Cryptographie asymétrique

19 septembre 2023

1 CTL

syntaxe:

- E il existe un chemin..
- A pour tout chemin..
- μ jusqu'à..
- X a la prochaine étape..
- F chemin ou a un moment..
- G chemin ou on a toujours..
- $\wedge$, &.

structure de Kripke:

Definition 1.0.1. $\S = (S, s_o, \rightarrow, l)$, ou S est un ensemble fini d'état, $\rightarrow \subset S \times S$, $l : S \rightarrow 2^{Al}$: associe un ens de prop atomiques à tout état de $\S$.

remarque 1.1. Plusieurs anomalies, sans successeurs $AX\phi \equiv T$. Si $\rightarrow$ est "totale", $AX\phi = \neg tX\neg\phi$ sinon $\neg EX\phi = AX\neg\phi$.

1.2 model-checking

Question, étant donné une structure de Kripke $\S$ et une formule ϕ. Est-ce qu'il existe un algorithme qui renvoie $\S, s_0 \vDash \phi$. Oui ce qu'on fait c'est qu'on découpe la formule en sous formule puis récursion, et on vérifie les formules atomiques. On marque chaque sous formules puis on monte petit à petit.

Algorithme, Cas $\phi = A\phi_1\mu\phi_2$:

- Marquage(ϕ_1)
- Marquage(ϕ_2)
- Pour tout $s \in S$:
  - $s.\phi := false$
  - $s.nbsucc := deg(s)$(on est sur un graphe)
  - si $s.\phi_2 = T$ alors $L = L \cup \{s\}$
- Tant que $L \neq \emptyset$:
  - Piocher s dans L
  - $s.\phi := T$
  - Pour tout $s' \to s$:
    - $s'.nbsucc- = 1$
    - si $s'.nbsucc = 0 s'.\phi_1 = T s'.\phi_2 \neq T$: $L := L \cup \{s'\}$

Proposition 1.2.1. Décider si $\phi \in CTL$ est vraie pour $\S$ se fait en temps $\mathcal{O}(|\phi||\S|)$, $(|\S| = |S| + | \to |)$. (polynomial)

Le model checking de LTL est un pb PSPACE-complet $(2^{|\phi|}|\S|)$.

remarque 1.3. $A\phi_1\mu\phi_2 \equiv AF\phi_2 \neg E(\neg\phi_2)\mu(\neg\phi_1\neg\phi_2)$ veut simplement dire, on peut pas atteindre ϕ_2 en croisant un état ou on a ni ϕ_1 ni ϕ_2.

2 PCTL

Definition 2.0.1 (Discrete Time Markov Chain)**.** Une chaine de Markov: $M = (S, P, s_{init}, l)$ consiste en, S un ensemble d'états (dénombrable), s_{init} l'état de départ, $P : S \times S \to [0, 1]$ une matrice de probabilités, $l : S \to 2^{Al}$ l'étiquetage des états des props atomiques.

Si M est finie (i.e. S est fini), $|M| = |S| + \{(s, s')|P(s, s') > 0\}$.

Definition 2.0.2. Une chaine de Markov M induit une structure de Kripke $K_M = (S, s_{init}, \rightarrow, l)$ par $(s, s') \in \rightarrow \Leftrightarrow P(s, s') > 0$.

... defs a rajouter

2.1 Probabilités

Definition 2.1.1 (Tribu, σ-algèbre sur $@W$)**.** Ensemble de partie stable par complémentaire, union dénombrable et contenant le vide.

Definition 2.1.2 (mesure de Probabilité)**.** Mesure μ tq $\mu(@W) = 1$.

Definition 2.1.3. On définit $Path^F(M)$ les chemins finis.

Soit $M = (S, s_0, P, l)$ une chaine de Markov. Soit π_0 un prefixe de $\pi \in Path(M)$.

Definition 2.1.4. $Cyl(\pi_0) := \{\text{Chemins tq}\pi_0\text{en est un prefixe}\}$.

Pour nous, $@W$ est l'ens des chemins et $\mathring{A}$ la tribu des cylindres de M.

Definition 2.1.5. La mesure de probabilité sur $\mathring{A}$ est déf par la proba sur le préfixe.(produit des transitions)

2.2 Propriétés d'accessibilité

M une chaine de Markov et $A, B \subset S$ des ensembles d'états.

