

Complexité algorithmique

Timothée Pecatte

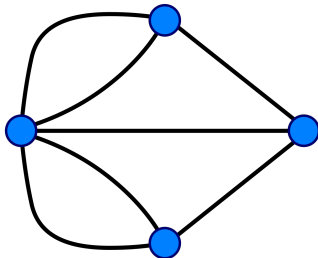
DIU Bloc 5
25/06/2020

.

Table des matières

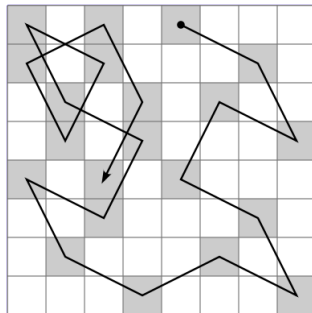
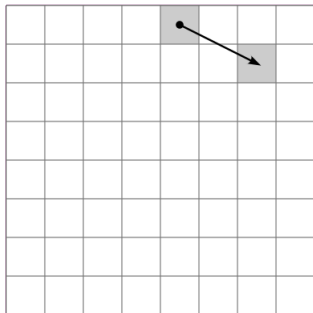
- 1 Introduction
- 2 Rappels et définitions
- 3 Classes de complexité

Introduction

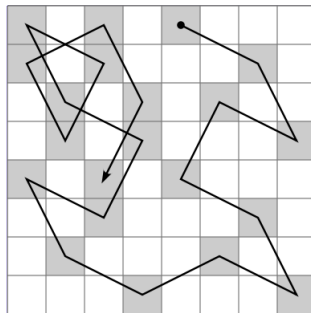


3 / 38

Introduction : chemin hamiltonien

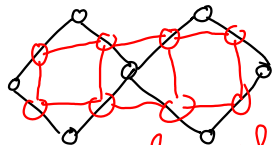


Existe-il un cycle passant par chaque sommet exactement une fois ?



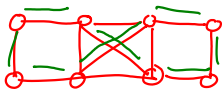
5 / 38

G a un cycle eulérien \Leftrightarrow



en rouge le graphe dual
obtenue en remplaçant une
arête par un sommet et en
reliant 2 sommets dans G' si les
2 arêtes dans G sont incidentes à un même sommet.

G' a un cycle hamiltonien



— cycle hamiltonien
qu'on convertit en
cycle eulérien
dans G

Pourquoi Hamiltonien plus dur que eulérien
si on a une équivalence ! Parce qu'on construit
le graphe hamiltonien

G a un cycle eulérien $\Rightarrow M(G')$ oui

G n'a pas de cycle eulérien $\Rightarrow M(G')$ non

on a même une bijection entre les cycles eulériens
de G et les cycles hamiltoniens de G'

Hamiltonien est plus dur
car si je sais résoudre hamiltonien
alors je sais résoudre eulérien.

7 / 38

Problèmes de décision

Definition

Un **problème de décision** = sortie **booléenne**.

Exemple (Problème de décision du cycle Hamiltonien)

Étant donné un graphe G , existe-t-il un cycle Hamiltonien dans G ?

Example

Étant donné un entier n , est-il premier?

Example

Étant donné un entier n sous forme de produit de nombres premiers, est-il premier ?

- Dans beaucoup de cas il est plus facile de déterminer si une solution existe que de la construire.
- Pour les deux derniers exemples, la spécification de l'entité (son codage) est important.

D'autres exemples

Exemple

Étant donné un graphe G , est-il 3-coloriable ?

Exemple

Étant donné un graphe planaire G , est-il 4-coloriable ?

Exemple

Étant donné un programme C , le programme s'arrête-il toujours ?

Exemple

Étant donné une formule logique (composée de OU, ET, NEG), existe-il une assignation des variables qui rend la formule vraie ?

Temps de calcul

Definition (Résolution)

A résout un problème de décision $P : \forall$ entrée I (instance) valide pour P , $A(I) = \text{VRAI}$ si et seulement si $I \in P$.

Definition (Complexité)

$t_A(I)$ = temps de calcul de A sur I (nombre d'instructions élémentaires).

complexité pire cas
 $T_A(n) = \max\{t_A(I) \mid \text{taille}(I) = n\}$

$$T_P(n) = \min\{t_A(n) \mid A \text{ résout } P\}$$

Remarque

D'autres mesures de complexité possibles : mémoire, temps de calcul sur architecture parallèle, ...

