


Diapositive
1

 SDRP & MA


Modèles et Approches Formels pour les Systèmes Distribués

-Algorithmes distribués *probabilistes*
- *Analyse probabiliste* des algorithmes distribués

A. Zemmari
zemmari@labri.fr
www.labri.fr/vissidia/

01/12/2004 1

Diapositive
2


 SDRP & MA

Algorithmes distribués probabilistes

- L'algorithme exécuté par les processus est un algorithme probabiliste.
- **Définition** : (algorithme probabiliste) un algorithme où le hasard intervient.
 - Le processus « fait un tirage aléatoire » pour décider des actions à entreprendre;
 - le démarrage d'un algorithme est effectué par un processus choisi au hasard;
 - ...
- Pourquoi les algorithmes distribués probabilistes ?
 - Quand on ne peut pas faire autrement :
 - résultats d'impossibilité à cause des hypothèses sur le système :
anonymat \Rightarrow élection déterministe impossible
 - parfois plus performants que les algorithmes déterministes.
 - Plus tolérants aux pannes que les algorithmes déterministes.
 - ...

01/12/2004 2

Diapositive
3

 SDRP & MA

Analyse probabiliste des algorithmes distribués

- L'algorithme exécuté par le processeur est (ou peut être) déterministe mais l'algorithme exécuté par le système est lui probabiliste.
- Exemples :
 - Les algorithmes distribués dans un système asynchrone;

01/12/2004 3

Diapositive
4



 SDRP & MA

Table des matières

- Rappels de probabilités.
- Algorithmes distribués probabilistes.
- Analyse probabiliste d'algorithmes distribués.
- Applications :
 - Le problème du rendez-vous.
 - le problème de l'élection locale.
 - Algorithmes d'élection.
 - Résolution de conflits.

01/12/2004 4

Diapositive
5


 SDRP & MA

Références

- F. DRESS, *Probabilités et Statistique*, Dunod, 1997.
- R. Motwani et P. Raghavan, *Randomized Algorithms*, Cambridge.
- G. Tel, *Introduction to Distributed Algorithms*, Cambridge Press.
- C. Lavault, *Analyse d'algorithmes distribués*, Hermès

01/12/2004 5

Diapositive
6


 SDRP & MA

Rappels de Probabilités

- Distribution de probabilité
- Variable aléatoire
- Espérance mathématique
- Linéarité de l'espérance
- Variance
- Ecart type
- Probabilités conditionnelles
- Lois usuelles

01/12/2004 6

Diapositive
7


SDRP & MA


Probabilités Discrètes

- Exemple : on lance deux dés.

$$\Omega = D \times D = \{(1,1), (1,2), \dots, (6,6)\}$$
- Avec $D = \{1, 2, \dots, 6\}$
- L'espace Ω contient $6 \times 6 = 36$ éléments.

01/12/2004
7

Diapositive
8



SDRP & MA

- Distribution uniforme :
 - Tous les éléments de Ω sont de même probabilité $1/36$
 - tous les éléments de D sont de même probabilité $1/6$.
- **Définition.** Une mesure de probabilité P est une application de l'ensemble des événements \mathcal{Q} dans l'intervalle $[0, 1]$, qui satisfait les deux propriétés (ou « axiomes »)

$$P(A \cap B) = P(A)P(B) \iff P(A \cup B) = P(A) + P(B)$$

01/12/2004
8

Diapositive
9



SDRP & MA

- Ω : espace des événements élémentaires
- $A \in \mathcal{Q}$: événement
- P : une loi (ou distribution) de probabilité sur Ω
- On prolonge P sur $\mathcal{P}(\Omega)$ par :

$$Pr(A) = \sum_{\omega \in A} P(\omega) \quad \forall A \subset \Omega$$
- **Proposition**
 - $Pr(\emptyset) = 0$
 - $\overline{P(A)} = \sum_{\omega \in \overline{A}} P(\omega)$ pour toute famille au plus dénombrable $A_i, i \in I$ d'éléments de $\mathcal{P}(\Omega)$, 2 à 2 disjoints.

