Méthodes de composition en logique

Alexis Bès

LACL, UPEC

Exposé LAIC Juin 2010

Introduction

- Définissabilité et décidabilité en logique
- Méthodes de composition
- Le cas des sommes de structures ordonnées
- Théorème de (dé)composition de Shelah (MSO)
- Quelques applications

Décidabilité des théories logiques

- Problème : un formalisme logique et une théorie T, le problème de savoir si un énoncé φ est conséquence de T est-il décidable ?
- Autre problème : pour une structure M, peut-on décider si un énoncé φ est vrai dans M ?
- Techniques classiques de décidabilité :
  - Complétude
  - Elimination des quantificateurs
  - Automates
  - **Composition**
  - Interprétation, jeux,...

Logique du premier ordre

- L un langage (*signature*) relationnel
- M une L-structure
- $FO(M)$: ensemble des énoncés φ tels que $M \models \varphi$
- $FO(M)$ est *décidable* si le problème "$M \models \varphi$?" est décidable
  Exemples : $FO(\mathbb{N};+)$ est décidable, $FO(\mathbb{N};+,\times)$ ne l'est pas

Logique du second-ordre monadique

- Extension de la logique du premier ordre dans laquelle on peut quantifier sur des ensembles d'éléments du domaine
- Formalisme :
  - variables du 1er ordre : $x, y, z, \ldots$
  - variables du 2nd ordre monadique : $X, Y, Z, \ldots$
  - on introduit $x \in X$
- Notation : $MSO(M)$
- Exemples :
  - $MSO(\mathbb{N}; <)$ décidable (Büchi 1962)
  - $MSO(\mathbb{N}; +)$ indécidable (R.Robinson 1958)
- k-type de M : ensemble des énoncés de hauteur de quantification $\leq k$ satisfaits par M
- Second-ordre monadique *faible* (WMSO) : ensembles *finis*

Méthodes de composition

- Principe : construire une $L-$structure M à partir d'une famille $(M_i)_{i \in I}$ de $L-$structures.
- Ramener l'étude de $FO(M)$ (ou $WMSO$, MSO) à celle des théories $FO(M_i)$
- Point de vue décidabilité : réduire $FO(M)$ aux $FO(M_i)$
- Souvent : $FO(M)$ se réduit aux $FO(M_i)$ ("facteurs") et à $MSO(I, ...)$ ("structure des indices")

Comment composer les facteurs M_i ?

- Union disjointe
- Produit direct, puissance directe (Mostowski)
- Produits/puissances réduits, généralisés, ultraproduits (Los, Feferman-Vaught)
- **Somme de structures ordonnées** (Lauchli, Shelah)
- Autres formes (Courcelle, Makowsky, Muchnik, Caucal...)

Premier exemple : union disjointe de deux structures

- Structures : graphes simples dirigés, avec un prédicat $R(x, y)$ pour les arêtes
- $G_1 = (S_1, R^1)$, $G_2 = (S_2, R^2)$ avec S_1, S_2 disjoints
- $G = (S, R)$ avec $S = S_1 \uplus S_2$ et $R^G = R^1 \uplus R^2$
- Soit φ : "le graphe contient un cycle" (MSO). On a $G \models \varphi$ ssi $(G_1 \models \varphi$ ou $G_2 \models \varphi)$
- Soit φ : "le graphe contient au moins deux 5-cliques" (MSO). On a $G \models \varphi$ ssi $G_1 \models \varphi$, ou $G_2 \models \varphi$, ou $(G_1 \models \varphi'$ et $G_2 \models \varphi')$ avec φ' : "le graphe contient au moins une 5-clique"
- Plus généralement : pour toute formule MSO φ on peut construire effectivement des formules $\varphi_{1,1}, \varphi_{1,2}, \ldots, \varphi_{n,1}, \varphi_{n,2}$ telles que $G \models \varphi \Leftrightarrow \bigvee_{i=1}^{n} (G_1 \models \varphi_{i,1} \wedge G_2 \models \varphi_{i,2})$
- Corollaire : $MSO(G)$ se réduit à $MSO(G_1)$ et $MSO(G_2)$

