

# Recherche Opérationnelle 2

Exercices préparatoires à l'examen de 31 mai 2016

## 1 Plus courts chemins

**Exercice 1.1** Trouver les plus courts chemins du sommet  $s$  à tous les autres sommets du graphe de la figure 1. Dessiner l'arbre des plus courts chemins. Quel algorithme faut-il utiliser, et pourquoi ?

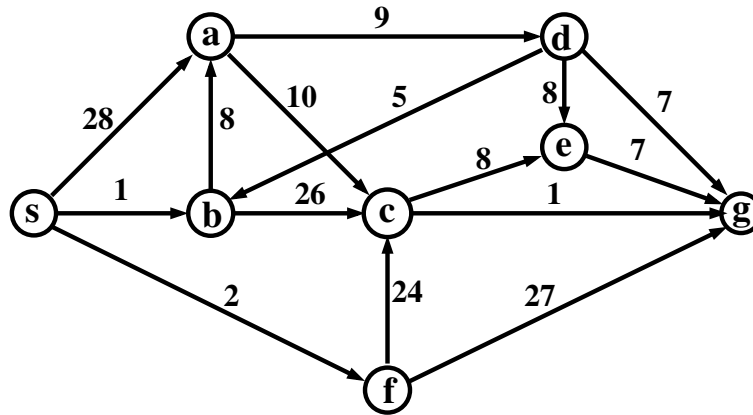


FIGURE 1 – Trouver les plus courts chemins ; dessiner l'arbre des plus courts chemins.

**Exercice 1.2** Trouver les plus courts chemins du sommet  $a$  à tous les autres sommets du graphe de la figure 2. Dessiner l'arbre des plus courts chemins. Quel algorithme faut-il utiliser, et pourquoi ?

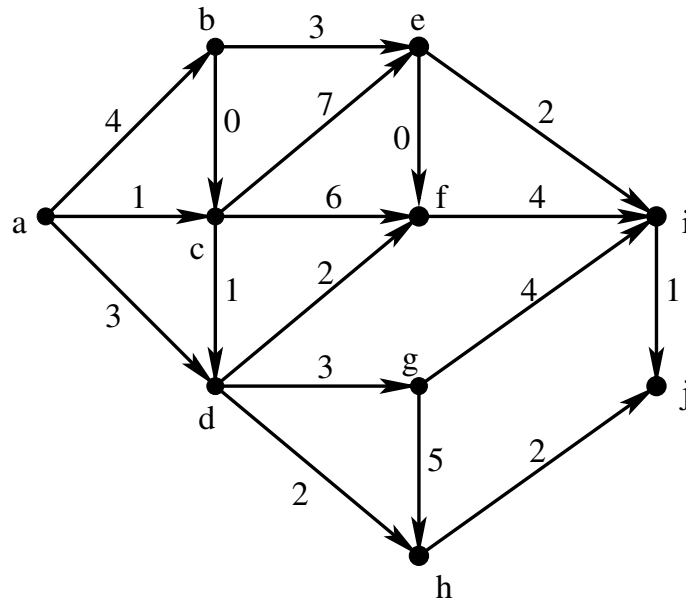


FIGURE 2 – Trouver les plus courts chemins ; dessiner l'arborescence des plus courts chemins.

**Exercice 1.3** Déterminer les plus courts chemins de  $s$  à tous les sommets du graphe de la figure 3. Tracer l'arborescence de plus courts chemins.

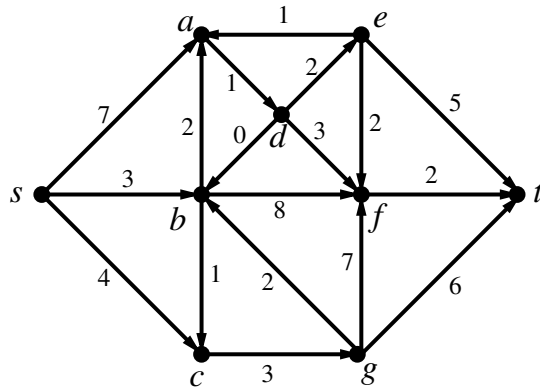


FIGURE 3 – Plus courts chemins de  $s$  aux autres sommets.

**Exercice 1.4** Trouver les plus courts chemins de tout sommet à tout autre sommet du graphe de la figure 4. Donner la matrice des distances entre les sommets. (Attention, certaines distances peuvent être infinies.)

Vous pouvez faire cet exercice “à la main”, sans utiliser un quelconque algorithme spécifique.

