

Chapitre 1 : Principes et mécanismes de base des systèmes distribués

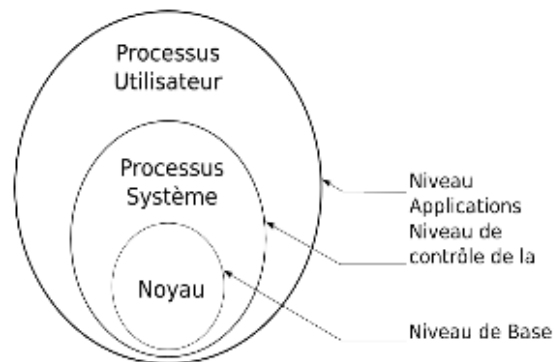
1) Introduction

1.1 Rôles d'un SD

Système réparti = système distribué

Système monosite (d'exploitation) : 2 grandes parties :

- le noyau
- les processus (système et utilisateur)



Les différents niveaux d'un système d'exploitation

Système distribué : machines sur plusieurs sites à faire fonctionner ensemble

Système dans lequel les processus vont communiquer entre eux, sur plusieurs machines différentes, pour réaliser une application.

Système d'exploitation distribué \neq SD : doit faire le travail d'exploitation.

Assuré les mécanismes de base des systèmes d'exploitation sur plusieurs machines (E/S, file system, ordonnancement).

Problème général avec les systèmes distribués : savoir si le processus est terminé (problème de variation de bande passante dans le réseau par exemple) \rightarrow Mécanismes de contrôles liés à la distribution = nouveaux problèmes.

Appli a récupérer un ensemble de processus défini par qqn avec des contraintes, assurer quelle fonctionne correctement.

Contrôle de la
distribution

Base

Rôle d'un OS distribué : offrir aux applications les moyens de s'exécuter.
Assurer le partage et la communication d'informations entre les applications.
Assurer l'exécution parallèle.
Partager les ressources physiques et logiques sur un ensemble d'utilisateurs.

Mécanismes à mettre en place :
L'ordonnancement, placement de processus.
Synchronisation, terminaison.
Désignation, nommage, partage d'informations.
Contrôle de l'état global.
Cohérence.
Diffusion d'informations.
Exclusion mutuelle.
Reprise sur panne.
Sécurité.
Administration.
Transactions.

Communication entre deux processus :
sur la même machine : mémoire partagée à architecture fortement couplée, lorsque les processus communiquent via une mémoire globale.
Durée d'une communication est négligeable.

sur des machines différentes : par messages à architecture faiblement couplée, lorsque les processus communiquent par échange de messages (via le réseau).
Il faut tenir compte de la durée des communications (en plus possibilité de pertes de messages).

Système symétrique (turing) \neq système distribué.
Architecture parallèle avec mémoire globale à le système va être symétrique.

1.2 Caractéristiques des SD

On étudiera que des systèmes distribués faiblement couplés.

- Absence d'état global :
Comment faire pour savoir en quel état doit reprendre le processus après une panne. On n'est pas capable de savoir ce qu'il y a sur le réseau.
Un processus ne connaît que les événements qu'il a provoqués sur son site.
Un processus ne connaît que les messages qu'il a envoyés ou reçus.
Il n'y a pas d'ordre temporel naturel entre les événements.

Il est difficile de synchroniser deux horloges (impossible)
Il n'y a pas d'échelle.

- Distribution des données

Deux cas :

- distribution inhérente aux problèmes : le concepteur se voit imposé, par exemple, une distribution

géographique (disques de Bases de données sur plusieurs sites, ...)

- distribution inhérente à la mise en oeuvre : les utilisateurs veulent pouvoir travailler sur des sites distants.

d'où

- duplication : une donnée peut se trouver dupliquée sur plusieurs sites => problème de cohérence
- partitionnement : une grande BD peut être coupée en plusieurs sous-BD sur des sites différents => problème de désignation (comment retrouver une donnée de la base : il faut d'abord savoir sur quel site elle se trouve)

Bien évidemment, les deux peuvent se faire en même temps.

- **Contrôle**

On dira qu'il y a contrôle distribué lorsqu'il n'y a pas de relation hiérarchique statique

entre les processus : il n'y a pas de processus qui joue de rôle particulier a priori. Ainsi,

il n'y a pas de maître qui assure en permanence le contrôle global.

