

Réductions - Transformations

Idée

Soient A et B deux problèmes. Pour résoudre A, on va le *réduire* à B, c'est-à-dire qu'on va transformer le problème A en des problèmes du type B qui, une fois résolus et combinés, donneront la solution de A.

Définitions

Soient A et B deux problèmes.

A est **linéairement réductible** à B si l'existence d'un algorithme prenant un temps $\in O(t(n))$ pour résoudre chaque instance de B de taille n implique l'existence d'un algorithme prenant un temps $\in O(t(n))$ pour résoudre chaque instance de A de taille n. On note $A \leq^l B$.

Si $A \leq^l B$ et $B \leq^l A$, alors A est dit **linéairement équivalent** à B et on note $A =^l B$.

En d'autres termes, si $A \leq^l B$, et si on connaît un algorithme prenant un temps $\in O(t(n))$ pour résoudre chaque instance de B de taille n, alors on peut résoudre chaque instance I_A de A de taille n de la manière suivante :

1. Construire un nombre constant d'instances I_B^1, \dots, I_B^c de type B tel que
 - chaque instance I_B^i ($i=1, \dots, c$) est de taille $\leq n$
 - la construction de chaque instance I_B^i ($i=1, \dots, c$) se fait en temps $O(t(n))$Cette construction prend donc un temps $O(t(n))$
2. Résoudre chaque instance I_B^1, \dots, I_B^c de B
Cette résolution prend un temps $\in O(c t(n)) = O(t(n))$
3. Faire $O(t(n))$ opérations élémentaires pour combiner les résultats de I_B^1, \dots, I_B^c et déduire la solution de I_A .

Remarque

Si $t(n)$ est une fonction harmonieuse, alors on peut construire des instances I_B^i de taille $\in O(n)$ (au lieu de se limiter à une taille $\leq n$). En effet, chaque instance I_B^i aura alors une taille $\leq kn$, où k est une constante. On pourra donc résoudre les instances I_B^1, \dots, I_B^c de B en un temps $\in O(c t(kn)) = O(c c' t(n)) = O(t(n))$.

Exemple

C : calcul du carré d'un entier

M : multiplication de deux entiers

- Il est évident que $C \leq^l M$ puisque $x^2 = x \cdot x$
- Nous allons montrer que $M \leq^l C$ si on suppose que le temps de résolution du problème C est une fonction harmonieuse. La démonstration qui suit est basée sur l'égalité suivante :

$$x \cdot y = \frac{(x+y)^2 - (x-y)^2}{4}$$

Supposons que les entiers sont représentés à l'aide de vecteurs binaires et soit n le nombre de bits nécessaires au codage d'un entier. Notons $t(n)$ le temps nécessaire à la résolution du problème C. Tel que mentionné ci-dessus, nous allons supposer que $t(n)$ est harmonieuse.

Il est clair que $t(n) \geq n$ car il faut au moins lire l'entier. Pour multiplier deux entiers x et y de taille n (avec n suffisamment grand), on peut s'y prendre comme suit :

1. Calculer $x+y$ et $x-y$. Ces deux nouveaux entiers sont de taille au plus $n+1 \in O(n)$. Leur construction se fait facilement en un temps $\in O(n) \subseteq O(t(n))$. Les entiers $x+y$ et $x-y$ correspondent à I_C^1 et I_C^2 .
2. Calculer $(x+y)^2$ et $(x-y)^2$, ceci prend un temps $\leq 2t(n+1) \leq 2t(2n) \leq 2c t(n) \in O(t(n))$ (car t est harmonieuse)
3. Soustraire $(x+y)^2 - (x-y)^2$ et diviser le résultat par 4 (enlever 2 bits). Ceci se fait aisément en un temps $\in O(n) \subseteq O(t(n))$.

On déduit qu'on peut multiplier 2 entiers en temps $O(t(n))$, ce qui veut dire que $M \leq^l C$.

