Lecture 10

L’algorithme du simplexe est-il efficace ?

Le diamètre des polytopes

Cours Optimisation Discrète 5 mai 2011

Friedrich Eisenbrand
EPFL

Algorithmes en temps polynômial

Définition (Algorithme en temps polynômial)

Un algorithme s'exécute en temps polynômial s'il existe une constante k telle que le nombre d'opérations de base que l'algorithme effectue est majoré par $O(n^k)$, où n est la longueur de l'entrée de l'algorithme.

Exemple

Le tri fusion et le tri à bulles sont des algorithmes en temps polynômial. Mais le tri fusion est meilleur en pire cas, et aussi en pratique.

Exercice de 5 minutes

L'algorithme suivant est-il en temps polynômial ?
Entrée : Entier naturel k en notation unaire
$s = 2$
Répéter k fois : $s = s^2$
Supposer que s est stocké en notation binaire !

L'algorithme du simplexe est-il en temps polynômial ?

Nombre d'opérations arithmétiques

- Chaque itération de l'algorithme du simplexe nécessite un nombre polynômial d'opérations arithmétiques.
- On peut montrer que si les nombres rationnels sont sans facteurs communs (c'est-à-dire que leurs numérateur et dénominateur sont premiers entre eux) pendant l'élimination de Gauss-Jordan, alors tous les nombres sont de longueur polynômiale durant les étapes intermédiaires de l'élimination de Gauss-Jordan.
- Donc chaque itération s'exécute en temps polynômial.
- On ne sait pas s'il existe une variante de l'algorithme du simplexe qui n'effectue qu'un nombre polynômial (en n et m) d'opérations.
- But du cours d'aujourd'hui : comprendre le coeur de ce problème ouvert, ce qui est connu et ce qui doit encore être compris pour le résoudre.

Algorithme du simplexe primal vs. dual

Programme linéaire

$$\max\{c^T x \colon x \in \mathbb{R}^n, \ Ax \leq b\} \tag{47}$$

- L'approche avec les toits maintient une solution admissible du dual
$$\min\{b^T y \colon y \in \mathbb{R}^m, \ A^T y = c, \ y \geq 0\}$$
- Donc nous parlons de méthode du simplexe dual
- Nous exposons maintenant brièvement l'approche primale et les grandes lignes du grand mystère derrière la question de savoir si le simplexe est un algorithme en temps polynômial.

Algorithme du simplexe primal vs. dual

Principes

	Simplexe primal	Simplexe dual
maintient	x^* primal-admissible	z^* dual-admissible
essaie d'obtenir	faisabilité duale	faisabilité primale

***A* de plein rang-colonne**

Dans la suite, nous supposons de nouveau que $A \in \mathbb{R}^{m \times n}$ est de plein rang-colonne !

Bases admissibles et solutions de base admissibles

Définition

Base et solution de base

- $T \subseteq \{1, \ldots, m\}$ avec $A_T \in \mathbb{R}^{n \times n}$ inversible est appelée une base
- La solution x_T^* de $A_T\, x = b_T$ est la solution de base associée à T
- Si x_T^* est admissible (c-à-d $Ax_T^* \leq b$), alors T est une base admissible et x_T^* est une solution de base admissible
- Soit $j \in \{1, \ldots, n\} \setminus T$ un index

Algorithme primal du simplexe

- Le simplexe primal améliore itérativement une solution de base admissible x_T^* en en trouvant une de valeur objectif supérieure

Itération

- Calculer z^* solution de $zA_T = c$
- Si $z^* \geq 0$, alors renvoyer T et x_T^* comme base admissible optimale et solution optimale
- Sinon soit $i \in T$ avec $z^*_{f_T(i)} < 0$ et calculer d_{iT}, solution de $A_T x = -e_{f_T(i)}$
- Si $a_j d_{iT} \leq 0$ pour tous les $j \in \{1, \dots, n\} \setminus T$, alors affirmer que le PL est non borné.
- Sinon soit $J = \{j \colon a_j d_{iT} > 0\}$ et considérer

$$\min\{(b_j - a_j x_T^*)/a_j d_{iT} : j \in J\}$$

Soit $j^* \in J$ un index en lequel le minimum est atteint.
$T := T \setminus \{i\} \cup \{j^*\}$

