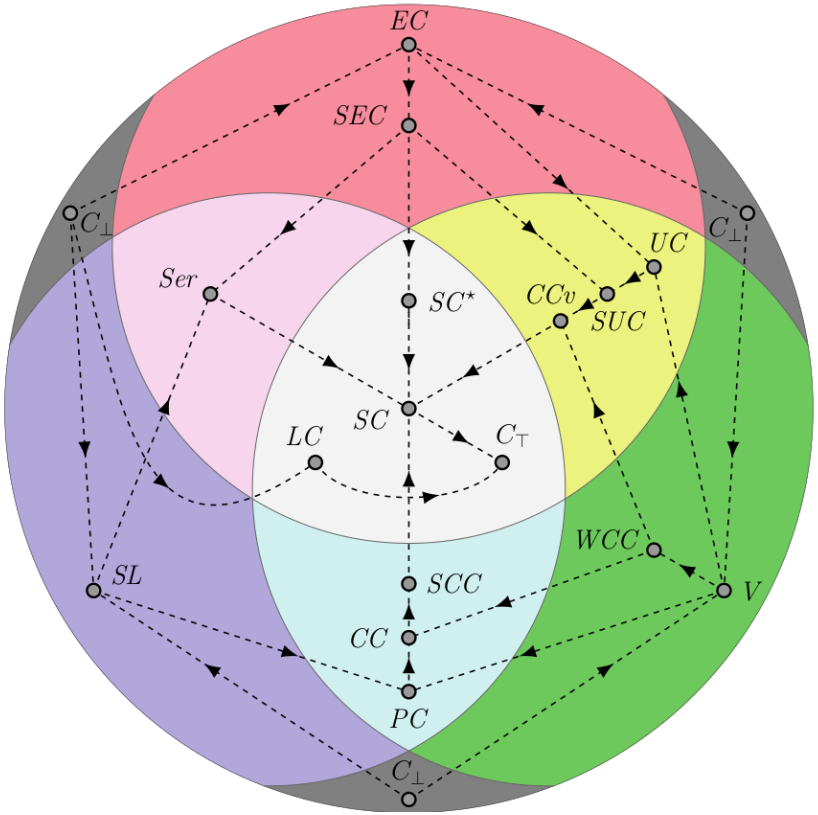
Les classes de la cohérence causale

- **WCC** : Weak Causal Consistency (V)
- **CCv** : Causal Convergence (V, EC)

On respecte les propriétés suivantes :

- Localité d'état (SL)
- Convergence (EC)

Cohérence Causale (Convergente)



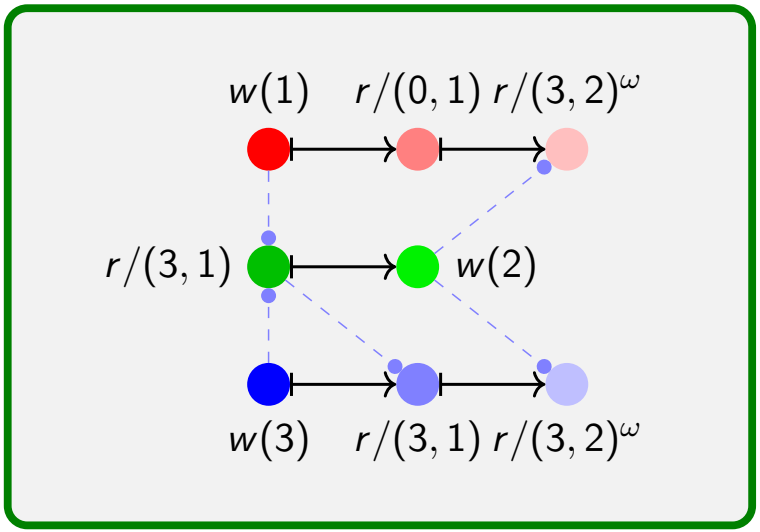
La cohérence causale selon Van Der Linde

Usage du terme **Causal Consistency** qui pourrait être confondue avec la Cohérence Causale de Perrin.
Mais s'approche plus de ce que Perrin qualifie de **Convergence Causale** (ou Causal Convergence (CCv)).
Les auteurs souhaitent privilégier la **Convergence** à la **Validité**.

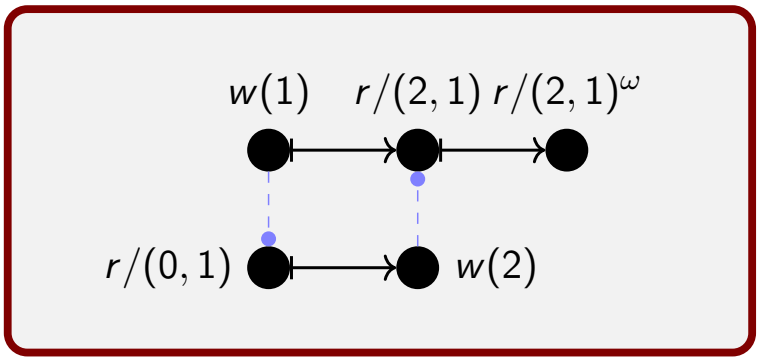
Cohérence Causale Faible (WCC)

Définition

Il existe un ordre causal tel que pour chaque lecture, il existe une linéarisation du passé causal de cet événement le justifiant.