Pourquoi :

- tolérance aux fautes faible voire nulle : si ce processus s'arrête => n du système ;
- goulet d'étranglement.

Il se peut que pour certaines fonctions du système, il y ait nécessité d'un maître : on utilisera alors un mécanisme d'élection.

2 Éléments de base des SD

2.1 Protocole

Un protocole définit le comportement d'un processus vis-à-vis d'autres processus : on va s'intéresser principalement (et presque uniquement) aux réactions du processus à la réalisation d'événements : réception d'un message, réalisation d'une condition, émission d'un message, etc. :

P_i: Processus réserve et utilise une imprimante

demande : D€M(1)

- emettre la demande à tous les autres processus
- compteur nb de processus compt=N-1
- attente

* Sur reception d'une demande D€M(j)

* Suivant l'état de P_i

- LIBRE : répondre (OK) à P_i
- OCCUPE : NOK
- ATTENTE : si (i<j) => NOK

* Sur NOK(j)

/* recommence le protocole demande() */

* Sur OK(j)

compteur de processus compt --

si (compt==0) => P_i passe à l'état OCCUPE

- On ne s'intéresse que très peu à ce qui se passe en local. En eet, on suppose que localement, on dispose de ressources logicielles pour réaliser les opérations. La seule contrainte est que le processus dispose de toutes les données nécessaires aux calculs.

- On considère que l'envoi et le réception de message est réalisé par le système d'exploitation

2.2 Processus

2.3 Liaisons

- structure de liaison inter-sites.
- comportement de liaisons.

2.3.1 Structure des réseaux "virtuels" (propriétés structurelles)

- maillage complet
- hiérarchie
- étoile
- anneaux (uni-directionnel, graphe de communication des sites)

2.3.2 Comportement du réseau (propriétés comportementales)

H1 - Les messages ne sont pas dupliqués.

H2 - Un message, s'il arrive, n'est pas altéré.

H3 - Pas de déséquence.

H4 - Le délai d'acheminement d'un message est fini. Tout message arrive en un temps fini.

H5 - Le délai d'acheminement d'un message est borné.

H1+H2+H3+H4 = FIFO

Il faudra toujours préciser les propriétés comportementales du réseau de communication inter-processus.

2.3.3 Trafic

Ordre d'optimisation :

- Nombre d'échange de messages.
- Taille des messages.
- Calculs locaux.

3 Techniques d'implantation des protocoles

P_{i0} veut diffuser ($i=1$)

P_{i0} envoie $M(i=1)$ à suivant (P_{i0})

P_i :

- Lorsque P_i reçoit $M(m=k,j)$

* si $i=j \Rightarrow$ FIN

* si $i \neq j$

// toutes M

envoie $M(n=k,j)$ à suivant P_i

3.1 Jeton circulant

3.2 Calcul diffusant

4 Conclusion

La construction d'algorithmes ???

M2 : mount -t nfs //M1:/users /home

Selon la version de Linux on utilisera plutot share (solaris) ou fstab

share => exportfs

fstab => export

d1 |-| M1 / | \ | M2 / | \ etudiant
système d'interprétation pour connaitre le contenu de /home,
|-| etc bin users | etc bin users
de contacter M1, il va envoyer un message à M1 en utilisant un service
/ nfsd
auparavant => on envoi read sur le nfsd.
d2 |-| master 1 |
|-| /
seul il attend des messages tels que read, write
f1 |

cat /home/master 1/f1
il doit faire un appel

le système va essayer
(demon) mis en place

nfsd ne fait rien tout

3.3 Cohérence des données

3.3.1 Definition

Utilisation du cache, cohérence faible

Schema 8

On ne veut pas sauvegarder à chaque fois les données dans la base principale, on a donc bd1 et bd2 qui sont des copies de la base principale mais qui ne contiennent pas forcément les dernières données à jour, d'ou une cohérence faible. Pour compenser il faut faire une mise à jour chaque soir pour réorganiser les données et que chaque base reçoive un contenu identique.

Pourquoi utiliser la cohérence faible ?

Car ca simplifie les manipulations sur les bases séparées, et utilisées par des utilisateurs différents.

Cohérence faible :

- une copie peut être temporairement incohérente

- l'ordre des mises à jour d'une information n'est pas nécessairement celui de sa modification première.

