

# Algorithmes et Complexité des Problèmes de Satisfaction de Contraintes (cours n° 8)

**Nicolas (Miki) Hermann**

LIX, École Polytechnique

`hermann@lix.polytechnique.fr`

## Question 1

Quid des CSP sur les domaines finis  $D = \{0, \dots, n - 1\}$  avec  $|D| > 2$ ?

## Réponse

C'est un vaste chantier très peu exploré, mais un sujet difficile.

## Question 2

Qu'est-ce que reste et qu'est-ce que change par rapport aux CSP booléennes ?

## Réponse

La correspondance de Galois et les égalités  $\text{Inv Pol } S = \langle S \rangle$  et  $\text{Pol Inv } F = [F]$  restent, mais à part cela, plus grand chose ne se transmet des CSP booléens aux CSP sur les domaines finis.

Le treillis de Post est **infini**, mais **dénombrable**. Par contre, l'équivalent du treillis de Post pour les domaines de cardinalité  $n > 2$  sont **non-dénombrables**. Voici la preuve pour  $n = 3$ , dont la généralisation aux cardinalités supérieures est évidente.

## Lemma

Soit  $D = \{0, 1, 2\}$ . Pour chaque  $k \geq 1$ , soit  $f_k$  la fonction d'arité  $k$  sur  $D$  telle que

$$f_k(a_1, \dots, a_k) = \begin{cases} 1 & \text{si } \exists i(a_i = 1) \wedge \forall j(j \neq i \rightarrow a_j = 0), \\ 2 & \text{sinon.} \end{cases}$$

Pour chaque  $p \geq 1$ , soit  $R_p$  la relation d'arité  $p$  sur  $D$  telle que

$$R_p = \{(a_1, \dots, a_p) \in D^p \mid \exists i(a_i = 1) \wedge \forall j(j \neq i \rightarrow a_j = 0)\} \\ \cup \{(a_1, \dots, a_p) \in D^p \mid \exists i(a_i = 2)\}$$

Alors,  $f_k \in \text{Pol } R_p$  si et seulement si  $k \neq p$ .

## Démonstration.

Si  $k = p$ , considérons la relation  $M$  d'arité et cardinalité  $k$  qui correspond aux lignes de la matrice d'identité  $I_k$ . Il est clair que  $M \subseteq R_k$ , mais  $f_k(M) \notin R_k$ .

Si  $k \neq p$ , soit  $M$  une relation arbitraire sur  $D$  d'arité  $p$  et de cardinalité  $k$ . Si l'un des vecteurs  $m_1, \dots, m_k \in M$  contient la valeur  $2$ , alors le vecteur  $f_k(m_1, \dots, m_k)$  contient aussi la valeur  $2$  et par conséquent  $f_k(m_1, \dots, m_k) \notin R_p$ . Supposons que chacun des vecteurs  $m_1, \dots, m_k \in M$  ne contient que des  $0$  et  $1$ . Si  $\{m_1, \dots, m_k\} \subseteq R_p$  alors le vecteur  $(m_1[j], \dots, m_k[j])$  contient exactement une valeur  $1$  et les autres sont des  $0$ , pour chaque  $j = 1, \dots, p$ . Étant donné que  $k \neq p$ , il existe un vecteur  $m_i \in M$  qui contient soit plusieurs valeurs  $1$ , soit il n'en contient aucun (vecteur  $0 \cdots 0$ ). Ceci implique qu'une valeur de  $f_k(m_1, \dots, m_k)$  est égale à  $2$ . Par conséquent  $f_k(M) \notin R_p$ .  $\square$

# Treillis non-dénombrable

## Théorème

Le treillis de clones sur le domaine  $D = \{0, 1, 2\}$  est **non-dénombrable**.

