Bac Systèmes Numériques, diffusion des savoirs

18 mai 2022

Déroulé de l'événement

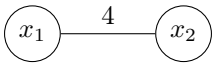
1. définition des groupes (3 ou 4 élèves par groupe)
2. choix du sujet
3. étude des problèmes du sujet
4. (*optionnel*) présentation des résultats au reste de la classe

Théorie des graphes

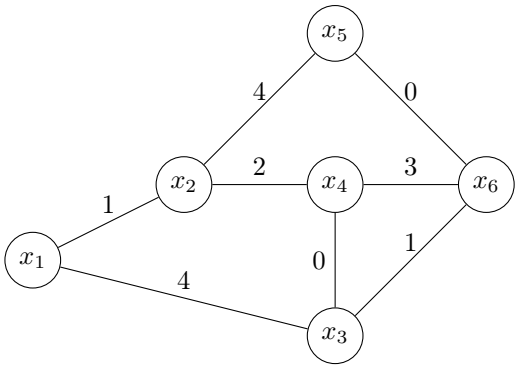
Graphe Un graphe est composé de sommets $x_1, x_2, \cdots, x_n$ et d'un ensemble d'arêtes qui relient les sommets $e_1, e_2, \cdots, e_m$. On peut associer des valeurs aux arêtes.

Un sommet est représenté par un cercle et son nom à l'intérieur,

et une arête par un segment qui relie deux sommets, avec sa valeur affichée à proximité,

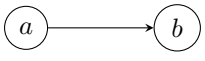


Voici un exemple de graphe :



Chemin Un chemin d'un sommet a à un sommet b est une succession d'arêtes connectées dont la première commence par a et la dernière se termine par b. Voici l'exemple d'un chemin entre x_1 et x_6 : $(x_1, x_3), (x_3, x_4), (x_4, x_6)$.

Arête orientée Lorsque l'on peut passer du sommet a au sommet b mais que l'inverse n'est pas possible, on dit que l'arête est orientée et est donc représentée avec un arc :



Algorithme de Dijkstra Cet algorithme permet de déterminer les plus courts chemins pour un sommet de départ.

Algorithme 1 Dijkstra

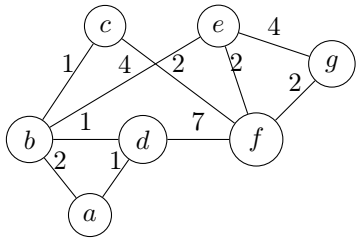
1: Définir des marques égales à l'infini pour tous les sommets
2: On choisit le sommet de départ que l'on nomme x. Changer la marque de x par zéro et fixer x (c'est à dire que sa marque ne peut plus changer).
3: Pour tous les sommets y qui sont non fixés et voisins à x, changer la marque de y par "min(marque de y, marque de x + valeur de l'arête(x, y))".
4: Choisir le sommet à marque minimale, le fixer. On remplace x par le nouveau sommet choisi. S'il reste des sommets non fixés, on applique la méthode précédente à x.

Problème 1 On considère les villes a, b, c, d, e, f, g qui ne sont pas connectées. On souhaite pouvoir communiquer entre a et g sachant que :

— connecter (a, b) prend 2 jours ;
— connecter (a, d) prend 1 jour ;
— connecter (b, c) prend 1 jour ;
— connecter (b, d) prend 1 jour ;
— connecter (b, e) prend 4 jours ;
— connecter (c, f) prend 2 jours ;
— connecter (d, f) prend 7 jours ;
— connecter (e, f) prend 2 jours ;
— connecter (e, g) prend 4 jours ;
— connecter (f, g) prend 2 jours.

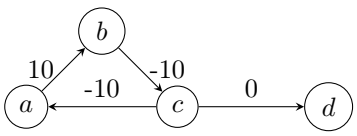
Comme on ne dispose que d'une équipe pour faire les installations, on ne peut faire qu'une seule connexion à la fois. Quelles villes faut-il connecter pour que ce soit le plus rapide possible ?

Réponse au problème 1 Ici en appliquant l'algorithme de Dijkstra, on trouve que le chemin le plus court est $(a, b), (b, c), (c, f), (f, g)$ avec un coût de 7 jours.



Problème 2 La machine a dispose d'un signal à envoyer à la machine d. Lorsque le signal est communiqué de a à b, sa taille augmente de 10 octets, de b à c sa taille diminue de 10 octets, de c à a sa taille diminue de 10 octets et de c à d le signal ne change pas. Sachant que ce sont les seules communications possibles et que le signal est initialement d'une taille de 35 octets, quel est le chemin à prendre pour que le signal reçu par d soit le plus léger possible ? Est-ce que l'algorithme de Dijkstra permet de répondre à ce problème ?