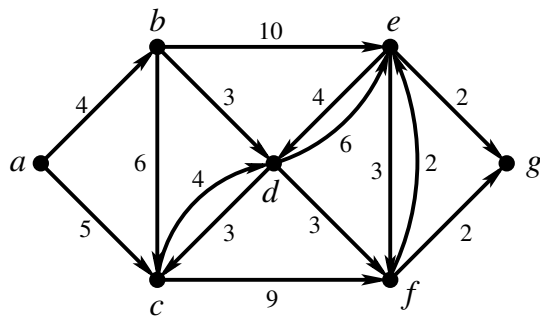


FIGURE 4 – Trouver les plus courts chemins de tout sommet à tout autre.

**Exercice 1.5** Trouver les plus courts chemins du sommet  $s$  à tous les autres sommets du graphe de la figure 5. Dessiner l’arbre des plus courts chemins. Quel algorithme faut-il utiliser, et pourquoi ?

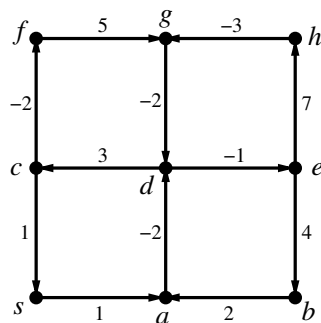


FIGURE 5 – Trouver les plus courts chemins ; dessiner l’arbre des plus courts chemins.

## 2 Flots

**Exercice 2.1** Trouver le flot maximum et une coupe  $(S, T)$  minimum entre les sommets  $s$  et  $t$  dans le réseau de la figure 6. Indiquer tous les arcs de  $S$  à  $T$  et de  $T$  à  $S$  ainsi que les flux correspondants.

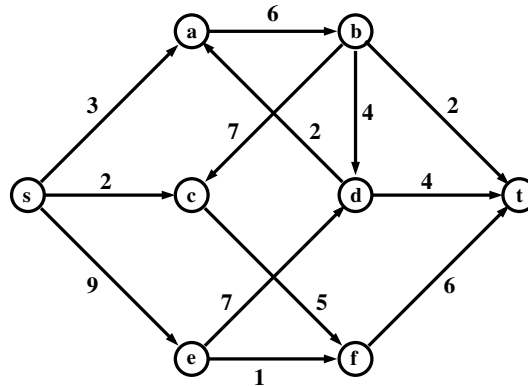


FIGURE 6 – Trouver un flot maximum et une coupe minimum.

**Exercice 2.2** La figure 7 représente un réseau avec trois sommets sources  $a, b, c$  et trois sommets destinations  $l, m, n$ . Trouver le flot maximum entre les sources et les destinations. Exhiber une coupe minimum.

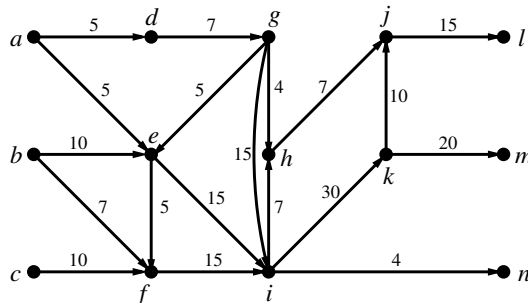


FIGURE 7 – Trois sources et trois destinations.

**Exercice 2.3** Soit le graphe donné sur la figure 8. On cherche, dans ce graphe, le nombre maximum de chemins de  $s$  à  $t$  que l'on peut trouver, disjoints au sens des arcs (c'est-à-dire, tels qu'un arc appartient au plus à un chemin retenu). Réduire ce problème à un problème de flot maximum. Trouver les chemins en question et montrer qu'il n'y en a pas plus que cela.

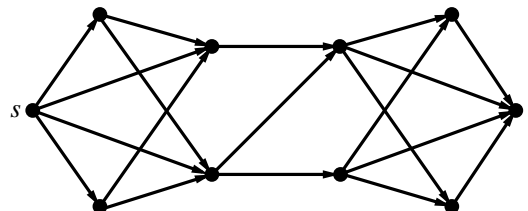


FIGURE 8 – Chemins arc-disjoints.

### 3 Graphes et planarité

**Exercice 3.1** Appliquer la procédure de tri topologique au graphe de la figure 9. À savoir, numéroter ses sommets de telle sorte que s'il existe un chemin orienté d'un sommet  $x$  à un sommet  $y$ , alors le numéro de  $x$  doit être inférieur à celui de  $y$ .

