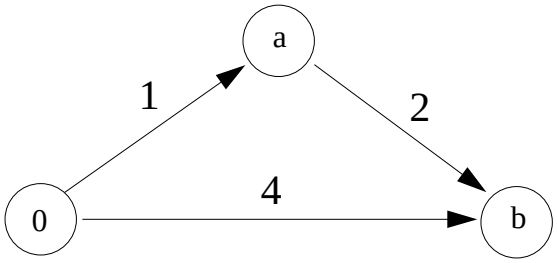
ALGORITHMIQUE ET COMPLEXITE

Master Informatique, première année, janvier 2015

TOUS VOS DOCUMENTS SUR PAPIER SONT AUTORISES.
COURRIEL ET TELEPHONE SONT INTERDITS.
REPONDEZ AUX QUESTIONS DANS L'ORDRE.
NUMEROTEZ VOS REPONSES.

1 Plus court chemin et programmation linéaire

Considérez le graphe ci-dessous :



Le coût (ou longueur) de l'arc $0a$ est 1, celui de l'arc ab est 2, celui de $0b$ est 4.

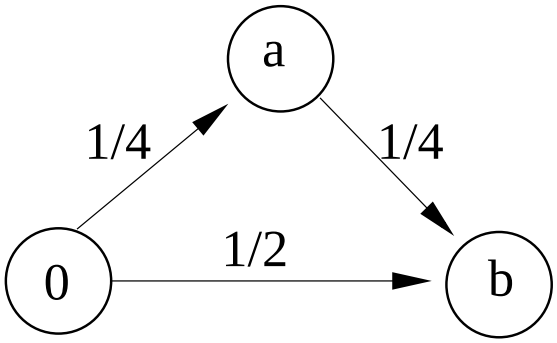
Exprimez le calcul des distances (longueurs des plus courts chemins) des sommets a et b au sommet source 0 comme un problème de programmation linéaire. Appelez a la distance du sommet a à la source. Appelez b la distance du sommet b à la source. Nommez a', b', b'' les variables d'écart. Résolvez par la méthode du simplexe ce problème de programmation linéaire.

2 Flot optimal et programmation linéaire

Pour le même graphe que précédemment, considérez le calcul de la distance de b au sommet source 0 comme un problème de flot de valeur 1 et de coût minimal. Posez le problème de programmation linéaire : appelez a le flot dans les arcs $0a$ et ab. Appelez b le flot dans l'arc $0b$. Donnez des noms logiques aux variables d'écart. Résolvez par la méthode du simplexe ce problème de programmation linéaire : seuls les tableaux initial et final sont demandés.

3 Graphes et probabilités

Par définition, la somme de la probabilité de mort et de la probabilité de survie pour un arc ou un chemin vaut 1. Dans le graphe suivant, chaque arc est étiqueté avec la probabilité de mourir quand l'arc est emprunté. Quelles sont les probabilités de survie des deux chemins $0, a, b$ et $0, b$? Quel est le chemin le plus sûr ? Aucune justification n'est demandée, et le recours à la programmation linéaire n'est pas requis.



4 Problème de la somme

n entiers naturels (donc non négatifs) e_i, avec $i \in 1..n$, sont donnés, ainsi qu'un entier naturel S.

a. Comment décider si S est la somme d'un des sous-ensembles des e_i ? Chaque entier e_i ne peut être utilisé qu'une seule fois. Réduisez ce problème au problème du sac à dos, que nous avons résolu par programmation dynamique.

b. La méthode fonctionne-t-elle pour des entiers relatifs (dans $\mathbb{Z}$) ? On suppose que S reste un entier positif.

5 Variante de la transformée de Fourier rapide

Arthur propose une variante de la transformée de Fourier rapide. Il considère les racines 3^k ièmes de l'unité (racines cubiques, 9 ième, 27 ième, etc) alors que l'algorithme classique considère les racines 2^k de l'unité. En conséquence, le temps d'exécution de son algorithme vérifie les relations de récurrence : $T(1) = 1, T(n = 3^k) = n + 3T(n/3)$.

a. Quelle est la complexité de la méthode d'Arthur ? La preuve par récurrence n'est pas demandée.

b. Est-elle meilleure que celle de la méthode classique ? Donnez la complexité de la méthode classique.

6 Un graphe non orienté est-il un arbre ?

Rappel : En théorie des graphes, un arbre est un graphe non orienté, acyclique et connexe.