01/12/2004
9

Diapositive
10



SDRP & MA

Exemple : Problème du rendez-vous

- Chaque processus p choisit uniformément un de ses voisins;
- Si le nombre de voisins est n , quelle est la probabilité qu'il choisisse un processus q en particulier ?
- Quelle est la probabilité pour que deux processus voisins p et q se choisissent mutuellement ?
- Quelle est la probabilité pour p d'obtenir un rendez-vous avec un de ses voisins ?

01/12/2004
10

Diapositive
11


SDRP & MA


Propriétés

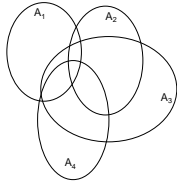
- Soient A, B deux éléments de $\mathcal{P}(S)$:
 $\overline{A \cup B} = \overline{A} \cap \overline{B}$
 $\overline{A \cap B} = \overline{A} \cup \overline{B}$
 si A et B sont disjoints, alors :
 $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- Généralisation : Principe d'inclusion-exclusion

$$P(A \cup B \cup C) = P(A) + P(B) + P(C) - P(A \cap B) - P(A \cap C) - P(B \cap C) + P(A \cap B \cap C)$$

01/12/2004
11


Diapositive
12


SDRP & MA



01/12/2004
12

Diapositive
13


SDRP & MA

Variable aléatoire

- Définition :** Soit (Ω, \mathcal{F}, P) un espace probabilisé discret et soit Ω' un ensemble non vide au plus dénombrable. Une variable aléatoire (v.a.) X à valeurs dans Ω' est une application de Ω dans Ω' . Nous prenons souvent pour Ω' un sous-ensemble de \mathcal{R} ou de \mathbb{C} . On pourra munir Ω' d'une loi de probabilité $P_{X'}$ en posant, pour tout $\omega' \in \Omega'$:

$$P_{X'}(\omega') = P(X^{-1}(\{\omega'\}))$$
- Proposition :** $P_{X'}$ est une loi de probabilité sur Ω' , i.e.


$$\sum_{\omega' \in \Omega'} P_{X'}(\omega') = 1$$

Nous avons de plus, pour tout $x \in \mathbb{R}$:

$$P_{X'}(x) = \sum_{\omega \in \Omega : X(\omega) = x} P(\omega)$$

01/12/2004 13

Diapositive
14



SDRP & MA

Exemple : Problème du rendez-vous (2)

- Pour tout processus p , on définit la v.a. $X_p(k)$ comme la v.a. qui compte le nombre de sommets avec qui p a obtenu un rendez-vous au bout de k rounds.
- Calculer $Pr(X_p(k) = m)$

01/12/2004 14

Diapositive
15


SDRP & MA

Espérance Mathématique et Variance

- Une v.a. admet un certain nombre de valeurs typiques. Nous considérons dans la suite les v.a. à valeurs dans \mathbb{R} .
- Définition :** En arithmétique, la valeur moyenne de n nombres est définie par leur somme divisée par n . En calcul des probabilités, l'espérance d'une v.a. est définie comme la somme des valeurs prises pondérées par les probabilités respectives, c'est-à-dire :

$$E[X] = \sum_{x \in \mathcal{X}} x P_X(x)$$

lorsque cette somme converge absolument. ($\mathcal{X}(\Omega)$ est l'ensemble des valeurs prises par la v.a. X). Sinon, on dit que X n'admet pas d'espérance.

01/12/2004 15

Diapositive 16

SDRP & MA

Exemple : Problème du rendez-vous (3)

- Quelle est l'espérance du temps que mettra p pour obtenir un rendez-vous ?
- Si tous les processus du système appliquent le même algorithme, quelle est l'espérance du nombre de rendez-vous dans tout le système ?
- ...

01/12/2004 16

Diapositive 17

SDRP & MA

Linéarité de l'espérance

- **Proposition** : Soit X et Y deux v.a. définies sur le même espace probabilisé discret (Ω, \mathcal{P}, P) et admettant toutes deux une espérance.