Avantage => mécanisme simple.

Inconvénient => une copie peut être incohérente à un moment donné.

Cohérence forte :

Deux méthodes :

- Centralisé :

1) on vérifie que la base de donnée locale est la bonne => on vérifie que notre n° de version correspond à celui de la base principale

2) on doit mettre à jour sur la base principale la donnée modifiée, pour éviter les accès simultanés et des modification de la donnée en même temps, on verrouille la donnée

quand

on effectue la vérification lors de l'étape 1).

Inconvénient : temps d'attente du au verrouillage de la donnée (exclusion mutuelle), et système centralisé.

Schema 9

- Distribuée :

On numérote les modifications de la donnée

Quand on veut accéder à la donnée on fait une demande au serveur et on attend l'aquittement

Si il y a plusieurs versions, on envoi celle dont le N° de modification est le plus grand (code opération). La donnée est renvoyée à la base locale en même temps que l'aquittement.

=> Cohérence forte : Chaque fois qu'un site accède sa copie, la valeur de cette copie doit refléter le résultat de toutes les modifications antérieures.

Avantage : Pour chaque accès à une copie de la donnée, sa valeur correspond bien au résultats des dernières modifications effectuées.

Inconvénient : Echanges de messages (demandes/aquittement) => temps perdu

Evenements:

Si il y a un lien de causalité entre deux evt, je veux que cela influe sur l'ordre des evt que la donnée devra traverser.

Cohérence causale : Si deux événements de modification peuvent être causalement ordonnés alors les prise en compte doivent être fait dans cet ordre.

3.3.2 Cohérence et cache

Schema 10

3.3.3 Détection de l'incohérence

Avant on définissait un protocole qui maintenant la cohérence, cependant il n'est pas forcément tjrs utile que ce protocole tourne tout le temps, on peut en fonction de la probabilité d'une incohérence détecter et corriger l'incohérence.

Mécanisme de détection de l'incohérence :

Précédement dans le shema distribué, la tolérance au pannes était nulle, si on perdait un message d'aquittement le système plantait.

On veut permettre à l'application de continuer à travailler malgré une interruption, on a la détection d'une incohérence et on veut donc reconstruire la donnée (la détection n'a d'ailleurs de sens que si on est capable de reconstruire la donnée)

Chapitre 5 : Exclusion mutuelles

5.1 Rappel

5.1.1 Propriété

Définition :

- une section qui correspond à du code auquel l'accès doit se faire de façon exclusive.
- le protocole d'exclusion mutuelle a pour but de garantir cette exclusivité, à un instant, au plus un processus peut se trouver en Section Critique (SC)

Propriété :

* **Atteignabilité** : Si plusieurs processus sont bloqués en attente de la Section Critique alors que aucun processus n'est en SC (la SC libre)

Alors un de ces processus entrera en SC en un temps fini (*le plus court possible indépendamment de l'application*).

* **Progression** : Un processus qui demande à entrer en SC, y parviendra dans un temps fini (*temps qui peut être grand ou petit mais dépend de l'application*).

* **Indépendance** : indépendance entre partie(s) conflictuelle(s) et non conflictuelle(s) : un processus hors de la SC (ou ne demandant pas) ne doit pas influencer sur le protocole d'Exclusion Mutuelle.

* **Banalisation de la solution** : il n'y a pas de processus privilégié.

5.1.2 Monoprocessus

Différentes solutions :

- variable de condition (*variable globale*)
- variable "test & set" (*on test puis modifie une variable (une seule)*)
- moniteur
- sémaphore (*2 opérations : si valeur 1 on peut décrémenter on entre en SC si la valeur 0 on reste bloqué*)

Pour être sûr de ne pas être interrompue le plus simple est de bloquer de le bus, on masque des interruptions, cependant ce système est incompatible avec les solution citées ci dessus en particulier les sémaphores qui ne partagent pas le bus. Ces solutions sont ainsi incompatibles avec des architectures distribuées.

Solutions totalement distribuées => démon

5.2 Algorithme de la boulangerie

5.2.1 Principe

- > un processus S1 voulant entrer en SC s'affecte un numéro $N_i = \max(N_{j \neq i} + 1)$
- > puis Si attend que $N_i = \min(N_{j \neq i} - 1)$
- > Lorsque Si quitte la SC, $N_i = -1$

Dans chaque processus, on dispose d'une table $num[i..N]$ initialisé a (-1), on veut avoir dans la table les numéros des processus en attente.

