
Institut
Mines-Telecom

# SDF – Analyse Quantitative

Thomas Robert,
thomas.robert@telecom-paristech.fr

Telecom ParisTech, Institut Mines Telecom

# Vocabulaire d'analyse (I)

## Nature de l'analyse

- évaluer une fonction : repose sur une notion de calcul formellement défini
- mesurer un attribut : la caractéristique est observable directement (e.g. longueur, hauteur) et l'on possède un dispositif de mesure direct.
- estimer une caractéristique : la caractéristique est non observable directement mais peut être déduite par mesure de certains attribut puis calcul.

# Vocabulaire d'analyse (2)

## Sémantique quantitative d'un modèle

**fonction F** appliquée à un **modèle M** telle que F(M) correspond à une caractéristique **numérique**, ou un vecteur de telles valeurs.

## Évaluation Quantitative Empirique

**Processus expérimental** permettant d'obtenir une **estimation ou mesure** d'une **caractéristique numérique** du système.

# Ordre partiel, total ou mesure

## Relation d'ordre

Principe : permet la comparaison d'éléments dans un ensemble.
définition : une relation binaire asymétrique sur $X \times X$.
ordre total : relation d'ordre où pour tout couple (x,y), x est plus petit que y ou y plus petit que x.

## tribu et mesure

Une tribu d'un ensemble $X$ est un ensemble de sous ensembles de $X$ stable par complément dans X, et union dénombrable.
Une mesure est une fonction, notée $\mu$, sur les éléments d'une tribu

- $\mu() = 0$
- soit $Y = \{E_i\}$ un ensemble dénombrable d'éléments de la tribu, $\mu(\bigcup_{z \in Y} z) = \sum_{z \in Y} \mu(z)$

# Exemples d'ordres sur ensembles structurés

## Mesure et ordres sur un arbre

Supposons un arbre A dont les nœuds sont étiquetés par des réels positifs.
Définissez 1 ordre partiel, 1 ordre total et une mesure pour les nœuds de l'arbre.

# Exemples d'ordres sur ensembles structurés

## Mesure et ordres sur un arbre

Supposons un arbre A dont les nœuds sont étiquetés par des réels positifs.
Définissez 1 ordre partiel, 1 ordre total et une mesure pour les nœuds de l'arbre.

## Ordre Partiel

Le nœud x est plus petit que y si x est un ancêtre de y

## Ordre Total

Hypothèse : parcourt infixe connu. Soit L, la séquence de nœuds de l'arbre selon un parcourt infixe de ce dernier.
Un nœud x est plus petit que y, si x précède y dans L.

# Exemple de mesure ensembles finis

## Hypothèses

Prenons un ensemble fini étiqueté par des poids (vision simplifiée de l'arbre)

## La tribu triviale $2^X$ (parties de X)

Pour un ensemble fini, l'ensemble des sous ensemble est une tribu

## Poids d'un ensemble

On définit $\mu$ comme la somme des étiquette de poids associées à chaque élément de l'ensemble.

# Formalisation de l'événement redouté

## De l'événement à l'état

Observation : Un événement est une transition

Un événement redouté peut être vu comme un état si seul l'événement peut déclencher l'entrée dans le dit état.

## De l'état à la formule

Une formule peut représenter un ensemble d'états correspondant à un même type d'événements redoutés

# Modélisation de la vraisemblance

## Vraisemblance et Probabilité

Objectif : caractériser la vraisemblance d'un risque par rapport à un ensemble de "XXX"
Approche : définir une mesure sur l'ensemble de "XXX".
**Mesurer l'ensemble vérifiant une certaine condition C**.

## Qu'est ce donc que "XXX"?

- des exécutions d'une tâche périodique d'un système logiciel
- des requêtes à un serveur
- des configurations d'origine d'un système inconnu ou mal caractérisé
- des échantillons d'une population de composants matériels

# Plan

# Attributs génériques

## Cas abordés dans la suite

- vraisemblance d'une défaillance sur un intervalle de temps (fiabilité, sens le plus usité)
- vraisemblance d'une défaillance par sollicitation (utilisé dans les standards de transports)
- temps jusqu'à la première défaillance (disponibilité)
- durée d'une opération de maintenance

## Portée de l'analyse

La qualité de l'évaluation de ces attributs dépend des hypothèses sur la **dynamique du système**, de son **environnement** et du processus de maintenance.

# Représentation de l'information en entrée

## Modélisation directe

Attribut = Variable aléatoire, définie par une loi distribution

## Modèles orientés architectures

Reliability block diagrams, Architecture Description langage (ADL) + modèle de faute et algèbre de propagation (AADL)

## Modèles comportementaux

Chaîne de markov, réseaux de Petri stochastiques, processus stochastiques...

## Modèles logiques

Logique à sémantique probabiliste, Arbres de fautes pondérés, arbres d'événements...