Soit $\alpha \in \mathbb{R}$. Alors :

$$E(\alpha X) = \alpha EX$$
$$E(X+Y) = EX + EY.$$

- Que peut-on dire de l'espérance d'un produit de v.a. ?

01/12/2004 17

Diapositive 18

SDRP & MA

Loi conjointe

- **Définitions** : Soit les v.a. X et Y définies sur le même espace probabilisé discret (Ω, \mathcal{P}, P) . La loi (ou distribution) conjointe est la donnée de

$$Pr_{X,Y}(X=x, Y=y) = Pr(\{\omega \in \Omega \mid X(\omega)=x, Y(\omega)=y\})$$

pour tout x et tout y possibles.

X et Y sont dites indépendantes, si pour tout x et tout y possibles, on a

$$Pr_{X,Y}(X=x, Y=y) = Pr_X(x) Pr_Y(y).$$

- **Proposition** : Si X et Y sont deux v.a. indépendantes admettant une espérance, alors la v.a. produit XY admet une espérance et

$$E(XY) = EXEY$$

01/12/2004 18

Diapositive
19

SDRP & MA

Variance

- **Définition** : la quantité qui mesure la dispersion d'une v.a. X définie sur (Ω, \mathcal{P}) est la variance. Elle est définie par
$$VX = E[(X - EX)^2].$$

01/12/2004 19

Diapositive
20

SDRP & MA

Ecart type

- **Définition** : la racine carrée de la variance est appelée écart-type et est notée par σ :
$$\sigma X = \sqrt{VX}$$
- **Proposition** : Nous avons :
$$VX = E[X^2] - (EX)^2$$
- **Proposition** : Si X et Y sont deux v.a. indépendantes admettant chacune une variance, alors la v.a. $X+Y$ admet une variance qui est la somme des deux variances.

01/12/2004 20

Diapositive
21

SDRP & MA

Indépendance

- **Définitions** :
 - Deux événements A et B sont dit indépendants, si :
$$\Pr(A \cap B) = \Pr(A)\Pr(B)$$
 - Une famille $A_i, i=1, \dots, n$, d'événements est dite indépendante dans son ensemble, si pour tout sous-ensemble $J \subset \{1, \dots, n\}$:
$$\Pr\left(\bigcap_{i \in J} A_i\right) = \prod_{i \in J} \Pr(A_i)$$
- **Remarque** : Pour démontrer l'indépendance d'une famille $A_i, i=1, \dots, n$, il suffit de prouver que les A_i sont 2 à 2 indépendants.

01/12/2004 21

Diapositive 22

SDRP & MA

Probabilités conditionnelles

- C'est une notion introduite pour formaliser le concept de la probabilité de l'occurrence d'un événement B sachant qu'un autre A s'est produit.
- **Remarque** : B conditionné par A n'implique pas que A précède nécessairement B (dans l'ordre chronologique).
- **Exemple** : Un dé uniforme est lancé et nous savons que le point obtenu est pair (événement A). Quelle est la probabilité pour que le point soit au moins 4 (événement B) ?

01/12/2004 22

Diapositive 23

SDRP & MA

- Il est clair que le nouvel espace (conditionné par l'événement A) sur lequel les événements élémentaires sont à définir est $\Omega' = A$, qui contient 3 éléments.

Or, la portion de A qui est en même temps favorable à B en contient 2.

Il est donc raisonnable de définir la probabilité de B conditionné par A par le ratio $2/3$.

- **Définition** : Soit (Ω, \mathcal{P}, P) un espace probabilisé discret et soit A un événement de probabilité non nulle. On définit sur $\mathcal{P}(A)$, l'application $Pr(\cdot/A)$ à valeurs dans $[0,1]$ par :

$$Pr(B/A) = \frac{Pr(A \cap B)}{Pr(A)}, \forall B \in \mathcal{P}(A)$$

On appelle $Pr(B/A)$ probabilité conditionnelle de B sachant A .