En pratique

- Rarement accès à $T_P(n)$: utilisation de O
 - Etude asymptotique : pas toujours utile sur des données réelles
 - Modèles de calculs réels complexes à modéliser
-
- Problème Eulérien et Hamiltonien : vérification facile $O(n)$
 - Énumération de tous les sous-ensembles d'arêtes : $O(n2^n)$
 - Caractérisation des graphes Eulériens $\Rightarrow O(n)$
 - Cycle Hamiltonien : ???

m nombre
d'arêtes

- Cycle Hamiltonien

on s'intéresse
de plus
de décision,
pas de construction

Quelle granularité utiliser pour séparer les problèmes ?

Réduction polynomiale

Definition (Réduction - avec les mains)

Le problème P est plus facile que le problème Q si l'on peut se servir d'un algorithme pour le problème Q afin de résoudre le problème P .

Remarque

Si un algorithme A consiste en $O(f(n))$ appels à un algorithme B avec des entrées de taille $O(g(n))$, et que la complexité de B est $O(h(n))$ opérations élémentaires, alors la complexité de A est $O(f(n) \times (g \circ h)(n))$.

Algorithme linéaire ($O(n)$) + stabilité par réduction “raisonnable”
 \Rightarrow tous les algorithmes de complexité polynomiale.

Si un algo en $O(n)$ fait
appel à chaque itération à un
algo en $O(n)$ on a du $O(n^2)$
boîte noire

On recherche des classes
de complexité stables par réduc-
tion



Definition

Un problème A appartient à la classe P s'il existe un algorithme qui résout A en temps polynomial.

Example

- Eulérien
- 2-couleur
- Accessibilité : étant donné un graphe G et deux sommets $s, t \in G$, existe-t-il un chemin de s à t ?
- Connexité : est-ce qu'un graphe donné est connexe ?
- PGCD
- Primalité
- Recherche de motif dans un texte

La classe P

Facile ou difficile ?

Problème dans P ou pas dans P ?

- Si le problème $\in P$:
 - fournir un algorithme
 - montrer qu'il est correct
 - montrer qu'il est polynomial en la taille des données
- Si le problème $\notin P$:
 - **montrer qu'aucun algorithme polynomial n'existe !**
 - en général très compliqué

voir le problème
de programmation
dynamique qui
est exponentiel en
la taille des
données $O(2^n)$
soit

Exemple

Hamiltonien $\in P$??

Au-delà de P ?

- Hamiltonien $\in P$??
- Algorithme en $O(n2^n)$, Hamiltonien $\in EXP \rightarrow$ pas suffisant ?
- Supposons qu'une opération prend $1\mu s = 10^{-6}s$:

$n/f(n)$	n	n^2	n^3	2^n	3^n	$n!$
10	$10\mu s$	$0.1ms$	$1ms$	$1ms$	$59ms$	$3.63s$
20	$20\mu s$	$0.4ms$	$8ms$	$1s$	58 min	77094 ans
40	$40\mu s$	$1.6ms$	$64ms$	12.73 j	385253 ans	$2.58 \cdot 10^{34}\text{ ans}$
60	$60\mu s$	$3.6ms$	$216ms$	36533 ans	$1.34 \cdot 10^{15}\text{ ans}$	$2.63 \cdot 10^{68}\text{ ans}$

- Et si on “boostait” ma machine ?
- Et si on utilisait un serveur de calcul ?
- Et si on parallélisait massivement les calculs ?

P or not P ?

Quand on ne sait pas...

- Pour beaucoup de problème, on ne sait pas :
 - aucun algo polynomial connu \Rightarrow tous sont exponentiels...
 - ...mais aucune preuve que le problème $\notin P$!
- Idée : inventer une classe intermédiaire : $P \subseteq \text{NP} \subseteq \text{EXP}$

ATTENTION

NP veut dire Nondeterministic Polynomial

NP ne veut pas dire NON POLYNOMIAL !

Classe NP : définition avec certificats

Definition

$P \in NP$ si pour chaque **instance positive** I (réponse OUI), il existe un **certificat** $C(I)$ (de sa positivité) vérifiant :

- ① taille de $C(I)$: **polynomiale** en la taille des données du problème
- ② **vérification** à partir de $C(I)$: en temps **polynomial**

Exemple

Hamiltonien $\in NP$, Eulérien $\in NP$.

