

## Exercices préparatoires à l'examen du mois de mai Semestre du printemps 2015

### 1 Programmation linéaire

Dans tous les systèmes qui suivent, on suppose  $x_1 \geq 0$ ,  $x_2 \geq 0$ ,  $x_3 \geq 0$ .

**Exercice 1.1** Soit le système suivant :

$$\begin{aligned} -x_1 + x_2 &\leq 2 \\ x_2 &\leq 4 \\ 2x_1 + x_2 &\leq 10 \\ x_1 + 3x_2 &= z \rightarrow \max \end{aligned}$$

1. Résoudre le système graphiquement.
2. Résoudre le système par la méthode du simplexe, en suivant l'évolution des variables sur le graphe.
3. Écrire le système dual et donner sa solution.

**Exercice 1.2** Résoudre le système suivant, d'abord graphiquement, puis par la méthode du simplexe.

$$\begin{aligned} x_1 + x_2 &\leq 5 \\ x_1 - x_2 &\leq 2 \\ 2x_1 + x_2 &\leq 7 \\ x_1 + 3x_2 &= z \rightarrow \max \end{aligned}$$

En se basant sur la solution du système primal, écrire le système dual et donner sa solution.

**Exercice 1.3** Résoudre le système suivant, d'abord graphiquement, puis par la méthode du simplexe. Écrire le système dual et trouver sa solution.

$$\begin{aligned} 2x_1 + x_2 &\leq 14 \\ 2x_1 - x_2 &\leq 5 \\ x_1 + 2x_2 &\leq 16 \\ 3x_1 + 4x_2 &= z \rightarrow \max \end{aligned}$$

**Exercice 1.4** Résoudre le système suivant, d'abord graphiquement, puis par la méthode du simplexe. Écrire le système dual et trouver sa solution.

$$\begin{aligned} 2x_1 + x_2 &\leq 10 \\ -x_1 + x_2 &\leq 1 \\ x_1 + 2x_2 &\leq 8 \\ x_1 + 3x_2 &= z \rightarrow \max \end{aligned}$$

**Exercice 1.5** Soit le programme linéaire

$$\begin{aligned} x_1 - x_2 &\leq 3 \\ x_1 + 2x_2 &\leq 6 \\ -x_1 + 2x_2 &\leq 2 \\ 2x_1 + x_2 &= z \rightarrow \max. \end{aligned}$$

Résoudre le programme, d'abord graphiquement, puis par la méthode du simplexe, en suivant toutes les étapes du calcul sur le dessin. Écrire le système dual et trouver sa solution.

## 2 Flots

**Exercice 2.1** Trouver un flot maximum et une coupe minimum entre les sommets  $s$  et  $t$  dans le réseau de la figure 1. Pour la coupe minimum  $(S, T)$  indiquer tous les arcs allant de  $S$  vers  $T$  et tous les arcs allant de  $T$  vers  $S$  ainsi que les flux passant par ces arcs.

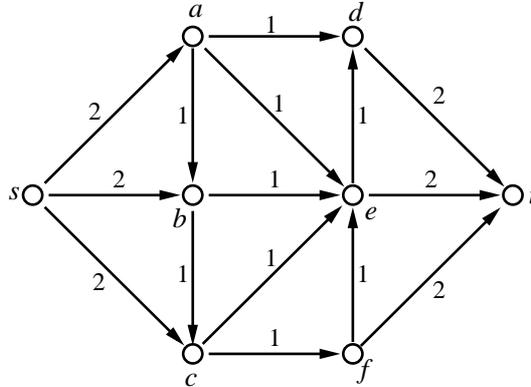


FIG. 1 – Trouver un flot maximum et une coupe minimum.

**Exercice 2.2** Trouver un flot maximum et une coupe minimum entre les sommets  $s$  et  $t$  dans le réseau de la figure 2. Pour la coupe minimum  $(S, T)$  indiquer tous les arcs allant de  $S$  vers  $T$  et tous les arcs allant de  $T$  vers  $S$  ainsi que les flux passant par ces arcs.

