

MATH-F307 - Mathématiques Discrètes
Laurent LA FUENTE
Notes de cours

André MADEIRA CORTES
Nikita MARCHANT

Table des matières

1	Théorie des Graphes	3
1.1	Définitions	3
1.2	Chemins dans les graphes	4
1.3	Arbres	5
1.3.1	Définitions	5
1.3.2	Arbres couvrants et arbres à poids	6
1.4	Isomorphisme	6
1.5	Graphes hamiltoniens	7
1.6	Graphes Eulériens	8
1.7	Application : le problème du voyageur de commerce (TSP)	9
1.7.1	Énoncé du problème	9
1.7.2	Arbres couvrant minimum	10
1.8	Ordres partiels	10
2	Arithmétique Modulaire	12
3	Combinatoire énumérative	13
4	Théorie des Codes	14
5	Transformées de Fourier discrètes	15

1 Théorie des Graphes

1.1 Définitions

Définition 1

Un graphe Γ est un triplet (V, E, γ) où V est un ensemble fini dont les éléments sont appelés sommets, E est un ensemble fini dont les éléments sont appelés arêtes, γ est une fonction $\gamma : E \rightarrow \text{Paires}(V)$. On nottera le plus souvent $\Gamma = (V, E)$ en omettant la fonction γ .

Soit $\gamma(e) = \{x, y\}$ pour $e \in E, x, y \in V$:

1. On dit que x et y sont adjacents.
2. On dit que e est incidente à x et y .

Définition 2

Soit $\Gamma = (V, E, \gamma)$ un graphe.

1. $\gamma(e) = \{x, x\}$ pour $e \in E, x \in V$ est appelé un lacet.
2. Si au moins 2 arêtes sont incidentes à 2 mêmes sommets, on les appelle arêtes multiples.
3. Un graphe est simple s'il n'a ni lacet, ni arêtes multiples. Dans ce cas, on omet la fonction γ , on note $\Gamma = (V, E)$ et E est identifié un sous-ensemble de $\text{Paires}(V)$.

Définition 3

Soit $\Gamma = (V, E)$ un graphe. Le degré d'un sommet $v \in V$ est le nombre d'arêtes incidentes à v , les lacets comptant pour 2 arêtes. On note le degré de v par $\deg(v)$.

Exemple

Dans la figure suivante, nous avons 2 sommets de degré 4 et 6 sommets de degré 1.

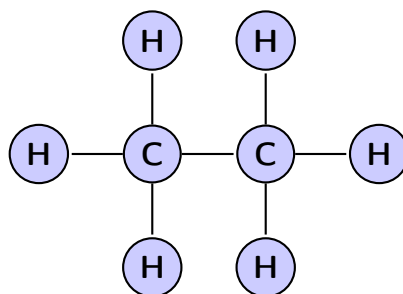


FIGURE 1 – Exemple degrés des sommets dans la molécule C_2H_6 .

Théorème 1

Soit $\Gamma = (V, E)$, alors

$$\sum_{i=1}^{\#V} \deg(v_i) = 2\#E$$

Démonstration

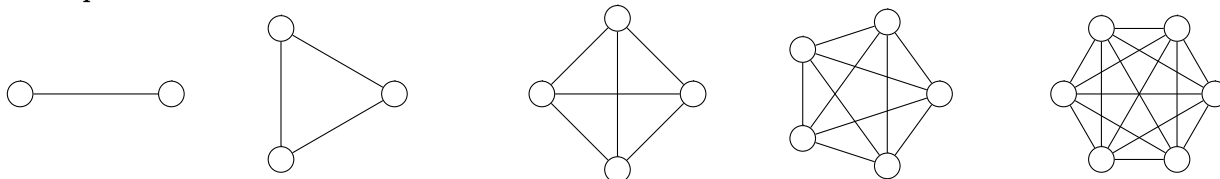
Chaque arête contribue 2 fois dans la somme des degrés.

Corollaire

La somme des degrés des sommets d'un graphe est paire.

Définition 4

Le graphe complet K_n est le graphe simple à n sommets pour lequel chaque paire de sommets est une arête.

