TELECOM ParisTech

Institut Mines-Télécom

Système à transitions probabilistes et vérification

Structure du cours

- **Motivations**
- **Quelques éléments de contexte : les bases en probabilités**
  - **Vocabulaire clés, notations importantes**
  - **Théorèmes et principes requis**
- **Modèle de chaine de Markov à Temps Discret**
- **Problèmes de vérification vs quantification**
  - **Solution 1 : extension de CTL => PTCL**
  - **Solution 2 (seulement évoqué) : Récompense et intervalle de confiance**
- **Prise en compte de la concurrence**
  - **Exécution concurrente de CTMD**
  - **non déterminisme vs probabilité (intuition du PMD)**
  - **Produit de CTMD endogène (i.e. reste une CMTD)**
- **Prism, un outil de vérification / une syntaxe de spécification**

Motivations

Evaluer des objectifs de fiabilité / disponibilité

- Fiabilité : capacité du système à produire un résultat correct
- Pb : incertitude sur l'occurrence de l'activation des fautes et l'apparition de défaillances
- Idée : modéliser l'activation comme un phénomène aléatoire mais quantifiable (e.g. probabilité).
- Objectif :
  - Quels formalismes peuvent être utiles ?
  - Quelles sont les analyses faisables sur de tels modèles ?

- Un petit exemple peut être ?

Vous n’avez pas confiance dans votre régulateur ? Dupliquez le….

- Pb : vous souhaitez intégrer un composant de détection de panneaux de signalisation dans un drone terrestre.
  - Vous ne faites pas trop confiance aux solutions clés en main mais vous ne pouvez pas développer votre solution
  - Vous pouvez en acheter plusieurs … de différentes sources/ utilisant différentes technologies
- Solution : embarquez 2, ou 3 ou N versions différentes de la même fonction et fusionnez les résultats…
  - Pour 3 instances, résultat correct en sorti si 2 parmi 3 corrects… si temps d’exécution borné.
  - Pb annexe : comment quantifie t on le gain de fiabilité ?

Petit rappel …. Réplication active notre exemple fil rouge

- Principe 1 fonction dont on veut augmenter la fiabilité
  - On obtient N implémentation indépendantes
  - On exécute à chaque usage de la fonction, les N instances en parallèle (sur des calculateurs différents si possible).
  - On récupère les résultats et on vote ou on fusionne les données.
- Preuve de correction : sous une hypothèse de système synchrone (i.e. on peut définir une borne supérieure au temps d'exécution de f)
    - Si nombre d'instances défaillantes f < nombre d'instances correctes c, cela fonctionne
- Pb condition logique, souvent peu parlant au niveau gestion de risque…

Autres application des modèles probabilistes

- Algorithmes reposant sur un aléa :
  - Synchronisation
  - Diffusion par commérage
  - Sécurité (aléa de génération de défis)
- Quid de CTL / LTL ?
- Il faut pouvoir quantifier la vraisemblance des chemins d'exécution les uns par rapports aux autres.

Quelques bases en probabilités …

Kit de survie pour les probabilité

- **Espace de probabilité :** $(\Omega, \mathscr{F}, P)$
  - Ω **ensemble des « cas possibles »**
  - $\mathscr{F}$ **ensemble de parties de** Ω **permettant de définir une mesure (surtout utile si** Ω **est infini non dénombrable)**
  - P **mesure dans [0,1] définie sur** $\mathscr{F}$ **(i.e. cette fonction doit par extension permettre de « mesurer » toute partie de** Ω
- **Evénement = sous ensemble de** Ω
- **Variable aléatoire X (le truc vraiment manipulé)**
  Fonction de Ω **vers le E domaine mesurable de la variable**
  $A \subseteq E, P_X(B) = P(X^{-1}(A)) = P(X \in A)$
- **On oubliera souvent** $(\Omega, \mathscr{F}, P)$ **(à tort) car cela permet de montrer les correlations**
- **2 variables aléatoires X1,X2 booléennes t.q.** $P(X1 \in \{true\}) = 0.4$,
  $P(X2 \in \{true\}) = 0.4$ **=>** $P(X1{,}X2 \in \{(true, true)\}) \in [0{,}0.4]$
  tout dépend de la mesure de $X1^{-1}(\{true\}) \cap X2^{-1}(\{true\})$

