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 §.

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 § 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 § 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. $Cyl(\pi_0) := \{$Chemins tq$\pi_0$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 $A\mu B$:

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

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 $s \vDash EA\mu^{\leq n}B \equiv$ 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

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

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

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

- 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.

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

Enfin on def $x_s = Pr(s \vDash GFB)$

Definition 2.3.2. Un élt F est dit presque sur sous l'hyp d'un evt D ssi $Pr(D) = Pr(D \cap F)$

Propriété GF: Pour une chaine de Markov M (possiblement infinie) et $s, t \in S$, alors on :

$$Pr(s \vDash GFt) = Pr(s \vDash \bigwedge_{\pi\in Path^F(t)} GF\pi)$$

(pour tout π préfixe fini partant de t.)

Preuve: $\pi = ts_1 \ldots s_n$ et on note $p = \prod_i Pr(s_i, s_{i+1})$. On montre les proba

- $GFt \wedge G\neg\pi$ nulle.
- $GFt \wedge FG\neg\pi$ nulle

On déf $E_n(\pi) =$"on visite au moins n fois t et pas π avant au moins n étapes. On a

$$Pr(E_n(\pi)) \leq (1-p)^n$$

On pose $E(\pi) = \bigcap E_n(\pi)$, on croise jamais π. On a $E_{n+1}(\pi) \subseteq E_n(\pi)$ d'ou

$$Pr(E_(\pi)) = \lim_{n\to\infty} Pr(E_n(\pi)) \leq \lim_{n\to\infty} (1-p)^n = 0$$

On déf mtn $F_n({}_pi) = GFt \wedge X^n \neg F\pi$ puis $F(\pi) = \bigcup F_n(\pi)$, on a $F_n \subset F_{n+1}$ d'ou:

$$Pr(s \vDash F(\pi)) = \lim_{n\to\infty} Pr(s \vDash F_n(\pi))$$

Et on a en fait $Pr(s \vDash F_n(\pi)) = \sum_{s' \in S} Pr(s \vDash X^n s') Pr(s' \vDash E(\pi)) = 0$. Enfin

$$F := \bigcup_{\pi} F(\pi)$$

et

$$Pr(s \vDash F) \leq Pr(\sum_{\pi} F(\pi)) = 0$$

d'ou

$$Pr(s \vDash GFt) = Pr(s \vDash GFt \wedge \bigwedge_{\pi} GF\pi) + Pr(s \vDash GFt \wedge \bigwedge \vee_{\pi} FG\neg\pi)$$

et le deuxième terme vaut 0. □

Autrement dit on visite infiniment souvent t si et seulement si on visite tout les préfixes finis sortant de t infiniment souvent.

Definition 2.3.3. $CFC(M)$ les composantes fortement connexes (i.e. digraphe ou on peut accéder achaque point de chaque point.).

Definition 2.3.4. Une cfc est terminale si $Post^*(C) \subseteq C$ i.e. pas de chemin sortant. On appelle $CFCT$ l'ens.

On note $inf(\pi)$ les états de π qui apparaissent infiniment.

Proposition 2.3.5. Si M est une chaine finie. Alors

$$Pr(\{\pi / \inf(\pi) \in CFCT(M)\}) = 1$$

Preuve:$I(C) := \{\pi / \inf(\pi) \in C\}$,

$$\sum_{C \in CFC(M)} Pr(I(C)) = 1$$

Soit $C \in CFC(M)$ tq $Pr(I(C)) > 0$ et $t \in \inf(\pi)$. On a $Pr(s \vDash GFt) > 0$ d'ou $\forall \pi \in Path^F(t)$, $Pr(passerpar\pi) > 0$(en fait 1). Si C n'est pas terminale on peut en sortir, contradictoire avec $\inf(t) = C$. Tout les π doivent rester dans $C \rightarrow$terminale. □

Corollaire 2.3.6. *Si M est une CM finie:*

$$Pr(s \vDash GFt) = \begin{cases} 0 & t \notin C \subset CFCT(M) \\ Pr(s \vDash FC) & sinon \end{cases}$$

Objectifs: On suppose que M est finie.
Calculer $S_{\sim\alpha}(c\mu B)$, états vérifiant $c\mu b$. On a

$$\sim \in \{=, <, >, \leq, \geq\}$$

$$\alpha \in \{0, 1\}$$

$\rightarrow S_{=0}(c\mu B)$...
$\rightarrow S_{=1}(c\mu B)$. $(c, B \subseteq S,\ M(S, P, s_0, l))$

On construit de chaine de Markov M' a partir de M ou les états de $B \cup (S \backslash C)$. Sont absorbantes. (i.e. bouclent sur eux meme avec proba 1)
$M' = (S, P', s_0, l)$, avec :

$$P'(s,t) = \begin{cases} 1 & si\ t = s\ et\ s \in B \cup S \backslash C \\ 0 & si\ t \neq s\ et\ s \in B \cup S \backslash C \\ P'(s,t) & sinon \end{cases}$$

Pour les états de $B \cup S \backslash C$ on connait leur proba de vérifier $c\mu B$.

$$B \rightarrow 1$$

$$S \backslash (C \cup B) \rightarrow 0$$

On a

$$Pr^M(s \vDash c\mu B) = Pr^{M'}(s \vDash FB)$$

ET

$$Pr^M(s \vDash c\mu B) = Pr^{M'}(s \vDash FB) = 1\ si\ s \in B$$
$$Pr^M(s \vDash c\mu B) = Pr^{M'}(s \vDash FB) = 0\ si\ s \in S \backslash (C \cup B)$$

cas général ? Le pb est désormais de calculer

$$S_{=1}(FB)$$

i.e. $\{s | Pr(s \vDash FB) = 1\}$.

On a l'**équivalence** suivante:

1. $Pr(s \vDash FB) = 1$
2. $Post^*(t) \cap B \neq \emptyset$, $\forall t \in Post^*(s)$.
3. $s \in S \backslash Pre^*(S \backslash Pre^*(B))$.

Preuve: 1. $\Longrightarrow$ 2. est clair. 2. $\Longrightarrow$ 1. Une execution depuis s finit avec proba 1 dans une CFCT. Celles ci étant de deux types.

1. Singleton dans B.
2. Cycle d'états dont aucun est dans B.

(faut se rappeler que $Post^*(C) = C$) Pour tout état d'une CFCT, on a $t \in Post^*(C)$ donc $Post^*(t) \cap B \neq 0$. Donc on peut pas avoir une CFCT comme 2. donc la proba d'avoir $G\neg B$ est nulle. 2. $\equiv$ 3.

$$
\begin{aligned}
& Post^*(t) \cap B \neq \emptyset \quad \forall t \in Post^*(s) \\
\Leftrightarrow\ & Post^*(s) \subseteq Pre^*(B) \\
\Leftrightarrow\ & Post^*(s) \cap S \backslash Pre^*(B) = \emptyset \\
\Leftrightarrow\ & s \notin Pre^*(S \backslash Pre^*(B)) \\
\Leftrightarrow\ & s \in S \backslash Pre^*(S \backslash Pre^*(B))
\end{aligned}
$$

□

Corollaire 2.3.7. *Pour calculer $S_{=1}(c\mu B)$ on construit M' puis on calcule $S \backslash Pre^*(S \backslash Pre^*(B))$. Temps linéaire en $|M|$.*