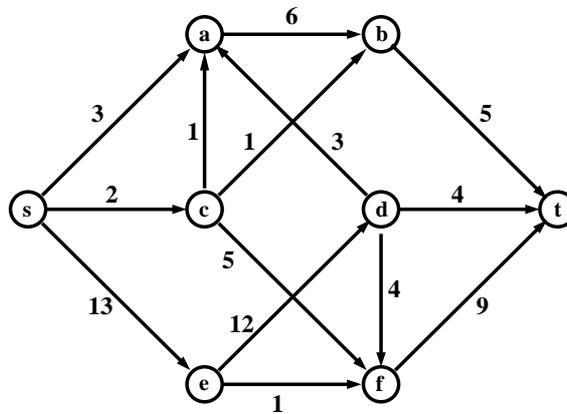


FIG. 2 – Trouver un flot maximum et une coupe minimum.

**Exercice 2.3** Trouver un couplage maximum dans le graphe biparti de la figure 3.

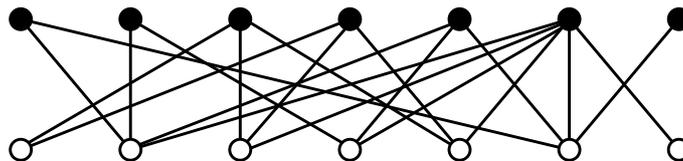


FIG. 3 – Trouver un couplage maximum.

### 3 Graphes

**Exercice 3.1** Soit un graphe  $G = (V, E)$ . On dit qu'un ensemble de sommets  $S \subseteq V$  est un *ensemble indépendant* si pour tous  $i, j \in S$  le graphe ne contient pas d'arête  $(i, j)$ .

Soit le système

$$\begin{array}{rcccccc} x_1 & + & x_2 & & & & \leq & 1 \\ x_1 & + & & x_3 & + & x_4 & \leq & 1 \\ & & & & & x_4 & + & x_5 \leq & 1 \\ x_1 & + & x_2 & + & x_3 & + & x_4 & + & x_5 = & z \rightarrow \max \end{array}$$

où les variables  $x_i$  ne prennent que des valeurs 0 ou 1. Représenter ce problème comme un problème de recherche d'un plus grand ensemble indépendant dans un graphe. Dessiner le graphe en question. Trouver l'ensemble indépendant maximum et résoudre le système.

**Exercice 3.2** Est-il possible de tracer, sans relever le crayon, une ligne coupant, une fois et une seule, chaque segment de la figure 4? (Les segments sont les portions de droites limitées par deux points.) Justifier la réponse.

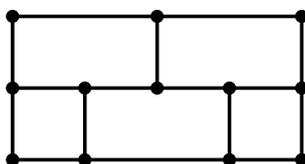


FIG. 4 – Peut-on tracer une ligne coupant toutes les arêtes?

**Exercice 3.3** Colorier les sommets du graphe de la figure 5 en trois couleurs.

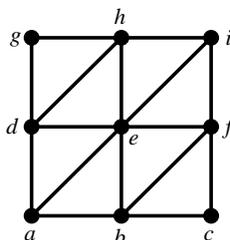


FIG. 5 – Colorier les sommets en trois couleurs

**Exercice 3.4** Soit le graphe complet  $K_5$ . Enlever une arête (n'importe laquelle) et montrer que le graphe ainsi obtenu soit planaire. Appliquer le même procédé au graphe complet biparti  $K_{3,3}$ .