Indépendance, probabilités conditionnelles et échantillonnage

- **2 événements de Ω = 2 sous ensembles**
  Questions : est ce que le fait d'appartenir au sous ensemble A change la probabilité d'être aussi dans B …
  ~ à mesure de $(A \cap B)$ dans A proportionnellement identique à mesure de B dans Ω == indépendance …
- **Probabilités conditionnelles $P(\cdot \mid \cdot)$:**
  $P(B \mid A) \cdot P(A) = P(A \cap B)$
- **Independence v2:** $P(B) \cdot P(A) = P(A \cap B)$
- **Evénements disjoints :** $P(A \cup B) = P(A) + P(B)$

De l’automate fini à la chaîne de Markov

Chaine de Markov à temps discret

Machine à état fini + probabilités sur transitions et état initial

CMTD sur D = séquence de variables aléatoire (Xi),i entier tel que

- **Chaque Xi est une variable aléatoire dans D**
- **Xi représente l'état du système à la date discrète i**
- **$P(X_i=v_i \mid X_{i-1}=v_{i-1}, X_{i-2}=v_{i-2},\dots X_0=v_0)= P(X_i=v_i \mid X_{i-1} =v_{i-1})$ est une constante (i.e. ne change pas en fonction de i — du temps) == chaîne homogène**
- **Si |D|=n, alors on prend usuellement D= {1,…,n}**

Matrice de transition

- **Distribution de probabilité pour un état « incertain »,** $v = (v_1, \ldots, v_n)$**, t.q.** $\sum_{1 \leq i \leq n} v_i = 1$
- **Matrice de transition =** $(M_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}$**, tq pour tout k,** $P(X_{k+1} = j \,|\, X_k = i) = M_{i,j}$
  - **Propriété 1 : si v distribution de probabilité pour l'état** X_k**, alors** ${}^t v \,.\, M$ **représente la probabilité d'occuper les états de 1 à n après 1 transition à partir de** X_k
  - **Propriété 2 :** M^k**, matrice des probabilités de transitions pour k transitions consécutives dans la chaine de Markov (k=0, cas trivial)**
- **Caractérisation d'une chaine : (M,v0) matrice + distribution initiale**

Présentation « graphique » d'une CMTD

- Définition d'un système à transitions à partir de (M,v0)
  - Etats : {1,…,n}
  - Transitions : {i,j} / $M_{i,j}$>0
  - Initiaux : $\{j \mid v0_j > 0\}$
  - Étiquetage : $(i,j) \rightarrow M_{i,j}$
- Remarques : le système à transition ne contient aucun sans transition sortante = aucune impasse.
- La somme de l'ensemble des valeurs sur les transitions sortantes d'un état vaut 1.

Un petit exemple lié à la fiabilité

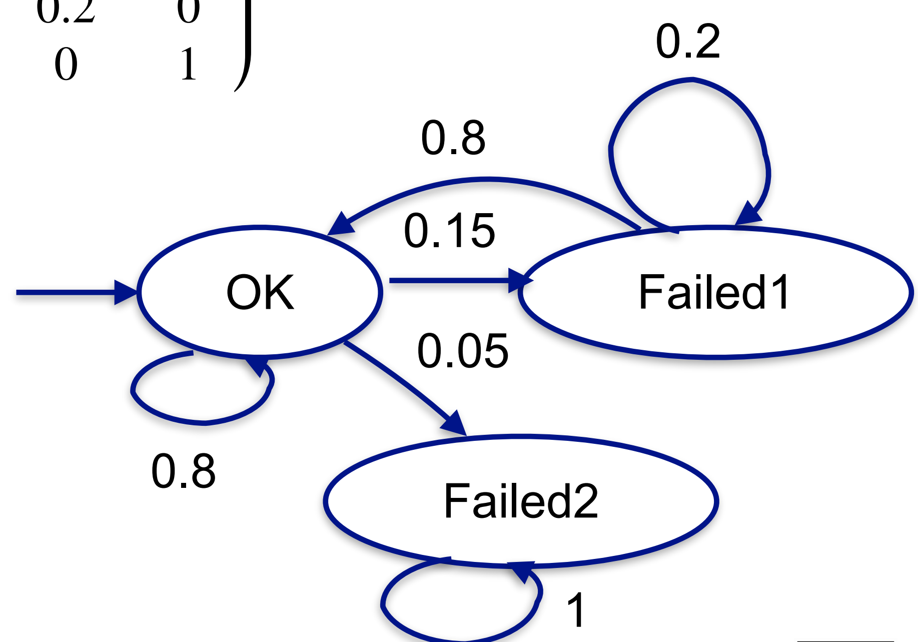
**3 états possibles fonctionne (ok—1),
défaillance temporaire (failed1— 2),
défaillance permanente (failed2—3),**