- NP : solution **facile à vérifier**
- P : solution **facile à trouver**
- On a bien $P \subseteq NP$

NP– Intuitivement

Coloration de graphe

- j'ai un graphe G et un entier k (une instance I)
- je me demande si G peut être proprement colorié en $\leq k$ couleurs
- quelqu'un observe par-dessus mon épaule, réfléchit et répond "oui" (instance positive)
- je doute : je lui demande une "preuve" (certificat $C(I)$)
- je vérifie, sur la base de sa "preuve", qu'il dit vrai
- si la taille de $C(I)$ et l'algorithme de vérification sont polynomiaux (en la taille des données), le problème est dans NP

NP : définition non-déterministe

Definition

Un problème A appartient à la classe NP s'il existe un algorithme **non-déterministe** qui résout A en temps polynomial.

↳ un algorithme qui a des chemins à faire qui on ne précise pas

Algorithme 1 Hamiltonien(V, E)

1: choisir un sommet $s \in V$

2: $\text{chemin} \leftarrow \emptyset$

3: **tant que** $V \neq \emptyset$ **faire**

4: **si** s n'a pas de voisin **alors retourner** IMPOSSIBLE

5: choisir t un voisin de s

6: $V \leftarrow V \setminus s$

7: $\text{chemin} \leftarrow (s, t) :: \text{chemin}$

8: $s \leftarrow t$

9: **fin tant que**

↳ Il existe une manière pour choisir qui revient à ça.

] on ne dit pas comment choisir le voisin

NP, et alors ?

Proposition

$$P \subseteq NP$$

- NP ne nous permet pas de distinguer entre des problèmes qu'on sait être dans P et des problèmes qui ont l'air plus durs.
- Exemple : Eulérien \in NP et Hamiltonien \in NP.
- **Idée** : se restreindre aux problèmes de NP les "plus durs"
- Pour rendre "plus durs" plus précis, on va maintenant formaliser la notion de **réduction**

On voudrait distinguer les nbs
les + durs qui sont dans NP car $P \subseteq NP$

Réduction polynomiale “many-one”

Definition

$Q \leq_m^P P$ (Q se réduit à P) si et seulement si $\exists f$, calculable en temps polynomial, telle que : $\forall I$ entrée valide de Q , $I \in Q \Leftrightarrow f(I) \in P$.

\forall entrée valide de Q \xrightarrow{P} Polynomial
 $Q \leq_m P \xrightarrow{P}$ $\text{many one reductions}$
 entrées dans Q peuvent avoir

réduction illustrée précédemment. len^1
 codage

Example

Eulérien \leq_m^P Hamiltonien : réduction illustrée précédemment.

Remarque

Attention : si Q se réduit à P , c'est que Q est plus simple que P (d'où la notation $Q \leq_m^P P$)

Proposition

La classe P est close par réduction polynomiale "many-one".

La classe P est bien stable
par réduction polynomiale.
Si on a un algo¹ poly-
-nomial et qu'on l'applique
à une réduction polynomiale
alors on a encore un algo
polynomial

Problèmes équivalents

Example

MAX-clique : étant donné un graphe G , trouver une **clique** maximale. (*une clique est un ensemble de sommets tous reliés deux-à-deux*)

Example

MAX-indépendant : étant donné un graphe G , trouver un **ensemble indépendant** maximal. (*un ensemble indépendant est un ensemble de sommets qui ne sont reliés par aucune arête*)

Proposition

$$\begin{aligned} \text{MAX-clique} &\leq_m^p \text{MAX-indépendant} \\ \text{MAX-indépendant} &\leq_m^p \text{MAX-clique}. \end{aligned}$$

24 / 38

L'œuf et la poule

Montrer qu'un problème est NP-complet implique de réduire un problème NP-complet vers lui...mais il faut bien commencer quelque part !

Remarque

Il n'est a priori pas évident qu'il existe au moins un problème NP-complet

Theorem (Cook 1971)

*Le problème **SAT** est NP-complet*

$$(x_1 \vee \neg x_2) \wedge (\neg x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee x_4 \vee \neg x_3) \wedge (\neg x_2 \vee \neg x_4)$$

SAT est NP-complet : preuve avec les mains

SAT \in NP : étant donné les valeurs, il suffit d'évaluer la formule pour voir si celle ci est satisfaite.

Plus dur que tous les problèmes de NP :

- $P \in \text{NP}$: soit A un algorithme non-déterministe qui le résout.
- Choix de A réalisés en “lançant une pièce” \rightarrow variables booléennes c_1, c_2, \dots, c_p
- Soit I une instance de P .
- Formule $\varphi_A(0, 1, 1, \dots)$ qui est satisfiable si et seulement si l'algorithme A répond OUI sur l'entrée I avec les résultats de lancers $0, 1, 1, \dots$

Le modèle de calcul des machines de Turing permet d'écrire une telle formule.