Autre exemple

Considérons les 5 problèmes suivants

MQ : multiplication de 2 matrices de taille $n \times n$

MT : multiplication de 2 matrices triangulaires supérieures de taille $n \times n$

MS : multiplication de 2 matrices symétriques de taille $n \times n$

IT : inversion d'une matrice triangulaire supérieure de taille $n \times n$

IT² : inversion d'une matrice triangulaire supérieure de taille $n \times n$, avec $n=2^k$ pour $k \in \mathbb{N}$

Nous noterons $t_{MQ}, t_{MT}, t_{MS}, t_{IT}, t_{IT^2}$ les fonctions représentant les temps nécessaires pour résoudre ces 5 problèmes. Les fonctions $t_{MQ}, t_{MT}, t_{MS}, t_{IT}, t_{IT^2}$ sont au moins quadratiques car on doit lire la donnée.

Nous allons montrer que si $t_{MT}, t_{MS}, t_{IT}, t_{IT^2}$ sont harmonieuses et si t_{MQ} est fortement quadratique, alors ces 5 problèmes sont linéairement équivalents.

Notons qu'on a bien évidemment $MT \leq^{\ell} MQ, MS \leq^{\ell} MQ$ et $IT^2 \leq^{\ell} IT$.

Propriété Si t_{MT} est harmonieuse, alors $MQ \leq^{\ell} MT$

Preuve

Remarquons tout d'abord que $3n \left\{ \begin{bmatrix} 0 & A & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & B \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & AB \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \right.$

On déduit que $t_{MQ}(n) \leq t_{MT}(3n) + cn^2$, le dernier terme est une borne supérieure sur le nombre d'opérations élémentaires nécessaires à la construction des matrices $3n \times 3n$ (avec c =constante).

Comme t_{MT} est au moins quadratique, il existe a et $n_0 \in \mathbb{N}$ tel que $t_{MT}(n) \geq an^2 \forall n \geq n_0$.

De plus, comme t_{MT} est harmonieuse, il existe b et $n_1 \in \mathbb{N}$ tel que $t_{MT}(3n) \leq bt_{MT}(n) \forall n \geq n_1$.

Soit $n_2 = \max\{n_0, n_1\}$. On a $t_{MQ}(n) \leq t_{MT}(3n) + cn^2 \leq bt_{MT}(n) + (c/a)t_{MT}(n) \forall n \geq n_2$, et donc $t_{MQ}(n) \in O(t_{MT}(n))$.

Propriété Si t_{MS} est harmonieuse, alors $MQ \leq^{\ell} MS$

Preuve

Par un raisonnement similaire à celui ci-dessus, et en remarquant que $2n \left\{ \begin{bmatrix} 0 & A \\ A^t & 0 \end{bmatrix} \begin{bmatrix} 0 & B^t \\ B & 0 \end{bmatrix} = \begin{bmatrix} AB & 0 \\ 0 & A^t B^t \end{bmatrix} \right.$,

on déduit que $t_{MQ}(n) \leq t_{MS}(2n) + cn^2 \in O(t_{MS}(n))$

Propriété Si t_{IT} est harmonieuse, alors $MQ \leq^{\ell} IT$

Preuve

Par un raisonnement similaire à celui ci-dessus, et en remarquant que $3n \left\{ \begin{bmatrix} I & A & 0 \\ 0 & I & B \\ 0 & 0 & I \end{bmatrix} \begin{bmatrix} I & -A & AB \\ 0 & I & -B \\ 0 & 0 & I \end{bmatrix} = \begin{bmatrix} I & 0 & 0 \\ 0 & I & 0 \\ 0 & 0 & I \end{bmatrix} \right.$,

on déduit que $t_{MQ}(n) \leq t_{IT}(3n) + cn^2 \in O(t_{IT}(n))$

Propriété Si t_{IT^2} est harmonieuse, alors $IT \leq^{\ell} IT^2$

Preuve

Remarquons tout d'abord que $2^{\lceil \log n \rceil} \left\{ \begin{bmatrix} A & 0 \\ 0 & I \end{bmatrix}^{-1} = \begin{bmatrix} A^{-1} & 0 \\ 0 & I \end{bmatrix} \right.$

Soit a une constante et n_0 un entier tel que

- $t_{IT^2}(n) \leq t_{IT^2}(n+1) \forall n \geq n_0$ (car t_{IT^2} est harmonieuse et donc éventuellement non-décroissante)
- $t_{IT^2}(2n) \leq a t_{IT^2}(n) \forall n \geq n_0$ tel que n est une puissance de 2 (car t_{IT^2} est harmonieuse)

(On suppose que t_{IT^2} est définie pour tout n ; lorsque n est une puissance de 2, $t_{IT^2}(n)$ est le temps pris pour inverser une matrice triangulaire supérieure de taille $n \times n$; lorsque n n'est pas une puissance de 2, $t_{IT^2}(n)$ n'a aucune signification particulière)

Soit $n \geq 2n_0$, et soit N la plus petite puissance de 2 supérieure ou égale à n . On a donc $N \geq n > N/2 \geq n_0$.