## Démonstration.

Soient  $f_k$  la fonction et  $R_p$  la relation définies dans le Lemme précédent. Pour chaque  $I \subseteq \mathbb{N}$ , soit  $C_I = [F_I]$  le clone engendré par l'ensemble de fonctions  $F_I = \{f_k \mid k \in I\}$ . Alors nous avons  $f_k \in C_I$  si et seulement si  $k \in I$ . L'une des implications est triviale. Pour l'autre, supposons que  $k \notin I$ . Alors pour chaque  $f \in [F_I]$  nous avons  $f(R_k) \subseteq R_k$ . Par conséquent,  $f_k \notin C_I$ . Donc, pour chaque paire de sous-ensembles  $I, J \subseteq \mathbb{N}$  telle que  $I \neq J$ , nous avons  $C_I \neq C_J$ . Etant donné qu'il y a un nombre **non-dénombrable** sous-ensembles de  $\mathbb{N}$ , il existe un nombre **non-dénombrable** de clones sur le domaine  $D = \{0, 1, 2\}$ .  $\square$

## Remarque

Malgré ce résultat, nous pouvons toujours espérer d'avoir une caractérisation par des bases finies, mais **il y a pire**.

## Théorème

Soit  $D$  un domaine de cardinalité  $|D| > 2$ . Il existe des clones de fonctions sur  $D$  ne possédant pas de base finie.

## Démonstration.

Soit  $f_i$  la fonction définie dans le Lemme précédent et

$$F = \{f_i \mid i \in \mathbb{N}^{++}\}$$

où  $\mathbb{N}^{++} = \mathbb{N} \setminus \{0, 1\}$ . Donc  $F$  ne contient aucune fonction unaire ni constante. Nous allons démontrer que l'ensemble infini  $F$  est la base du clone  $[F]$ .

Soit  $h(x_1, \dots, x_r) = f_k(\varphi_1, \dots, \varphi_k)$  une nouvelle fonction  $h \in [F]$  construite à partir des fonctions  $F$ . ... / ...

Démonstration (cont).

Rappelons que  $h(x_1, \dots, x_r) = f_k(\varphi_1, \dots, \varphi_k)$ ,  $k \geq 2$  et

$$f_k(a_1, \dots, a_k) = \begin{cases} 1 & \text{si } \exists i(a_i = 1) \wedge \forall j(j \neq i \rightarrow a_j = 0), \\ 2 & \text{sinon.} \end{cases}$$

Si au moins **deux** formules  $\varphi_i$  ne sont pas des variables, alors  $h \equiv 2$ , car il existe deux indices  $i \neq j$  telles que  $\varphi_i, \varphi_j \in \{1, 2\}$ . Donc  $h \notin F$ .

Si **une seule** des formules  $\varphi_i$  ne pas une variable et  $k \geq 2$ , il existe  $j \neq i$  avec  $\varphi_j = y_j$  où  $y_j \in \{x_1, \dots, x_r\}$ . En substituant  $y_j = 1$  et  $x = 0$  pour chaque variable  $x \in \{x_1, \dots, x_r\} \setminus \{y_j\}$  dans  $h(x_1, \dots, x_r)$ , cette fonction prendra la valeur **2**. Par conséquent  $h \notin F$ .

Si **toutes** les formules  $\varphi_i$  sont des variables et  $k > r$ , il existe deux indices  $i \neq j$  telles que  $\varphi_i = \varphi_j = y$  pour  $y \in \{x_1, \dots, x_r\}$ . En substituant  $y = 1$  et  $x = 0$  pour chaque variable  $x \in \{x_1, \dots, x_r\} \setminus \{y\}$ , la fonction  $h(x_1, \dots, x_r)$  prendra la valeur **2**. Par conséquent  $h \notin F$ .      ... / ...

## Démonstration.

Nous venons de prouver que nous ne pouvons jamais construire d'autres fonctions  $f_i$  par composition et identification de variables à partir d'un sousensemble de fonctions  $F$ . Par conséquent l'ensemble infinie de fonctions  $F$  est la base du clone  $[F]$ .  $\square$

## Conséquence

Si  $S \subseteq D^k$  est une relation sur un domaine non-booléen et  $\text{Pol } S$  est un clone avec une base infinie, on n'a **pas de caractérisation finie** pour  $S$ .

## Remarque

Nous pouvons espérer encore d'avoir une possibilité de caractérisation avec des bases infinies en les schématisant, mais **il y a encore pire**.