Deuxième exemple : produit direct de deux structures

- $M_1 = (A_1, R^1)$, $M_2 = (A_2, R^2)$ (R binaire)
- $M = M_1 \times M_2$ structure de domaine $A_1 \times A_2$ avec $M \models R(x, y)$ ssi $M_i \models R^i(x_i, y_i)$ ($i = 1, 2$)
- Exemple : si $M_1 = M_2 = (\mathbb{Z}, +)$ alors $M_1 \times M_2 = (\mathbb{Z}^2, +)$
- Pour toute énoncé FO φ on a $M \models \varphi$ ssi $M_i \models \varphi$ pour tout i
- Corollaire : $FO(M_1 \times M_2)$ se réduit à $FO(M_1)$ et $FO(M_2)$ (ici : $FO(\mathbb{Z}^2, +)$ se réduit à $FO(\mathbb{Z}, +)$)
- Attention : ne passe pas à MSO

Troisième exemple : puissance directe d'une structure (Mostowski)

- Exemple : $I = \mathbb{N}$
- Puissance directe : $M = (\mathbb{N}, +)$. On peut définir $M^{\mathbb{N}} = (\mathbb{N}^{\mathbb{N}}, +)$ où : pour tous $f, g, h \in \mathbb{N}^{\mathbb{N}}$, on a

  $$M^{\mathbb{N}} \models f + g = h$$

  ssi

  $$M \models f(i) + g(i) = h(i)$$

  pour tout $i \in \mathbb{N}$
- $FO(M^{\mathbb{N}})$ se réduit à $FO(M)$
- Derrière le rideau : $FO(M^{\mathbb{N}})$ se réduit à $FO(M)$ *et* $MSO(\mathbb{N})$

Quatrième exemple : puissance faible d'une structure

- $M^{\mathbb{N}}$ puissance directe de $M = (\mathbb{N}, +)$
- Puissance directe faible : $M = (\mathbb{N}, +, 0)$. On définit $M_0^{\mathbb{N}}$ comme la sous-structure de $M^{\mathbb{N}}$ de domaine l'ensemble $\mathbb{N}_0^{\mathbb{N}}$ des fonctions $f : \mathbb{N} \to \mathbb{N}$ presque toujours nulles.
- $FO(M_0^{\mathbb{N}})$ se réduit à $FO(M)$ (Mostowski)
- Derrière le rideau : $FO(M_0^{\mathbb{N}})$ se réduit à $FO(M)$ *et* $WMSO(\mathbb{N})$
- Application : décidabilité de l'arithmétique de Skolem $FO(\mathbb{N} - \{0\}, \times)$
  - la fonction $c : \mathbb{N} - \{0\} \to \mathbb{N}_0^{\mathbb{N}}$ qui à $n = \prod_i p_i^{n_i}$ associe $f_n : i \mapsto n_i$ définit un isomorphisme de $(\mathbb{N} - \{0\}, \times)$ dans $M_0^{\mathbb{N}}$.
  - $FO(\mathbb{N} - \{0\}, \times) \rightsquigarrow FO(M_0^{\mathbb{N}}) \rightsquigarrow FO(\mathbb{N}, +, 0)$
  - $FO(\mathbb{N}, +, 0)$ est décidable (Presburger)
- Feferman-Vaught : produits généralisés, où FO du produit se réduit à FO des facteurs et MSO d'une expansion de I

