

Université Bordeaux 1. Master Sciences & Technologies,  
Informatique. Examen UE IN7W11, Modèles de calcul.

Responsable A. Muscholl

Session 1, 2011–2012. 12 décembre 2011, 14h-17h.

*Documents autorisés : transparents du cours et notes de TD.*

*Le barème est indicatif. A noter que le barème total dépasse 20 points.*

*On attachera une grande importance à la clarté et à la concision des justifications.*

**Exercice 1 (7 points)** Répondez par “Vrai” ou “Faux” aux questions suivantes. **Détachez et joignez cette première feuille à votre copie.** Notation : 0,5 par réponse juste et  $-0,5$  par réponse fausse (l’absence de réponse vaut 0 points). Le résultat final sera le maximum entre 0 et la somme des points réalisés.

*Rappels* :  $A \leq_P B$  signifie que le problème  $A$  se réduit au problème  $B$  par une réduction calculable en temps polynomial. Par PCP on note le problème *Correspondance de Post* (dominos), et par SAT le problème de satisfaisabilité de formules propositionnelles. **P** est la classe des problèmes où on peut *trouver* une solution en temps polynomial, et **NP** la classe des problèmes où on peut *vérifier* une solution en temps polynomial.

	Vrai	Faux
1 On peut énumérer les sous-parties de $\mathbb{N}$ de taille au plus 99.	<input type="checkbox"/>	<input type="checkbox"/>
2 On peut énumérer les fonctions récursives.	<input type="checkbox"/>	<input type="checkbox"/>
3 Les mots d’un langage semi-décidable peuvent être énumérés en ordre hiérarchique.	<input type="checkbox"/>	<input type="checkbox"/>
4 Si $A \subseteq \mathbb{N}$ et son complémentaire $\mathbb{N} \setminus A$ sont des ensembles semi-décidables, alors $A$ est décidable.	<input type="checkbox"/>	<input type="checkbox"/>
5 Si $A, B$ sont des ensembles tels que $A \subseteq B$ et $B$ est décidable, alors $A$ est aussi décidable.	<input type="checkbox"/>	<input type="checkbox"/>
6 Si $A$ se réduit à $B$ et $B$ se réduit à $C$ , alors $A$ se réduit à $C$ .	<input type="checkbox"/>	<input type="checkbox"/>
7 On sait décider s’il y a une infinité de nombres premiers.	<input type="checkbox"/>	<input type="checkbox"/>
8 On sait décider si un programme WHILE s’arrête sur au moins une entrée.	<input type="checkbox"/>	<input type="checkbox"/>
9 On sait réduire le problème PCP au problème SAT.	<input type="checkbox"/>	<input type="checkbox"/>
10 On sait décider si une instance de PCP a une solution de longueur au plus 99.	<input type="checkbox"/>	<input type="checkbox"/>
11 $\mathbf{P} = \mathbf{NP}$ si au moins un problème <b>NP</b> -difficile appartient à <b>P</b> .	<input type="checkbox"/>	<input type="checkbox"/>
12 On sait décider si deux programmes WHILE calculent la même fonction.	<input type="checkbox"/>	<input type="checkbox"/>
13 Si $A \in \mathbf{NP}$ et $A \leq_P B$ , alors $B \in \mathbf{NP}$ .	<input type="checkbox"/>	<input type="checkbox"/>
14 Si $B \in \mathbf{NP}$ et $A \leq_P B$ , alors $A \in \mathbf{NP}$ .	<input type="checkbox"/>	<input type="checkbox"/>



**Exercice 2 (4 points)** Justifiez que les ensembles suivants sont dénombrables.

- L'ensemble des polynômes à une variable, avec coefficients entiers.
- L'ensemble des matrices avec entrées rationnelles.

**Exercice 3 (6 points)** Soit *Premier* le problème suivant :

- *Entrée* : entier  $n$ .
- *Sortie* : OUI si  $n$  est premier, NON sinon.

On peut voir *Premier* aussi comme une fonction, en remplaçant OUI par 1 et NON par 0.

Décrivez une solution pour *Premier* dans **un** des modèles de calcul suivants (*vous pouvez donc en choisir un !*)

1. Fonctions primitives-récurrentes.
2. Programmes LOOP.
3. Machines de Turing.

Vous pouvez utiliser une machine de Turing  $M_{div}$  qui travaille sur une entrée de la forme  $\underbrace{1 \cdots 1}_n \# \underbrace{1 \cdots 1}_k$ . La machine  $M_{div}$  finit son calcul avec le même contenu sur la bande (et la tête sur le premier 1), ainsi qu'en état final si  $k$  divise  $n$ , et état non-final sinon.