Réponse au problème 2 On remarque que le cycle $(a, b), (b, c), (c, a)$ est de coût -10, en le répétant infiniment on peut atteindre $-\infty$, mais cela n'est pas réaliste. En appliquant Dijkstra, on va choisir le chemin $(a, b), (b, c), (c, d)$ et d va recevoir un signal de 35 octets ce qui n'est pas la bonne solution car avec le chemin $(a, b), (b, c), (c, a), (a, b), (b, c), (c, d)$ le signal aura une taille de 25 octets. Si on applique une contrainte de positivité sur la taille, alors la meilleure solution permet à d de recevoir un signal de 5 octets.



Problème 3 On considère un réseau composé des machines a, b, c, d, e, f, g. Par quelles machines faut-il passer pour transmettre un signal de a à g sachant que la probabilité de succès de chaque liaison est de,

— 90% pour (a, b) ;
— 70% pour (a, c) ;
— 80% pour (a, d) ;
— 90% pour (b, c) ;
— 70% pour (b, e) ;
— 80% pour (c, e) ;
— 80% pour (d, f) ;
— 90% pour (e, g) ;
— 80% pour (f, g)

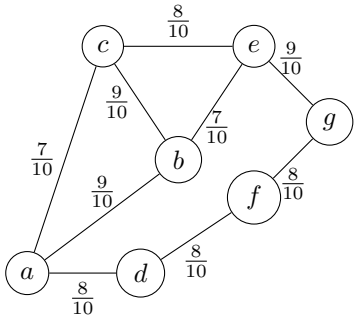
Quelle est la probabilité que le message ne contienne pas d'erreur ?

Réponse au problème 3 Ici le problème est particulier, la chance d'erreur ne s'exprime pas par la somme des valeurs des arêtes mais par leur produit (par exemple, si la probabilité de succès de (a, b) est x et (b, c) est y, alors celle du chemin (a, b, c) est $x \times y$). La deuxième particularité est que l'on cherche le chemin le plus long entre a et g.

On peut appliquer des opérations pour pouvoir appliquer l'algorithme de Dijkstra :

— L'algorithme effectue une somme sur les arêtes mais nous avons un produit. On peut s'en sortir en sommant le logarithme des probabilités, en effet le logarithme vérifie $\log(x \times y) = \log(x) + \log(y)$.
— L'algorithme choisit le minimum mais on cherche le maximum car on souhaite obtenir la probabilité de succès la plus haute possible. On va donc également changer le signe.

Ici le chemin le plus court est (a, b, c, e, g) avec un coût de $-\log(\frac{9}{10}) - \log(\frac{9}{10}) - \log(\frac{8}{10}) - \log(\frac{9}{10})$, d'où on déduit la probabilité $\frac{9}{10} \times \frac{9}{10} \times \frac{8}{10} \times \frac{9}{10}$.



Remarque : Si l'on considère la probabilité d'échec de transmission (à la place de la probabilité de succès), il sera nécessaire de déterminer, sur le chemin le plus fiable, tous les cas où la transmission a échouée. L'algorithme de Disjktra trouvera ce chemin, il sera en suite nécessaire de faire des calculs supplémentaires pour déterminer la probabilité d'échec (le procédé est moins direct mais ça reste possible, il faut sommer les différentes probabilités).

Théorie des probabilités

Problème 1 On considère un canal de transmission fiable à 25%. On envoie quatre signaux par ce canal, quelle est la probabilité qu'il y ait au moins une erreur ?

Réponse au problème 1 La transmission sans erreur est la probabilité conditionnelle de quatre réussites consécutives, c'est donc le produit $1/4^4 = 1/256$. La probabilité qu'il y ait une erreur est donc de $255/256$, c'est à dire plus de 99% de chance.

Problème 2 On considère un réseau à trois liaisons et l'une d'entre elles est défectueuse. On choisit une des trois liaisons que l'on nomme A, la probabilité qu'elle soit défectueuse est de $\frac{1}{3}$. Après avoir choisi A, on apprend que *parmi les autres liaisons* (c'est à dire que A n'a pas été considéré), l'une est fonctionnelle. On nomme la liaison restante B, il en résulte que la liaison défectueuse est soit A, soit B. Quelle est la probabilité pour chacune de ces deux liaisons ?

Réponse au problème 2 Initialement A a une chance sur trois d'être défectueuse. Comme elle n'a pas été considérée par la suite, la probabilité n'a pas changé. La seule solution possible pour B est que sa probabilité est $\frac{2}{3}$.

Problème 3 On considère un système qui doit recevoir un signal dans les 10 prochaines secondes. Il a autant de chance d'arriver, quel que soit le moment.

Soit $t \in]0, 10]$.

— Quelle-est la probabilité qu'il arrive au t-ième instant ?

— Quelle-est la probabilité qu'il arrive avant le t-ième instant ?