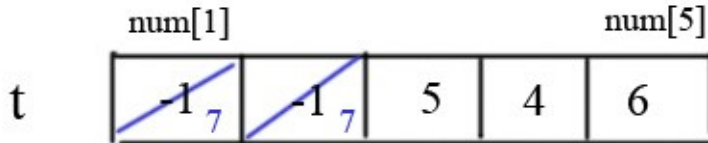
(on a besoin de maintenir cette table à jour uniquement lorsque l'on veut entrer en SC)

-> dem_num(j) (demande le numéro du processus j) \Leftrightarrow if (num(j) != -1)

->

```
Entrer SC() {
  num[i]=max(num[j≠i])+1
  Attendre que (num[i]=min(num[j≠i]) avec num[j]≠-1 )
}
sortie SC() { num[i]=-1 }
```

Exemple:



t=2 S2 veut entrer en SC il s'affecte 7
S2 test num[3] -> 5
S2 test num[4] -> 4

t=3 S1 veut entrer en SC il s'affecte 7
S2 test num[5] -> 6
S1 test num[2] -> -1 => S1 se met dans num[2] et affecte 7
S2 test num[1] -> -1 => S2 se met dans num[1] et affecte 7

Problème il y a désormais deux case initialisées à 7

Solution : lors de l'affectation on ajoute le num à la valeur à affecter => S1 on affecte 7+1

- Accès au tableau \leftrightarrow correspond à un ou plusieurs messages
 - > attente active avec un grand nombre de messages
 - > attente passive avec "inscription" (cette solution réduit le nb de message mais nécessite que le client s'identifie)

5.3 Exclusion mutuelle basée sur un jeton

- Cas de l'anneau : trivial
- Cas général :
 - Hypothèse : * P_i dispose d'un moyen d'envoyer un message à tous les autres processus
 - * Pas de perte de message.

Principe du protocole :

Idée : Un jeton unique circule entre les processus, un processus ne peut entrer en S.C. (Section critique) que s'il dispose du jeton

Mise en place : * P_i veut entrer en SC, il diffuse une requete vers tous les sites (lui compris)

- * P_i reçoit une requête
 - > il dispose du jeton - Si P_i n'est pas dans la SC, il l'envoi au demandeur
 - Sinon P_i mémorise la requête
 - > il ne dispose pas du jeton => il ne fais rien (NOP)
- * P_i reçoit le jeton (qui lui est destiné) => P_i entre en SC
- * Lorsque P_i quitte la SC()

-> Si : P_i a au moins une requête mémorisée, il envoie le jeton à un des processus en attente
Sinon : NOP

Schema 11

Schema 12

Chaque site mémorise la liste des sites ayant fait une demande de jeton, et le nombre de demandes pour chaque site.

Pour éviter de rester bloqué on va mémoriser dans le jeton la liste des sites ayant reçu le jeton ainsi que le nb de fois où ils l'ont reçu. Dès qu'un site reçoit le jeton il s'ajoute à la liste sur le jeton.

Quand un site a terminé il compare la liste des demandes et la liste des reçus et envoie le jeton à un des sites qui a plus de demande que de réception.

Explications Algorithmes:

- Sur réception d'une demande de P_j , P_i exécute $DEMi[j]++$;

- Lorsque P_i quitte la SC, $JETON.SATIF[i]++$;

-> Si $DEMi[j] == JETON.SATIF[j] \quad \forall j$

NOP

-> Sinon

for ($j=(i++)\%N$, $j!=i+1$, $j=(j+1)\%N$)

| Ca implique que P_i

doit avoir le jeton et que P_i n'est pas en SC

Si $JETON.SATIF[j]$

| => il faut que ce soit

Atomique

envoi JETON à P_j

break

Sinon NOP

Si P_i a encore le jeton et que $DEMi[i] > JETON.SATIF[i]$

Alors il se l'envoie

Problème :

On a : - Tolérance aux pannes NULL : si perte de message

- Coût en $(N+1)$

5.4 Exclusions Mutuelles par liste d'attente répartie

Réseau FIFO :

Principe : on va dater les demandes

Schema 13

Chap 9 : Ordonnancement et placement de processus

9.1 Introduction

Une Application est un ensemble de tâches.