- $f(l) = \varphi_A(c_1, \dots, c_p)$ satisfiable si et seulement l est positive

Et après : c'est les soldes !

Richard Karp, 1972, *Reducibility Among Combinatorial Problems*

- CLIQUE : le problème de la clique (voir aussi le problème de l'ensemble indépendant)
 - SET PACKING : Set packing (empaquetage d'ensemble)
 - VERTEX COVER : le problème de couverture par sommets
 - SET COVERING : le problème de couverture par ensembles
 - FEEDBACK ARC SET : feedback arc set
 - FEEDBACK NODE SET : feedback vertex set
 - DIRECTED HAMILTONIAN CIRCUIT : voir graphe hamiltonien
 - UNDIRECTED HAMILTONIAN CIRCUIT : voir graphe hamiltonien
- 0-1 INTEGER PROGRAMMING : voir optimisation linéaire en nombres entiers

graphe
hamiltonien
NP-complet

Quand y'en a plus...

3-SAT : satisfaction avec clause comportant 3 littéraux

- CHROMATIC NUMBER : coloration de graphe
 - CLIQUE COVER : partition en cliques
 - EXACT COVER : couverture exacte
 - MATCHING à 3 dimensions : appariement à 3 dimensions
 - STEINER TREE : voir arbre de Steiner
 - HITTING SET : ensemble intersectant
 - KNAPSACK : problème du sac à dos
 - JOB SEQUENCING : séquençage de tâches
 - PARTITION : problème de partition
 - MAX-CUT : problème de la coupe maximum

“Computers and Intractability : A Guide to the Theory of NP-Completeness” de Garey et Johnson, 1979 $\Rightarrow \geq 300$ problèmes NP-Completeness

A quoi ça sert ?

Proposition

*Les problèmes NP-complet sont de complexité "équivalente".
En particulier :*

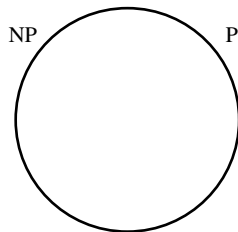
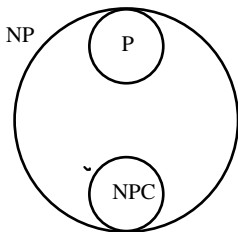
- ① *Si **un seul** problème NP-complet est polynomial
 $\Rightarrow NP = P$!*
- ② *Inversement, si un seul problème NP-complet n'est pas polynomial \Rightarrow tous les problèmes NP-complet aussi !*

Actuellement :

- Aucun algorithme polynomial n'a été trouvé pour un problème NP-complet
- L'impossibilité de trouver des algorithmes polynomiaux n'a pas été prouvée non plus.

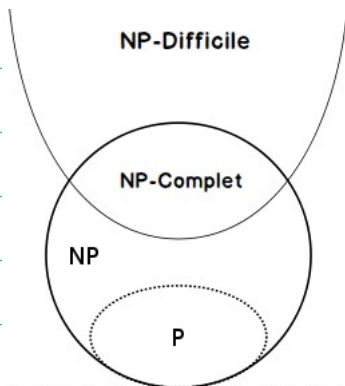
P vs NP

Quel est le bon schéma ?



Conjecture

$P \neq NP$



NP-Difficile

NP-Comple

NP

P

P ≠ NP

La grande question

P=NP ?

- Recherches innombrables sur le sujet depuis des dizaines d'années
- Fait partie des 7 problèmes du millénaire du Clay Mathematics (1 million à la clé)
- Les implications sont multiples et réelles ! Exemple : transactions bancaires cryptées sur le web (codage RSA)
- Gerhard J. Woeginger : liste avec 62 preuves de $P = NP$, 50 preuves de $P \neq NP$, 2 preuves que le résultat n'est pas prouvable, et une preuve qu'il n'est pas décidable.
- Meilleure borne inférieure pour SAT : $T \cdot S \geq \Omega(n^{2-o(1)})$

Concrètement

Que faire face à un problème inconnu ?

On observe notre problème P

- soit on pense que le problème est **facile** \Rightarrow on cherche un algorithme **correct** et polynomial (avec le meilleur temps possible !) qui le résout.
- soit on pense que le problème est **difficile** \Rightarrow on cherche à montrer qu'il est NP-complet, c-à-d
 - toute solution proposée peut être polynomialement **vérifiable** (appartenance à NP)
 - prendre un problème NP-complet et le **réduire** polynomialement à P

Que faire face à un problème NP-complet ?