## Théorème

Soit  $D$  un domaine de cardinalité  $|D| > 2$ . Il existe des clones de fonctions sur  $D$  ne possédant pas de base.

## Démonstration.

Soit  $D = \{0, 1, 2\}$ . Soit  $f_0 = 2$  et pour chaque  $k \geq 1$ , soit  $f_k$  la fonction d'arité  $k$  sur  $D$  telle que

$$f_k(a_1, \dots, a_k) = \begin{cases} 1 & \text{si } a_1 = \dots = a_k = 0, \\ 2 & \text{sinon.} \end{cases}$$

Soit  $F = \{f_i \mid i \in \mathbb{N}\}$ . Nous ne pouvons jamais obtenir une autre fonction  $f_i$  par composition à partir d'un sousensemble de fonctions  $F$ , car chaque **composition** de fonctions  $F$  construit la fonction **constante** égale à  $2$ . Par contre, à partir de la fonction  $f_i$  on obtient toutes les fonctions  $f_j$  pour  $j < i$  par identification de variables.  $\dots / \dots$

## Démonstration.

Supposons que le clone  $[F]$  possède une base. Alors cette base contient une fonction  $g$  obtenue à partir de la fonction  $f_{k_0} \in F$  avec l'indice  $k_0$  minimale parmi toutes les fonctions dans la base.

Deux cas sont possibles :

- 1 La base contient une autre fonction  $g'$ . Cette fonction a été construite à partir de la fonction  $f_{k_1} \in F$  où  $k_1 > k_0$ . Or  $f_{k_0}$  peut être construite à partir de  $f_{k_1}$  par identification de variables. Par conséquent, la fonction  $g$  s'exprime en fonction de  $g'$ , ce qui contredit la définition de la base.
- 2 La base est composé de la seule fonction  $g$ . Dans ce cas, aucune fonction  $f_k$  pour  $k > k_0$  ne peut être construite à partir de la fonction  $g$ , puisque chaque composition de la fonction  $f_{k_0}$  avec elle-même construit la fonction constante égale à 2, ce qui aboutit à nouveaux à une contradiction.



## Hypothèse

Les clones utilisés pour la caractérisation de la frontière entre les cas polynomiaux et NP-complets possèdent-ils tous une base finie ?

# Clones minimaux non-triviaux

Peut-être qu'il ne nous faut pas connaître tous les clones, mais uniquement le clone trivial  $I_2$  et les clones minimaux non-triviaux.

Théorème de Rosenberg, 1983

Soit  $D$  un domaine fini de cardinalité  $k$ . Le nombre de clones minimaux non-triviaux est fini pour chaque  $k \geq 3$ .

Nombre de clones minimaux non-triviaux

Néanmoins, le nombre de clones croît très vite.

- Pour  $k = 2$  il y a 7 clones minimaux non-triviaux  $I_0, I_1, N_2, E_2, V_2, L_2$  et  $D_2$ .
- Pour  $k = 3$  Csákány a énuméré tous les clones : il y en a 84, dont 24 principaux et le reste des conjugués !
- Pour  $k \geq 4$  seulement une caractérisation très sommaire est connue.

Pour  $k \geq 3$ , les clones minimaux non-triviaux ne suffisent pas pour la classification en complexité.

## Exemple

Soit  $D = \{r, g, b\}$  et  $\text{Perm}$  l'ensemble de toutes les permutations sur  $D$ . Il est clair que  $\text{Perm}$  est un clone, car les projections sont des permutations et la composition de permutations est une permutation. Le clone  $\text{Perm}$  n'est pas un clone minimal non-trivial (Csákány).

La relation  $3col = \{rg, rb, gr, gb, br, bg\}$  appartient à  $\text{Inv}(\text{Perm})$ , car l'inclusion  $\pi(3col) \subseteq 3col$  est valide pour chaque permutation  $\pi \in \text{Perm}$ . Par conséquent,  $\text{Perm}$  caractérise des CSP NP-complets.