=> organiser au mieux l'exécution de cet ensemble de façon à ce que l'exécution globale soit le plus rapide possible.

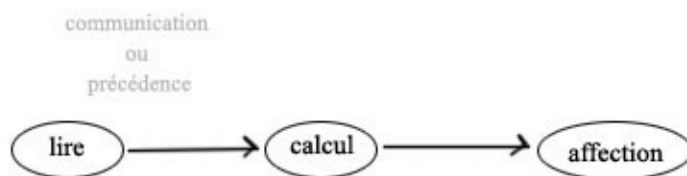
Hypothèses:

Hyp 0 : le nombre de tâches est fixe

Hyp 3 : les communications entre tâches ne peuvent avoir lieu qu'à la fin / ou au début des tâches (réception). Et les Entrée/Sorties sont pas pré-emptives.

(pré-emptive = une fois sur le processeur le processus y reste jusqu'à la fin)

On peut truffer un peu pour que des tâches pré-emptives puissent qd mm être exécutées, pour cela on leur donne une priorité telle que dès qu'elles ont fini leur E/S et qu'elles sortent, on les recharge en processeur, ainsi on conserve la non pré-emptivité.



Hyp 1 : Exécution statique, on connaît a priori :

- l'ensemble des tâches
- leurs durées
- les liens de communications / précédences entre elles

Hyp 2 : Durée des tâches invariante

(quelque soit le processeur, si on lance 10X la même tâche on obtiendra toujours le même temps)

=> 2 techniques : * durée théorique, on calcul

* on fait du profiling, on conserve les durées lors des sessions précédente et en fonction de celles-ci on fait une moyenne

Hyp 4 : Les communications ne prennent pas de temps

=> 2 techniques : * Soit on a pas de communication

* Soit toute communication ce fait entre deux processus sur le même processeur.

Hyp 5 : On dispose de suffisamment de processeurs

=> on a pas à s'occuper du nombre de processeurs, quelque soit le moment si on a besoin de X processeur on aura X processeurs disponibles

Hyp 6 : Pas de priorité entre les tâches

Hyp 7 : Les ressources sont suffisantes (RAM, etc ...)

A partir de ces Hypothèse on en déduit l'algorithme suivant :

Un ordonnancement est une relation ORD qui à chaque tâche T associe une date de début et un processeur

ORD -> (début(T), proc(T))

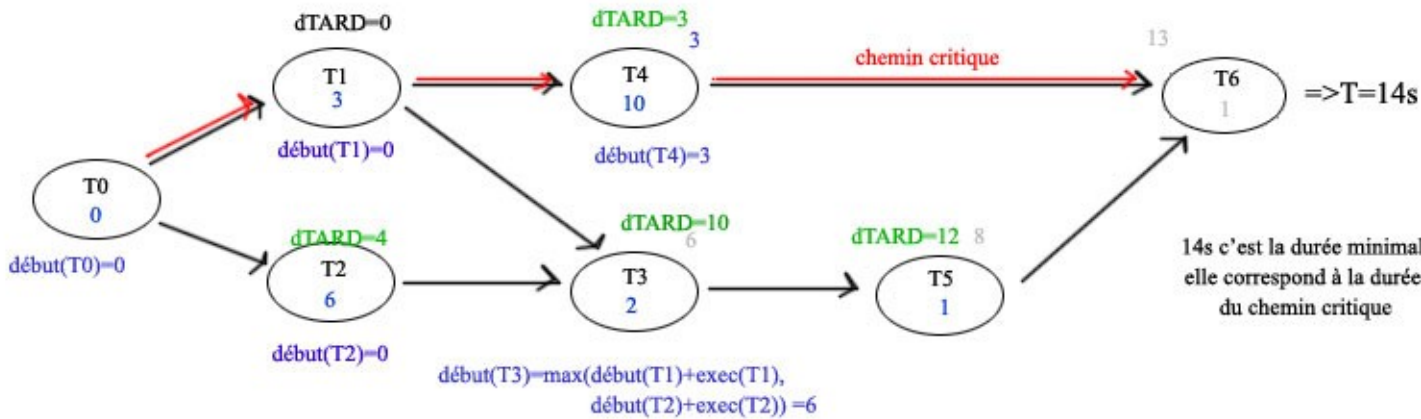
Si $T_1 \rightarrow T_2$

Alors $\text{début}(T_2) \geq \text{début}(T_1) + \text{exec}(T_1)$

ici $\text{exec}(T_1)$ correspond à la durée de T_1

Si $\text{début}(T_1) \leq \text{début}(T_2) \leq \text{début}(T_1) + \text{exec}(T_1)$