Exemple**Définition 5**

Un graphe $\Gamma' = (U, F)$ est un sous-graphe de $\Gamma = (V, E)$ si $U \subseteq V$ et $F \subseteq E$. On nottera $\Gamma' \leq \Gamma$.

Exemple

$K_m \leq K_n$ si $m \leq n$.

Exercice

Montrer que K_m possède $q = \frac{1}{2}n(n-1)$ arêtes.

1.2 Chemins dans les graphes**Définition 6**

Soit $\Gamma = (V, E)$ et $v, w \in V$. Un chemin de v à w de longueur n est une séquence alternée de $(n+1)$ sommets v_0, v_1, \dots, v_n et de n arêtes e_1, e_2, \dots, e_n de la forme

$$(v_0, e_1, v_1, e_2, \dots, e_n, v_n)$$

dans laquelle chaque e_i est incident à v_{i-1} et v_i pour $1 \leq i \leq n$ et $e_i \neq e_j, \forall i \neq j \in 1, \dots, n$

Un chemin est simple si aucun sommet ne se répète sauf peut-être v_0 et v_n .

Dans un graphe simple on nottera juste la suite des sommets lorsque l'on décrit un chemin.

Définition 7

Un graphe $\Gamma = (V, E)$ est connexe si $\forall x, y \in V : \exists$ un chemin de x à y .

La composante connexe de Γ contenant x est le sous-graphe Γ' de Γ dont les sommets et les arêtes sont contenus dans un chemin de Γ démarrant en x .

Définition 8

Soit $\Gamma = (V, E)$ et $v \in V$.

Un cycle est un chemin de v à v .

Un cycle simple est un cycle de v à v dans lequel aucun sommet n'est répété (mis à part le départ et l'arrivée).

1.3 Arbres

1.3.1 Définitions

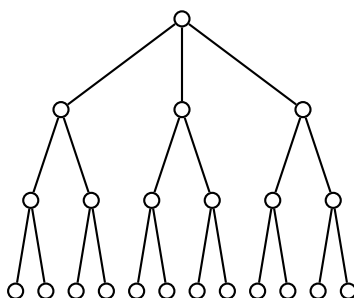
Définition 9

Un arbre est un graphe simple connexe qui ne contient aucun cycle.

Définition 10

Dans un arbre, les sommets de degré 1 sont appelés les feuilles.

Exemple



Proposition 1

Si T est un arbre avec $p \geq 2$ sommets, alors T contient au moins 2 feuilles.

Démonstration

T a p sommets. Tous les chemins sont de longueur inférieure ou égale à p . Considérons un chemin v_0, v_1, \dots, v_r pour $v_i \in V$, $i = 0, \dots, r$ de longueur maximale. Alors, v_0 et v_r sont de degré 1.

Théorème 2

Soit T un graphe simple à p sommets. Alors les 3 assertions suivantes sont équivalentes :

- i T est un arbre.
- ii T a $(p - 1)$ arêtes et aucun cycle.
- iii T a $(p - 1)$ arêtes et est connexe.

Démonstration

(i) \Rightarrow (ii) : **Montrer qu'un arbre à p sommets a $(p-1)$ arêtes.**

Par récurrence :

1. $p = 1$ OK
2. Supposons que ce soit vrai pour tout arbre à $k \geq 1$ sommets et montrons le pour un arbre à $(k+1)$ sommets. Soit T un tel arbre, il a au moins 2 feuilles. Enlevons une de ces feuilles ainsi que l'arête incidente. On obtient un arbre T' à k sommets. Par l'hypothèse de récurrence : T' a $(k-1)$ arêtes, donc T a k arêtes.

(ii) \Rightarrow (iii) : **Supposons (ii) et T ne soit pas connexe.**

Notons T_1, T_2, \dots, T_t les composantes connexes de T avec $t \geq 2$. Chaque T_i est un arbre, pour $1 \leq i \leq t$ (car pas de cycle). Soit p_i le nombre de sommets de T_i , alors chaque T_i a $(p_i - 1)$ arêtes.

$$\sum_{i=1}^t p_i = p$$

et

donc $\Rightarrow t = 1$

$$p - 1 = \sum_{i=1}^t (p_i - 1) = p - t$$

(iii) \Rightarrow (i) : **Supposons que T ne soit pas un arbre.**

Alors, T contient un cycle C . Enlevons une arête de C . On obtient le sous-graphe T' de T qui est toujours connexe. Si T' contient un cycle, alors on itère le processus. Sinon, T' est un arbre à p sommets qui a strictement moins que $(p-1)$ arêtes.

