EXAMEN ALGORITHMIQUE AVANCEE

LICENCE 2, MODULE I31

18 décembre 2014

AUCUN INSTRUMENT ELECTRONIQUE N'EST AUTORISE. LA COPIE EST NOTEE ZERO DES QU'IL Y A UN PROGRAMME.

1. Déroulez l'algorithme d'Euclide généralisé pour calculer le PGCD g de $a = 185$ et $b = 76$. Outre le PGCD de 185 et 76, vous devez aussi calculer deux entiers relatifs u et v tels que $au + bv = g$. Utilisez une présentation sous forme de tableau, comme en TD.

2. Une autre méthode de calcul du PGCD de a et b utilise des matrices :

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ r \end{pmatrix}$$

où q est le quotient de a par b, et r est $a \mod b$. Le déterminant de cette matrice est -1. Par exemple, pour $a = 35$ et $b = 10$:

$$\begin{pmatrix} 35 \\ 10 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 10 \\ 5 \end{pmatrix}$$

Puis :

$$\begin{pmatrix} 10 \\ 5 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 5 \\ 0 \end{pmatrix}$$

L'algorithme termine quand le reste est nul ; alors le PGCD est en haut du vecteur. Donc :

$$\begin{pmatrix} 35 \\ 10 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 5 \\ 0 \end{pmatrix} = \begin{pmatrix} 7 & 3 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 5 \\ 0 \end{pmatrix}$$

La matrice carrée finale M contient, dans sa colonne gauche, $\frac{a}{g}$ et $\frac{b}{g}$, et dans sa colonne droite deux entiers u et v tels que $|M| = \frac{a}{g}u - \frac{b}{g}v = \pm 1$ (car le déterminant de chaque matrice vaut -1, et le déterminant d'un produit de matrices est le produit des déterminants). On en déduit les deux nombres de Bézout pour a et b : $au - bv = \pm g$.

Faites les calculs avec cette forme matricielle pour $a = 185$, $b = 76$.

3. Un ensemble d'entiers est dit non consécutif s'il ne contient pas deux entiers consécutifs (n et $n+1$ sont consécutifs, pour $n \in \mathbb{N}$). Par définition, F_k est l'ensemble des sous-ensembles non consécutifs d'entiers dans l'intervalle $[1 \ldots k]$ (zéro est inutilisé, pour simplifier). On note f_k le nombre d'éléments (de sous ensembles) de F_k. Par exemple :

$F_0 = \{\emptyset\}$, $f_0 = 1$,
$F_1 = \{\emptyset, \{1\}\}$, $f_1 = 2$,
$F_2 = \{\emptyset, \{1\}, \{2\}\}$, $f_2 = 3$,
$F_3 = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,3\}\}$, $f_3 = 5$,
$F_4 = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1,3\}, \{1,4\}, \{2,4\}\}$, $f_4 = 8$.

Dans ce problème, vous pourrez utiliser la notation :

$$F_k \oplus v = \bigcup_{E \in F_k} \{v\} \cup E$$

Par exemple,

$$F_2 \oplus 4 = \{\{4\}, \{1,4\}, \{2,4\}\}$$

3.a Quelle condition sur v assure que $F_k \oplus v$ est un ensemble non consécutif ?

Réponse. $v \geq k + 2$

3.b Trouvez une définition récursive pour F_k, en fonction de F_{k-1} et F_{k-2}.

Réponse. $F_0 = \{\emptyset\}$, $F_1 = \{\emptyset, \{1\}\}$ *et pour* $k > 1$: $F_k = F_{k-1} \cup (F_{k-2} \cup k)$;

3.c En déduire une formule récursive pour f_k.

Réponse. $f_0 = 1, f_1 = 2, f_k = f_{k-1} + f_{k-2}$.

3.d Reconnaissez vous f_k ?

Réponse. C'est la suite de Fibonacci, décalée.

4.a Que valent

$$(1, \quad 2) \begin{pmatrix} 3 \\ 4 \end{pmatrix} = ?$$

Réponse. C'est la matrice (11), ou le vecteur (11), ou bien le nombre 11. Cet abus de langage est consacré par l'usage.

$$\begin{pmatrix} 1 \\ 2 \end{pmatrix} (3, 4) = ?$$

C'est la matrice

$$\begin{pmatrix} 3 & 4 \\ 6 & 8 \end{pmatrix}$$

4.b Soient A et B deux matrices données. A a a lignes et a' colonnes. B a b lignes et b' colonnes. Soit $M = AB$. La matrice M a m lignes et m' colonnes. Définissez m et m' en fonction de a, a', b, b'. Quelles sont les contraintes sur a, a', b, b' pour que le produit AB soit possible ?

