

Algorithmes et Complexité des Problèmes de Satisfaction de Contraintes (cours n° 4)

Nicolas (Miki) Hermann
Manuel Bodirsky

LIX, École Polytechnique

`hermann@lix.polytechnique.fr`

Étudions la relation affine suivante :

$$[x + y + z = 1] = \{001, 010, 100, 111\} = S$$

Choisissons trois vecteurs $m = 010$, $m' = 100$, $m'' = 111$ et calculons la fonction **affinité**, parfois appelée **minorité** ou fonction de Mal'tsev

$$\text{aff}(m, m', m'') = (\text{aff}(m[1], m'[1], m''[1]), \dots, \text{aff}(m[3], m'[3], m''[3]))$$

définie par

$$\text{aff}(m, m', m'') = m + m' + m'' \bmod 2 = m - m' + m''$$

On constate que $\text{aff}(m, m', m'') \in S$. Ceci est vrai pour chaque triplet de vecteurs $m, m', m'' \in S$.

Definition

Soient $m, m', m'' \in \{0, 1\}^k$ trois vecteurs booléens d'arité k .

L'**affinité** ou **minorité** $\text{aff}(m, m', m'')$ est le vecteur

$$(\text{aff}(m[1], m'[1], m''[1]), \dots, \text{aff}(m[k], m'[k], m''[k]))$$

construit coordonnée par coordonnée avec la fonction booléenne **aff**.

Une relation booléenne $R \subseteq \{0, 1\}^k$ est **fermée** par affinité (ou minorité)

si pour chaque triplet de vecteurs $m, m', m'' \in R$ nous avons

$\text{aff}(m, m', m'') \in R$. Formellement :

$$\forall m \forall m' \forall m'' (m, m', m'' \in R \rightarrow \text{aff}(m, m', m'') \in R)$$

Remarque

Dans le cas affine on travaille toujours dans le corps $(\mathbb{Z}_2, +, *)$.

La propriété constatée dans l'exemple précédent n'est pas un hasard.

Theorem

Si φ est une formule affine alors l'ensemble de ses modèles $[\varphi]$ est fermé par affinité.

Démonstration.

Chaque formule affine correspond à un système d'équations linéaires $A\vec{x} = \vec{b}$ sur \mathbb{Z}_2 . Les solutions du système $A\vec{x} = \vec{b}$ constituent un espace affine \mathcal{A} , qui est lui-même l'espace vectoriel \mathcal{V} engendré par les solutions du système homogène sous-jacent $A\vec{x} = \vec{0}$, translaté par une solution \vec{a} du système $A\vec{x} = \vec{b}$. Formellement : $\mathcal{A} = \mathcal{V} + \vec{a}$. Chaque espace vectoriel est fermé par addition de deux vecteurs, i.e., $\vec{a}_1, \vec{a}_2 \in \mathcal{V}$ implique $\vec{a}_1 + \vec{a}_2 \in \mathcal{V}$. Par conséquent, chaque espace affine est fermé par addition de trois vecteurs : $\vec{a}, (\vec{a}_1 + \vec{a}), (\vec{a}_2 + \vec{a}) \in \mathcal{A}$ implique $(\vec{a}_1 + \vec{a}) + (\vec{a}_2 + \vec{a}) + \vec{a} = \vec{a}_1 + \vec{a}_2 + \vec{a} \in \mathcal{A}$. □

Question

Peut-on établir l'inverse du théorème précédent ?

Réponse

OUI, mais la réponse habituelle n'est pas constructive. En effet, nous avons le théorème suivant en algèbre linéaire.

Theorem

Si un ensemble de vecteurs $M \subseteq \mathbb{Z}_2^k$ d'arité k est fermé par addition alors M est un espace vectoriel.

Corollary

Si un ensemble de vecteurs $M \subseteq \mathbb{Z}_2^k$ d'arité k est fermé par affinité alors M est un espace affine.

Démonstration.

Il suffit de choisir un vecteur $m_* \in M$ et de construire l'ensemble de vecteurs $M_* = \{m - m_* \mid m \in M\} = \{m + m_* \mid m \in M\}$.

L'ensemble M est un espace affine si et seulement si M_* est un espace vectoriel. □

Remarque

La preuve du Corollaire n'est pas constructive et, par conséquent, n'engendre pas directement un algorithme. La réponse constructive correspond à la recherche d'une base d'un espace vectoriel. On ne fait pas d'usage de l'algorithme général, suivi par une transformation, comme dans les cas précédents, mais on construit directement le système linéaire affine $A\vec{x} = \vec{b}$. Néanmoins, il vaut mieux construire un système $(I \ B)\vec{x} = \vec{b}$, où I est la matrice d'identité. La matrice B est composée de lignes B_i et l'élément de la matrice B se trouvant à la ligne i et la colonne j est noté par B_i^j .