Réponse au problème 3 Il est improbable qu'il arrive exactement à l'instant t, la probabilité est donc zéro. En revanche, il y a $t/10$ chances qu'il arrive avant le t-ième instant. On peut représenter la probabilité par l'air d'un rectangle de hauteur $1/10$ et de longueur t.

Arithmétique

Définition : Un **nombre premier** est un entier n divisible uniquement par 1 et n tel que $1 \neq n$.

Définition : Le **plus grand diviseur commun** (PGCD) de deux nombres entiers a et b est le plus grand entier qui les divise.

Définition : Deux nombres entiers a et b sont **premiers entre eux** (que l'on note $a \wedge b$) si $\text{PGCD}(a, b) = 1$.

Définition : La décomposition en facteurs premiers est l'écriture d'un nombre sous la forme du produit des nombres premiers. Exemple : $18 = 3 \times 3 \times 2 = 3^2 \times 2$ (et non pas 2×9 car 9 n'est pas premier).

Définition : La fonction **indicatrice d'Euler**, notée $\varphi(n)$ est le nombre d'éléments strictement plus petits que n qui sont premiers avec n.

On donne ci-dessous le tableau de la fonction φ entre 1 et 30.

n	1	2	3	4	5	6	7	8	9	10
φ(n)	1	1	2	2	4	2	6	4	6	4
n	11	12	13	14	15	16	17	18	19	20
φ(n)	10	4	12	6	8	8	16	6	18	8
n	21	22	23	24	25	26	27	28	29	30
φ(n)	12	10	22	8	20	12	18	12	28	8

Problème 1 Soit a tq $a = 1 \mod d$. Montrer par récurrence que $a^n = 1 \mod d$.

Réponses au problème 1 Vrai pour $n = 1$:

$$a = k \times d + 1 \tag{1}$$

On considère que c'est vrai pour un rang n, montrons que c'est vrai au rang $n + 1$:

$$a^{n+1} = a^n \times a \tag{2}$$

Comme c'est vrai au rang n, il existe un entier M tel que $a^n = Md + 1$:

$$a^n \times a = (Md + 1)(kd + 1) = (Mkd + M + k)d + 1 \tag{3}$$

Propriétés

1. Si p est un nombre premier, $\varphi(p^n) = p^n - p^{n-1}$
2. Si $a \wedge b$ alors $\varphi(a \times b) = \varphi(a) \times \varphi(b)$
3. Si $a \wedge n$ alors le reste de la division de $a^{\varphi(n)}$ par n est égale à 1.

Problème 2 Quel est le reste de la division de 9^{1000} par 1000 ? *(Indice :* $9^{1000} = 3^{2000}$*)*

Réponses au problème 2 On cherche le reste d'une division par 1000, si $a \wedge 1000$ alors on peut utiliser la propriété 3 :

$$a^{\varphi(1000)} = 1 \tag{4}$$

Or :

$$\varphi(1000) = \varphi((2 \times 5)^3) \tag{5}$$

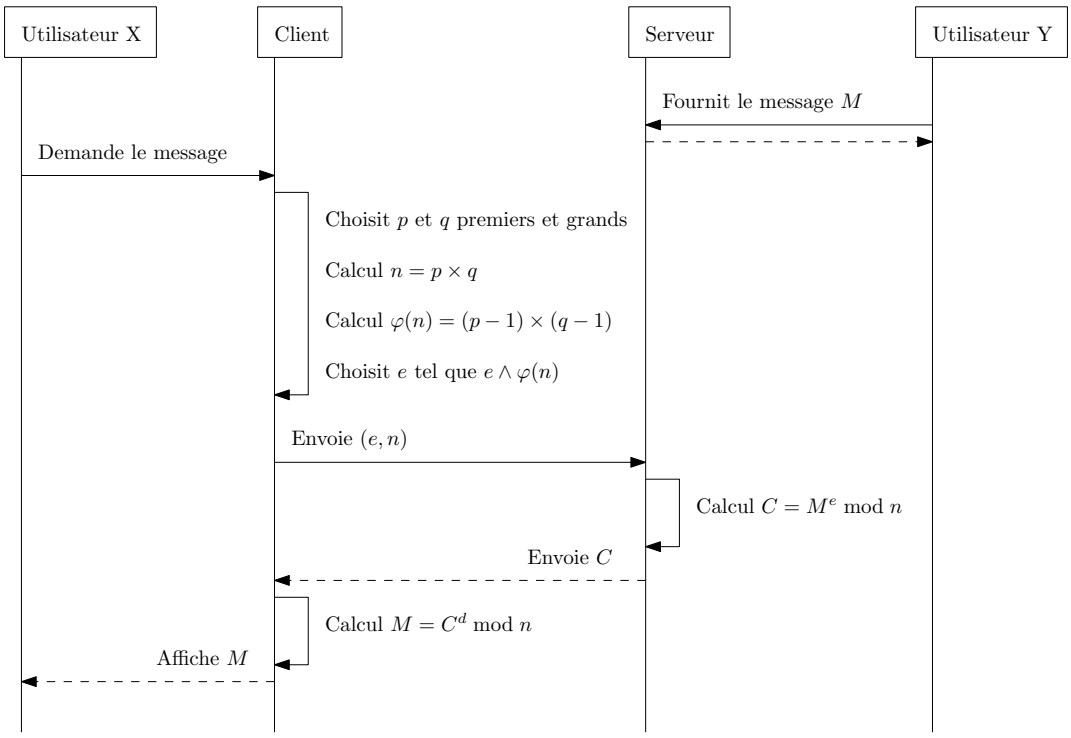
Grâce à la propriété 2 et la propriété 1 :