1.3.2 Arbres couvrants et arbres à poids

Définition 11

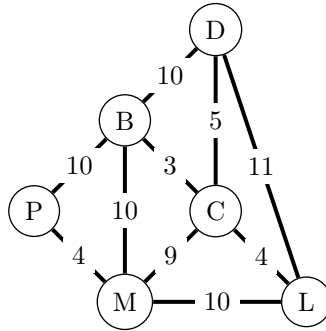
Un arbre couvrant dans un graphe Γ est un arbre qui est un sous-graphe de Γ et qui contient tous les sommets de Γ .

Dans certains problèmes, certaines arêtes sont plus importantes que d'autres. En théorie des graphes, on modélise cela en assignant une valeur à chaque arête.

Définition 12

Un arbre à poids est un couple (Γ, w) où Γ est un arbre w est une fonction $w : E \rightarrow \mathbb{R}^+$. Le nombre $w(e)$ est appelé le poids de l'arête e .

Exemple



1.4 Isomorphisme

Définition 13

Deux graphes $\Gamma_1 = (V_1, E_1, \gamma_1)$ et $\Gamma_2 = (V_2, E_2, \gamma_2)$ sont isomorphes s'il existe une bijection $f : V_1 \rightarrow V_2$ et une bijection $g : E_1 \rightarrow E_2$ telles que $\forall e \in E_1 : e$ est incident à $v, w \in V_1$ ssi $g(e)$ est incident à $f(v), f(w) \in V_2$. Le couple (f, g) est appelé un isomorphisme de graphe et on note $\Gamma_1 \cong \Gamma_2$.

Deux graphes isomorphes ont les mêmes propriétés.