On a $t_{IT}(n) \leq t_{IT^2}(N) + cn^2 = t_{IT^2}(2N/2) + cn^2 \leq a t_{IT^2}(N/2) + cn^2 \leq a t_{IT^2}(n) + cn^2 \in O(t_{IT^2}(n))$.

Propriété Si t_{MQ} est fortement quadratique, alors $IT^2 \leq' MQ$

Preuve

Remarquons tout d'abord que $\begin{bmatrix} B & C \\ 0 & D \end{bmatrix}^{-1} = \begin{bmatrix} B^{-1} & -B^{-1}CD^{-1} \\ 0 & D^{-1} \end{bmatrix}$.

On déduit $t_{IT^2}(n) \leq 2t_{IT^2}(n/2) + 2t_{MQ}(n/2) + cn^2$.

On sait qu'il existe une constante a et un entier $n_0 \in \mathbb{N}$ tel que

- que $t_{MQ}(n) \geq an^2 \forall n \geq n_0$ (car t_{MQ} est au moins quadratique)
- $t_{MQ}(n) \geq 4t_{MQ}(n/2) \forall n \geq n_0$ qui est pair (car t_{MQ} est fortement quadratique).

On a donc $t_{IT^2}(n) \leq 2t_{IT^2}(n/2) + (1/2 + c/a)t_{MQ}(n) \forall n \geq n_0$ qui est une puissance de 2.

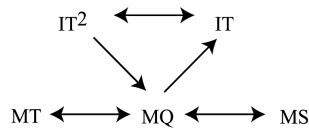
Soit n_1 la plus petite puissance de 2 supérieure ou égale à n_0 , et soit $b = \max \{t_{IT^2}(n_1)/t_{MQ}(n_1); 1+2c/a\}$.

On a $t_{IT^2}(n_1) \leq bt_{MQ}(n_1)$. Par récurrence, on a également $t_{IT^2}(n) \leq bt_{MQ}(n) \forall n \geq n_1$ qui est une puissance de 2.

En effet, $t_{IT^2}(n) \leq 2t_{IT^2}(n/2) + (\frac{1}{2} + \frac{c}{a})t_{MQ}(n) \leq 2bt_{MQ}(n/2) + \frac{b}{2}t_{MQ}(n) \leq \frac{b}{2}t_{MQ}(n) + \frac{b}{2}t_{MQ}(n) = bt_{MQ}(n)$.

On déduit que $t_{IT^2}(n) \in O(t_{MQ}(n)) \mid \exists k \in \mathbb{N}$ tel que $n=2^k$

En supposant que les fonctions t_{MT} , t_{MS} , t_{IT} , t_{IT^2} sont harmonieuses, et que t_{MQ} est fortement quadratique, nous avons démontré que les 5 problèmes sont linéairement équivalents, puisque on a



Définitions

Soient A et B deux problèmes.

A est **polynomialement réductible** à B s'il existe un algorithme polynomial pour résoudre chaque instance de A, en autant que soit comptée à coût unitaire chaque résolution d'une instance de B. On note $A \leq^p B$.

Si $A \leq^p B$ et $B \leq^p A$, alors A est dit **polynomialement équivalent** à B et on note $A =^p B$.

En d'autres termes, supposons que l'on dispose d'une *boîte noire* permettant de résoudre chaque instance de B. Si $A \leq^p B$, alors on peut résoudre A en faisant un nombre polynomial d'opérations élémentaires, chaque appel à la *boîte noire* étant compté comme une opération élémentaire.

Corollaire 1

Soit $t(n)$ le temps nécessaire pour résoudre une instance de B de taille n.

Si $A \leq^p B$, alors on peut résoudre chaque instance de A de taille n en un temps $\in O((1+t(p(n)))p(n))$, où $p(n)$ est un polynôme en n.

Corollaire 2

Si $A \leq^p B$, alors l'existence d'un algorithme polynomial pour résoudre B implique l'existence d'un algorithme polynomial pour résoudre A.