Transitions conditionnelles

V_{i-1}	V_i	CPD
ok	ok	0.8
ok	failed1	0.15
ok	failed2	0.05
Failed1	ok	0.8
Failed1	Failed1	0.2
Failed2	Failed2	1

Matrice de transition

$$\begin{pmatrix} 0.8 & 0.15 & 0.05 \\ 0.8 & 0.2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$



V0=(1,0,0)

Modélisation de séquence d'exécution par CMTD

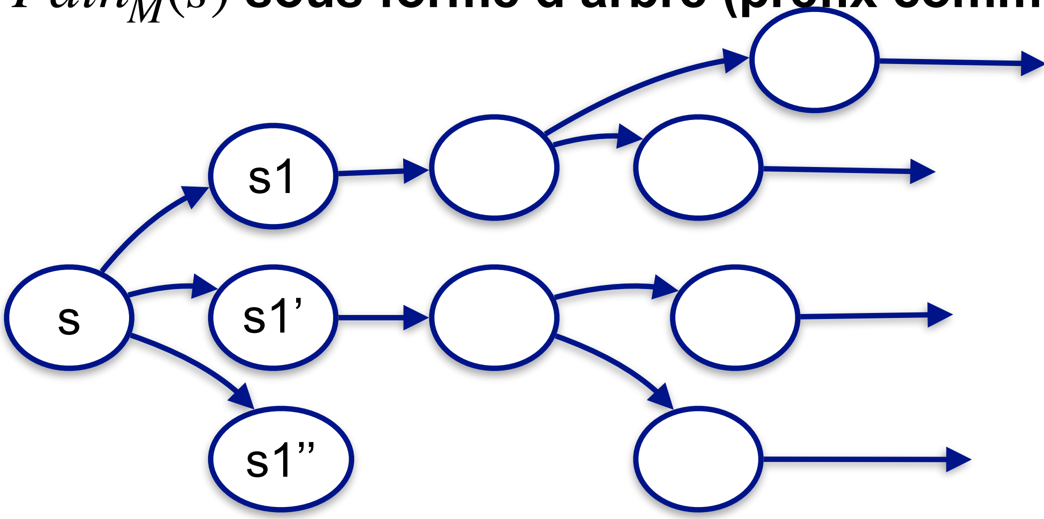
- Pas d'impasse => possibilité de définir les séquences d'états infinies correspondant au système à transition d'une chaine de Markov à temps discret.
- Extension :
  - Ensemble de variables propositionnelles AP
  - Étiquetage supplémentaire état de chaque état de {1,… n} par une formule propositionnelle construite sur AP.
  - Ensemble de symboles de transition ∑
  - Etiquetage (optionnel) de chaque transition par un symbole représentant une action
- Exécution = chemin = séquence d'état dans le graphe de la chaîne de Markov

Chemins d'exécution (formalisation)

- **Chaine (M, v0) de système à transition T = (Q, I, ∆, Lp, Lap, L∑),**
  Q états, I états initiaux, ∆ transitions, Lp étiquetage de probabilités, Lap étiquetage de formules d'état, et L∑ étiquetage d'action des transitions
- **Chemin dans (M, v0) depuis s = chemin dans T depuis s = une séquence d'état de Q (i.e. {1,…,n}) finie ou non :**
  $s\,.\,s1.s2.\cdots.\,sk\cdots$
- **On notera** $\{1,..,n\}^{\omega}$ **l'ensemble des chemins infinis, et path(p,s,M) est vrai si p est un chemin depuis s dans (M,s)**
- $Path_M^{\omega}(s) = \{p \,|\, p \in \{1,..,n\}^{\omega}, path(p,s,M)\}$ **est l'ensemble des exécution de M à partir de s**
- $Path_M^{*}(s) = \{p \,|\, p \in \{1,..,n\}^{*}, path(p,s,M)\}$ **ensemble des chemins finis.**