## Avantage

Le clone  $\text{Perm}$  a une base finie par les fonctions  $x + 1 \pmod{3}$  et  $\{0 \mapsto 1, 1 \mapsto 0, 2 \mapsto 2\}$ . La structure du treillis entre  $\text{Perm}$  et le clone  $\Omega_3$  de toutes les fonctions sur  $D$  avec  $|D| = 3$  est connue, d'autant plus que ce sous-treillis est fini.

## Inconvénient

Ce n'est qu'une toute petite partie du treillis.

A la fin des années 90, Feder et Vardi ont lancé le défi suivant pour prouver ou réfuter l'hypothèse suivante :

## Hypothèse

Soit  $D$  un domaine fini. Pour chaque ensemble de relations  $S$  sur  $D$ , le problème  $\text{CSP}(S)$  est soit NP-complet, soit décidable en temps polynomial.

## Situation de l'hypothèse

- $|D| = 2$  : Résolu par le Théorème de Schaefer (Théorème dichotomique). Réponse positive.
- $|D| = 3$  : Bulatov a présenté une preuve compliquée en 2002 avec 10 cas polynomiaux, le reste étant NP-complet.
- $|D| > 3$  : Quelques travaux de Jeavons *et co.* sur les propriétés de fermeture, mais en général très peu de connaissances.

## Definition

Soit  $f: D^k \rightarrow D$  une fonction d'arité  $k$  sur le domaine  $D$ . La fonction  $f$  est une opération

- de **demi-treillis** si  $f$  est binaire ( $k = 2$ ) et elle satisfait les trois identités suivantes :

$$\text{idempotence : } f(x, x) = x$$

$$\text{commutativité : } f(x, y) = f(y, x)$$

$$\text{associativité : } f(f(x, y), z) = f(x, f(y, z))$$

- de **presque unanimité** si  $k \geq 3$  et elle satisfait les identités suivantes :

$$f(y, x, \dots, x) = f(x, y, x, \dots, x) = \dots = f(x, \dots, x, y) = x$$

- de **Mal'tsev** si elle est ternaire ( $k = 3$ ) et satisfait les identités suivantes :

$$f(x, y, y) = f(y, y, x) = x$$

- conservative** si  $f(x_1, \dots, x_k) \in \{x_1, \dots, x_k\}$  pour chaque  $x_i$ .

## Definition

Soit  $f: D^k \rightarrow D$  une fonction d'arité  $k$  sur le domaine  $D$ . La fonction  $f$  est une opération

- **essentiellement unaire** si  $f$  n'est pas constante, il existe une fonction unaire  $g$  et une indice  $i \in \{1, \dots, k\}$  qui satisfont l'identité suivante :

$$f(x_1, \dots, x_k) = g(x_i)$$

- de **majorité** si elle est ternaire ( $k = 3$ ) et satisfait les identités suivantes :

$$f(x, x, y) = f(x, y, x) = f(y, x, x) = x$$

- d'**affinité** si elle est ternaire ( $k = 3$ ) et satisfait l'identité

$$f(x, y, z) = x - y + z$$

où  $+$  et  $-$  sont des opérations du groupe commutatif  $(D, +, -)$ .

## Theorem

*Chaque opération d'affinité est une opération de Mal'tsev.*

*Chaque opération de majorité est une opération de presque unanimité.*

## Definition

Soit  $f: D^k \rightarrow D$  une fonction d'arité  $k$  sur le domaine  $D$ . La fonction  $f$  est une **semi-projection** si  $k \geq 3$  et il existe une indice  $i \in \{1, \dots, k\}$ , telle que l'identité  $f(x_1, \dots, x_k) = x_i$  est satisfaite s'il existe des indices  $j$  et  $\ell$  où  $x_j = x_\ell$  est satisfaite.

## Définition alternative

Autrement dit,  $f$  est une **semi-projection** s'il existe une indice  $i$  telle que pour tout  $d_1, \dots, d_k \in D$  avec  $|\{d_1, \dots, d_k\}| < k$ , nous avons  $f(d_1, \dots, d_k) = d_i$ .

