

# Notes de cours de Vérification

Yann Miguel

6 janvier 2022

## Table des matières

1	Cours 1	2
2	Cours 2	4

# 1 Cours 1

Le  $\mu$ -calcul est une logique modale à points fixes.

Symboles du  $\mu$ -calcul:

- tt: vrai
- ff: faux
- $\wedge$ : conjonction
- $\vee$ : disjonction
- $\Box$ : universel (successeur toujours vrai)
- $\Diamond$ : existentiel (au moins un successeur vrai)
- $\mu X.\varphi$ : plus petit point fixe
- $\nu X.\varphi$ : plus grand point fixe

L'existentiel ne peut pas être vrai si il n'existe pas de successeur à l'état courant.

Formules importantes:

- $\Diamond tt$ : indique la présence d'au moins un successeur
- $\Box ff$ : indique l'absence de successeur
- $\Diamond ff$ : comme ff, toujours faux
- $\Box tt$ : comme tt, toujours vrai

$$\mu X^0.\varphi = \varphi[\frac{ff}{X}] . \mu X^{0+1}.\varphi = \varphi[\frac{\mu X^0.\varphi}{X}] . \llbracket \mu X.\varphi \rrbracket = \bigcup_{i \in \mathbb{N}} \mu X^i.\varphi$$

$$\mu X^0.a \vee \Diamond X = a \vee \Diamond ff = a$$

$$\mu X^1.a \vee \Diamond X = a \vee \Diamond a$$

$$\mu X^2.a \vee \Diamond X = a \vee \Diamond(av \Diamond a)$$

Donc,  $\mu X^i.a \vee \Diamond X \rightarrow \exists a$  dans au plus i pas.

Le plus petit point fixe dit donc qu'il existe un a accessible, sans préciser quand.

$$\mu X^0.a \wedge \Box X = a \wedge \Box ff$$

$$\mu X^1.a \wedge \Box X = a \wedge (a \wedge \Box ff)$$

$\mu X^i.a \wedge \Box X$ : a est vrai jusqu'à la profondeur i.

$\mu X^i.a \wedge \Box X = \Box a$ , et tout les chemins sont finis.

$$\nu X^0.\varphi = \llbracket \frac{tt}{X} \rrbracket . \nu X^1.\varphi = \llbracket \frac{\nu X^0.\varphi}{X} \rrbracket . \llbracket \nu X.\varphi \rrbracket = \bigcap_{i \in \mathbb{N}} \nu X^i.\varphi$$

$$\varphi = \nu X; a \wedge \Diamond X$$

$$\varphi^0 = a \wedge \Diamond tt$$

$$\varphi^1 = a \wedge \Diamond(a \wedge \Diamond tt)$$

$$\varphi^2 = a \wedge \Diamond(a \wedge \Diamond(a \wedge \Diamond tt))$$

$\varphi^i$ :  $\exists$  un chemin de longueur  $i + 1$ , ayant un successeur,  $\wedge \Box a$ . J'ai un chemin infini avec des  $a$  partout.

$$\varphi = \nu X; a \wedge \Box X$$

$$\varphi^0 = a \wedge tt$$

$$\varphi^1 = a \wedge \Box(a \wedge tt)$$

$\varphi^i$ :  $a$  est vrai pendant  $i$  pas. Donc,  $\varphi$ :  $a$  est toujours vrai. Quelques formules:

- $\mu X. \Box X$ : indique que tout chemin se termine, car la formule finira toujours par  $\Box \text{ff}$ , qui est l'absence de successeur
- $\mu X. (\Diamond X) \vee (\nu Y a \wedge \Box Y)$ : Il existe une partie accessible où  $a$  est toujours vrai.
- $\nu Y. (\Box Y) \wedge (\mu X. a \vee \Diamond X)$ : Il existe toujours un  $a$  accessible.
- $\nu Y. (\Box Y) \wedge (\neg \text{req} \vee (\mu X. \text{ack} \vee (\Box X \wedge \Diamond X)))$ : si on voit un  $\text{req}$ , il y aura toujours un  $\text{ack}$  dans le futur.
- $\nu X. \mu Y. \Diamond Y \vee (a \wedge \Diamond X)$ :  $\exists$  un chemin avec  $a$  infiniment souvent présent.
- $\mu X. \nu Y. (\Box Y \wedge \neg a) \vee a \wedge \Box X$ :  $\exists$  un nombre fini de  $a$  pour toute exécution.

Un jeu de parité réponds à la question: Si j'ai un graphe, est-ce que la formule est vraie dedans?

