De la complexité des problèmes de contraintes

Florent Madelaine

Université d'Auvergne en délégation au LIX

Algo et Complexité sur le plateau de Saclay,
le 18 octobre 2011

Un problème central en informatique

De l'ubiquité des problèmes de contraintes

Plusieurs définitions équivalentes

- Définition IA classique "variables-valeurs-constraintes"
- Problème d'homomorphisme
- Inclusion de requêtes conjonctives
- Problème du *Model-checking* pour $\{\exists, \wedge\}$-FO

De plus la complexité peut être caractérisée algébriquement

Définition IA classique

Une instance du problème de satisfaction de contraintes CSP est un triplet $(\mathrm{Var}, \mathrm{Dom}, \mathcal{C})$ où

- Var est un ensemble de variables,
- Dom est un ensemble de valeurs et
- $\mathcal{C}$ est un ensemble de contraintes:
  - chaque contrainte étant de la forme $(v_{i_1}, \ldots, v_{i_r}, R)$ où r est l'arité de la contrainte et $R \subseteq \mathrm{Dom}^r$.

Une *solution* est une application des variables aux valeurs qui satisfait simultanément toutes les contraintes.

Un cas particulier important

Le cas booléen

SAT correspond à CSP avec un domaine booléen. Comme l'entrée est codée de manière différente, on parle de *Generalized Satisfiability*

Example

clause
$x \vee y \vee \bar{z}$

contrainte

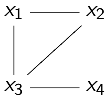
- (x, y, z)
- $\{0,1\}^3 \setminus \{(0,0,1)\}$

Modéliser 3-col

Pour un graphe $G := (V, E)$ on a l'instance de CSP suivante

- variables $\mathrm{Var} := V$,
- valeurs $\mathrm{Dom} := \{1, 2, 3\}$ et
- contraintes $\mathcal{C} := \{(x_i, x_j, \neq) : \text{ pour chaque } (x_i, x_j) \in E\}$.

Example



- instance: $\mathrm{Var} = \{x_1, x_2, x_3, x_4\}$, $\mathrm{Dom} = \{1, 2, 3\}$ et $\mathcal{C} = \{((x_1, x_2), \neq), ((x_1, x_3), \neq), ((x_3, x_2), \neq), ((x_3, x_4), \neq)\}$
- une solution: $x_1 = 1, x_2 = 2, x_3 = 3, x_4 = 1$

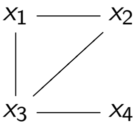
Deux structures sous-jacentes

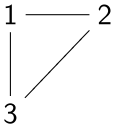
Notre exemple

- instance: $\mathrm{Var} = \{x_1, x_2, x_3, x_4\}$, $\mathrm{Dom} = \{1, 2, 3\}$ et $\mathcal{C} = \{((x_1, x_2), \neq), ((x_1, x_3), \neq), ((x_3, x_2), \neq), ((x_3, x_4), \neq)\}$
- une solution: $x_1 = 1, x_2 = 2, x_3 = 3, x_4 = 1$

Deux structures

Variables $\mathcal{A}$





Valeurs $\mathcal{B}$

homomorphisme : $x_1 \mapsto 1, x_2 \mapsto 2, x_3 \mapsto 3, x_4 \mapsto 1$

rappel

Un homomorphisme préserve les relations. Pour des graphes, une arête est envoyée sur une arête. Pour des digraphes, on préserve en plus l'orientation des arcs.

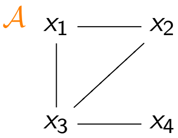
CSP vu comme un problème d'homomorphisme

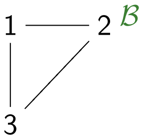
- instance : une paire de structures relationnelles similaires $(\mathcal{A}, \mathcal{B})$
- question : existe-t-il un homomorphisme de $\mathcal{A}$ dans $\mathcal{B}$?

où $\mathcal{A}$ représente la structure des contraintes et

$\mathcal{B}$ représente le language des contraintes

Example (3-col comme un homomorphisme dans K_3)





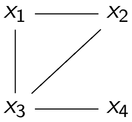
homomorphisme : $x_1 \mapsto 1, x_2 \mapsto 2, x_3 \mapsto 3, x_4 \mapsto 1$

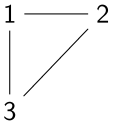
CSP comme problème de *model checking*

- instance: $\varphi_{\mathcal{A}}$ une formule de $\{\exists, \wedge\}$-$\textsc{fo}$ et une structure $\mathcal{B}$
- question: $\mathcal{B} \models \varphi_{\mathcal{A}}$?

