

IFT503/711 – Théorie du calcul  
Université de Sherbrooke

## Devoir 4

Enseignants: Michael Blondin  
 Date de remise: jeudi 17 mars 2022 à 10h29  
 À réaliser: individuellement ou à deux au 1<sup>er</sup> cycle  
 Modalités: individuellement aux cycles supérieurs  
 Pointage: remettre en ligne sur Turnin  
 sur 40 points au 1<sup>er</sup> cycle (+ 5pts bonus pour ★)  
 sur 50 points aux cycles supérieurs

### Logique.

#### Question 1.

- (a) Rappelons que l'arithmétique de Peano, c.-à-d.  $\text{FO}(\mathbb{N}, +, \times, \leq)$ , est indécidable. Considérons une logique 5 pts similaire où, plutôt que la multiplication de variables «  $xy$  », nous avons accès au carré «  $x^2$  » d'une variable. Expliquez formellement pourquoi cette logique, c.-à-d.  $\text{FO}(\mathbb{N}, +, \cdot^2, \leq)$ , est indécidable.
- (b) Nous avons vu que l'arithmétique de Presburger, c.-à-d.  $\text{FO}(\mathbb{N}, +, \leq)$ , est décidable. Expliquez formellement 5 pts pourquoi cette logique étendue aux entiers, c.-à-d.  $\text{FO}(\mathbb{Z}, +, \leq)$ , est aussi décidable.

#### Question 2.

10 pts

Soit la formule  $\varphi(x, y) := (y = 3x + 1)$  de l'arithmétique de Presburger. **Donnez un automate qui reconnaît le langage associé à  $\varphi$ .**

Plus formellement, dénotons par  $\text{val}(z)$  la valeur numérique associée au mot  $z \in \{0, 1\}^*$  dont le bit de poids faible est à gauche. Par exemple,  $\text{val}(0010) = 4$  et  $\text{val}(1011) = 13$ . Dans ce contexte, le mot vide est également valide:  $\text{val}(\varepsilon) = 0$ .

Le langage associé à  $\varphi$  est

$$L := \{(x, y) \in (\{0, 1\} \times \{0, 1\})^* : \text{val}(y) = 3 \cdot \text{val}(x) + 1\}.$$

Par exemple, le mot  $w := (0, 1)(0, 0)(1, 1)(0, 1)$  appartient à  $L$ . En effet,  $w$  représente les nombres  $\text{val}(0010) = 4$  et  $\text{val}(1011) = 13$ , et nous avons bien  $13 = 3 \cdot 4 + 1$ .

*Indice: considérez cette reformulation de  $\varphi$ :  $\exists a (y = a + 1) \wedge (\exists b (a = b + x \wedge b = 2x))$  et construisez itérativement l'automate.*

## Calcul parallèle.

### Question 3.

10 pts

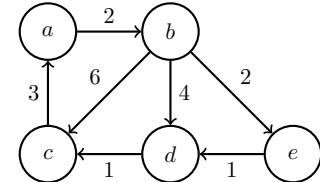
La *distance* d'un sommet  $s$  vers un sommet  $t$  dans un graphe dirigé pondéré est le coût d'un plus court chemin de  $s$  vers  $t$ . Par exemple, dans le graphe ci-dessous, la distance de  $a$  vers  $c$  est de 6.

**Montrez que le problème PCC appartient à NC:**

#### PCC

ENTRÉE: un graphe dirigé pondéré  $\mathcal{G} = (V, E)$  décrit par une matrice de coûts positifs, deux sommets  $s, t \in V$ , et un entier positif  $k$  sous représentation binaire;

QUESTION: la distance de  $s$  vers  $t$  dans  $\mathcal{G}$  est-elle égale à  $k$ ?



Il n'est pas nécessaire d'argumenter que votre famille de circuits est uniforme sous espace logarithmique, mais il faut brièvement expliquer pourquoi elle est uniforme sous temps polynomial.

### Question 4.

10 pts

Soit  $X$  un ensemble fini. Nous disons que  $S \subseteq X$  engendre  $t \in X$  sous une opération binaire  $\star: X \times X \rightarrow X$  s'il est possible d'appliquer  $\star$  à partir d'éléments de  $S$  jusqu'à l'obtention de  $t$ . Par exemple, pour l'opération décrite par la table ci-dessous,  $S = \{a, c\}$  engendre  $e$  car  $(a \star a) \star (c \star a) = b \star d = e$ .

**Montrez que le problème GÉNÉRATION est P-complet:**

#### GÉNÉRATION

ENTRÉE: un ensemble fini  $X$ , une opération binaire  $\star: X \times X \rightarrow X$  représentée sous forme de table, un sous-ensemble  $S \subseteq X$ , et un élément  $t \in X$ ;

QUESTION: est-ce que  $S$  engendre  $t$  sous l'opération  $\star$ ? Indice: voyez une porte comme deux éléments.

$\star$	$a$	$b$	$c$	$d$	$e$
$a$	$b$	$b$	$a$	$a$	$a$
$b$	$b$	$d$	$a$	$e$	$b$
$c$	$d$	$a$	$a$	$a$	$a$
$d$	$c$	$c$	$a$	$d$	$c$
$e$	$c$	$c$	$a$	$d$	$e$

Il n'est pas nécessaire d'expliquer pourquoi votre réduction se calcule en espace logarithmique.

## ★ Question 5. (cycles supérieurs)

Montrez que  $\text{REG} \subseteq \text{NC}^1$ , où  $\text{REG}$  est l'ensemble des langages réguliers.

★ 10 pts

Indice: afin de déterminer si un automate accepte un mot  $w$ , considérez des sous-mots de  $w$  de taille 1, 2, 4, ...