Terminaison

Définition

Le système $Ax \leq b$ est primal non-dégénéré si pour chaque $x^* \in \mathbb{R}^n$ admissible on a :

$$|\{i \in \{1, \ldots, m\} \colon a_i x^* = b_i\}| \leq n.$$

Théorème

L'algorithme du simplexe primal termine si le système $Ax \leq b$ de (47) *est primal non-dégénéré*

Exercice

Démontrer le théorème ci-dessus et montrer que l'algorithme du simplexe est correct. *Indice : En cas de terminaison avec une solution optimale, quelle est la valeur objectif du z^* dual-admissible ?*

Interprétation combinatoire

Définition (Voisins)

Soient T et T' deux bases admissibles. T et T' sont voisins si $|T \cap T'| = n - 1$.

Exercice

Soient T et T' deux bases admissibles voisines l'une de l'autre. Montrer que

- x^*_T et $x^*_{T'}$ sont des sommets de $P = \{x \in \mathbb{R}^n \colon Ax \leq b\}$
- que l'enveloppe convexe $\mathrm{conv}\{x^*_T, x^*_{T'}\} = \{\lambda x^*_T + (1-\lambda)x^*_{T'} \colon \lambda \in [0,1]\}$ est une face de P

Interprétation combinatoire

Itération du simplexe primal (perspective combinatoire)

- $P = \{x \in \mathbb{R}^n \colon Ax \leq b\}$ définit un graphe $G_P = (V, E)$, où V est l'ensemble des bases admissibles et deux bases sont liées par une arête si elles sont voisines l'une de l'autre.
- L'algorithme du simplexe parcourt les arêtes du graphe, en améliorant chaque fois la fonction objectif, jusqu'à ce qu'il atteigne un sommet (base admissible) dont la valeur de l'objectif est au moins aussi grande que celles de tous ses voisins.

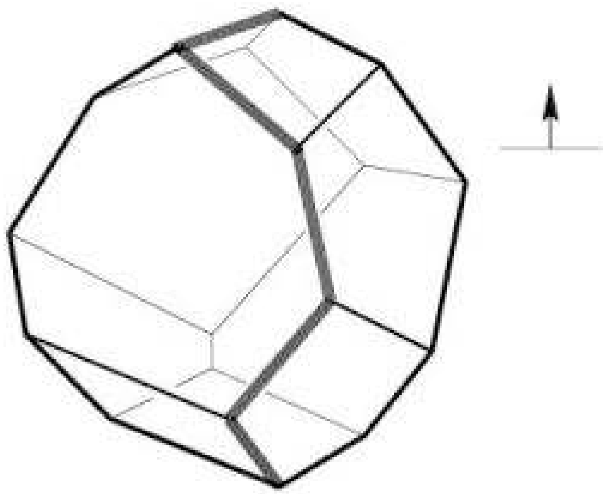


FIGURE: Dessin du chemin du simplexe (prise dans un article de Günter M. Ziegler)

Propriétés de G_P

Théorème

Le graphe G_P est connexe.

Démonstration.

- T et T' des bases admissibles. À montrer : il y a un chemin de T à T'
- Soit $c^T = \mathbf{1}^T A_{T'}$. $x^*_{T'}$ l'unique solution optimale de $\max\{c^T x : Ax \leq b\}$ (Pourquoi ?)
- Puisque le simplexe primal termine, il terminera en T' s'il a débuté en T.
- Donc G_P est connexe

$\square$

Propriétés de G_P

Théorème

Soient T et T' deux bases admissibles, il y a un chemin de T à T' tel que chaque sommet intermédiaire (base admissible) contienne $T \cap T'$.

Démonstration.

