Université du Sud-Toulon-Var / UFR-Sciences et Techniques

Maîtrise de mathématiques – TD B

1. Complexité

Exercice 1. On considère l'algorithme d'Euclide soustractif :

Algorithme 1 : Euclide

Entrée : deux entiers positifs a et b, $a \leq b$.
Sortie : $d = (a, b)$.
Règles :

(1a) $(a, b) \mapsto (a, b - a)$, si $0 < u \leq v$.

(1b) $(a, b) \mapsto (a - b, b)$, si $0 < v \leq u$.

(1c) $(a, b) \mapsto a$, si $b = 0$.

(1d) $(a, b) \mapsto b$, si $a = 0$.

L'objet de l'exercice est de montrer que le nombre de règles à appliquer pour calculer le pgcd de deux entiers a et b à l'aide de cet algorithme est majoré par $1 + \frac{3}{2}\log_2(f_{n+1})$ où $(f_n)_{n\in\mathbf{N}}$ désigne la suite de Fibonacci :

$$f_0 := 0, \quad f_1 := 1, \quad f_{n+1} := f_n + f_{n-1}.$$

(1) Calculez F_n en fonction de n. On rappelle que la suite (f_n) est une combinaison linéaire des suites de la famille

$$n \mapsto n^k \lambda_i^n, \quad 1 \leq i \leq p,\ 0 \leq k \leq r_i - 1,$$

où λ_i, $1 \leq i \leq p$ sont les p valeurs propres de multiplicités respectives r_i de l'endomorphisme représenté par la matrice

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

(2) Déduisez que f_n est l'entier le plus proche de $\phi^n/\sqrt{5}$ où $\phi = (\sqrt{5}+1)/2$ est le nombre d'or. Montrez alors que $n \leq 1 + \frac{3}{2}\log_2(f_{n+1})$.

(3) Montrez par récurrence le théorème de Lamé (1845) : si l'algorithme d'Euclide s'arrête après l'application de n règles, alors

$$a \geq df_{n+2}, \quad b \geq df_{n+1},$$

en supposant que $a > b$. Concluez.

(4) Donnez une majoration du nombre d'opérations arithmétiques nécessaires et une majoration élémentaire du coût de chaque opération en fonction de la taille des entiers manipulés.

Exercice 2. Évaluez la complexité du crible d'Erathostène pour déterminer si un entier N est premier.

Exercice 3. Montrez que le problème du circuit hamiltonien se transforme polynomialement en le problème du voyageur de commerce :

VOYAGEUR DE COMMERCE
Instance : Un graphe $G = (V, E)$, une distance $d : V \times V \to \mathbf{R}_+$, un entier positif B.
Question : Existe-t-il $\sigma \in \mathfrak{S}_n$ tel que

$$d(v_{\sigma(n)}, v_{\sigma(1)}) + \sum_{1\leq i<n} d(v_{\sigma(i)}, v_{\sigma(i+1)}) \leq B \ ?$$

en notant $V = \{v_1, \ldots, v_n\}$? Qu'en déduisez-vous ?

Exercice 4. Le principe général pour démontrer qu'un problème Π est NP-complet se décompose en quatre étapes :

(1) Montrer que $\Pi \in$ NP ;
(2) Choisir un problème Π' NP-complet "proche" de Π ;
(3) Construire une transformation f de Π' vers Π ;
(4) Montrer que f est une transformation polynomiale.

Montrez que le problème 3SAT est NP-complet. pour cela, transformez chaque clause c_i de SAT en un ensemble C_i de clauses à trois littéraux de manière à ce que c_i soit satisfaisable si et seulement si les clauses de C_i le sont.

Exercice 5. Montrez que le problème du décodage d'un code linéaire binaire est NP-complet à l'aide du problème des mariages tri-dimensionnels :

DÉCODAGE
Instance : H une matrice de contrôle binaire $n \times n-k$, un syndrome s de longueur $n-k$ et un poids w.
Question : Existe-t-il $y \in \mathbf{F}_2^n$ tel que $yH = s$?

MARIAGES TRIDIMENSIONNELS
Instance : Un sous-ensemble $T \subseteq X \times Y \times Z$, où X, Y et Z sont trois ensembles finis de même cardinal q.
Question : Existe-t-il une partie $M \subseteq T$ de cardinal q telle que $\forall x \in X$ (resp. $\forall y \in Y$, $\forall z \in Z$), $\exists!(x, b, c) \in M$ resp. $\exists!(a, y, c) \in M$, $\exists!(a, b, z) \in M$?

Indication : Considérez la matrice binaire à $|T|$ lignes et $n = 3q$ colonnes définie de la manière suivante : chaque ligne est indexée par un triplet (x, y, z) de T, les q premières colonnes sont indexées par les éléments de X, les q suivantes par ceux de Y et les q dernières par les éléments de Z. Sur chaque ligne de la matrice il y a exactement trois termes non-nuls, les colonne indicées par x, y et z en supposant que c'est le triplet (x, y, z) qui indice cette ligne.