- 3 propriétés d'accessibilités:
  - $FB = \{$chemin qui croise eventuellement B$\}$
  - $A\mu B = \{$chemin dans A jusqu'a croiser B, + croise B eventuellement$\}$
  - $GFB = \{$croise B une infinité de fois$\}$.

Etant donné ϕ d'un des types décrits avant.

$$P(s \vDash \phi) = P(\{\pi \in Path(M, s)|\pi \vDash \phi\})$$

Faut vérifier que c'est mesurable:

- Pour FB on prend l'union dénombrable des chemins ayant leur bout dans B.
- Pour $A\mu B$, pareil que FB mais ou le chemin est d'abord dans A.
- Pour GFB on prend l'intersection de FB et $A\mu B$:

$$\cap_n \cup_{m \geq n} \cup_{s_n \in B} Cyl(s_0 \ldots s_n)$$

2.3 Propriétés d'accessibilité

Pour $s \in S$, on déf $x_s = P(s \vDash FB)$:

- $s \in B$, $x_s = 1$.
- $s \nvDash EFB$, alors $x_s = 0$. (exprimable en CTL)
- Pour les autres $s \in S_? := \{s \in S | s \notin B \wedge s \vDash EFB\}$:

$$x_s = \sum_{t \in B} p(s,t) + \sum_{t \in S_?} p(s,t) x_t$$

Si $\overline{x} = (x_s)_{s \in S_?} \rightarrow \overline{x} = \overline{b} + M\overline{x}$. $(M = (p(s,t))_{s,t})$

On déf aussi $x_s = Pr(s \vDash A\mu B)$:

- $s \in B$, $x_s = 1$.(noté $S_{=1} \subseteq \{Pr(s \vDash A\mu B) = 1\}$, pas d'égalité)
- $s \nvDash\rightarrow E(A\mu B)$ (il existe un etat qui atteint B en restand dans A), alors $x_s = 0$. (noté $S_{=0} := \{s \in S | Pr(s \vDash A\mu B) = 0\}$, egalité ici, permet de pas considérer les probas)
- $S_? = S - (S_{=0} \cup S_{=1})$

Soit $\overline{x} = (x_s)_{s \in S_?}$.

Proposition 2.3.1. $\overline{x}$ est la solution du système d'équations $\overline{y} = M\overline{y} + \overline{b}$ avec M carrée. $(\overline{b} = (b_s)_{s \in S_?}$ et $b_s = \sum_{t \in B} p(s,t))$

(**On résoud $M\overline{x} = \overline{x}$, clair+unicité.**)

On peut aussi caractériser par points fixes. On regarde:

$$\Gamma : [0,1]^{S_?} \rightarrow [0,1]^{S_?}$$

$$\Gamma(\overline{y} = M\overline{y} + \overline{b})$$

alors $\overline{x} = (x_s)$ avec $x_s = Pr(s \vDash A\mu B)$ est le plus petit point fixe de Γ. On a

$$\Gamma^n(x_s) = Pr(s \vDash A\mu^{\leq n} B)$$

avec $s \models EA\mu^{\leq n}B \equiv$ il existe un chemin depuis s, π, tq $\exists i \leq n$, $\pi(i) \in B$ et $\forall 0 \leq j < i$, $\pi(j) \in A$. En gros on arrive dans B avant n étapes. Si on pose

$$x_s^{(n)} = Pr(s \models A\mu^{\leq n}S_{=1})$$

et on a

$$\overline{x}^{(0)} \leq \ldots \leq \overline{x}^{(i)} \leq \ldots \leq \overline{x}$$

(pour $x \leq y$ si $\forall i,\ x_i \leq y_i$) On prouve

$$x_s^{(n)} = Pr(s \models A\mu^{\leq n}S_{=1})$$

- récurrence: $x_s^{(n+1)} = \sum_{(s,t)\in S_?} p(s,t)x_t^{(n)} + \sum_{t\in S_{=1}} p(s,t)$
- le premier terme est en degré n et l'autre 1.

Et on prouve $\overline{x}$ est un point fixe, et le plus petit.

- $x_s = \sum_{t\in S_{=0}} p(s,t)x_t + \sum_{t\in S_{=1}} p(s,t)x_t + \sum_{t\in S_?} p(s,t)x_t$