## Theorem (Rosenberg, 1965)

Soit  $S$  un ensemble de relations sur le domaine  $D$ . Le clone  $\text{Pol } S$  contient

- soit seulement des fonctions essentiellement unaires,
- soit une fonction  $f$  qui est
  - une constante, ou
  - une fonction de majorité, ou
  - une fonction idempotente binaire qui n'est pas une projection, ou
  - une fonction affine, ou
  - une semi-projection.

## Theorem

*Soit  $S$  un ensemble de relations sur le domaine  $D$ . Si le clone  $\text{Pol } S$  ne contient que des fonctions essentiellement unaires, alors  $\text{CSP}(S)$  est NP-complet.*

## Démonstration.

Soit  $|D| = n$  et

$$nCOL = \{(d_1, \dots, d_n) \in D^n \mid (d_i = d_j) \rightarrow (i = j)\}.$$

Chaque fonction  $f$  essentiellement unaire est soit une permutation, soit elle n'est pas injective. Si  $f$  est une permutation, alors  $f(nCOL) = nCOL$  et  $CSP(nCOL)$  est NP-complet pour  $n \geq 3$ . Pour  $n = 2$ , la négation  $\neg$  et l'identité  $id$  sont des permutations.

Si  $f$  n'est pas injective, alors  $|f(D)| < |D|$ . Maintenant

- soit  $CSP(f(S))$  est NP-complet, ce qui implique que  $CSP(S)$  est NP-complet aussi,
- soit on peut récursivement descendre de  $CSP(S)$  vers  $CSP(f(S))$ . Cette descente est forcément finie.

Donc, à la fin  $CSP(f^k(S))$  est soit NP-complet, soit  $f^k(S)$  est fermé par rapport à une fonction non-unaire. La dernière est une contradiction avec l'énoncé. □

## Theorem

Soit  $S$  un ensemble de relations sur le domaine  $D$ . Si le clone  $\text{Pol } S$  contient l'une de fonctions suivantes :

- constante (généralise 0 et 1)
- demi-treillis (généralise  $\wedge$  et  $\vee$ )
- presque unanimité (généralise la majorité  $\text{maj}$ )
- Mal'tsev (généralise l'affinité  $\text{aff}$ )
- binaire commutative conservative

alors  $\text{CSP}(S)$  est décidable en temps polynomial.

## Remarque

Comparez les deux théorèmes précédents avec le Théorème dichotomique de Schaefer.

## Theorem

Pour chaque domain fini  $D$  avec  $|D| \geq 3$  il existe une relation  $R$  sur  $D$ , telle que  $R$  est fermée par toutes les semiprojections sur  $D$  et  $\text{CSP}(R)$  est NP-complet.

## Démonstration.

Soient  $d_0, d_1 \in D$ . Soit

$$R = \{(d_0, d_0, d_1), (d_0, d_1, d_0), (d_1, d_0, d_0)\}.$$

L'homomorphisme  $h: D \rightarrow \{0, 1\}$  avec  $h(d_0) = 0$  et  $h(d_1) = 1$  construit la relation  $h(R) = 1\text{-in-}3$ . Si  $\text{CSP}(h(R))$  est NP-complet alors  $\text{CSP}(R)$  est NP-complet aussi.  $\square$

Travail en stage puis en thèse . . .

## Problème MAXCSP( $S$ )

*Entrée:* Un ensemble fini de contraintes  $C = \{R_1(\vec{x}_1), \dots, R_p(\vec{x}_p)\}$  sur  $D$  et  $V$ , où  $R_j \in S$  pour chaque  $j$ .

*Sortie:* Nombre maximal de contraintes satisfaisable parmi  $C$ .

## Situation

Résultats partiels par Krokhin, Johnson et co.

## Problème $APX(S)$

**Entrée:** Un ensemble fini de contraintes  $C = \{R_1(\vec{x}_1), \dots, R_p(\vec{x}_p)\}$  sur  $D$  et  $V$ , où  $R_j \in S$  pour chaque  $j$  et où chaque solution  $m$  de  $C$  possède une valeur  $w(m) \in \mathbb{R}^+$ .