**Exercice 4 (8 points)**

1. Montrez que le problème suivant est décidable. Justifiez bien votre réponse.
  - *Entrée* : programme WHILE  $P$ , avec variables  $x_0, \dots, x_{k-1}$ , et entier  $N$ .
  - *Sortie* : OUI, si le calcul de  $P$  à partir des valeurs initiales  $\underbrace{0, \dots, 0}_k$  est tel qu'aucune des variables ne dépasse la valeur  $N$  au cours du calcul.
2. Quel est le temps de calcul de votre algorithme pour la question précédente ?
3. Montrez que le problème suivant est indécidable. Justifiez bien votre réponse.
  - *Entrée* : programme WHILE  $P$  avec variables  $x_0, \dots, x_{k-1}$ .
  - *Sortie* : OUI s'il existe un entier  $N$  tel que le calcul de  $P$  à partir des valeurs initiales  $\underbrace{0, \dots, 0}_k$  est tel qu'aucune des variables ne dépasse  $N$ .

**Exercice 5 (5 points)** Rappels : un problème  $P$  appartient à la classe **NP** s'il existe un vérificateur polynomial  $V$  pour  $P$  : l'algorithme  $V$  reçoit en entrée un couple  $\langle x, y \rangle$  et son temps de calcul est polynomial en fonction de la taille de  $x$  et de  $y$ . Une instance  $x$  de  $P$  est positive, si et seulement si il existe un  $y$  de taille polynomiale en  $|x|$  et tel que  $V$  accepte  $\langle x, y \rangle$ .

*Vous pouvez supposer pour cet exercice, ainsi que l'exercice suivant, que  $y$  est une séquence de bits (0 ou 1). La taille de  $y$  est donc la longueur de la séquence.*

Justifiez que tout problème de la classe **NP** possède un algorithme dont le temps de calcul est exponentiel.

**Exercice 6 (5 points)** Soit  $P$  un problème et  $f : \mathbb{N} \rightarrow \mathbb{N}$  une fonction. Un  $f$ -vérificateur  $V$  pour  $P$  est un vérificateur polynomial (en fonction de la taille de  $x$  et de  $y$ ) où la taille de  $y$  est bornée par  $f(|x|)$ .

Soit  $\mathcal{C}_f$  la classe des problèmes qui possèdent un  $f$ -vérificateur.

1. Dans quelle classe de problèmes se trouve  $\mathcal{C}_f$  quand  $f$  est un polynôme ? Justifiez votre réponse.
2. Montrez que  $\mathcal{C}_f \subseteq \mathbf{P}$ , quand  $f$  est une fonction constante,  $f(n) = c$  pour tout  $n \in \mathbb{N}$ . Généralisez votre argument pour  $f(n) = \log(n)$ .

**Exercice 7 (5 points)** Pour le problème *Chemin long* on prend en entrée un graphe orienté  $G = (V, E)$  (donc  $V$  ensemble de sommets et  $E$  ensemble d'arcs) et un entier  $k$ . On veut savoir s'il existe dans  $G$  un chemin *simple* avec  $k$  sommets. Un chemin simple est une suite  $v_1, \dots, v_k$  de sommets  $v_i \in V$  tel que  $v_i \neq v_j$  pour tout  $i \neq j$ , et  $(v_i, v_{i+1}) \in E$  pour tout  $1 \leq i < k$ .

Dans cet exercice on construit une réduction polynomiale de *Chemin long* au problème SAT (satisfaisabilité des formules booléennes propositionnelles). La formule  $\varphi_G$  associée au graphe  $G$  sera la conjonction des trois formules demandées ci-dessous.

La formule  $\varphi_G$  a  $k|V|$  variables booléennes de la forme  $x_{v,i}$ , pour  $v \in V$  et  $1 \leq i \leq k$ . On veut que la variable  $x_{v,i}$  prend la valeur "vrai" si le sommet  $v$  est le  $i$ -ème sommet du chemin.

1. Ecrivez une formule propositionnelle qui exprime que pour chaque  $i \in \{1, \dots, k\}$ , il y a au moins un sommet qui est le  $i$ -ème sommet du chemin.
2. Ecrivez une formule propositionnelle qui exprime que pour chaque  $i \in \{1, \dots, k\}$ , il n'y a pas deux sommets différents qui sont le  $i$ -ème sommet du chemin
3. Ecrivez une formule propositionnelle qui exprime que la solution représente bien un chemin.