Réponse. M a a lignes et b' colonnes. M_{lc} est le produit scalaire de la ligne l de A par la colonne c de B ; Il faut donc que $a' = b$.

4.c Définissez $M_{l,c}$ par une formule avec un signe $\sum$ (les indices commencent à 0 ; l est le numéro de ligne et c le numéro de colonne). Combien de multiplications (entre nombres flottants) sont nécessaires pour calculer $M_{l,c}$?

Réponse.

$$M_{l,c} = \sum_{k=0}^{b-1} A_{l,k} B_{k,c}$$

Il y a $b = a'$ multiplications pour calculer $M_{l,c}$.

4. Deux vecteurs A, B donnés, à coordonnées entières dans $\mathbb{Z}$, génèrent un réseau de points $aA + bB$, avec $a \in \mathbb{Z}, b \in \mathbb{Z}$. Sur la figure, $A = (5, 3)^T$ et $B = (4, 1)^T$ et chaque disque noir représente un sommet (ou vecteur, ou point) du réseau. Le réseau est infini, et la figure n'en montre qu'une partie finie. Les vecteurs $I = (1, 2)^T$ et $J = (-3, 1)^T$ sont plus courts que A et B, et génèrent le même réseau. En fait les quatre paires $\pm I, \pm J$ sont les bases les plus courtes. On peut calculer les deux vecteurs les plus courts (au sens près et à l'ordre près) par une généralisation de la méthode d'Euclide.

4.a Proposez, **en français**, le principe d'une méthode pour calculer une paire de vecteurs les plus courts possibles, et qui génère le même réseau que deux vecteurs donnés A et B ; il existe plusieurs méthodes envisageables ; aucune formule n'est demandée à ce stade. Illustrez votre méthode avec l'exemple de la figure.

Réponse. Algorithme 1 : on suppose que A est plus long que B ; soit R le vecteur le plus court de $A \pm B$. Si R n'est pas plus court que A, alors (A, B)

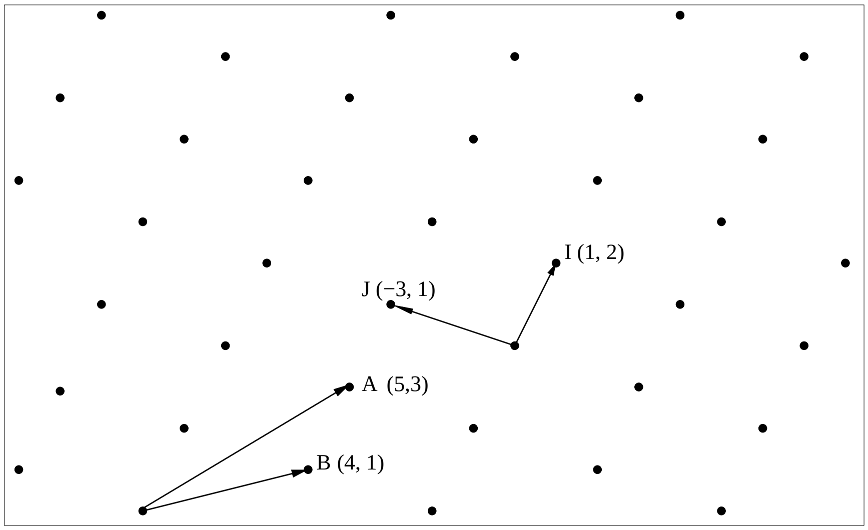

FIGURE 1 – Un exemple de réseau généré par deux vecteurs A et B. Le même réseau est généré par I, J, plus courts que A et B.

est une paire la plus courte ; sinon on recommence sur la paire (B, R) (ou bien (R, B)). Cette méthode est similaire à la méthode d'Euclide qui utilise la différence. Voici les étapes :

Etape 1 : Les deux vecteurs de base sont $A = (5, 3), B = (4, 1)$. Le vecteur $A - B = (1, 2)$ est plus court que A et le remplace.

Etape 2 : On échange les deux vecteurs de base, qui sont $A = (4, 1), B = (1, 2)$. Le vecteur $A - B = (3, -1)$ est plus court que $A + B = (5, 3)$, et plus court que A et le remplace.