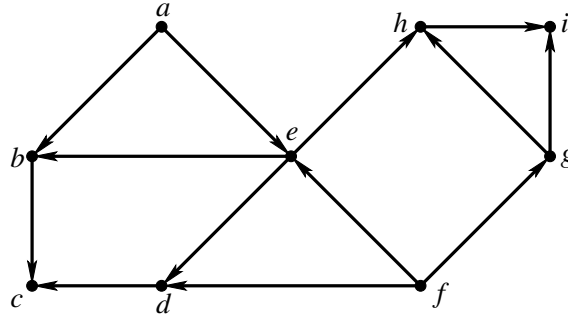


FIGURE 9 – Appliquer la procédure de tri topologique.

**Exercice 3.2** Montrer que le graphe de la figure 10 est planaire. Cela veut dire qu'*il est possible* de dessiner ce graphe sur le plan de telle manière que ses arêtes ne se coupent pas.

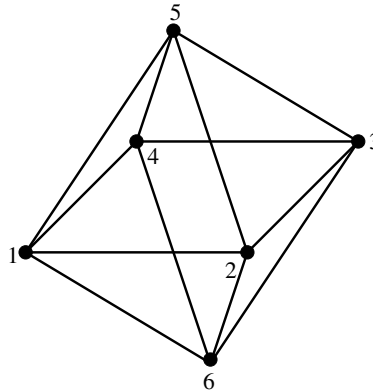


FIGURE 10 – Montrer que ce graphe est planaire.

**Exercice 3.3** Montrer que le graphe de la figure 11 est planaire. Cela veut dire qu'*il est possible* de dessiner ce graphe sur le plan de telle manière que ses arêtes ne se coupent pas.

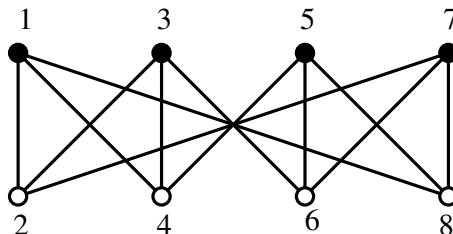


FIGURE 11 – Montrer que ce graphe est planaire.

## 4 Algorithmes randomisés

**Exercice 4.1** Il y a trois polynômes  $P(x)$ ,  $Q(x)$ ,  $R(x)$ ,  $\deg P = 80$ ,  $\deg Q = 120$ ,  $\deg R = 200$ . On cherche à tester si  $P \cdot Q = R$ . Pour cela, on calcule les valeurs de  $P \cdot Q$  et de  $R$  pour des valeurs de  $x$  tirées au hasard dans l'ensemble des entiers de 0 à 1000. On répète l'opération 10 fois, et chaque fois les valeurs sont égales. Quelle est la probabilité que les polynômes ne soient *pas* égaux ? Combien de fois faut-il répéter l'opération pour garantir que la probabilité d'une réponse erronée soit inférieure à  $2^{-100}$  ?

**Exercice 4.2** On dispose d'une fonction  $\text{rand}(i, j)$  qui, pour deux entiers  $i, j$  donnés,  $i \leq j$ , retourne un entier aléatoire  $k$ ,  $i \leq k \leq j$ . Proposer un algorithme de génération d'un sous-ensemble aléatoire de taille  $m$  sur un ensemble donné de taille  $n$ .

**Exercice 4.3** Calculer la fonction  $\varphi(n)$  d'Euler pour  $n = 60$ .

**Exercice 4.4** Soit  $n = 66$ . Appliquer le test de Fermat à  $x = 7$  et à  $x = 25$ . Que peut-on conclure ?

**Exercice 4.5** Déterminer l'inverse de 29 modulo 64. On détaillera les étapes du calcul.

**Exercice 4.6** Une clé publique RSA a la valeur  $(n, e) = (391, 15)$ .

1. Quel est le résultat du codage de l'entier 2 ?
2. Déterminer la clé privée  $d$  correspondant à la clé publique.

On détaillera les étapes de calcul.

**Exercice 4.7** On rappelle la méthode  $\rho$  de Pollard pour déterminer un facteur d'un entier  $n$  : la fonction  $f : [0, n - 1] \rightarrow [0, n - 1]$  étant définie par  $f(x) = x^2 + 1 \pmod n$ ,

- 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  $x_i = f(x_{i-1})$ ,  $y_i = f(f(y_{i-1}))$  ;
- on s'arrête quand le PGCD  $d_i$  de  $|x_i - y_i|$  et  $n$  est différent de 1 : si  $d_i = 0$  l'algorithme échoue ; sinon,  $d_i$  est le facteur cherché.

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 4.8** On fabrique un graphe aléatoire à  $n$  sommets de la manière suivante : pour toute paire de sommets  $(i, j)$ , on connecte  $i$  et  $j$  par une arête avec la probabilité  $1/2$ , et avec la même probabilité on laisse ces deux sommets non connectés. Soit  $X$  le nombre de triangles dans ce graphe. Déterminer l'espérance  $E(X)$ .