**Exercice 3.5** Montrer que les graphes de la figure 6 ne son pas isomorphes.

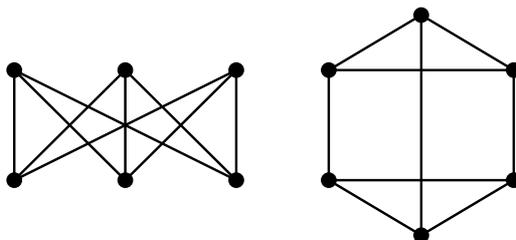


FIG. 6 – Graphes non isomorphes

## 4 Algorithmes randomisés

**Exercice 4.1** On veut vérifier, pour trois matrices  $A, B, C$  de taille  $n \times n$ , si  $AB = C$  ou non. On applique l'algorithme randomisé vu en cours, et on veut limiter la probabilité d'erreur par  $2^{-100}$ . À partir de quelle taille  $n$  des matrices cette méthode devient plus performant que la méthode direct consistant en multiplication de  $A$  par  $B$  et vérification si le résultat est égal à  $C$  ?

**Exercice 4.2** Une clé publique RSA a la valeur  $(493, 33)$ .

1. Quel est le résultat du codage de l'entier 2 ?
2. Déterminer la clé privée correspondant à la clé publique.
3. Montrer que le décodage par la clé privée trouvée ci-haut donne effectivement l'entier de départ 2.

**Exercice 4.3** La méthode  $\rho$  de Pollard pour déterminer un facteur non-trivial d'un entier  $n$  consiste en les opérations suivantes. Soit la fonction  $f(x) = x^2 + 1 \pmod n$  :

- on tire un entier  $x_0$  dans  $[0, n - 1]$  et on pose  $y_0 = x_0$  ;
- on calcule les termes successifs des suites  $x_i$  et  $y_i$  définies, pour  $i \geq 1$ , par les relations de récurrence  $x_i = f(x_{i-1})$ ,  $y_i = f(f(y_{i-1}))$  ;
- à chaque étape on calcule  $d_i = \text{pgcd}(|x_i - y_i|, n) \pmod n$ , et on s'arrête quand on obtient  $d_i \neq 1$  ;
- si  $d_i = 0$  l'algorithme échoue ; sinon,  $d_i$  est le facteur cherché.

Justifier l'algorithme. Appliquer cet algorithme au cas  $n = 77$  en choisissant pour  $x_0$  la valeur 0. Appliquer l'algorithme au cas  $n = 1001$  en prenant la valeur de  $x_0$  à votre choix. On précisera à chaque fois le facteur retourné et le nombre d'itérations.

**Exercice 4.4** Soit  $\pi(N)$  dénote la quantité des nombres premiers  $p \leq N$ . Le *théorème des nombres premiers* affirme qu'une bonne approximation à cette fonction est donnée par la formule  $N / \ln(N)$  où la notation "ln" signifie le logarithme sur la base  $e$ .

1. On choisit un entier entre 1 et  $10^{100}$  au hasard. Quelle est la probabilité de tomber sur un nombre premier ?
2. On choisit des entiers uniquement parmi ceux qui sont égaux à 1 ou à 5 modulo 6 (expliquer pourquoi). Quelle est alors la probabilité de tomber sur un nombre premier ?

**Exercice 4.5** Soient trois ensembles disjoints  $X, Y, Z$  de tailles  $|X| = m$ ,  $|Y| = n$ ,  $|Z| = k$ . On considère l'union  $V = X \cup Y \cup Z$  comme l'ensemble de sommets de graphes *tripartis* pour lesquels il est interdit de tracer des arêtes entre deux points d'un même ensemble. (Seules donc les arêtes entre  $X$  et  $Y$ , entre  $X$  et  $Z$ , et entre  $Y$  et  $Z$ , sont autorisées.) Quel est le nombre des graphes vérifiant cette propriété pour des valeurs données de paramètres  $m, n, k$  ? Calculer ce nombre pour  $m = n = k = 10$ .

Justifier la proposition suivante : un graphe est coloriable en trois couleurs si et seulement si il est triparti.

Quelle est la probabilité qu'un graphe choisi au hasard ne contient pas d'arêtes entre deux sommets  $i, j \in X$ , ni entre  $i, j \in Y$ , ni entre  $i, j \in Z$  ? Calculer cette probabilité pour  $m = n = k = 10$ .