Quelques résultats de décidabilité sur les ordres

- Ordinaux :
  - Büchi : $MSO(\omega, <)$ décidable
  - Beaucoup de résultats autour de $MSO(\omega, <, P)$, pour P unaire
  - Büchi : $MSO(\alpha, <)$ décidable pour tout ordinal $\alpha < \omega_2$
  - Gurevich-Magidor-Shelah : $MSO(\omega_2, <)$ indépendant de ZFC
- Autres ordres :
  - $MSO(\mathbb{Z}, <)$ est décidable (corollaire du résultat pour ω)
  - $MSO(\mathbb{Z}, <, P)$ pour P unaire (Semënov, Perrin-Schupp, Compton)
  - Rabin : $MSO(\mathbb{Q}, <)$ décidable, de même que MSO(ordres dénombrables)
  - Shelah : $MSO(\mathbb{R}, <)$ indécidable
- Méthodes : automates, composition

Somme de structures (totalement) ordonnées

- On considère des structures $M = (A, <, P_1, \ldots, P_n)$ avec P_i prédicats unaires, et où $(A, <)$ ordre total
- Somme de structures : pour $M_1 = (A_1, <^1, \overline{P}^1)$ et $M_2 = (A_2, <^2, \overline{P}^1)$ avec $A_1 \cap A_2 = \emptyset$ on définit $M = M_1 + M_2$ par $M = (A, <, \overline{P})$ où
  - $A = A_1 \cup A_2$
  - $x < y$ si $x <^1 y$, $x <^2 y$ ou $(x \in A_1$ et $y \in A_2)$
  - $\overline{P} = \overline{P}^1 \cup \overline{P}^2$
- Généralisation : on définit $M = \sum_{i \in I} M_i$ pour $(I, <)$ ordre total et $(M_i)_{i \in I}$ famille de structures sur le langage $\{<, P_1, \ldots, P_n\}$.

Vers un théorème de composition

- En utilisant des jeux d'Ehrenfeucht-Fraïssé on peut démontrer que le $k-$type de $M = M_1 + M_2$ est complètement déterminé (et calculable) par celui de M_1 et M_2
- Théorème de composition de Shelah : calculer $MSO(\sum_{i \in I} M_i)$ à partir de $MSO(M_i)$ et $MSO(I, <)$

Exemple de composition :

- Exemple : $M = \sum_{i \in \mathbb{Z}} M_i$ avec $M_i = (\mathbb{N}, <, P^i(x))$
- φ : "P est infini"
- On a $M \models \varphi$ ssi
  1. P est infini dans au moins l'un des M_i, ou
  2. l'ensemble des M_i qui contiennent au moins un élément de P est infini
- On trouve ψ tel que $M \models \varphi$ ssi $(\mathbb{Z}, <, Q_1, Q_2) \models \psi$ avec
  - $Q_1 = \{i : \ M_i \models \varphi\}$
  - $Q_2 = \{i : \ M_i \models \exists x P(x)\}$
- Plus généralement, à tout φ on peut associer ψ tel que

$$M \models \varphi \ \text{ ssi } \ (\mathbb{Z}, <, (Q_\tau)) \models \psi$$

où $Q_\tau(x)$ si M_x est de type τ.

Théorème de composition (Shelah)

Théorème

- Soient $(I,<)$ ordre, $(M_i)_{i\in I}$ une famille de structures sur le langage $\{<, P_1, \ldots, P_n\}$, et $M = \sum_{i\in I} M_i$.
- Il existe une fonction récursive f telle que le k-type de M est calculable à partir du $f(k)$-type de la structure $(I, <, Q_1, \ldots, Q_p)$ où $Q_j = \{i \in I : M_i \text{ a pour } k\text{−type } \tau_j\}$ avec $\tau_1, \ldots, \tau_p$ liste de tous les $k-$types (formellement) possibles pour les M_i

Remarques

- la transformation préserve le nombre d'alternance de quantificateurs
- preuve : très proche de celle de Feferman-Vaught