$w(1) \bullet r/(0,1)$
$w(3) \bullet w(1) \bullet r/(3,1)$
$w(3) \bullet w(1) \bullet r \bullet r/(3,1)$
$w(1) \bullet w(3) \bullet r \bullet w(2) \bullet r/(3,2)$
$w(1) \bullet w(3) \bullet r \bullet w(2) \bullet r \bullet r/(3,2)$

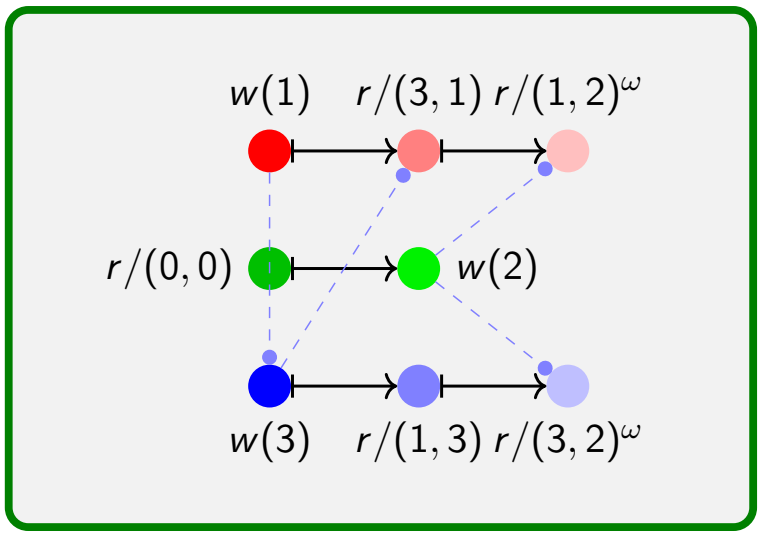


$w(1) \bullet r/(0,1)$
Ici il n'est pas possible de trouver un ordre causal qui permette de linéariser le passé causal de $r/(2,1)$.

Cohérence Causale Faible (WCC)

Définition

Il existe un ordre causal tel que pour chaque lecture, il existe une linéarisation du passé causal de cet événement le justifiant.



$r/(0,0)$

$w(1) \bullet w(3) \bullet r/(3,1)$

$w(3) \bullet w(1) \bullet r/(1,3)$

$w(1) \bullet w(3) \bullet r \bullet w(2) \bullet r/(1,2)^\omega$

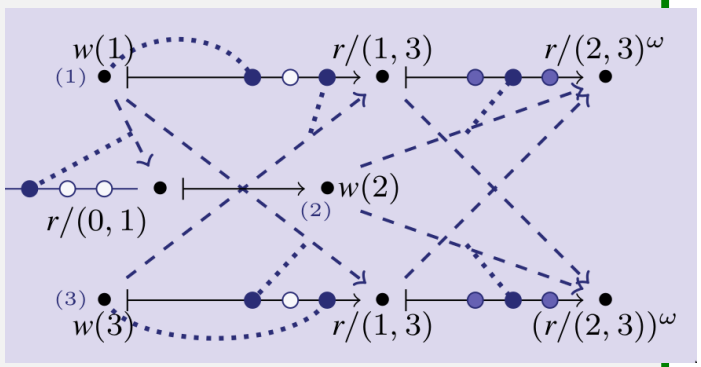
$w(3) \bullet w(1) \bullet r \bullet r \bullet w(2) \bullet r/(3,2)^\omega$

Cet exemple respecte la validité, mais pas la convergence.

Convergence Causale (CCv)

Définition

Il existe un ordre causal et un ordre total tel que pour chaque lecture, il existe une linéarisation du passé causal de cet événement trié suivant l'ordre total le justifiant.



Résumé de l'article

Apports

- Formalisation des attaques possibles sur les systèmes satisfaisant la convergence causale.
- Définition de propriétés permettant de contrer ou de limiter ces attaques.
- Formalisation de "nouvelles" classes de cohérence faible étendant la cohérence causale à ces propriétés : "Secure Causal Consistency".
- Présentation d'algorithmes produisant des histoires satisfaisant cette classe.
- Expérimentation de ces algorithmes et comparaison avec les algorithmes existants.

Résumé de l'article

Attentes

Les auteurs cherchent à produire un algorithme maximisant l'interactivité et donc minimisant la latence.
L'architecture étudiée est une architecture client-serveur, avec une connectivité en pair à pair entre les clients.

Illustration de l'architecture

Attaques

Attaques

- **Tempering** : Anticipation d'une opération reçue par le système, mais pas encore exécutée par l'ensemble des nœuds.
- **Omitting Dependencies** : Création d'une opération suivant un sous ensemble des dépendances réelles.
- **Unseen Dependencies** : Anticipation d'une opération non reçue par le système, mais probable d'arrivée.
- **Sibling Generation** : Création de deux opérations différentes possédant le même identifiant. Réalisant ainsi une divergence entre les nœuds.

Propriétés

Propriétés

- **Immutable History** : Chaque opération est envoyée avec son passé causal. (Parade le **Tempering**)
- **No Future Dependencies** : Chaque opération est envoyée avec l'état qu'il connait des nœuds. (Parade l'**Unseen Dependencies**, il devient impossible de créer une opération à l'avance).
- **Causal Execution** : Toute opération o_i appartenant au passé causal d'une opération o doit être sérialisable t.q. : $o_i < o$. (Fait office de synchronisation entre les nœuds)
- **Eventual Sibling Detection** : Les opérations sont considérées comme des "jumeaux" éventuels et sont donc "révocables" via une nouvelle opération dédiée. (Parade (relativement) le **Sibling Generation**)
- **Limited Omission** : à travailler

Ces propriétés définissent la première classe que les auteurs introduisent : **Secure Causal Consistency**.

Les différentes classes de cohérence faible

Les différentes classes de cohérence faible

- **Secure Causal Consistency** : Respecte les propriétés précédentes ainsi que celles introduites par la convergence causale.
- **Secure Strict Causal Consistency** : Extension de la précédente, mais avec un ordre total basé sur la vision d'un observateur externe.
- **Extended Secure Causal Consistency** :