Alors $\text{proc}(T1) \neq \text{proc}(T2)$



On dira qu'une relation d'ordonnement est minimale, si quelque soit le graphe proposé, la durée du chemin correspond à la durée du chemin critique

/!\ Attention : minimal \neq optimal

- minimal : $T_n = \text{chemin critique}$
- optimal : dans la configuration donnée T_n ne peut être plus petit

Problème : Il n'existe pas de d'algorithme exact d'ordonnement minimal

Durée de table d'exécution d'un système de tâche : c'est le temps écoulé entre le début de T_0 et la fin de T_{n+1} , où n est le nombre de tâche dans le système.

Un ordonnancement O est minimal si quelque soit le nombre de processeurs, il n'existe pas d'autres ordonnancements dont la durée total d'exécution soit inférieure à celle de O .

Un ordonnancement O est optimal si pour la configuration processeur donnée, il n'existe pas d'autres ordonnancements dont la durée total d'exécution soit inférieure à celle de O .

9.2 Cas d'une execution statique (H1) sans communication (H4)

9.2.1 Cas ou l'on dispose d'assez de processeurs (H5)

Algo: * Calculer la date au plus tôt / au plus tard \Rightarrow algo de Bellman

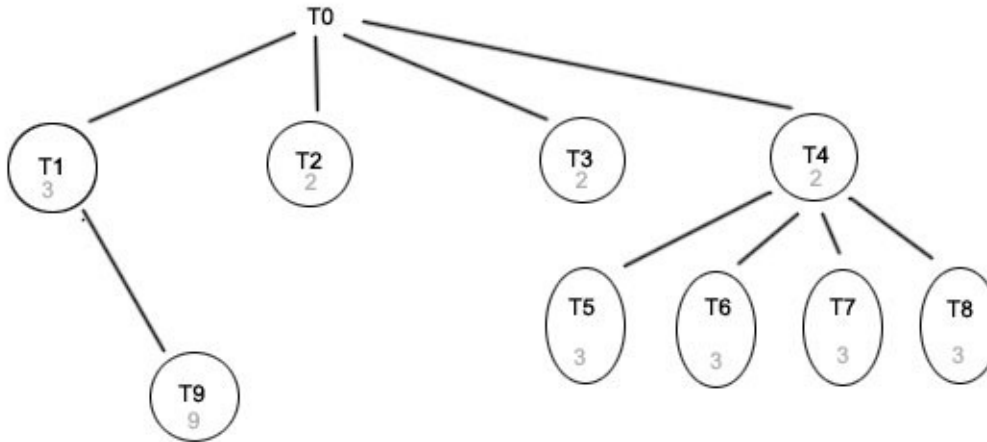
* Affecter à chaque tâche une date de début (T_i) comprise entre $\text{date_au_plus_tôt}(T_i)$ et $\text{date_au_plus_tard}(T_i)$ *

* Affecter à T_i un nouveau processeur

9.2.2 Cas avec pas assez de processeurs (non H5)

- > On calcule les dates au plus tôt / ou plus tard
- > on maintient une liste de tâches executables :
 - la tâche dont la date au plus tôt est passée
 - la tâche dont tous les processeurs ont terminés

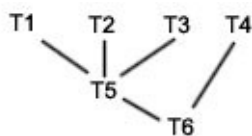
* Chaque fois qu'un processeur se libère, l'ordonnancement choisit une tâche et



- > 3 processeurs : minimal 12s
schema feanor 16bis
- > 4 processeurs : minimal 14s
schema feanor 16bisbis
- > 3 processeurs: / on diminue chacun d'une seconde

=> H1, H4, non-H5

- * minimalité : il n'existe pas d'algorithme, que des euristiques
- * optimalité :
 - 1 processeur : OK
 - 2 processeurs : OK
 - p processeurs + "graphe" anti-arborescence : OK