Example

$\varphi_{\mathcal{A}} = \exists x_1 \exists x_2 \exists x_3 \exists x_4 E(x_1, x_2) \wedge E(x_2, x_3) \wedge E(x_3, x_4) \wedge E(x_3, x_4)$





$\mathcal{B}$

Remarques

- Cette formulation permet de définir facilement des extensions de CSP comme QCSP.
- les formules de $\{\exists, \wedge\}$-$\textsc{fo}$ sont connues sous le nom de requêtes conjonctives en BdD.

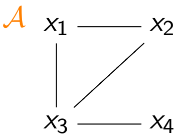
CSP vu comme un problème d'homomorphisme

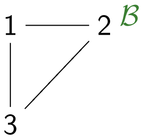
- instance : une paire de structures relationnelles similaires $(\mathcal{A}, \mathcal{B})$
- question : existe-t-il un homomorphisme de $\mathcal{A}$ dans $\mathcal{B}$?

où $\mathcal{A}$ représente la structure des contraintes et

$\mathcal{B}$ représente le language des contraintes

Example (3-col comme un homomorphisme dans K_3)





homomorphisme : $x_1 \mapsto 1, x_2 \mapsto 2, x_3 \mapsto 3, x_4 \mapsto 1$

Un exemple avec plusieurs relations : 2-Sat

Soit $R_{ab}^{\mathcal{B}} = \{0,1\}^2 \setminus \{(a,b)\}$ et $\mathcal{B} = (\{0,1\}; R_{00}^{\mathcal{B}}, R_{01}^{\mathcal{B}}, R_{11}^{\mathcal{B}})$.
Une instance de 2-Sat, par exemple

$$F = (\neg x \vee \neg z) \wedge (x \vee y) \wedge (y \vee \neg z) \wedge (u \vee x) \wedge (x \vee \neg u) \ldots$$

devient une structure $\mathcal{A}$ de domaine $\{x, y, z, u, \ldots\}$ et
$R_{00}^{\mathcal{A}} = \{(x,y), (u,x), \ldots\}$
$R_{01}^{\mathcal{A}} = \{(y,z), (x,u), \ldots\}$
$R_{11}^{\mathcal{A}} = \{(x,z), \ldots\}$

Alors $h : \mathcal{A} \to \mathcal{B}$ ssi h est une assignation satisfaisant la formule propositionnelle F.

Restrictions de CSP

Généralisant SAT et permettant de modéliser 3-col, CSP est difficile (NP-complet) en général.

Quelles restrictions rendent ce problème polynomial?

Il y a deux types de restrictions :

1. Restrictions structurelle sur la manière dont les variables sont contraintes, c'est-à-dire sur la "structure des variables" $\mathcal{A}$
2. Langages de contraintes sur le type de contraintes autorisées, c'est-à-dire sur la "structure des valeurs" $\mathcal{B}$

Plus récemment

Restrictions hybrides portant à la fois sur les deux structures.

Requêtes arborescentes

Pour les restrictions structurelles, on sait que si $\mathcal{A} \in \mathcal{F}$, une classe de structures dont les *cores* ont une *largeur arborescente bornée* alors le problème est polynomial (généralisation des resultats de Freuder).

Il est difficile de calculer le *core*. L'algorithme polynomial repose sur le fait qu'on peut calculer efficacement une stratégie gagnante pour un jeu associé à une certaine logique (Dalmau, Kolaitis et Vardi CP'02).

En fait, on sait que pour toute les autres classes $\mathcal{F}$, le problème est difficile sous couvert d'une hypothèse de complexité paramétrée (Grohe JACM'07).

Languages de contraintes

Nous fixons le langage des contraintes $\mathcal{B}$ et considérons que seule la structure $\mathcal{A}$ est en entrée. On parle de CSP non-uniforme.

$\mathrm{CSP}(\mathcal{B})$

- entrée : une structure relationnelle similaire $\mathcal{A}$
- question : existe-t-il un homomorphisme de $\mathcal{A}$ dans $\mathcal{B}$?

On considère des exemples $\mathcal{B}$ de domaine D et dont les relations appartiennent à un ensemble Γ de relations sur D.

On va voir que des propriétés algébriques de Γ caractérisent la complexité du problème.