- Considérer $c^T = \mathbf{1}^T A_{T'} + M \cdot \mathbf{1}^T A_{T \cap T'}$, où M est un grand nombre positif.
- L'unique sol opt de $\max\{c^T x \colon Ax \leq b\}$ est $x^*_{T'}$ (pourquoi ?) et le simplexe termine en T' s'il a débuté en T.
- Supposer que B est une base qui ne contient pas $T \cap T'$
- Alors il existe $i \in T \cap T'$ tel que $a_i x^*_B \leq b_i - \gamma$ pour $\gamma > 0$
- Si M est suffisamment grand, $c^T x^*_T > c^T x^*_B$ ce qui entre en contradiction avec le fait que le simplexe ne fait qu'améliorer l'objectif

$\square$

Le mystère

Question

Y a-t-il toujours un chemin entre T et T' qui utilise un nombre polynômial (en n et m) d'arêtes ? En d'autres termes, y a-t-il une constante k telle qu'il existe une chemin qui joigne T et T' en n'utilisant que $k \cdot n^k \cdot m^k$ arêtes ?

Remarque

- C'est nécessaire pour que le simplexe puisse être un algorithme en temps polynômial.
- Nous allons maintenant prouver la meilleure borne connue.

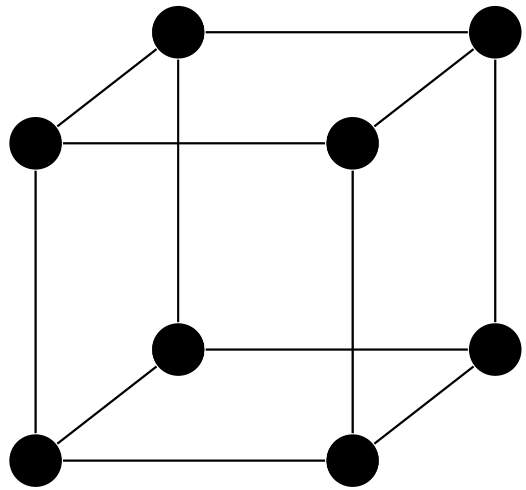
Diamètre

Définition (Diamètre d'un graphe)

Soit $G = (V, E)$ un graphe connexe. Le diamètre de G est le plus petit entier $\triangle$ tel que pour tous $u, v \in V$, il existe un chemin de longueur $\leq \triangle$ qui joigne u et v.

Diamètre d'un polyèdre

- $P = \{x \in \mathbb{R}^n \colon Ax \leq b\}$ un polyèdre non-vide
- $\mathrm{diam}(P)$ est le diamètre de G_P
- $\Delta(n, m)$ est le diamètre maximum du graphe G_P, où $P = \{x \in \mathbb{R}^n \colon Ax \leq b\}$, $A \in \mathbb{R}^{m \times n}$ de plein rang-colonne et $Ax \leq b$ (primal) non-dégénéré



Diamètre d'un polyèdre

Problème ouvert très en vue

$\Delta(n, m)$ est-il borné par un polynôme en n et m ?

- Conjecture de Hirsch : $\Delta(n, m) \leq m - n$
  - vrai pour $n \leq 3$ et $m - n \leq 5$ (Klee, Walkup 1967)
  - vrai pour de nombreuses classes de polytopes
  - faux pour les polyèdres non-bornés
- Nous allons montrer : $\Delta(n, m) \leq m^{1+\log n}$ (Kalai, Kleitman 1992)

Diamètre d'un polyèdre

Problème ouvert très en vue

$\Delta(n, m)$ est-il borné par un polynôme en n et m ?

- Conjecture de Hirsch : $\Delta(n, m) \leq m - n$
  - vrai pour $n \leq 3$ et $m - n \leq 5$ (Klee, Walkup 1967)
  - vrai pour de nombreuses classes de polytopes
  - faux pour les polyèdres non-bornés
  - **Également faux pour les polytopes (Santos 2010)**
- Nous allons montrer : $\Delta(n, m) \leq m^{1+\log n}$ (Kalai, Kleitman 1992)

Abstraction de la base

Notre abstraction de la base est un graphe $G = (V, E)$ où $V \subseteq \binom{[m]}{n}$ est tel que

- chaque paire $u, v \in V$ est connectée par un chemin de G dont les sommets contiennent tous $u \cap v$.

