IFT503/711 – Théorie du calcul

Université de Sherbrooke

Examen fictif pour étude

Enseignants: Michael Blondin, Manuel Lafond, Dave Touchette

Date: —

Durée: 3 heures

Directives:

- Répondez aux questions dans le **cahier de réponses**, pas sur ce questionnaire;
- **Toute documentation** est permise;
- Donnez **une seule réponse** par sous-question;
- L'examen comporte **6 questions** sur **3 pages** valant un total de **60 points**;
- La correction se base notamment sur la **clarté**, l'**exactitude** et la **concision** de vos réponses, ainsi que sur la **justification** pour les questions qui en requièrent une.

Cet « examen » est un exemple qui combine des questions d'examens antérieurs. Les six thématiques seront les mêmes, et l'esprit de l'examen sera le même, mais la forme exacte des questions varie d'année en année. Les questions s'inspirent respectivement des six devoirs.

Question 1: calculabilité

Soit ce langage sur alphabet $\Sigma \coloneqq \{a, b, c\}$:

$$L \coloneqq \{a^n b^n c^n : n \in \mathbb{N}\}.$$

Par exemple, $aabbcc \in L$, $aabcc \notin L$ et $aaccbb \notin L$.

(a) Donnez le diagramme (avec états et transitions) d'une machine de Turing à *un seul* ruban qui décide L. Vous ne pouvez pas utiliser de macro de haut niveau, mais vous pouvez supposer que l'entrée débute par \$. Afin d'alléger le diagramme, ne tracez pas les transitions vers l'état rejetant. 7 pts

(b) Quel est le temps d'exécution asymptotique de votre machine? Est-il possible d'obtenir un meilleur temps en utilisant plusieurs rubans? Justifiez. 3 pts

Question 2: décidabilité

(a) Si $A \leq_m B$ et B est un langage fini , i.e., $|B| = n \in \mathbb{N}$, est-ce que ça implique que A est un langage fini ? Justifiez votre réponse. 3 pts

(b) Soit le langage $K = \{w : w = a2b, \text{ pour } a \in HALT_{TM}, b \in \overline{HALT_{TM}}\}$ sur alphabet $\Sigma = \{0, 1, 2\}$. Montrez que ni K ni $\bar{K}$ n'est Turing-reconnaissable. 4 pts

(c) Est-ce qu'il est vrai que pour toute paire de langages A et B, il existe un langage C tel que $C \leq_m A$ et $C \leq_m B$? Justifiez votre réponse. 3 pts

Question 3: P versus NP

Soit ϕ une formule booléenne. On dénote par $\mathcal{V}(\phi)$ l'ensemble des variables qui apparaissent dans ϕ (par exemple, $x_1, x_2, \ldots, x_n$). De plus, on dénote par $\mathcal{A}(\phi)$ l'ensemble des assignations de $\mathcal{V}(\phi)$ qui satisfont ϕ. Soit le langage 10 pts

$$\text{DIFF-SAT} = \{\langle \phi, \psi \rangle : \phi \text{ et } \psi \text{ sont des formules booléennes telles que } \mathcal{V}(\phi) = \mathcal{V}(\psi) \text{ et } \mathcal{A}(\phi) \neq \mathcal{A}(\psi)\}.$$

Montrez que DIFF-SAT est NP-complet.

Suggestion. Réduction via SAT. Notez que $\phi \in \text{SAT}$ si et seulement si $\mathcal{A}(\phi) \neq \emptyset$.

Question 4: calcul parallèle

Vous n'avez pas à montrer que vos familles de circuits sont uniformes, mais elles doivent l'être.

(a) Montrez que ce problème appartient à AC^0 (ou à AC pour la moitié des points): 6 pts

TRIBIN

ENTRÉE: $x \in \{0,1\}^+$ (une suite non vide de bits)

QUESTION: x est triée en ordre croissant?

Par exemple, nous avons 001 ∈ TRIBIN, 011 ∈ TRIBIN, 000 ∈ TRIBIN, 1011 ∉ TRIBIN et 11100 ∉ TRIBIN.

(b) Considérons ce problème qui appartient à FAC^0: 4 pts

MAX

ENTRÉE: deux nombres binaires x et y avec le même nombre de bits

SORTIE: $\max(x, y)$

Expliquez pourquoi ce problème appartient à NC^2 (ou à NC pour la moitié des points):

EST-MAX

ENTRÉE: une suite de nombres binaires $x_1, x_2, \ldots, x_k, y$ avec le même nombre de bits

QUESTION: $\max(x_1, x_2, \ldots, x_k) = y$?

Remarque: k n'est pas une constante, il s'agit de suites de taille arbitraire.