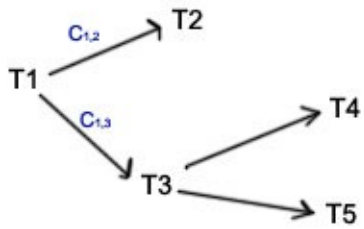


9.3 Execution statique (H1) avec communication (non H4)

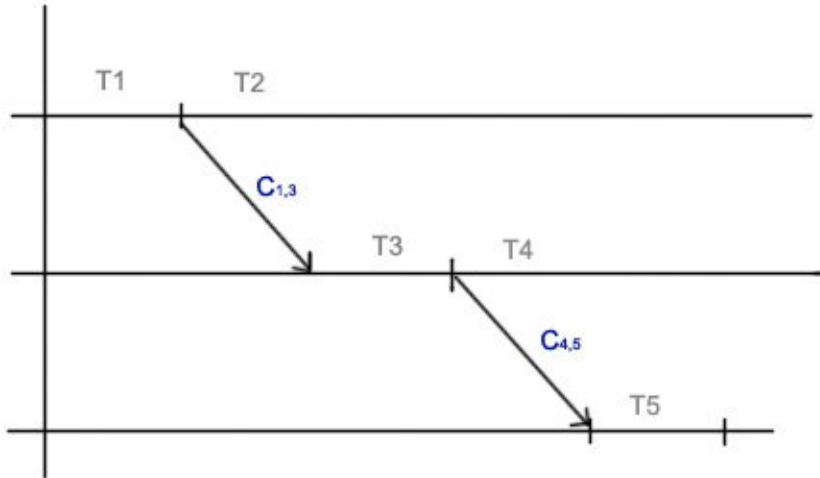
9.3.1 Communication et ordonnancement

On cherche la date au plus tôt : $date_au_plus_tôt(T_i) = \max(date_tot(T_j) + exec(T_j) + C_{i,j}) ?$

Idée : on considère que $C_{j,i} = 0$ si $proc(T_j) = proc(T_i)$

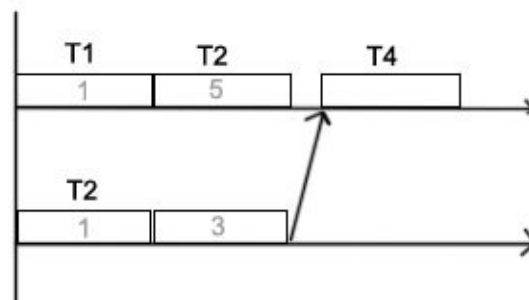
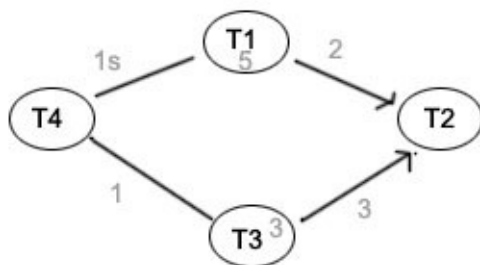
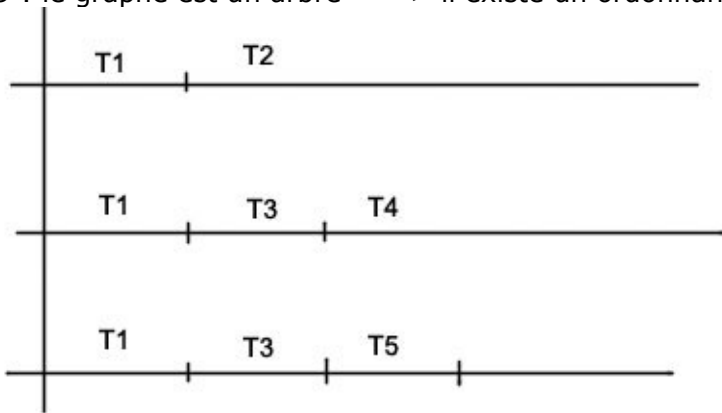


Les tâches sont duplicables :



H8 : les tâches sont duplicables

H9 : le graphe est un arbre => il existe un ordonnancement minimal



T4 sur le même processeur que la tâche prédecesseur formant le chemin critique jusqu'à T4