Soit A le nombre d'arêtes de G et S le nombre de sommets de G.

a. Quelle relation lie A et S quand G est un arbre ?

b. Quelle relation lie A, S, T quand G est une forêt avec T arbres ?

c. Citez un des (au moins trois) algorithmes vus en cours permettant de décider que G est connexe. Vous pouvez supposer que la relation de (a) est vérifiée.

d. On suppose que G est non orienté, acyclique et connexe (c'est un arbre). Proposez en 5 lignes au plus un algorithme calculant tous les plus courts chemins (et leurs longueurs) depuis un sommet donné. Votre algorithme doit être plus efficace que celui de Dijkstra.

7 Cryptographie asymétrique et bon sens

Rappel. Avec la cryptographie asymétrique, tout le monde peut crypter un message (un grand entier) m : cela revient à calculer $m' = C(m)$, ce qui se fait en temps polynomial avec $\log m$. Par contre, seul le destinataire peut décrypter m', autrement dit calculer $C^{-1}(m')$.

Un étudiant programme une de ces méthodes (par exemple RSA). Il crypte chaque bit du message, et concatène les résultats, pour obtenir le message crypté.

a. Où est l'erreur ?

b. Si l'étudiant encrypte chaque octet, est-ce mieux ?

8 Réseau

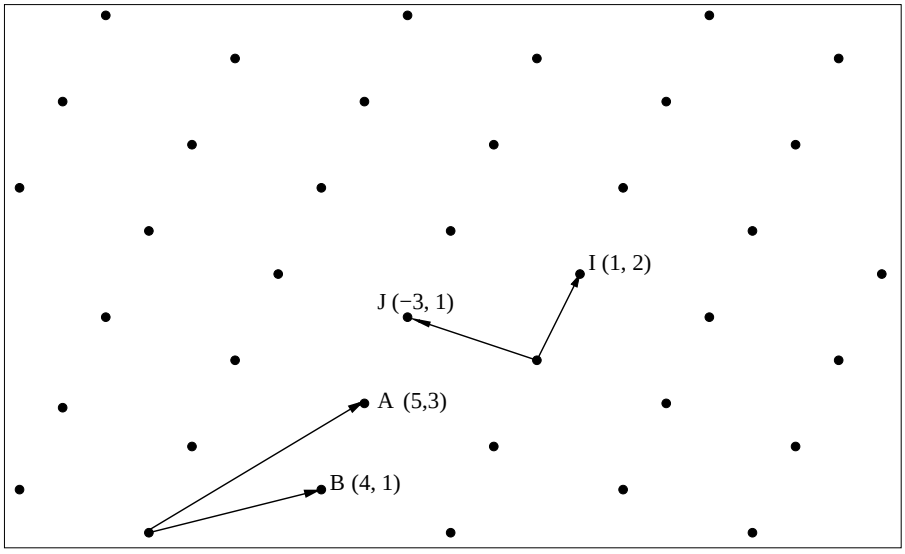
Rappels. On note $\mathbb{N}$ l'ensemble des entiers naturels : $0, 1, 2, 3 \ldots$. On note $\mathbb{Z}$ l'ensemble des entiers relatifs : $\ldots, -3, -2, -1, 0, 1, 2, 3 \ldots$.

Le dessin suivant montre une partie d'un réseau R généré par deux vecteurs $A = (5, 3)$ et $B = (4, 1)$. R est l'ensemble des points (les disques noirs sur le dessin) $aA + bB$ avec $a \in \mathbb{Z}$, et $b \in \mathbb{Z}$. R est aussi généré par $I = (1, 2)$ et $J = (-3, 1)$, qui sont plus courts que A et B. Il n'existe pas de base strictement plus courte que $\pm I, \pm J$.

Rappels. La longueur, ou norme euclidienne, de $A = (A_x, A_y)$ est $||A|| = \sqrt{A_x^2 + A_y^2}$. L'aire du parallélogramme généré par A, B est la valeur abosolue du déterminant

$$\begin{vmatrix} A_x & A_y \\ B_x & B_y \end{vmatrix} = A_x B_y - A_y B_x$$

Propriété : toutes les bases d'un même réseau génèrent des parallélogrammes de même aire (au signe près).