Construction

Soit $M \subseteq \{0, 1\}^k$ un ensemble de vecteurs booléens d'arité k . Il faut d'abord vérifier si la cardinalité $|M|$ est égale à une puissance de 2, sinon M ne peut pas être un espace affine sur \mathbb{Z}_2 . Dans le cas positif, le système $(I \ B)\vec{x} = \vec{b}$ aura $l = k - \log_2 |M|$ lignes. Donc, I est la matrice identité de taille $l \times l$ et B est une matrice de taille $l \times (k - l)$ sur \mathbb{Z}_2 . La i^{e} ligne du système $(I \ B)\vec{x} = \vec{b}$ est

$$x_i + B_i^1 x_{l+1} + \dots + B_i^{k-l} x_k = b_i$$

Algorithmme pour les formules affines

Pour chaque ligne $x_i + B_i^1 x_{l+1} + \dots + B_i^{k-l} x_k = b_i$, où $i = 1, \dots, l$, du système $(I \ B) \vec{x} = \vec{b}$ nous procédons de la manière suivante :

- 1 Pour chaque vecteur $m \in M$, substituer m aux variables \vec{x} , i.e., substituer $m[j]$ pour x_j , $j = 1, \dots, k$. On obtient alors un système d'équations

$$m[i] + B_i^1 m[l+1] + \dots + B_i^{k-l} m[k] = b_i \quad (1)$$

pour chaque $m \in M$, i.e., avec 2^{k-l} lignes, où $B_i = (B_i^1, \dots, B_i^{k-l})$ et b_i sont des variables.

- 2 Résoudre le système (1) pour déterminer les valeurs de la ligne B_i et de b_i .

Exemple

La relation $M = \{000, 111\}$ est affine, car

$000 + 000 + 111 = 111 + 111 + 111 = 111$ et

$000 + 000 + 000 = 000 + 111 + 111 = 000$. L'algorithme construit le système linéaire $(I \ B)(xyz)^T = \vec{b}$ avec 2 lignes et 3 colonnes :

$$\begin{array}{rcl} x & + & B_1^1 z = b_1 \\ & y & + B_2^1 z = b_2 \end{array}$$

Nous allons substituer les modèles de M aux variables du système précédent. La première équation donne $0 = b_1$ et $1 + B_1^1 = b_1$, ce qui implique que $B_1^1 = 1$. La deuxième équation donne $0 = b_2$ et $1 + B_2^1 = b_2$, ce qui implique que $B_2^1 = 1$. Alors le système recherché est

$$\begin{array}{rcl} x & + & z = 0 \\ & y & + z = 0 \end{array}$$

Question

Quelles sont les propriétés (de fermeture) satisfaites par les autres relations que nous avons vu pendant le Cours 2 ?

nae et la négation

Il nous reste deux relations à considérer :

$$\begin{aligned}nae &= \{001, 010, 011, 100, 101, 110\} \\1\text{-in-3} &= \{001, 010, 100\}\end{aligned}$$

Pour la relation *nae*, choisissons un vecteur $m = 010$ et calculons sa **négation**

$$\neg m = (\neg m[1], \neg m[2], \neg m[3])$$

coordonnée par coordonnée. On obtient $\neg m = 101 \in nae$. Ceci est vrai pour chaque vecteur $m \in nae$.

Résistance de 1-in-3

Par contre, la relation 1-in-3 résiste à chaque tentative de caractérisation.

Definition

Soit $m \in \{0, 1\}^k$ un vecteur booléen d'arité k . La **négation** $\neg m$ est le vecteur

$$(\neg m[1], \dots, \neg m[k])$$

construit coordonnée par coordonnée avec la fonction booléenne \neg . Une relation booléenne $R \subseteq \{0, 1\}^k$ est **fermée** par négation si pour chaque vecteur $m \in R$ nous avons $\neg m \in R$. Formellement :

$$\forall m (m \in R \rightarrow \neg m \in R)$$

Definition

Une relation $R \subseteq \{0, 1\}^k$ est **complémentive** si elle est fermée par négation.

Exemple

La relation $nae = \{001, 010, 100, 110, 101, 011\}$ est complémentative. Par contre,

- elle n'est pas Horn, car $001 \wedge 010 = 000 \notin nae$;
- elle n'est pas dual Horn, car $010 \vee 101 = 111 \notin nae$;
- elle n'est pas bijonctive, car $\text{maj}(001, 010, 100) = 000 \notin nae$;
- elle n'est pas affine car $001 + 010 + 100 = 111 \notin nae$;
- elle n'est ni 0-valide, ni 1-valide, car $000 \notin nae$ et $111 \notin nae$.