Pour tous les "prédecesseurs" Tj de Ti
Calculer $Ch_j = date_tot(T_i) + ex(T_j) + C_{j,i}$
Soit Ch_{jm} tel que Ch_i soit maximal
Placer Tjm et Ti sur le même processeur
 $Ch_{jm} = date_tot(T_{jm}) + ex(T_{jm})$
 $date_tot(T_i) = \max(Ch_{jm}, Ch_{j\neq jm})$

Schéma

T1 : $d(T1)=0$
T2 : $d(T2)=0$
T5 : $d(T5)=3$ $proc(T5) = proc(T2)$
T3 : $d(T3)=4$ $proc(T3) = proc(T1)$
T4 : | $Ch1=4+2$ | $proc(T4) = proc(T1)$
| $Ch2=3+1$ | $d(T4) = \max(Ch1=4, Ch2=4) = 4$
T7 : | $Ch2=4+2+1=7$ |
| $Ch4=4+3+3=10$ | $d(T7) = \max(7,7,9)$
| $Ch5=3+3+3=9$ |

Schéma

9.4 Cas où l'on dispose pas du graphe (non H1)

HS1 : quel que soit le site où Ti s'exécute, il a toujours accès aux ressources dont il a besoin.

HS2 : Un site est capable d'estimer sa charge.

HS3 : Un site est capable d'évaluer les besoins d'un processus/tâche

9.4.3 Ordonnancement sans migration

Une tâche est affecté de façon définitive à un processeur.

- Solution centralisée
- Solution distribuée
 - > demande à l'ensemble des machines
 - > sondage
 - > sous-chaîne de machines

9.4.2 Ordonnancement avec migration

"Load balancing" équilibre des charges des processeurs.

Attention : Migrer un processus consiste à déplacer son code et données mais aussi son contexte(fichier ouvert, sémaphore...)

Appel d'offre / Offre de service
M1 surchargé / M1 sous-charge
demande l'aide/ demande du travail

9.5 Clusters / Grappes de processeurs

Station de travail S

Lambda : débit et entrée de demande = 40 requetes/s

Mju: débit de sortie = 50rq/s

On peut montrer que temps d'attente moyen entre une demande et sa réponse : $T = 1 / Mju - \text{Lambda}$
 $T_i = 1/50-40 = 1/10 \text{ s}$

N stations du type S

$M_{jui} = M_{ju}$

mais $\text{lambda}_{dag} = N \text{ Lambda}$

On reparti Lambda_{dag} sur les N stations

$\text{Lambda}_{dai} = 1/N(N.\text{Lambda}) = \text{Lambda} \quad \Rightarrow \quad T_i = 1 / Mju - \text{Lambda}$

On achète un multiproc à N processeurs $\Rightarrow M_{juS} = N.M_{ju}$

$T_{\text{multi}} = 1/ M_{jus} - \text{Lambda}_S = 1/ N(M_{ju}-\text{Lambda})$

Chap 10 : Sécurité et tolérance aux fautes

10.1 intro

Défaillances : logiciel ou matériel malicieux

Défaillances malicieuses : sécurisation des échange ou des composants

10.2 System tolérants aux fautes

Défaillances --> fautes --> erreurs

2 grandes fautes :

- valeur
- perte de messages ou de résultat

Hypothèses les plus fréquentes :

- Les hypothèses de défaillances byzantine (il peut tout se passer)
- Les hypothèses de défaillance cohérente
 - ex: valeur : les messages sont altérés de la même façon sur chacun des sites.
 - ex: temporelle : arrivée bornée, éventuellement connue
- Les hypothèses uniquement temporelles
- Les hypothèses de silence sur défaillance

Résolution du problème :

- baisser l'hypothèse
- intégrer dans le protocole des mécanismes ad'hoc
- détection / traitement

Comment détecter des pertes de messages ou de valeur?

- > diagnostique d'erreur
- > recouvrement d'erreurs
 - recouvrement arrière (reprise)
 - recouvrement avant (plus loin)
 - compensation d'erreur (dégradation)
- > redondance
 - données
 - aux niveaux des sites
 - entre les sites
 - Calculs

10.3 Sécurité

ah ben... vous irez en vacances plus tôt !

bonne révisions a tous :)

Symboles mathématiques à copier :

$\forall \Sigma E \exists \leq \geq \neq$