Quelques langages de contraintes booléens

- Soit $D = \{0, 1\}$ et $R = \{0, 1\}^3 \setminus \{(0, 0, 0), (1, 1, 1)\}$. Si $\Gamma = \{R\}$ alors $\mathrm{CSP}(\mathcal{B})$ est Not-All-Equal Sat (NP-complet).
- Soit $D = \{0, 1\}$ et $R = \{(x, y, z) \mid y \wedge z \rightarrow x\}$. Si $\Gamma = \{R, \{0\}, \{1\}\}$ alors $\mathrm{CSP}(\mathcal{B})$ est Horn 3-Sat (P-complet).
- Soit $D = \{0, 1\}$ et $R_{ab}^{\mathcal{B}} = \{0, 1\}^2 \setminus \{(a, b)\}$. Si $\Gamma = \{R_{00}, R_{01}, R_{11}\}$ alors $\mathrm{CSP}(\mathcal{B})$ est 2-Sat (NLogspace-complet).

Autres exemples

- Si $\Gamma = \{\neq_D\}$ où $\neq_D$ est la relation “différent” sur D et $|D| = k$ alors $\mathrm{CSP}(\mathcal{B})$ est Graph k-colouring (L si $k \leq 2$, NP-complet si $k \geq 3$).

- Soit D avec $|D| = p$, p premier (on voit D comme $\mathbb{Z}_p$). Si $\Gamma = \{R, \{1\}\}$ où $R = \{(x, y, z) \mid x + y = z\}$ alors $\mathrm{CSP}(\mathcal{B})$ est (grosso modo) le problème Linear Equations sur $\mathbb{Z}_p$ (polynomial).

Deux cas historiquement importants

1. Graphes non orientés

Lorsque les structures sont des graphes et $\mathcal{B}$ est un graphe H fixé, on parle du problème de *H-coloring*

Example

Si H est K_3 (un triangle) on retrouve le problème 3-Col.

2. Le cas booléen

CSP à domaine booléen : *Generalized Satisfiability*

Example

clause
$x \vee y \vee \bar{z}$

contrainte

- (x, y, z)
- $\{0,1\}^3 \setminus \{(0,0,1)\}$

Le cas des graphes

Theorem (Hell & Nešetřil 1990)

Soit $\mathcal{B}$ un graphe non orienté fini.
$CSP(\mathcal{B})$ *est polynomial si* $\mathcal{B}$ *est biparti et* NP-*complet sinon.*

Remarques

- La preuve est combinatoire
- On peut en donner une forme algébrique (Bulatov).

Le cas booléen

Theorem (Schaefer 1978)

Si $\mathcal{B}$ est "Horn", ou "dual-Horn" ou "2-Sat", ... (6 cas en tout) alors $CSP(\mathcal{B})$ est polynomial, sinon $CSP(\mathcal{B})$ est NP*-complet.*

Remarques

- Une forme plus précise du théorème va suivre.
- La preuve est algébrique (classification par reduction à certains langages de contraintes qui sont les éléments d'un treillis)

Digression : la conjecture de la dichotomie

Le théorème de Ladner implique que, si P $\neq$ NP alors il y a des problèmes de complexité intermédiaire dans NP qui ne sont ni dans P ni NP-complet.
Dans un article qui a eut beaucoup d'influence, Feder et Vardi rappellent que les problèmes de contraintes non uniformes forment une sous-classe naturelle et large de NP et ont donné des argument étayant la conjecture suivante.

Conjecture de la dichotomie (Feder & Vardi, 1993)

$\mathrm{CSP}(\mathcal{B})$ est soit dans P soit NP-complet.

Remarque

Il existe de nombreuses classes de problèmes qui sont *dichotomie-complètes* (une dichotomie pour cette classe équivaut à la conjecture de la dichotomie). Par exemple, on peut se restreindre au cas où $\mathcal{B}$ est un digraphe.

Intuition de l'approche algébrique

Intuition: Plus Γ est riche (expressif), plus $\mathrm{CSP}(\Gamma)$ est difficile à résoudre.

Example

Si Γ contient deux relations binaire R_1 and R_2. Considérons l'instance

$$((x, z), R_1),\ ((z, y), R_2).$$

- La contrainte implicite sur (x, y) est $R_3 = R_1 \circ R_2$
- $R_3(x, y) = \exists z R_1(x, z) \wedge R(z, y)$.
- $R3 \notin \Gamma$, mais
- $\mathrm{CSP}(\Gamma)$ et $\mathrm{CSP}(\Gamma \cup \{R_3\})$ sont (logspace) équivalents.

Cette idée se généralise naturellement.

Clones relationnels

Definition

On note $\langle \Gamma \rangle$ l'ensemble des relations qui peuvent être simulées par les relations de Γ. Il s'agit de toutes les relations qui sont interprétables par une formule primitive positive sur Γ, c'est-à-dire utilisant

- des relations de $\Gamma \cup \{=_D\}$,
- la conjonction $\wedge$, et
- la quantification existentielle $\exists$.