Il pourrait également y avoir une question sur la P-complétude. Par exemple, montrer qu'un problème B est P-difficile. Pour ce faire, nous avons vu qu'on doit réduire CVP à B.

Question 5: complexité en temps et en espace

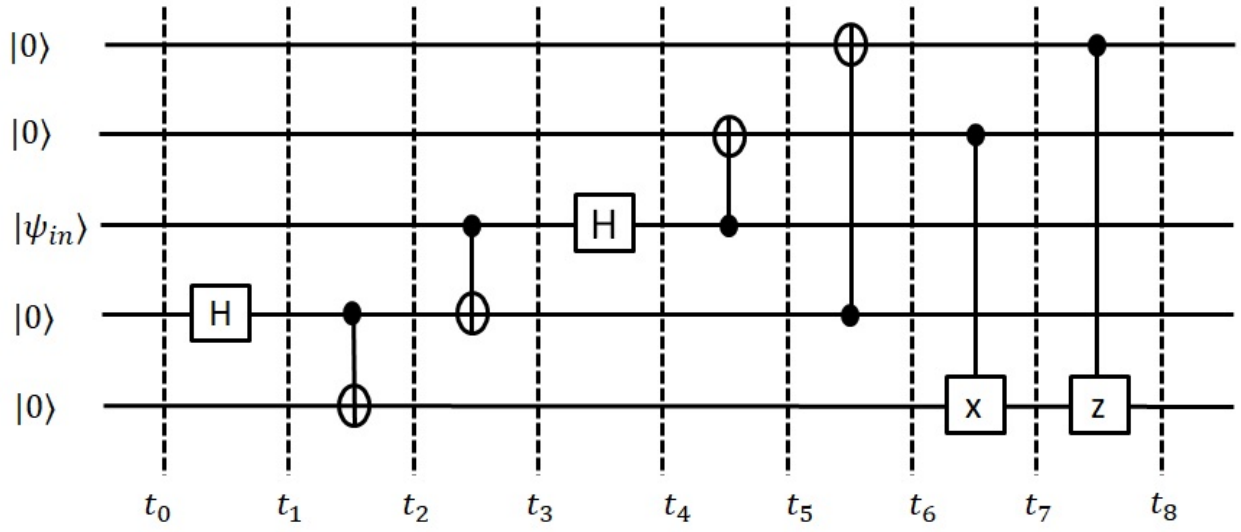
(a) Montrez que si la ETH est vraie, alors CLIQUE ne peut pas être décidé en temps $2^{o(\sqrt{m})}poly(n+m)$, où n est le nombre de sommets du graphe donné et m son nombre d'arêtes. Il suffit d'utiliser le fait que dans notre réduction de 3-SAT vers CLIQUE, le nombre de sommets était linéaire par rapport au nombre de clauses. 3 pts

(b) Dans le jeu policier-voleur, on a un graphe $G = (V, E)$, un sous-ensemble $P \subseteq V$ (les policiers) et un sommet $v \in V \setminus P$ (le voleur). Deux joueurs jouent chacun leur tour. À son tour, le joueur 1 choisit $p \in P$ et le déplace vers un sommet adjacent à p (formellement, P devient $(P \setminus \{p\}) \cup \{p'\}$, où p' est un voisin de p). À son tour, le joueur 2 déplace v vers un de ses voisins. Le joueur 1 gagne si, à n'importe quel moment, le voleur occupe la même case qu'un policier, c'est-à-dire que $v \in P$. Le joueur 2 gagne si ceci ne se produit jamais. 7 pts

Soit COP-WIN l'ensemble des instances (G, P, v) sur lesquelles le joueur 1 peut toujours attraper le voleur en moins de $|V(G)|$ tours. Montrez que COP-WIN $\in$ PSPACE.

Question 6: informatique quantique

Soit le circuit suivant, avec $|\psi_{in}\rangle = \alpha|0\rangle + \beta|1\rangle$.



(a) Quels sont les états $|\psi_0\rangle, |\psi_2\rangle, |\psi_4\rangle, |\psi_6\rangle, |\psi_8\rangle$ aux temps t_0, t_2, t_4, t_6, t_8, respectivement, en fonction des amplitudes α, β de $|\psi_{in}\rangle$? Montrez votre calcul. 8 pts

(b) Pouvez-vous réécrire l'état $|\psi_8\rangle$ comme $|\phi_{14}\rangle \otimes |\phi_5\rangle$ avec $|\phi_{14}\rangle$ l'état des 4 qubits du haut et $|\phi_5\rangle$ l'état du qubit du bas ? Si oui, quel est $|\phi_5\rangle$ en fonction de α, β ? 1 pt

(c) Donnez une interprétation de ce circuit. 1 pt

Il pourrait également y avoir une question sur BQP vs. les autres classes de langages vues dans le cours.