Abstraction de la base

Notre abstraction de la base est un graphe $G = (V, E)$ où $V \subseteq \binom{[m]}{n}$ est tel que

- chaque paire $u, v \in V$ est connectée par un chemin de G dont les sommets contiennent tous $u \cap v$.

Dictionnaire

Les éléments de $[m]$ sont appelés des symboles, n est la dimension.

abstraction de la base	polyèdre
symbole	facette
ensemble de symboles	face
ensemble de n symboles	sommet
$D(n, m)$	$\Delta(n, m)$

La borne et le prix

Kalai & Kleitman

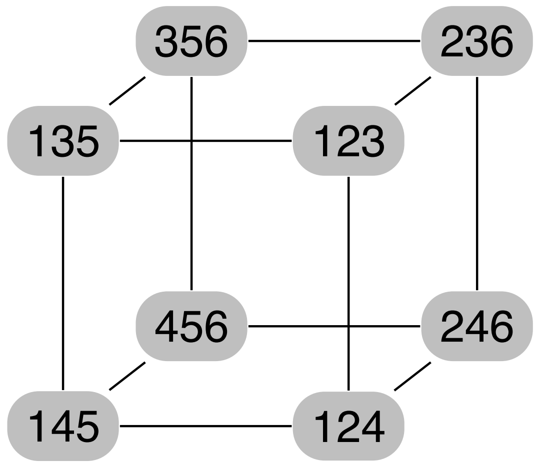
$D(n, m) \leq m^{1+\log n}$ (Kalai & Kleitman)

Prix de 1.000 Francs Suisses

Pour l'étudiant de mon cours (inscrit en Optimisation Discrète en 2011 à l'EPFL) qui prouvera une borne supérieure polynômiale sur $D(n, m)$ ou qui réfutera l'existence d'une telle borne pour l'abstraction de la base.

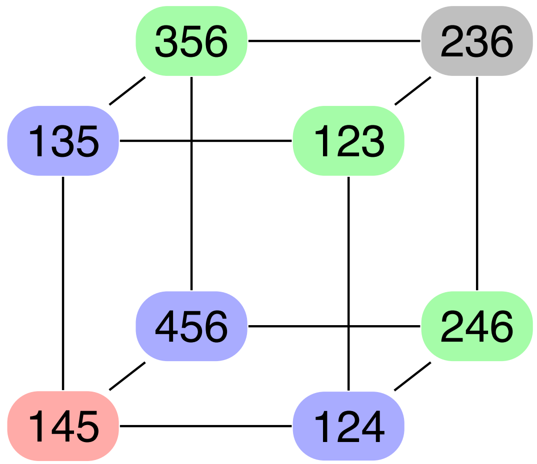
Familles de couches connectées

- Partitionner V en couches $\mathcal{L}_1, \ldots, \mathcal{L}_\ell$ telles que
  - chaque ensemble de $n-1$ ou moins symboles qui est couvert aux couches i et j, $i < j$, est aussi couvert aux couches intermédiaires.
- Une telle partition est une famille de couches connectées, ℓ est sa hauteur.
- Permet de partitionner une instance de l'abstraction de la base en utilisant des étiquettes de distances telles que $\ell = \mathrm{diam}(G) + 1$:



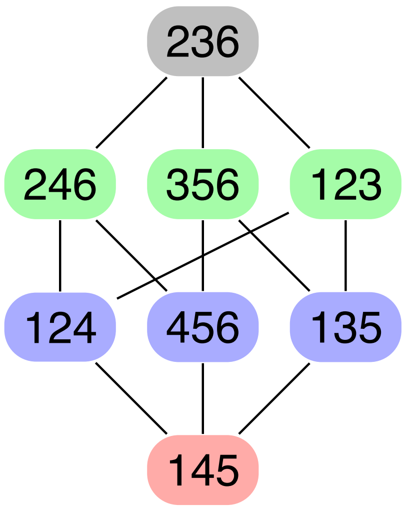
Familles de couches connectées

- Partitionner V en couches $\mathcal{L}_1, \ldots, \mathcal{L}_\ell$ telles que
  - chaque ensemble de $n-1$ ou moins symboles qui est couvert aux couches i et j, $i < j$, est aussi couvert aux couches intermédiaires.
- Une telle partition est une famille de couches connectées, ℓ est sa hauteur.
- Permet de partitionner une instance de l'abstraction de la base en utilisant des étiquettes de distances telles que $\ell = \mathrm{diam}(G) + 1$:



