COMPLEX - Partie 2
2023-2024

Énoncé

Nom ou numéro d'anonymat :

Durée : 2 heures

Les exercices sont indépendants.
Une rédaction claire et concise sera appréciée. Toute affirmation devra être **justifiée**.
Une question non résolue n'empêche pas de faire les suivantes
(dans ce cas indiquez clairement que vous admettez le(s) résultat(s) de la question non faite).

Exercice 1 : Classes de complexité probabilistes

1.a] Donner une définition formelle de la classe de complexité $\mathcal{ZPP}$

1.b] Donner une définition formelle de la classe de complexité $\mathcal{BPP}$

1.c] Donner une définition formelle de la classe de complexité $\mathcal{RP}$

Exercice 2 : Égalité de matrices creuses

Une matrice creuse est une matrice contenant beaucoup de zéros. Les matrices creuses interviennent dans de nombreux domaines de l'informatique. Afin d'économiser une quantité importante d'espace mémoire, il est généralement souhaitable de ne stocker que les coefficients non nuls d'une telle matrice.

Nous supposerons dans la suite qu'une matrice (définie sur un corps arbitraire) $M = (m_{i,j})_{1 \leq i \leq n, 1 \leq j \leq m}$ de taille $n \times m$ est représentée par un ensemble de triplets $(i, j, m_{i,j})$ pour tous les $m_{i,j} \neq 0$ de la matrice (pour $1 \leq i \leq n$ et $1 \leq j \leq m$). Si la matrice contient ℓ valeurs différentes de 0, les ensembles utilisés pour la représenter contiennent donc seulement ℓ triplets (dans un ordre arbitraire).

2.a] Proposer un algorithme déterministe qui étant donné deux matrices creuses représentées par deux ensembles de tels triplets (de cardinal au plus ℓ), détermine si les deux matrices associées sont égales en temps $O(\ell \log \ell)$.

2.b] En vous inspirant de l'algorithme de vérification de produits matriciels (de Freivalds) vu en TD, proposer un algorithme probabiliste (de type Monte-Carlo) qui étant donné deux matrices creuses représentées par deux ensembles de tels triplets de cardinal au plus ℓ, détermine si les deux matrices associées sont égales en $O(\ell)$ opérations sur le corps de définition des matrices.
Donner une borne supérieure sur sa probabilité d'erreur

Exercice 3 : Équations linéaires modulo un nombre premier

3.a] Soit p un nombre premier. Considérons un système linéaire en n variables et m équations modulo p. En vous inspirant de la version probabiliste de l'algorithme de Johnson pour MAX-3-SAT, proposer un algorithme probabilisite (de type Las Vegas) qui retourne un choix des n variables qui satisfait au moins m/p équations en temps polynomial en n, m et $\log(p)$.
Donner la complexité de votre algorithme et justifier qu'il retourne toujours une réponse correcte (c'est-à-dire, satisfaisant au moins m/p équations).