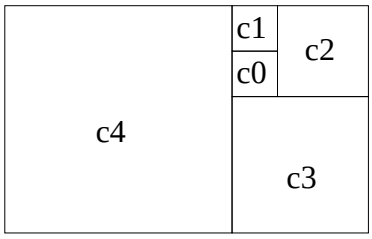
a. Deux vecteurs 2d indépendants à coordonnées dans $\mathbb{Z}$: $A = (A_x, A_y)$ et $B = (B_x, B_y)$, sont donnés. Proposez un test (utilisant un nombre constant d'opérations dans $\mathbb{Z}$) pour décider qu'il n'existe pas de vecteurs strictement plus courts que $\pm A, \pm B$ engendrant le même réseau. Vous pouvez supposer $||A|| \geq ||B||$. Répondre en une ligne au plus.

b. Déduisez-en un algorithme de calcul de la base la plus courte. Quel est son coût ? Répondre en 3 lignes au plus.

c. Le caractère entier des coordonnées de A et B est-il indispensable ? Argumentez en 2 lignes au plus.

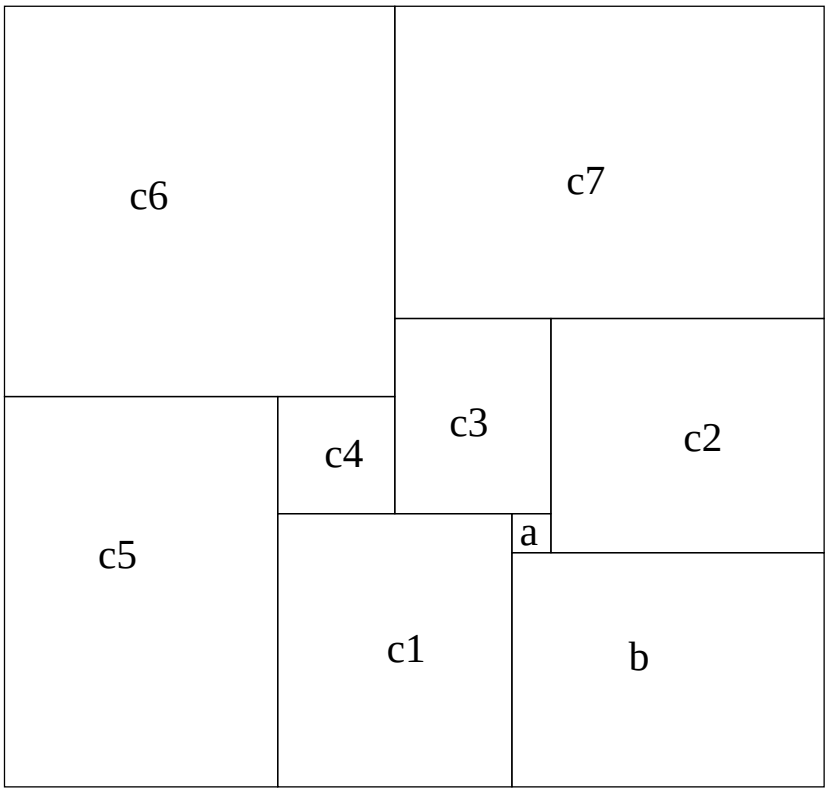
9 Rectangle pavé par des carrés

Ce rectangle est pavé par des carrés. Exprimez c_1, c_2, c_3, c_4 en fonction de c_0. Que constatez vous ? Vous pouvez poser $c_0 = 1$.



10 Rectangle pavé par des carrés tous différents

Le dessin suivant montre un rectangle pavé par des carrés ; il est faux, mais la topologie est correcte.



a. Exprimez les longueurs des côtés en fonction de a et b. Pour commencer : $c_1 = a+b$ et $a+b = c_2 \Rightarrow c_2 = b-a$. Pour vous aider, les carrés sont numérotés dans le "bon" ordre. Déduisez-en une relation entre a et b. Déduisez-en les longueurs entières les plus petites (non nulles) de tous les carrés.

Remarquez que, de façon plus générale, chaque trait intérieur maximal donne une équation linéaire, par exemple $c_4 + c_6 = c_3 + c_7$ pour le trait vertical en haut presque au milieu. On admettra qu'il y a toujours une équation de plus que d'inconnues.

b. Le dessin d'un pavage d'un rectangle en carrés est donné ; il faut calculer les longueurs entières minimales (non nulles) des carrés. Proposez en trois lignes au plus le principe d'une méthode, ou bien identifiez le problème mathématique sous-jacent.