Etape 3 : Les deux vecteurs de base sont $A = (3, -1)$ et $B = (1, 2)$. Ni $A + B = (4, 1)$, ni $A - B = (2, -3)$ ne sont plus courts que A. Donc la base la plus courte est $(3, -1)$ et $(1, 2)$.

Algorithme 2 : on calcule $q \in \mathbb{Z}$ tel que $A + qB$ est le plus court possible. Soit K la projection orthogonale de A sur B ; alors $K = \lambda B$, et q est l'entier le plus proche de λ. Si $q = 0$, alors A, B est la paire la plus courte, sinon on recommence sur $B, R = A + qB$. Détaillons le calcul de λ. $(A - \lambda B) \bullet B = 0 \Rightarrow \lambda = \frac{A \bullet B}{B \bullet B} = \frac{A_x B_x + A_y B_y}{B_x^2 + B_y^2}$, et $q = \lfloor \lambda \rceil$.

Soit A le vecteur

$$A = \begin{pmatrix} A_x \\ A_y \end{pmatrix}$$

qui est noté $A = (A_x, A_y)^T$ par commodité (T pour transposé). De même soit $B = (B_x, B_y)^T$. Notons $||A|| = \sqrt{A_x^2 + A_y^2}$ la norme, ou longueur, de A. On suppose que A est plus long que B : $||A|| \geq ||B||$ (sinon, il suffit d'échanger A et B).

4.b Proposez deux vecteurs, que vous définirez en fonction de A et B, susceptibles d'être plus courts que A. Il faut aussi que si aucun de ces vecteurs n'est plus court que A, alors il n'existe aucun vecteur du réseau strictement plus court que A.

Il suffit de considérer $A + B$ et $A - B$.

4.c On suppose que $||A|| \geq ||B||$ et qu'il existe un entier relatif q non nul et un vecteur R de norme strictement inférieure à celles de A, et tels que $A = qB + R$. En supposant $R = (R_x, R_y)^T$, écrivez cette dernière équation sous forme matricielle, avec des matrices de taille 2 par 2.

Réponse.

$$\begin{pmatrix} A_x & A_y \\ B_x & B_y \end{pmatrix} = \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} B_x & B_y \\ R_x & R_y \end{pmatrix}$$

On reconnaît la matrice de l'algorithme d'Euclide, celle qui contient q et qui est de déterminant -1.

Voici les étapes pour l'algorithme 2.

$$\begin{pmatrix} 5 & 3 \\ 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 1 & 2 \end{pmatrix} \text{ } car\ \lambda = \frac{23}{17}, q = 1$$

$$\begin{pmatrix} 4 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix} \text{ } car\ \lambda = \frac{6}{5}, q = 1$$

$$\begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 & -1 \\ 1 & 2 \end{pmatrix} \text{ } car\ \lambda = \frac{1}{10}, q = 0$$

Mais ce n'est pas fini bien que $q = 0$, car A est plus court que B. Cette étape permet donc d'échanger A et B.

$$\begin{pmatrix} 3 & -1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix} \text{ } car\ \lambda = \frac{1}{5}, q = 0$$

Ce coup ci, c'est terminé. A est plus long que B, et $q = 0$. Donc il est impossible de remplacer le plus long vecteur, A, par un plus court.

Donc :

$$\begin{pmatrix} 5 & 3 \\ 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix}$$

Après quelques calculs :

$$\begin{pmatrix} 5 & 3 \\ 4 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix}$$

Les deux vecteurs les plus courts sont donc $I = (1, 2)$ *et* $J = (3, -1)$. *De plus les deux vecteurs initiaux de base sont* $A = (5, 3) = 2I + J$ *et* $B = (4, 1) = I + J$.

4.d Pour $A = (1, 4)^T$, et $B = (2, 1)^T$, donnez q et les coordonnées de R. Le q correct est tel que R est plus court que A, et plus court (ou du moins pas plus long) que pour $q+1$ ou $q-1$. Donnez les coordonnées de R. Ecrivez ceci sous forme matricielle (comme dans la question précédente).

4.e Comment calculez vous la valeur de q et R, pour A, B donnés ? Indication : vous pouvez utiliser le produit scalaire, noté $A \bullet B = A_x B_x + A_y By$. Comment détectez vous que A ne peut pas être remplacé par un vecteur plus court (et donc que l'algorithme est terminé) ?

Réponse. q *a déjà été donné. L'algorithme a terminé quand* $q = 0$ *— et quand* $||A|| \geq ||B||$.