Familles de couches connectées

- Partitionner V en couches $\mathcal{L}_1, \ldots, \mathcal{L}_\ell$ telles que
  - chaque ensemble de $n-1$ ou moins symboles qui est couvert aux couches i et j, $i < j$, est aussi couvert aux couches intermédiaires.
- Une telle partition est une famille de couches connectées, ℓ est sa hauteur.
- Permet de partitionner une instance de l'abstraction de la base en utilisant des étiquettes de distances telles que $\ell = \mathrm{diam}(G) + 1$:



Équivalence

- Nous avons vu : Chaque abstraction de la base fournit une famille de couches connectées.
- Maintenant : Chaque famille de couches connectées fournit une instance de l'abstraction de la base.

236

246 356 123

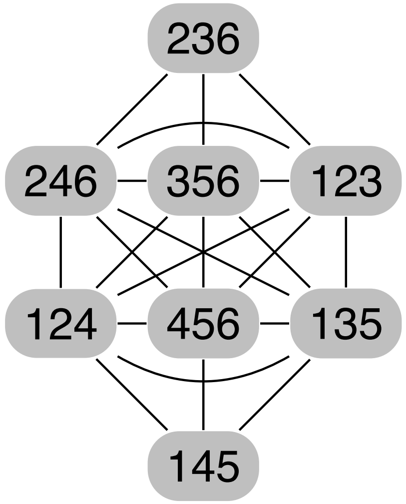
124 456 135

145

Soit $h(n, m)$ la hauteur maximale. Par cette équivalence, on obtient $h(n, m) = D(n, m) + 1$.

Équivalence

- Nous avons vu : Chaque abstraction de la base fournit une famille de couches connectées.
- Maintenant : Chaque famille de couches connectées fournit une instance de l'abstraction de la base.



Soit $h(n, m)$ la hauteur maximale. Par cette équivalence, on obtient $h(n, m) = D(n, m) + 1$.

Petites exemples

Définition

Une famille de couches connectées est une partition de $V \subseteq \binom{[m]}{n}$ en couches $\mathcal{L}_1, \ldots, \mathcal{L}_\ell$ telles que chaque ensemble de $n-1$ ou moins symboles qui est couvert aux couches i et j, $i < j$, est aussi couvert aux couches intermédiaires. Sa hauteur est ℓ.

Exercice de 5 minutes

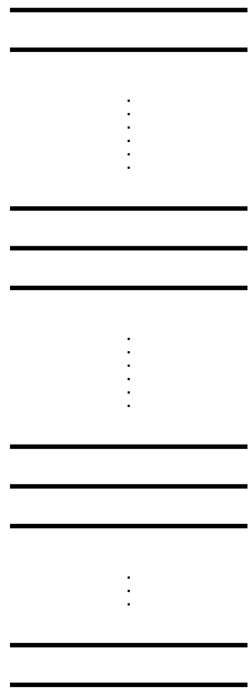
Trouver des familles de couches connectées telles que

- $n = 2$, $m = 4$, $\ell = 4$
- $n = 2$, $m = 6$, $\ell = 7$

Borne supérieure : Kalai & Kleitman

Théorème

$h(n,m) \leq m^{1+\log n}$



Démonstration.

Nous avons $h(n,m) \leq 2h(n, \lfloor m/2 \rfloor) + h(n-1, m-1)$.

$\square$

Borne supérieure : Kalai & Kleitman

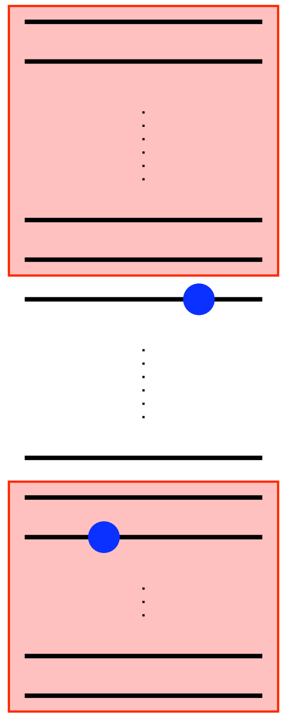
Théorème

$h(n, m) \leq m^{1+\log n}$

Démonstration.