Exemple

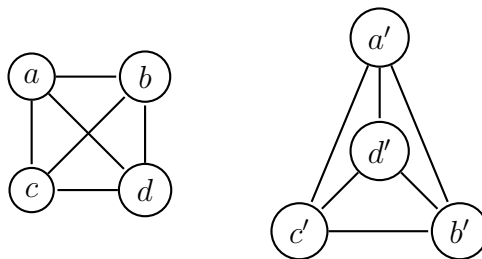


FIGURE 2 – Deux graphes isomorphes

1.5 Graphes hamiltoniens

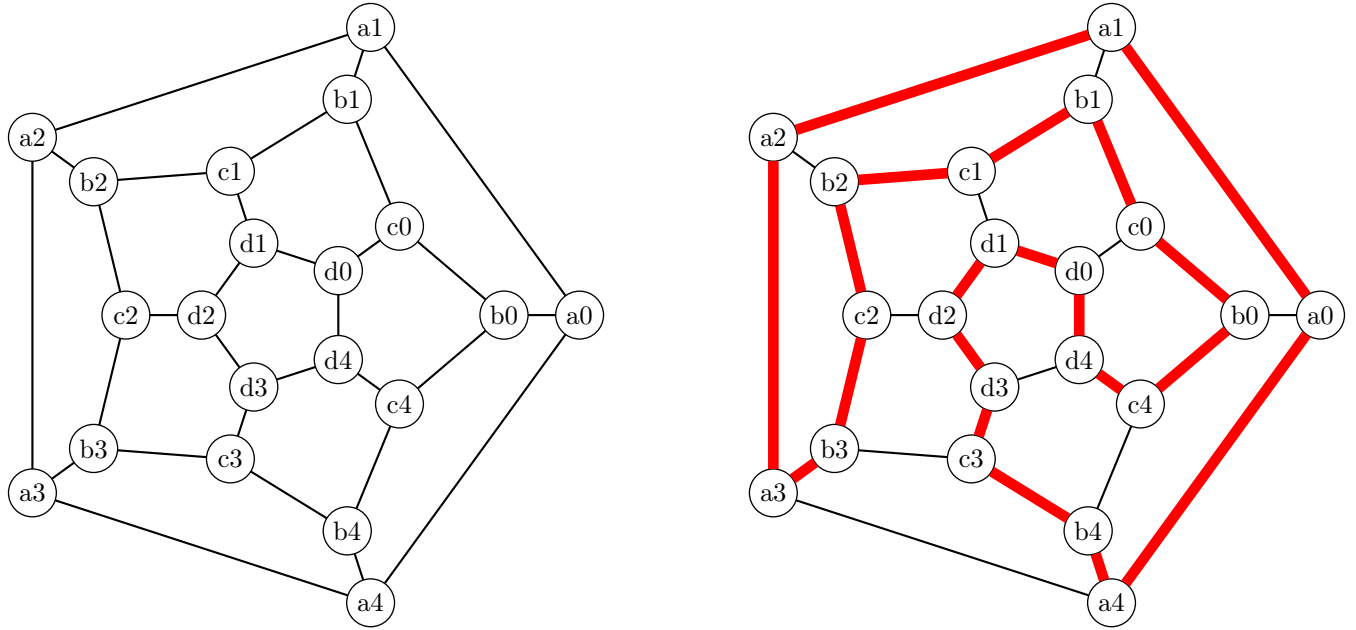


FIGURE 3 – Graphe hamiltonien et cycle hamiltonien

STUFF MISSING HERE

Théorème 3 (Dirac 1950)

Soit $\Gamma = (V, E)$ un graphe simple avec $p \geq 3$ sommets. Si $\forall v \in V : \deg(v) \geq \frac{1}{2}p$, alors Γ est Hamiltonien.

Démonstration

Γ est connexe. Soit $C = (v_0, v_1, \dots, v_k)$ un plus long chemin simple dans Γ avec $v_0 \neq v_k, k < p$.

$\deg(v_0) \geq \frac{p}{2}$, tous les sommets adjacents à v_0 sont dans $\{v_1, \dots, v_k\}$

$\deg(v_k) \geq \frac{p}{2}$, tous les sommets adjacents à v_k sont dans $\{v_0, \dots, v_{k-1}\}$

Comme $k < p$, il doit exister $i \in \{0, \dots, k-1\}$ tel que $\{v_i, v_k\} \in E$ et $\{v_0, v_{i+1}\} \in E$. On obtient un cycle $\tilde{C} = (v_0, v_1, \dots, v_i, v_k, v_{k-1}, \dots, v_{i+1}, v_0)$

On nq(?) \tilde{C} est un cycle Hamiltonien.

Supposons :

$\exists y \in \tilde{C} \Rightarrow$ On peut supposer que $\{v_j, y\} \in E$ pour $j = \{0, \dots, k\}$.

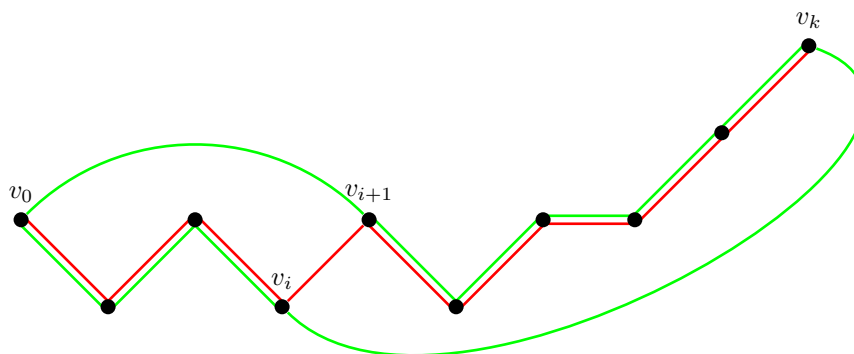
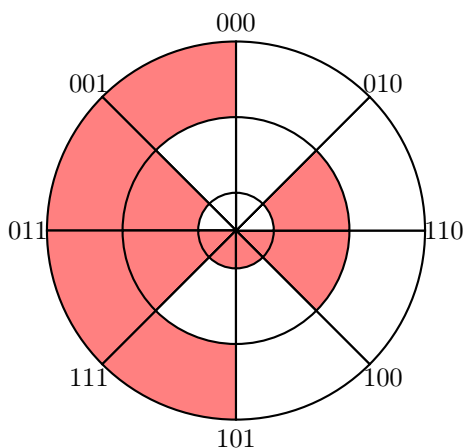
\Rightarrow On construit un chemin $\overline{C} = (y, v_j, v_{j-1}, \dots, v_0, v_{i+1}, \dots, v_k, v_i, v_{i-1}, \dots, v_{j-1})$. \overline{C} est un chemin plus long que C .