- 1 Par quelles fonctions booléennes mentionnées auparavant la relation $R_1 = \{001, 010, 101, 110\}$ est-elle fermée ?
- 2 Montrez que la relation $R_2 = \{011, 100, 101, 110, 111\}$ est fermée par implication et majorité.

Fermeture en général

La notion de **fermeture** des relations a été conçue de façon générale.

Definition

Soit $f: D^p \rightarrow D$ une fonction d'arité p . Une relation $R \subseteq D^k$ d'arité k est **fermée** par la fonction f (on dit aussi que f est un **polymorphisme** de R) si pour chaque choix de p vecteurs $m_1, \dots, m_p \in R$, pas nécessairement distincts, nous avons

$$(f(m_1[1], \dots, m_p[1]), \dots, f(m_1[k], \dots, m_p[k])) \in R .$$

Autrement dit, le nouveau vecteur construit coordonnée par coordonnée à partir d'un choix de vecteurs m_1, \dots, m_p par la fonction f appartient à la relation R .

Attention

Les arités de la fonction f et de la relation R sont différentes et perpendiculaires ! Visualisez les vecteurs m_1, \dots, m_p en forme de matrice de taille $p \times k$ et appliquez la fonction f par colonnes.

$$\begin{array}{rcccl} & & f & \cdots & f \\ & & \downarrow & & \downarrow \\ m_1 & = & (m_1[1], & \dots, & m_1[k]) \in R \\ \vdots & & \vdots & & \vdots \\ m_p & = & (m_p[1], & \dots, & m_p[k]) \in R \\ & & \parallel & & \parallel \\ f(m^\perp) & = & (m[1], & \dots, & m[k]) \in R \end{array}$$

Soit $R \subseteq D^k$ une relation. Nous allons nous intéresser à l'ensemble de **toutes** les fonctions f pour lesquelles la relation R est fermée. Ceci sera la **caractérisation** de la relation R .

Definition

Soit R une relation et S un ensemble de relations pas forcément de même arité.

- 1 **Pol R** est l'ensemble de toutes les fonctions qui sont des **polymorphismes** de R .
- 2 **Pol S** est l'ensemble de toutes les fonctions qui sont des **polymorphismes** pour **chaque** relation $R \in S$.

... et si on retourne la caractérisation ?

Soit B un ensemble de fonctions, pas forcément de la même arité. Nous nous intéressons à l'ensemble de toutes les relations fermées par les fonctions de B .

Definition

Soit B un ensemble de fonctions, pas nécessairement de la même arité. L'ensemble d'**invariants** $\text{Inv } B$ contient toutes les relations fermées par chaque fonction $f \in B$.

Attention

L'ensemble B n'est pas forcément fini.

Nous avons identifié deux problèmes de caractérisation de relations booléennes sur les transparents précédents.

Question 1

Etant donné un ensemble de relations booléennes S , quel est l'ensemble de polymorphismes $\text{Pol } S$?

Question 2

Etant donné un ensemble de fonctions booléennes B , quel est l'ensemble d'invariants $\text{Inv } B$?

Réponses

Pour pouvoir donner une réponse adéquate à ces questions, il nous faut étudier les ensembles de fonctions booléennes.

Si nous avons deux fonctions booléennes

$$bor_0(x, y) = (x \vee y) \quad \text{et} \quad not(x) = \neg x$$

nous pouvons construire une nouvelle fonction

$$bor_1(x, y) = (x \vee \neg y)$$

par la **composition** $bor_0(x, not(y))$.

Ainsi, nous pouvons construire la fonction **majorité** à partir de la **conjonction** $and(x, y) = (x \wedge y)$ et de la **disjonction** $or_0(x, y, z) = (x \vee y \vee z)$:

$$\begin{aligned} \text{maj}(x, y, z) &= or_0(\text{and}(x, y), \text{and}(y, z), \text{and}(z, x)) \\ &= (x \wedge y) \vee (y \wedge z) \vee (z \wedge x) \end{aligned}$$

Exercice 8

- 1 Construisez la fonction

$$\text{aff}(x, y, z) = x + y + z \pmod{2}$$

à partir des fonctions $\text{and}(x, y) = (x \wedge y)$ et $\text{not}(x) = \neg x$.

- 2 Construisez la fonction $\text{and}(x, y)$ à partir des fonctions $\text{bor}_0(x, y) = (x \vee y)$ et $\text{not}(x)$.
- 3 Construisez la fonction $\text{bor}_0(x, y)$ à partir de $\text{aff}(x, y, z)$ et $\text{and}(x, y)$.

Definition

Soit B un ensemble de fonctions pas forcément de même arité.
L'ensemble $[B]$ contient toutes les fonctions construites à partir de celles de B . L'ensemble $[B]$ est construit par **saturation** :

Introduction : Si $f(\vec{x}) \in B$ alors $f(\vec{x}) \in [B]$.