# Interprétation du résultat
# Comparaison ou valeur absolue

## Usage de la mesure

- Prédiction du comportement futur
- Prise de décision sur des opérations de maintenance
- Respect de contraintes réglementaires sur le processus de conception
- Sélection d'une conception parmi différentes alternatives

## Remarque de bon sens

Difficile de prédire le futur $\Rightarrow$ éviter de sur interpréter vos analyses
L'interprétation 1 doit être un consensus entre concepteur / évaluateur / utilisateur ...

# Plan

# Variable aléatoire

## Définition d'une variable aléatoire

Une variable aléatoire X est une fontion d'un espace probabilisé vers $\mathcal{R}$

$$\mathcal{E} : \Omega \rightarrow \mathcal{R}$$

$$\mathcal{P}(X = v) = \mu(\mathcal{E}^{-1}(\{v\}))$$

événements sur X = sous ensemble de $\mathcal{R}$

# Un exemple de caractérisation directe

## Temps jusqu'à défaillance

- Variable de loi exponentielle = temps jusqu'à défaillance indépendant du passé
- Variable de loi Weibull = modèle très flexible adaptable à des mesures

événements sur X = sous ensemble de $\mathcal{R}$

# Plan

# Interprétation Binaire de la fiabilité

## Problème

Comment raisonner sur la fiabilité d'un système complexe dont

- le fonctionnement correct dépend des sous-systèmes
- les dépendances inter sous systèmes sont complexes

## Abstraire la description du système

- Se limiter à une **séparation binaire** de l'état du système : fonctionnel / dysfonctionnel
- Identifier les dépendances entre l'état global du système et celui de ses composantes par une **formule logique**
- Extension possible du modèle binaire par une vision dynamique (évolution de l'état au cours du temps)

# Modèle logique binaire de fiabilité

## Definition - Systèmes et Composants

Composant : plus petite unité de description de l'état d'une partie d'un système du point de vue de sa fiabilité.
Système : assemblage de N composants ayant potentiellement des dépendances

## Etat du système

État de fiabilité = booléen : vrai si fonctionel, faux sinon.
*modélisation alternative avec des entiers (1≈ vrai, et 0 ≈ faux).*
Deux visions peuvent s'opposer concernant l'état du système :

- état détaillé : état de fiabilité composant par composant au sein du système
- état global : état de fiabilité du système complet

# Structure et état de fiabilité

## Definition - Fonction de structure (SF)

Fonction associant à une valuation de l'ensemble des états d'un système, l'état de fiabilité du système lui même caractérisé par la formule $\Phi$ sur des variables représentant l'état de chaque composant.

$$SF_{Sys}(x_1, ..., x_n) = \Phi[v_1 \leftarrow x_1, ..., v_n \leftarrow x_n]$$

## Remarque

La fonction de structure lorsqu'elle existe permet de relier l'état de fiabilité du système à celui de ses composants.
La formule doit être adaptée au type de ses variables.

# La fonction de structure et graphe

## Voir SF comme un graphe

Si SF est défini à partir d'une formule, alors il est possible de la présenter sous forme d'un graphe.

## Inférence de SF à partir d'une architecture

Trois modèles classique :

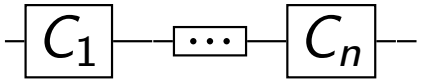
- Le modèle série : le service rendu correspond à un enchaînement de traitement réalisé en séquence
- Le modèle parallèle : le système est composé de sous systèmes tels que chacun peut rendre le service attendu complet.
- Le modèle k parmi n : le système est composé de sous systèmes tels que pour rendre le service, k parmi n doivent être fonctionnels.

# Modèle série et fonction de structure

## Fonction de structure :

$$SF(x_1, ..., x_n) = \prod_{1 \leq i \leq n} x_i$$

$$SF(x_1, ..., x_n) = \bigwedge_{1 \leq i \leq n} x_i$$

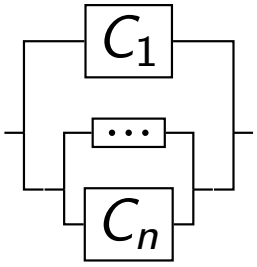


# Modèle parallèle et fonction de structure

## Fonction de structure :

$$SF(x_1, ..., x_n) = 1 - \prod_{1 \leq i \leq n} x_i$$

$$SF(x_1, ..., x_n) = \bigvee_{1 \leq i \leq n} x_i$$



# Modèle K parmi N, autre prédicats

## Sémantique k parmi n

Utilisation d'une condition arithmétique et logique pour la fonction de structure :

$$SF(x_1, ..., x_n) = min(1, max(0, \sum_{1 \leq i \leq n} x_i - (n - k + 1)))$$

## Remarque :

Cette architecture repose sur la duplication de composants pouvant rendre le service sans que chacun ne puisse le rendre seul. Un exemple typique est un ensemble de verrins sous une plateforme élévatrice. Imaginons que le système repose sur 3 verrins, 2 parmi trois assurent le bon fonctionnement.

# Analyse de la Structure

## Définition : Chemin (Path)

Ensemble X de composants tel que si ces composants sont fonctionnel alors le système est fonctionnel.
Rem : le terme chemin provient de l'idée qu'il doit exister un chemin parmi ces composants dans la représentation sous forme de graphe du système.