<Second Dessin>

Illustration : Code de Gray

Un code de Gray d'ordre n est un arrangement cyclique de 2^n mots binaires de longueur n tels que 2 mots adjacents ne diffèrent qu'en une seule position.

Exemple

FIGURE 4 – Les 2 chemins, C en rouge, \tilde{C} en vert.

Le code de Gray ci-dessus provient d'un cycles Hamiltonien.

<dessin cube et cycle>

Un code de Gray d'ordre $(n+1)$ se construit à partir d'un code de Gray d'ordre n comme suit :

1. On écrit le code de Gray donné d'ordre n en ajoutant à la fin de chaque mot un zéro.
2. On le fait suivre par le même code de Gray parcouru dans l'autre sens et en ajoutant à la fin de chaque mot un 1.

1.6 Graphes Eulériens

Définition 14

Un cycle Eulérien dans un graphe Γ est un cycle qui contient toutes les arêtes de Γ . Un graphe est Eulérien s'il contient un cycle Eulérien.

Exemple

SOME EXAMPLE

Proposition 2

Si un graphe est Eulérien, alors tous ses sommets sont de degré pair.

Lemme

Soit Γ un graphe dans lequel chaque sommet est de degré pair, alors l'ensemble E se partitionne en une union de cycles (arête-)disjointe.

Exemple

<DRAWING 3 CYCLES>

Démonstration

Par récurrence, sur le nombre d'arêtes

1. Le lemme est vrai pour $q = 2$.
2. Supposons qu'il soit vrai pour tout graphe à $q \leq k$ arêtes et montrons-le pour un graphe à $(k+1)$ arêtes.
3. Soit v_0 un sommet de Γ . On démarre un chemin en v_0 et on le suit jusqu'à ce qu'un sommet soit répété 2 fois. On le note v_j et C le cycle de v_j à v_j .
4. Soit Γ' le sous-graphe de Γ , obtenu par $V = V'$ et $E' = E \setminus C$. Γ' a $\#E' \leq k$ arêtes. Par hypothèse de récurrence, les arêtes de Γ' se partitionnent en une union arête-disjointe de cycles $C_1 \cup C_2 \cup \dots \cup C_n$.
5. Donc, $C_1 \cup C_2 \cup \dots \cup C_n$ est une partition arête-disjointe des arêtes de Γ .
6. RECHECK THIS DEMO, SEEMS FISHY

Théorème 4

Soit Γ un graphe connexe. Alors, Γ est eulérien si et seulement si chaque sommet a un degré pair.

Démonstration

\Rightarrow OK par proposition précédente.

\Leftarrow Par le Lemme : E se partitionne en une union (arête-)disjointe de cycles $C_1 \cup C_2 \cup \dots \cup C_n$.

1. Si $n=1$, c'est bon.
2. Si $n > 1$, comme Γ est connexe, \exists une arête incidente à un $v \in C_1$ et un $w \notin C_1$. Cette arête est dans C_j pour un $j = 2, \dots, n$ (car on a une partition de E). On attache ce cycle en v . S'il reste des cycles dans la partition, on itère ce procédé jusqu'à avoir utilisé tous les cycles.

1.7 Application : le problème du voyageur de commerce (TSP)**1.7.1 Énoncé du problème**

Énoncé : Un vendeur de livres démarre de chez lui et doit visiter un certain nombre de librairies avant de rentrer chez lui. Comment doit-il choisir sa route pour minimiser la distance parcourue ?