Si P_b est NP-complet

- Premier constat : ne pas s'acharner à trouver un algorithme exact et rapide qui fonctionne sur toutes les instances
- Baisser ses exigences :
 - a) soit sur la **rapidité** d'exécution :
Je veux la réponse exacte, je suis prêt à attendre (si la taille est petite, ça ira)
 - b) soit sur l'**exactitude** de la réponse :
Je veux une réponse rapide, tant pis si elle n'est pas tout à fait exacte
 - c) soit sur l'**ensemble des instances** autorisées :
Je peux avoir un algorithme rapide et exact si mes données d'entrée sont "gentilles"

→ la coloration est NP-complet
mais si on se restreint à des cubes ou à des graphes de
degré ≤ 2 c'est polynomial.

Que faire face à un problème NPC ?

Retour sur le cas (c)

Je peux avoir un algorithme rapide et exact si mes données d'entrée sont "gentilles"

- NP-complet signifie qu'**au moins une instance** est "difficile" ...
- ...mais **pas forcément toutes** !
- Pour **certaines instances**, le problème (pourtant NP-complet) pourrait être résolu en temps polynomial

Exemple

- **MIN-COL** limité aux graphes de degré maximum 2
- **MIN-COL** limité aux arbres

MIN-COL limité aux graphes de degré maximum 2

MIN-COL limité aux graphes de degré maximum 2 :

Instance : un graphe G **de degré maximum 2**

Question : quel est le nombre minimum de couleurs nécessaires pour colorier G de façon propre ?

Exercice

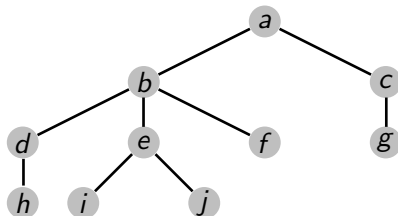
- Si G est connexe et de degré max. 2, à quoi ressemble G ?
- Si G n'est pas (forcément) connexe, à quoi ressemble-t-il ?
- Montrer que le problème **MIN-COL** limité aux graphes de degré max. 2 est dans P

MIN-COL limité aux arbres

MIN-COL :

Instance : un arbre G

Question : quel est le nombre minimum de couleurs nécessaires pour colorier G de façon propre ?



Exercise

Montrer que le problème **MIN-COL** limité aux arbres est dans P

Que faire face à un problème NPC ?

Retour sur le cas (b)

Je veux une réponse rapide, tant pis si elle n'est pas tout à fait exacte

- S'applique surtout aux problèmes d'optimisation
- Temps d'exécution exigé : **polynomial**
- Une possibilité : algorithmes d'**approximation**
 - algorithme polynomial
 - garantissant un résultat $\leq r \cdot c_{opt}$ (maximisation) ou $\geq r \cdot c_{opt}$ (minimisation)
 - pour **toutes les instances**
 - r est appelé le **ratio d'approximation**

nouveau Ce
 pl. des
 sac
 a' des
 ou
 par
 exemple

Conclusion

Pour l'examen: questions de cours

- Tout une théorie existe (seulement effleurée ici)
- Permet d'estimer la difficulté des problèmes (P vs NP)
- Si le problème est NP-complet, on adapte sa stratégie de résolution

Slides basés en partie sur ceux du DIU à Nantes.



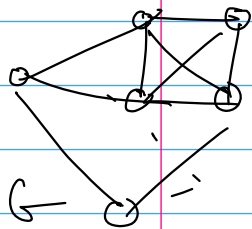
Retour sur MAX-CLIQUE

- Une clique est- ensemble de sommets sont- 2 à 2 reliés
- Réseau social \Rightarrow plus grde communauté tous connectés 2 à 2

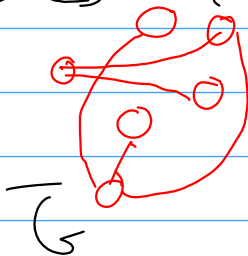
MAX
- INDEPENDANT

• PG complémentaire: plus gd ensemble tel que 2 éléments ne sont pas connectés \Rightarrow allocation de bandes de fréquence

MAX-CLIQUE sont équi-
-valents



on relie deux sommets
dans \bar{G} qui ne
sont pas
reliés
dans G



J'ai une arête dans G ssi
je n'ai pas une arête dans \bar{G}