$$\varphi((2 \times 5)^3) = \varphi(2^3) \times \varphi(5^3) = (8 - 4) \times (125 - 25) = 400 \tag{6}$$

Comme $3 \wedge 1000$:

$$3^{2000} = 3^{\varphi(1000) \times 5} = (3^{\varphi(1000)})^5 = 1 \mod 1000 \tag{7}$$

Transfert de données L'arithmétique est une partie des maths qui est fortement utilisée dans le domaine de la sécurité. Par exemple, l'algorithme *Rivest–Shamir–Adleman* (RSA) permet de transférer des données de manière sécurisée. On peut le décrire en utilisant ce que nous avons vu juste avant. Voici son diagramme de séquence,



Logique du premier ordre

La logique propositionnelle permet de s'assurer de la validité d'un raisonnement et peut être utilisée à des fins de déduction.

Connecteurs logiques : Pour deux formules A et B, voici une notation standard des connecteurs logiques,

non A	$\neg$ A
A ou B	A $\vee$ B
A et B	A $\wedge$ B
si A alors B	A $\implies$ B
A équivaut B	A $\iff$ B

TABLE 1 – Connecteurs logiques

Une formule peut être soit vraie, soit fausse, il est donc possible d'exprimer tous les cas possibles dans une table de vérité. Par exemple pour le connecteur $\neg$:

A	$\neg$ A
F	V
V	F

TABLE 2 – Table de vérité de $\neg$

Problème 1 Sachant que $A \implies B$ peut s'écrire $(\neg A) \vee B$, quelle est sa table de vérité ?

Réponses au problème 1 Voir table 3.

A	B	A $\implies$ B
F	F	V
F	V	V
V	F	F
V	V	V

TABLE 3 – Table de vérité de $\implies$

Parfois, on veut exprimer les propriétés de certains objets et pour cela, on utilise des prédicats. Par exemple *être connecté* peut être exprimé avec le prédicat C. Pour la phrase "Le PC a est connecté au réseau", cela donne $C(a)$. Maintenant, si un autre PC b n'est pas connecté au réseau, on peut le noter $\neg C(b)$. Ce que l'on vient de faire est une interprétation de la phrase et sa formalisation (en langage logique) à l'aide des objets a, b et du prédicat C.

Problème 2 Peut on exprimer la phrase "Le PC1 est plus rapide que le PC2" avec un prédicat ?

Réponses au problème 2 On pose R le prédicat "être plus rapide", a le PC1, b le PC2. Avec cette interprétation, la phrase devient $R(a, b)$.

Problème 3 Les PC a, b et c sont connectés à un switch. Étant donné que

1. a et b sont dans le même sous-réseau,
2. a et c ne sont pas dans le même VLAN,
3. le cache ARP de b contient l'adresse MAC de c,

que peut on déduire sur la configuration du switch ? (Tenter de le formaliser avec les notations formelles utilisées précédemment)

Réponses au problème 3 On pose d'abord les prédicats suivants :

— $S(x, y)$: x et y sont dans le même sous-réseau.
— $W(x, y)$: x et y sont dans le même VLAN.
— $A(x, y)$: le cache arp de x contient l'adresse MAC de y.
— R : le switch est configuré sur "VLAN par sous-réseau".

On peut alors considérer l'interprétation suivante :

— (1) $S(a, b)$
— (2) $\neg W(a, c)$
— (3) $A(b, c)$

On ajoute à cela trois propositions :

— (4) $A(x, y) \implies S(x, y)$
— (5) $S(x, y) \wedge S(y, z) \implies S(x, z)$
— (6) $S(x, y) \wedge \neg W(x, y) \implies \neg R$

Puis avec le raisonnement suivant, on monte $\neg R$:

— (7) : d'après (3) et (4), $S(b, c)$
— (8) : d'après (1), (5) et (7), $S(a, c)$
— (9) : d'après (2), (6) et (8), $\neg R$