Objet mathématique : Un graphe valué (à chaque arête est associé un nombre appelé poids) où les sommets représentent les librairies et les arêtes représentent les routes.

<VALUED K5 GRAPH HERE>

Objectif : Trouver un cycle hamiltonien de poids minimal.

Remarque : Un graphe complet K_n à n sommets possède $\frac{1}{2}(n-1)!$ cycles hamiltoniens différents. Par exemple, pour $n = 10 \Rightarrow 181440$ cycles. On ne connaît pas encore d'algorithme efficace qui donne une solution au problème.

1.7.2 Arbres couvrant minimum

Définition 15

Un arbre couvrant dans un graphe Γ est un arbre qui est un sous-graphe de Γ et qui contient tous les sommets de Γ .

Exemple

<GRAPH TO MIN SPANNING TREE EXAMPLES HERE>

Il existe un algorithme qui donne des arbres couvrants de poids minimum dans un graphe valué.

Algorithme de Kruskal :

- i Choisir une arête de plus petit poids.
- ii Choisir parmi les arêtes restantes une arête de plus petit poids dont l'inclusion ne crée pas un cycle.
- iii Continuer jusqu'à obtenir un arbre couvrant.

Exemple

<GRAPH K5 WITH PATH HERE>

Remarque : Si C est un cycle hamiltonien dans un graphe Γ , alors $\forall e \in E$ arête de C : $C \setminus \{e\}$ est un arbre couvrant.

\Rightarrow (Solution de TSP) \geq (longueur minimum d'un arbre couvrant)

Mieux : Soit v un sommet de Γ . Tout cycle hamiltonien contient 2 arêtes incidentes à v . Le reste du chemin est un arbre couvrant de $\Gamma \setminus \{v\}$.

\Rightarrow (Solution de TSP) \geq (\sum des longueurs des 2 plus courtes arêtes incidentes à v) + (longueur minimum d'un arbre couvrant de $\Gamma \setminus \{v\}$)

Remarque : \exists borne supérieure à TSP en utilisant des cycles eulériens.

1.8 Ordres partiels

Définition 16

Soit P un ensemble. Un ordre partiel sur P est une relation sur P , c'est à dire un ensemble de couples $(p_1, p_2) \in P \times P$, noté $p_1 \leq p_2$ tel que :

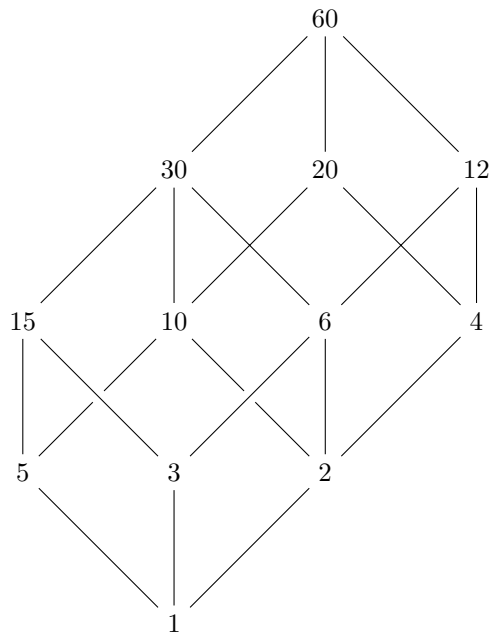
1. $p \leq p$ (réflexive)
2. $(p \leq q \text{ et } q \leq p) \Rightarrow p = q$ (anti-symétrique)
3. $(p \leq q \text{ et } q \leq r) \Rightarrow p \leq r$ (transitive)

On note (P, \leq) un ensemble partiellement ordonné.

Exemple 1. (\mathbb{N}, \leq)

2. $(\mathbb{N}, |)$ où $a \mid b$ si $\exists c \in \mathbb{Z}$ tel que $a \cdot c = b$ ($a, b \in \mathbb{Z}$)

Un ordre partiel (bla bla bla)



2 Arithmétique Modulaire

3 Combinatoire énumérative

4 Théorie des Codes

5 Transformées de Fourier discrètes