Chemins d'exécution, un espace probabiliste (formalisation)

- **Cylindre du prefix** $pref \in Path^*_M(s), pref = s\,.\,s1.s2.\cdots.\,sk$,
  $Cyl_M(pref) = \{pref\,.\,p \,|\, s_k\,.\,p \in Path^\omega_M(s_k)\}$
- **Représentation de** $Path_M(s)$ **sous forme d'arbre (prefix communs fusionnés)**



- **Mesure P :** $pref = s\,.\,s_1\,.\cdots.\,s_k, si\ pref = s\,.\,P(Cyl_M(pref) = 1$
  $P(Cyl_M(pref) = P(pref) = P(s_1 \,|\, s)\,.\,P(s_2 \,|\, s_1)\,.\cdots.\,P(s_k \,|\, s_{k-1})$
- **P est une mesure de probabilité sur** $(Path^\omega_M(s), \Sigma_{Cyl()})$**, [KSK76] pour les détails :)… ce qu'il faut retenir = construction correcte**

TELECOM ParisTech

Hum et en pratique …

- Que dire de P(pref) si la taille de pref tend vers l’infini ?
- Peut elle être non nulle ? Si oui sous quelles conditions ? (cycle répétant une séquence de transition de probabilité 1)
- Que vaut P(ok.ok.ok) ? 0.8*0.8*0.8
- Que vaut P(ok.ok.ok.failed1.ok. failed2) ? 0.8*0.8*0.15*0.8*0.05

Problèmes de vérification vs quantification

De CTL à PTCL

- **CTL => définit un sous ensemble du cylindre démarrant à l'état initial ….**
- **Question légitime : quelle est la probabilité qu'une formule CTL soit vraie à partir d'un état dans une chaine de Markov**
- **Syntax**
  - $\Phi :: true \mid false \mid a, a \in AP \mid \Phi \wedge \Phi \mid \neg\Phi \mid P < cstr > \Psi$
  - $< cstr >::< c \mid > c \mid \leq c \mid \geq c, c \in \mathbb{N}$
  - $\Psi :: X\Phi \mid \Phi \cup \Phi \; (opt. \mid \Phi \cup^{\leq c} \Phi)$
- **Une seule quantification sur les chemins P.**

Sémantique de PCTL

- **Sémantique des formules sur les états :**
  - **État s pour chaine induite de (M, s) avec Lap étiquetage de formules.**
  - **Pour tout s,** $s \models true$ **est vrai et** $s \models false$ **est faux**
  - $s \models a$**, si L(s) => a. (Rappel étiquetage par des formules)**
  - $s \models \Phi 1 \wedge \Phi 2$**,** $s \models \Phi 1$ **et** $s \models \Phi 2$
  - $s \models \neg \Phi$**,** $s \models \Phi$ **est faux.**
- **Sémantique sur les chemins** $w = s_0 . s_1 . \cdots . s_k . \cdots$
  - $s_0 . s_1 . path \models X\Phi$**, si** $s_1 \models \Phi$
  - $w \models \Phi 1 U^{\leq k} \Phi 2$**, si il existe j ≤k t.q.** $s_j . \cdots . s_k . \cdots \models \Phi 2$**, et pour tout i <j,** $s_i . \cdots . s_k . \cdots \models \Phi 1$
  - $w \models \Phi 1 U \Phi 2$**, si il existe j ≥0 t.q.** $s_j . \cdots . s_k . \cdots \models \Phi 2$**, et pour tout i <j,** $s_i . \cdots . s_k . \cdots \models \Phi 1$

Sémantique opérateur P

- $s \models P_{\sim p}\,[\psi] \Leftrightarrow \mathrm{Prob}(s, \psi) \sim p$

Prism, une petite démonstration…