01/12/2004 23

Diapositive 24

SDRP & MA

- **Proposition** : Soit A_1, A_2, \dots, A_n une partition de Ω . Si chacun de ces ensembles est de probabilité non nulle, alors :

$$Pr(B) = \sum_{i=1}^n Pr(A_i) Pr(B/A_i), \forall B \in \mathcal{P}(\Omega)$$

- **Exemple** : On lance deux dés uniformes. Quelle est la probabilité d'avoir obtenu un double sachant que la somme des points vaut 8 ?

01/12/2004 24

Diapositive 25

SDRP & MA

Espérance conditionnelle

- Soit X une v.a. et soit A un événement de probabilité non nulle. L'espérance de X sachant A est définie par :
ou
$$E(X|A) = E_{\text{Pr}(\cdot|A)} X$$
$$E(X|A) = \frac{1}{\text{Pr}(A)} \sum_{\omega \in A} X(\omega) \text{Pr}(\{\omega\})$$
- Exemple : Quelle est l'espérance d'un dé uniforme sachant que le nombre sorti est inférieur ou égal à 3 ?

Soit X la v.a. associée au lancer du dé. L'événement A associé à la condition est l'ensemble $\{1,2,3\}$. La probabilité de la condition A est $1/2$. L'espérance conditionnelle recherchée vaut :

$$E(X|A) = \frac{1}{2} \left[\frac{1}{6} + \frac{2}{6} + \frac{3}{6} \right] = 2$$

01/12/2004 25

Diapositive 26

SDRP & MA

Quelques distributions discrètes

- **Loi de Bernoulli**. La v.a. X prend deux valeurs : 1 avec probabilité p et 0 avec la probabilité q , on suppose que $p, q \in]0,1[$ et $p+q=1$. Nous avons :
 - $EX = p$
 - $IX = pq$
 - $\sigma X = \sqrt{pq}$
- **Utilisation** : Cette loi intervient souvent de façon implicite lorsqu'on veut traiter une probabilité comme une espérance. En effet c'est la loi de la v.a. qui est la fonction indicatrice d'un événement A de probabilité p :
$$\text{Pr}(A) = E \mathbb{1}_A$$

01/12/2004 26

Diapositive 27


SDRP & MA

- **Loi binomiale**. On effectue n épreuves identiques et indépendantes; la probabilité de succès dans chacune étant supposée égale à p et celle d'échec à $q=1-p$. Posons $X =$ le nombre total de succès obtenus dans les épreuves.
 X est une v.a. qui peut prendre la valeur k dans l'intervalle $]0,n[$ avec la probabilité :
$$p_k = \text{Pr}(X = k) = C_n^k p^k q^{n-k}$$

On dit alors que X suit une loi binomiale de paramètres n et p .
- **Remarque** : X peut être vue comme la somme de n v.a. de Bernoulli identiques et indépendantes de même paramètre p .
Nous avons donc $EX=np$, $IX=npq$ et $\sigma X = \sqrt{npq}$

01/12/2004 27

Diapositive 28


 SDRP & MA

- **Loi géométrique.** Soit $p > 0$ la probabilité de succès dans une épreuve, et $q = 1-p$. Nous répétons la même épreuve indépendamment jusqu'à l'obtention du premier succès.
Soit X la v.a. désignant le nombre d'épreuves effectuées. C'est une v.a. qui peut prendre la valeur k (entier naturel non nul) avec la probabilité
$$p_k = \text{Pr}(X = k) = q^{k-1}p$$
On dit que X suit une loi géométrique de paramètre p .

$$EX = \frac{1}{p}$$
$$VX = \frac{q}{p^2}$$
$$\sigma X = \frac{\sqrt{q}}{p}$$

01/12/2004 28

Diapositive 29

 SDRP & MA

- **Loi de Poisson.** Cette distribution intervient dans l'étude du nombre d'événements intervenant dans un intervalle de temps (file d'attente).
Une v.a. X suit une loi de poisson de paramètre λ , si X peut prendre la valeur k avec la probabilité :

$$p_k = \text{Pr}(X = k) = \frac{\lambda^k}{k!} e^{-\lambda}$$
$$EX = \lambda$$
$$VX = \lambda$$
$$\sigma X = \sqrt{\lambda}$$

01/12/2004 29