## Définition : Coupure (Cut)

Ensemble Y de composants tel que si ces composants sont défaillants alors le système est défaillant.
L'interprétation de SF en graphe donne l'origine du terme.

# Vecteurs d'états

## Vecteur d'état

Les valuations de l'état détaillé du système peuvent être représentées sous forme de vecteurs de taille fixe.

## Relation d'ordre sur les vecteurs

Soit x et y deux valuations d'états sur $\mathbb{B}^n$ ou $\{0,1\}^n$.

$$x \prec y \Leftrightarrow \forall i \in \{1,..,n\}, \exists j, (x_i < y_i \vee x_i = y_i) \wedge x_j < y_j$$

Un état en domine un autre si il contient plus de composants fonctionnels

# Coupures et Chemins minimaux

## Hypothèse

Nous utiliserons la notation entière pour les états dans la suite

## Chemin minimal

Le vecteur x caractérise un chemin minimal si $SF(x) = 1$,
et $\forall y, y \prec x \Rightarrow SF(y) = 0$

## Coupure minimale

Le vecteur x caractérise une coupure minimal si $SF(x) = 0$,
et $\forall y, x \prec y \Rightarrow SF(y) = 1$

# Un peu de pratique

## Exercice

Nous considérons un système fait de 4 composants tel que sa fonction de structure soit :

$$SF(x_1, ..., x_n) = (x_1 \wedge x_2) \vee (x_3 \wedge x_4)$$

Donnez la formule sur les entiers correspondant à SF.
Donnez un chemin et une coupure, puis idem en sélectionnant des vecteurs minimaux.

# Calcul de fiabilité

## Introduction des probabilités

Chaque état $x_i$ d'un composant devient une variable aléatoire à valeurs dans $\{0, 1\}$.
Le système possède un état aléatoire correspondant au vecteur de variables aléatoires $\mathbf{X}=(x_1, ..., x_n)$

## Definition

En supposant que la fonction de structure est bien définie.
La fiabilité d'un système $\mathbf{X}$ est :

$$R(X) = Pr(SF(X) = 1)$$

# Problème Général- RBD

## Calcul de probabilités sur une formule

SF une formule propositionnelle sur $RS$ ens. variable de fiabilité (aléatoires)
Calculer $\mathcal{P}(SF)$ = pb sommes disjointes = Complexité NP

La variable peut représenter une probabilité à la demande où une probabilité transitoire

# Bilan RBD

- Pratique pour cas simples
- Possibilité d'automatiser sur cas complex MAIS...
- Résolution générale = Probabilistic Datalog
- Modèle peu expressif de défaillance

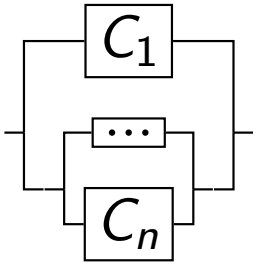
# Définition du problème

- disponibilité : capacité à rendre le service
- logique capturée : avec ou sans réparation ?
- Question : quelle est la disponibilité du système
- Critère 1 : ratio temps fonctionnel - non fonctionnel à l'infini
- Critère 2 : capacité du système à rester fonctionnel sur un intervalle (glissant - fixe)

# Exemple motivant 1

## Le détail :

- Modélisation de la réplication active
- modèle de défaillance : crash
- Question comment le modéliser par RBD
- Pour le crash : réplication active = architecture parallèle



# Disponibilité vs Fiabilité, et défaillances

Vision instantanée

## Distinction par les modes de défaillance

Si un unique mode de défaillance, alors pas de mode dégradé $\Rightarrow$ être disponible = être fiable = non défaillant

Vision dynamique

## Distinction par la mise en place de recouvrement

Si modèle de la dynamique de l'état du système défaillant/non défaillant, alors :

- fiabilité dépend de la transition vers l'état défaillant,
- disponibilité dépend de la durée des cycles état défaillant, état fonctionnel.

# Besoin en termes de modèles

- Modéliser différent modes de fonctionnement
- Modéliser les dates d'occurrences des défaillances, et événements de réparation
- Etre capable d'évaluer l'état de ces modèles au bout d'une durée déterminée

# Processus stochastique et Processus de Markov

## Processus stochastique

Etant donné un domaine D totalement ordonné modélisant le temps, un processus stochastique est une fonction de D qui retourne pour chaque valeur de D une variable aléatoire (usuellement entière ou réelle)

Deux types de domaines : discrets (entier) ou continus (réels).

## Processus Markovien à temps discret

Un processus X est dit markovien si la valeur de $X(n+1)$ dépend uniquement de $X(n)$ (indépendance avec les autres variables)

On notera ici qu'une réalisation de X n'est pas nécessairement un entier

# Chaine de Markov

## Chaine de Markov

Une chaine de markov est un processus de markov pour lequelle les réalisation de X(t) sont des entiers.

la suite du cours a été faite au tableau...