Définitions

Soient A et B deux problèmes.

A est **polynomialement transformable** en B si on peut ramener la résolution de chaque instance I_A de A en la construction et la résolution d'**UNE** instance I_B de B, la construction de I_B se faisant en temps polynomial.

On utilise la notation $A \infty B$.

En d'autres termes, $A \infty B$ signifie qu'on a $A \leq^p B$, et qu'on fait appel **UNE** seule fois à la *boîte noire*.

Quelques exemples

- Soit **HAM** le problème consistant à déterminer un cycle hamiltonien dans un graphe donné, s'il en existe un.
- Soit **HAMD** le problème consistant à déterminer si un graphe donné est hamiltonien.
- Étant donné un graphe G et une constante k , le problème **TSPD** consiste à déterminer s'il existe dans G un cycle hamiltonien de longueur inférieure ou égale à k .
- Notons **ϵ -rel-TSP** le problème consistant à déterminer un cycle hamiltonien C dans un graphe G donné, tel que la longueur de C est inférieure ou égale à $(1+\epsilon)L$, où L est la longueur du cycle hamiltonien le plus court dans G .

Théorème	HAMD $\stackrel{p}{=} \text{HAM}$
-----------------	-----------------------------------

Preuve

Montrons tout d'abord que HAMD \leq^p HAM, ce qui impliquera HAMD \leq^p HAM. Soit *Ham* une procédure qui reçoit un graphe G en input et qui retourne un cycle hamiltonien dans G si G est hamiltonien, et n'importe quoi d'autre si G n'est pas hamiltonien. On peut alors résoudre HAMD comme suit

Fonction *Hamd*(G)

Si *Ham*(G) est un cycle hamiltonien dans G alors retourner OUI ;
Sinon retourner NON.

On a aussi HAM \leq^p HAMD. En effet, on peut résoudre HAM comme suit

Fonction *Ham*($G=(V,E)$)

Si *Hamd*(G) = NON alors retourner « il n'existe pas de solution » ;

Sinon pour chaque arête $e \in E$ faire

Si *Hamd*($G'=(V,E-\{e\})$)=OUI alors poser $E:=E-\{e\}$;

Retourner E ; (l'ensemble des arêtes restantes induit un cycle hamiltonien)

Théorème	HAMD ∞ TSPD
-----------------	--------------------

Preuve

Étant donné un graphe $G=(V,E)$, notons H_G le graphe complet ayant V comme ensemble de sommets. La longueur d_{xy} d'une arête reliant x à y dans H_G est définie comme suit :

$$d_{xy} = \begin{cases} 1 & \text{si } \{x, y\} \in E \\ 2 & \text{sinon} \end{cases}$$

On peut alors résoudre HAMD en faisant appel à une fonction *Tspd* qui résout TSPD :

Fonction *Hamd*($G=(V,E)$)

Construire H_G ;

Retourner *Tspd*(H_G, n) ;

Théorème	HAMD ∞ ϵ -rel-TSP
-----------------	-----------------------------------

Preuve

Étant donné un graphe $G=(V,E)$, notons H_G le graphe complet ayant V comme ensemble de sommets. La longueur d_{xy} d'une arête reliant x à y dans H_G est définie comme suit :

$$d_{xy} = \begin{cases} 1 & \text{si } \{x, y\} \in E \\ 2 + \lfloor \epsilon |V| \rfloor & \text{sinon} \end{cases}$$

On peut alors résoudre HAMD en faisant appel à une procédure ϵ -relTSP qui résout ϵ -rel-TSP :

Fonction *Hamd*($G=(V,E)$)

Construire H_G ;

Si le cycle produit par ϵ -relTSP(H_G) est de longueur $\leq (1+\epsilon)|V|$ alors retourner OUI

Sinon retourner NON

En effet, si G contient un cycle hamiltonien, alors H_G contient un cycle de longueur $|V|$, et la fonction ϵ -relTSP produira donc un cycle de longueur au plus $(1+\epsilon)|V|$. Par contre, si G ne contient pas de cycle hamiltonien, ϵ -relTSP produira un cycle de longueur $\geq 2 + \lfloor \epsilon |V| \rfloor + |V| - 1 = |V| + (\lfloor \epsilon |V| \rfloor + 1) > |V| + \epsilon |V| = (1+\epsilon)|V|$.