Nous avons $h(n, m) \leq 2h(n, \lfloor m/2 \rfloor) + h(n-1, m-1)$.

$\square$



Borne supérieure : Kalai & Kleitman

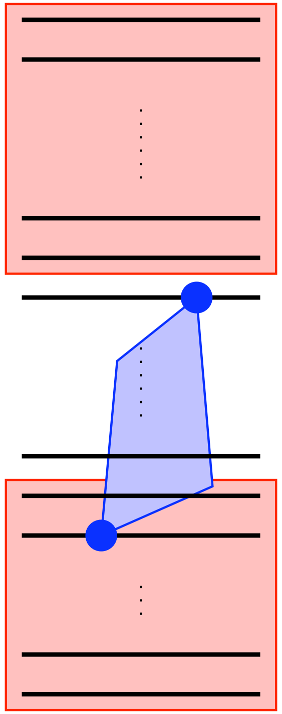
Théorème

$h(n, m) \leq m^{1+\log n}$

Démonstration.

Nous avons $h(n, m) \leq 2h(n, \lfloor m/2 \rfloor) + h(n-1, m-1)$.

$\square$



Borne supérieure : Kalai & Kleitman

Théorème

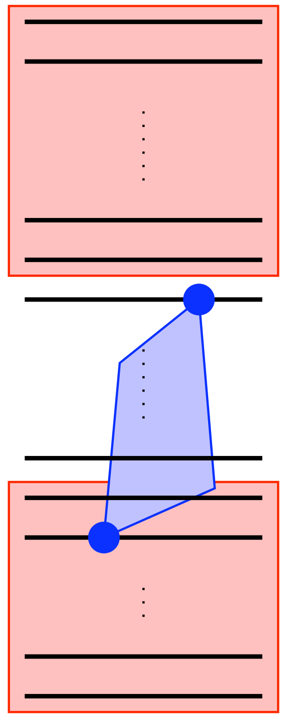
$h(n, m) \leq m^{1+\log n}$

Démonstration.

Nous avons $h(n, m) \leq 2h(n, \lfloor m/2 \rfloor) + h(n-1, m-1)$.
Résoudre par récurrence sur n et m :

$$\begin{aligned} h(n, m) &\leq 2h(n, \lfloor m/2 \rfloor) + h(n-1, m-1) \\ &\leq 2\sum_{i=2}^{n} h(i, \lfloor m/2 \rfloor) + h(1, m) \\ &\leq 2(n-1)(2n)^{\log m - 1} + m \\ &\leq (2n)^{\log m} \end{aligned}$$

$\square$



Toutefois, il existe un algorithme polynômial pour la programmation linéaire

Taille de l'entrée

- Taille de l'entier a : $\lceil \log(|a| + 1) \rceil$
- Taille du nombre rationnel p/q avec $\gcd(p, q) = 1$: $\text{taille}(p) + \text{taille}(q)$
- Taille de la matrice $A \in \mathbb{Q}^{m \times n}$: $m \cdot n \cdot \text{taille}(U)$, où U est un majorant des numérateurs et dénominateurs des entrées.
- Taille du vecteur $v \in \mathbb{Q}^n$: $n \cdot \text{taille}(U)$, où U est un majorant des numérateurs et dénominateurs des entrées.

Algorithme en temps polynômial pour la programmation linéaire

Théorème (Khachiyan 79)

Il existe un algorithme pour résoudre le programme linéaire

$$\max\{c^T x : x \in \mathbb{R}^n,\ Ax \leq b\}$$

qui effectue un nombre polynômial d'opérations arithmétiques sur des nombres rationnels de taille polynômiale. Polynômial signifie ici $O(n^k)$ pour une constante k, et n est un majorant des tailles de A, b et c.