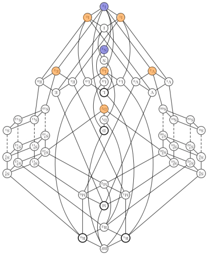
$\langle \Gamma \rangle$ est appelé le clone relationnel généré par Γ.

Theorem (Jeavons '98)

Si Γ_1 et Γ_2 sont des langages de contraintes tels que $\langle \Gamma_1 \rangle \subseteq \langle \Gamma_2 \rangle$ alors $CSP(\Gamma_1)$ se (logspace-)réduit à $CSP(\Gamma_2)$.

Slogan: $\langle \Gamma \rangle$ capture l'expressivité de Γ.

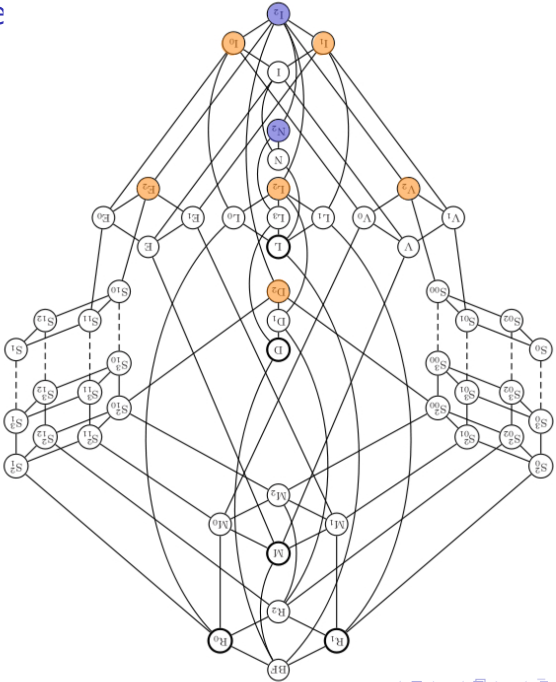
Le treillis de Post



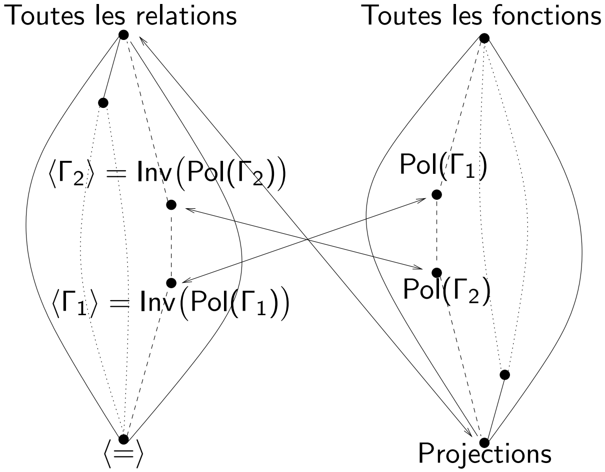
Méthodologie pour démontrer le théorème de Schaefer

- Les éléments du treillis sont les clones relationnels $\langle \Gamma \rangle$ sur le domaine booléen $D = \{0, 1\}$.
- Il suffit de classifier la frontière entre facile et difficile dans le treillis pour obtenir le résultat
  - Clones oranges faciles (donner des algos polynomiaux)
  - clones bleus sont durs (réduction depuis des problèmes NP-complets)

Post Lattice

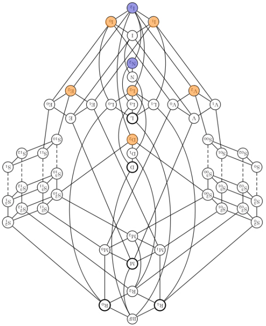


Correspondance de Galois

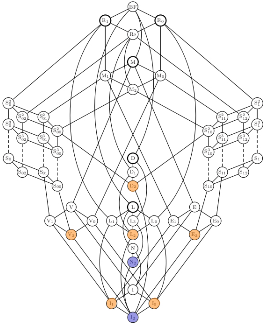


Correspondance de Galois

Clones relationnels



clones fonctionnels



Le cas booléen : Generalized Satisfiability

Theorem (Post, 1941)

Pour tout langage de contrainte Γ *sur* $D = \{0, 1\}$*, on est dans l'un des cas suivants*