**Question:** La solution optimale (max ou min) est-elle approximable en temps polynomiale par une constante ?

## Situation

$|D| = 2$  : Solution complète par Creignou en 1995.

$|D| > 2$  : Aucun résultat.

## Problème $\text{RATIO}(S)$

*Entrée:* Un ensemble fini de contraintes  $C = \{R_1(\vec{x}_1), \dots, R_p(\vec{x}_p)\}$  sur  $D$  et  $V$ , où  $R_j \in S$  pour chaque  $j$  et où chaque solution  $m$  de  $C$  possède une valeur  $w(m) \in \mathbb{R}^+$ .

*Sortie:* Le meilleur taux d'approximation polynomiale de la solution optimale.

## Situation

$|D| = 2$  : Résultat partiel de Zwick.

$|D| > 2$  : Aucun résultat.

## Definition

Soit le domaine  $D = \{0, \dots, n-1\}$  ordonné par  $<$ , où  $0 < 1 < \dots < n-2 < n-1$ . L'**ordre partiel**  $\prec$  sur les tuples de  $D^k$  est défini par

$$m \prec m'$$

si

- $m \neq m'$ ,
- $m[i] \leq m'[i]$  pour chaque  $i \in \{1, \dots, k\}$ .

La relation  $m \preceq m'$  signifie  $m \prec m'$  ou  $m = m'$ .

## Definition

Un **modèle minimal** de  $R(x_1, \dots, x_k)$  est un tuple  $m \in R$  tel que chaque  $m' \in R$  satisfait  $m \preceq m'$  ou  $m$  et  $m'$  sont incomparables.

## Problème $\text{MININF}(S)$

**Entrée:** Un ensemble fini de contraintes  $C = \{R_1(\vec{x}_1), \dots, R_p(\vec{x}_p)\}$  sur  $D$  et  $V$ , où  $R_j \in S$  pour chaque  $j$ , et une contrainte  $R(\vec{x})$ .

**Question:** La contrainte  $R(\vec{x})$  est-elle satisfaisable dans tous les modèles minimaux de  $C$ ?

## Difficulté

La notion de minimalité n'est pas compatible avec la quantification existentielle.

## Situation

$|D| = 2$  : Résultat récent de Durand, H. et Nordh (5 ans de travail) pour l'arité de  $R$  non-bornée, suite aux résultats partiels de Kirousis et Kolaitis.

$|D| > 2$  : Aucun résultat.

## Problème $\#_{\text{CIRC}}(S)$

**Entrée:** Un ensemble fini de contraintes  $C = \{R_1(\vec{x}_1), \dots, R_p(\vec{x}_p)\}$  sur  $D$  et  $V$ , où  $R_j \in S$  pour chaque  $j$ .

**Sortie:** Nombre de modèles minimaux de  $C$ .

## Situation

$|D| = 2$  : Résultat partiels de Durand, H. et Kolaitis.

$|D| > 2$  : Aucun résultat.

## Problème $\text{GENCSP}(S, O)$

*Entrée:* Une formule  $\varphi$  construite à partir des contraintes atomiques  $R(\vec{x})$  sur les relations  $R \in S$  par les opérations  $O$ .

*Question:* La formule  $\varphi$  est-elle satisfaisable ?

## Situation

$O = \{\exists, \wedge\}$  : CSP classiques

$O = \{\exists, \wedge, \vee, =\}$  : Résolu récemment par H. et Richoux (domaines finis), ainsi que par Bodirsky, H. et Richoux (cas infini).

**Autres configurations d' $O$  :** Aucun résultat.

## Configurations d' $O$ particulièrement intéressantes

$\{\text{maj}\}$ ,  $\{\text{maj}, =\}$  — satisfaction de la majorité de contraintes

$\{\oplus\}$  — satisfaction du nombre impaire de contraintes

- CSP floues
- CSP engendrés par les égalités entre les fonctions finies
- CSP randomisés
- CSP avec différentes structures
- à vous d'inventer ...

L'examen aura lieu le  
29 novembre, 14h15 — 15h45.

Good luck !

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