Un jeu de parité peut créer deux types de cycles avec les points forts, qui sont nommés en fonction du gagnant lorsqu'on entre dans le cycle; Ils sont:

1. cycle  $\mu$ -perdant
2. cycle  $\nu$ -gagnant

## 2 Cours 2

Un jeu de parité est un ensemble  $G=(V,E,\Omega)$ , avec:

- $V$ , des positions
- $E$ , des arrêtes
- $\Omega$ , une fonction

Les positions du jeu de parité peuvent appartenir à un des deux joueurs.

Joueur 1(aussi appelé Eve):

- Possède les positions circulaires
- Gagne si la plus grande priorité vue infiniment souvent est paire

Joueur 2(aussi appelé Adam):

- Possède les position carrées
- Gagne si la plus grande priorité vue infiniment souvent est impaire

Une stratégie  $\sigma$  est une fonction qui regarde l'historique du jeu.

Elle est dite positionnelle si elle ne regarde pas le dit historique.

Dans la partie  $\pi$ , si  $\pi_1 \in V_2$ , alors  $\pi_{i+1} = \sigma(\pi[0, i])$ .

**Théorème:** Si un joueur gagne dans  $G$ , il gagne avec une stratégie

positionnelle.

Algorithme de résolution des jeu de parité:

Complexité  $\Theta(n^d)$ :

Une variante des jeux de parité sont les jeux à registres. En plus

---

### Algorithm 1 Algorithme de Lielonka

---

```

f1(G,d)
repeat
  Nd = {v ∈ V | Ω(v)=d}
  G' = G \ Att1(G, Nd)
  W2 = f2(G, d-1)
  G = G \ Att2(G, W2)
until W2 = ∅
return G

```

---

de jouer, à chaque tour, le joueur 1 range la valeur sortie dans un registre. Il existe  $k$  registres.

Fonctionnement des registres:

- mise à jour(le joueur 1 met à jour le registre  $i$ ):
  - $j < i$ :  $r_j = 0$ .
  - $r_i = p$ (la valeur sortie)

- $j > i$ :  $r_j = \max(r_j, p)$
- priorité de sortie:
  - $2i$  si  $\max(r_i, p)$  est pair
  - $2i+1$  sinon

Les conditions de victoire sont les mêmes que pour les jeux de parité.

**Lemme:** Si le joueur 2 gagne  $G$ , il gagne  $G_k$ ,  $\forall k$ . Si le joueur 1 gagne

$G$ ,  $\exists k$  tel que le joueur 1 gagne  $G_k$ .

**Théorème:** Joueur 1 gagne  $G$  si et seulement si elle gagne  $G_{\log(n)+1}$ .

Par conséquent,  $J_1$  gagne  $G_{\log(n)+1} \Rightarrow J_1$  gagne  $G$ .

**Induction:**  $J_1$  gagne  $G_{\log(n)+1}$  avec une stratégie telle que, si  $r_k \geq p$  est paire, alors il n'y a pas de sortie  $2k+1$ .

Cette stratégie ne fonctionne que si il n'y a un composant fortement connexe utilisant tout les registres. Dans ce cas, il faut un registre de plus pour cette stratégie.

**Corollaire:** Algorithme  $2^{\Theta(\log^3(n))}$ : résoudre  $G_{\log(n)+1}$  au lieu de  $G$ , et le nombre de priorités est  $\Theta(\log(n))$ .

$f_1(G, d, p_2, p_1)$ . Un dominion est un ensemble tel que un joueur a une

stratégie gagnante à partir du dominion et qui n'en sort pas.

$f_1$  doit contenir tout les dominions  $J_1$  de taille  $\leq p_1$ , et n'intersecte

pas avec les dominions de  $J_2$ , de taille  $\leq p_2$ .

$f_2(G, d, p_1, p_2)$  existe aussi.

---

#### Algorithm 2 Algorithmme

---

```

 $f_1(G, d, p_2, p_1)$ 
if  $G = \emptyset \vee p \leq 1$  then
  return  $G$ 
end if
 $G_1 = f_1(G, d, p_2, \lfloor \frac{p_1}{2} \rfloor)$ 
 $N_d = \{v \mid \Omega(v) = d\}$ 
 $H = G_i \setminus \text{Att}_1(N_d, G)$ 
 $W_2 = f_2(H, d-1, p_1, p_2)$ 
 $G_2 = G_1 \setminus \text{Att}_2(W_2, G_2)$ 
 $G_3 = f_1(G_2, \lambda, p_2, \lfloor \frac{p_1}{2} \rfloor)$ 
return  $G_3$ 

```

---