- *Les constantes 0 or 1 sont dans* $\mathrm{Pol}(\Gamma)$ — $CSP(\Gamma)$ *est trivial*
- $min \in \mathrm{Pol}(\Gamma)$ — $CSP(\Gamma) \subseteq$ **Horn-Sat**
- $max \in \mathrm{Pol}(\Gamma)$ — $CSP(\Gamma) \subseteq$ **dual Horn-Sat**
- $majority \in \mathrm{Pol}(\Gamma)$ — $CSP(\Gamma) \subseteq$ **2-Sat**
- *affine* $(x - y + z)$ *est dans* $\mathrm{Pol}(\Gamma)$ — $CSP(\Gamma) \subseteq$ **équations linéaires**
- $\mathrm{Pol}(\Gamma) \subseteq \mathrm{Pol}\langle R_{NAE} \rangle$. — **NAE-Sat** $\subseteq CSP(\Gamma)$

Corollary (Schaefer, 1978)

Pour tout langage de contrainte Γ *sur* $D = \{0, 1\}$, $CSP(\Gamma)$ *est soit polynomial soit* NP*-complet.*

L'approche algébrique pour d'autres questions

- Dans le cas booléen, le treillis de Post permet de classifier la complexité pour d'autres questions : circomscription, abduction, comptage, énumération
- mais pas toujours : MaxSat, approximation.

- Il existe aussi des correspondances de Galois qui permettent d'étudier la complexité pour d'autres problèmes : pour QCSP, pour QCSP avec $\vee$, mais aussi pour étudier plus finement la complexité des CSP (*frozen partial co-clones*).

CSP au delà du booléen?

- Jeavons et d'autres chercheurs ont proposés de nombreuses classes naturelles qui sont polynomiales.
- Mais le treillis des clones n'est pas dénombrable et on ne dispose pas de sa description.
- Il faut une autre approche qui fasse abstraction du treillis pour pouvoir obtenir une classification.
- C'est ce que Bulatov a fait pour le cas à 3 éléments (2002) et pour le cas conservatif (2006), deux résultats de dichotomie remarquables.

Second théorème de Bulatov : le cas conservatif

- concerne un domaine fini quelconque et un langage de contraintes autorisant toutes les contraintes unaires.
- pas simple à énoncer.
- par contre ce résultat confirme ce que Feder et Vardi avaient suggéré dans leur papier fondateur, à savoir la pauvreté relative de l'arsenal algorithmique polynomial.
- Il existe essentiellement deux algorithmes, pour résoudre un problème non-uniforme : l'un généralise la cohérence et correspond à l'existence d'un programme Datalog, et l'autre découle du fait qu'on peut dans certain cas représenter de manière compacte l'ensemble des solutions.

chronologie de la conjecture

- 1993: conjecture de la dichotomie (Feder & Vardi)
- de 1993 à 1998, beaucoup de progrès (Jeavons *et. al.*)
- à partir de 2002, Bulatov revampe l'approche algébrique
  - + dichotomie (3 éléments)
  - + dichotomie pour les langages conservatifs
- Depuis 5 ans, la communauté s'est étoffée et des preuves mélangeant de manière subtile algèbre, logique et combinatoire apparaissent
  - + La conjecture est étendue à d'autres classes de complexité
  - + Il y a beaucoup d'efforts concernant l'aspect complexité descriptive
  - + La conjecture se réduit à une question assez simple (à expliquer).
  - – la conjecture reste ouverte...

Pour démontrer la conjecture

Conjecture (dernière forme connue)

Si Pol(Γ) *contient un terme de Siggers alors* CSP(Γ) *est polynomial.*

Un terme de Siggers est une opération d'arité 4 satisfaisant les identités $f(x, x, x, x) = x$ et $f(y, x, y, z) = f(x, y, z, x)$.

Il suffit de traiter le cas de digraphes.

Activité de notre groupe

Nous travaillons presque tous sur des questions liées à la complexité de problèmes apparentés aux problèmes de contraintes.

- Complexité de SAT au delà du problème de décision
- Optimisation et approximation des CSP
- CSP de domaines infinis
- CSP quantifiés (QCSP)
- Complexité descriptive des CSP (lien entre logique et complexité)

Biblio

N. Creignou, P. G. Kolaitis, and H. Vollmer, editors.

Complexity of Constraints - An Overview of Current Research Themes [Result of a Dagstuhl Seminar], volume 5250 of *Lecture Notes in Computer Science*. Springer, 2008.

H. Chen.

A rendezvous of logic, complexity, and algebra. volume 42 of *ACM Comput. Surv.*, 2009.

Beaucoup de ressources récentes disponibles

Summer Thematic Program on the Mathematics of Constraint Satisfaction at the Fields Institute, Toronto (June 26th – August 16th)

http://www.fields.utoronto.ca/programs/scientific/11-12/constraint/index.html