Permutation : Si $f(x_1, \dots, x_k) \in [B]$ et π est une permutation de $\{1, \dots, k\}$, alors nous avons $f(x_{\pi(1)}, \dots, x_{\pi(k)}) \in [B]$.

Diagonalisation : Si $f(x_1, \dots, x_{k-1}, x_k) \in [B]$ et
 $f'(x_1, \dots, x_{k-1}) = f(x_1, \dots, x_{k-1}, x_{k-1})$, alors
 $f'(x_1, \dots, x_{k-1}) \in [B]$.

Composition : Si $f(\vec{x}, y) \in [B]$ et $g(\vec{z}) \in [B]$, alors $f(\vec{x}, g(\vec{z})) \in [B]$.

Cylindrification : Si $f(\vec{x}) \in [B]$ alors $f'(\vec{x}, y) = f(\vec{x}) \in [B]$.

La dernière règle peut être remplacée par une autre, plus simple, de sorte que nous avons :

Introduction : Si $f(\vec{x}) \in B$ alors $f(\vec{x}) \in [B]$.

Permutation : Si $f(x_1, \dots, x_k) \in [B]$ et π est une permutation de $\{1, \dots, k\}$, alors nous avons $f(x_{\pi(1)}, \dots, x_{\pi(k)}) \in [B]$.

Diagonalisation : Si $f(x_1, \dots, x_{k-1}, x_k) \in [B]$ et $f'(x_1, \dots, x_{k-1}) = f(x_1, \dots, x_{k-1}, x_{k-1})$, alors $f'(x_1, \dots, x_{k-1}) \in [B]$.

Composition : Si $f(\vec{x}, y) \in [B]$ et $g(\vec{z}) \in [B]$, alors $f(\vec{x}, g(\vec{z})) \in [B]$.

Projection : La fonction $pr_k^m(x_1, \dots, x_m, \dots, x_k) = x_m$ appartient à $[B]$ pour chaque k et $m = 1, \dots, k$.

Definition

Si $f \in [B]$, on dit que l'ensemble de fonctions B **construit** la fonction f .

Definition

Soit B un ensemble de fonctions. L'ensemble saturé de fonctions $[B]$ s'appelle un **clone**.

Attention

Ne pas confondre $\langle B \rangle$ et $[B]$.

Propriétés de clones

Les ensembles de fonctions B et leurs clones $[B]$ satisfont les quatre propriétés suivantes :

- 1 $B \subseteq [B]$
- 2 $B \subseteq B'$ implique que $[B] \subseteq [B']$
- 3 $[[B]] = [B]$

Remarque

Les mêmes identités sont satisfaites aussi par les ensembles de relations S et leurs co-clones $\langle S \rangle$, i.e.,

- 1 $S \subseteq \langle S \rangle$
- 2 $S \subseteq S'$ implique que $\langle S \rangle \subseteq \langle S' \rangle$
- 3 $\langle \langle S \rangle \rangle = \langle S \rangle$

Comment classifier les clones ?

Remarque

Pour chaque ensemble de fonctions B il existe un clone $[B]$, mais deux ensembles B et B' de fonctions différentes peuvent engendrer le même clone $[B] = [B']$. Pour pouvoir classifier les clones, nous avons d'abord besoin de quelques structures algébriques supplémentaires.

Definition

Une relation binaire $\leq \subseteq A \times A$ sur un ensemble A s'appelle un **ordre partiel** si elle satisfait les conditions suivantes pour chaque triplet d'éléments $a, b, c \in A$:

Reflexivité : $a \leq a$

Antisymétrie : $a \leq b$ et $b \leq a$ implique $a = b$

Transitivité : $a \leq b$ et $b \leq c$ implique $a \leq c$

Definition

Un ordre partiel \leq sur un ensemble A s'appelle un **ordre de treillis** s'il satisfait les deux conditions supplémentaires :

- 4 Pour chaque $a, b \in A$ il existe un $c \in A$, tel que $c \leq a$ et $c \leq b$, et pour chaque $d \in A$ les relations $d \leq a$ et $d \leq b$ impliquent $d \leq c$. L'unique élément c s'appelle l'**infimum** de a et b , noté par $a \sqcap b$.
- 5 Pour chaque $a, b \in A$ il existe un $c \in A$, tel que $a \leq c$ et $b \leq c$, et pour chaque $d \in A$ les relations $a \leq d$ et $b \leq d$ impliquent $c \leq d$. L'unique élément c s'appelle le **suprênum** de a et b , noté par $a \sqcup b$.
- 6 La structure (A, \sqcup, \sqcap) s'appelle un **treillis**.

C'est tout pour aujourd'hui.
Avez-vous des questions ?