Application : un cas simple

Cas particulier : $M = \sum_{i \in I} M_i$ où tous les M_i sont égaux

- tous les M_i ont le même type, i.e. $Q_\tau \in \{\emptyset, I\}$
- la question de savoir si $Q_\tau = \emptyset$ se réduit à $MSO(M_0)$
- Donc
  $MSO(M) \rightsquigarrow MSO(I, <, (Q_\tau)) \rightsquigarrow (MSO(I, <), MSO(M_0))$
- Exemple : $(\omega^2, <) = \sum_\omega (\omega, <)$ donc $MSO(\omega^2, <)$ se réduit à $MSO(\omega, <)$
- Plus généralement : pour tout $n < \omega$, $MSO(\omega^n, <)$ se réduit à $MSO(\omega, <)$ donc est décidable.

Application : MSO des ordres finis

- Calcul de l'ensemble des $k-$types des structures $(A, <, \overline{P})$ avec A fini
- Pour tout r et toute structure $M = (\{1, \ldots, r\}, <, \overline{P})$ on sait calculer le $k - type$ de M
- On calcule pour $r = 1, 2, \ldots$
- Il y a un nombre fini de $k-$types possibles, donc on trouve r_0 tel que le k-type de toute structure $M = (\{1, \ldots, r_0 + 1\}, <, \overline{P})$ est déjà apparu.
- Pour toute structure $M = (\{1, \ldots, r\}, <, \overline{P})$ avec $r > r_0 + 1$, il existe une structure plus petite que M et ayant même $k-$type (car $M = M_1 + M_2$ où M_1 a $r_0 + 1$ éléments).
- On peut donc s'arrêter à $r_0 + 1$
- Corollaire : décidabilité de MSO sur les mots finis (i.e. de $WMSO(\mathbb{N}, <)$)
- Autre méthode : automates

Application : structures décidables maximales

Elgot-Rabin (1966)

- Résultats de décidabilité de $MSO(\mathbb{N}; <, P)$ pour certains prédicats P
- Question : étant donnée une structure $\mathfrak{M} = (D; P_1, \ldots, P_k)$ telle que $FO(\mathfrak{M})$ est décidable, peut-on toujours étendre $\mathfrak{M}$ avec un prédicat non définissable R en une structure $\mathfrak{M}' = (D; P_1, \ldots, P_k, R)$ telle que $FO(\mathfrak{M}')$ est décidable ?
- i.e. **existe-t-il des structures décidables maximales ?**

Résultats partiels

Soprunov (1988)

- critère de non-maximalité : si un ordre régulier est interprétable dans M alors M n'est pas maximale
- pas de structure maximale pour WMSO

AB-P.Cégielski (2006)

- nouveau critère de non-maximalité basé sur la distance de Gaifman
- existence de structures décidables *faiblement maximales* : il existe $M = (\mathbb{N} \times \mathbb{Z}, <, P)$ tel que $MSO(M)$ est décidable, et $FO(M')$ indécidable pour toute expansion de M par une constante (s'appuie sur le thm de composition)

Cas des structures ordonnées ?

(AB-A.Rabinovich)

Pour toute structure $M = (A, <, \overline{P})$, si $(A, <)$ est dénombrable ou contient un intervalle de type $\pm\mathbb{N}$ alors M n'est pas maximale pour MSO

Exemples

$A = \mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, tout ordinal infini, tout ordre infini scattered (i.e. sans sous-ordre dense)

Résultats partiels pour FO

Idée de la preuve

- Soit $M = (A, <, \overline{P})$, où $(A, <)$ est dénombrable ou contient un intervalle de type $\pm\mathbb{N}$
- Principe :
  1. Découper A en petits intervalles de type $\pm\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{Q}$, à l'aide d'une relation d'équivalence $\approx$ définissable dans M
  2. Etendre séparément chaque intervalle
  3. Utiliser le thm de composition
- On prouve d'abord le résultat pour
  - $(\mathbb{N}, <, \overline{P})$
  - $(\mathbb{Z}, <, \overline{P})$
  - $(\mathbb{Q}, <, \overline{P})$ avec $\overline{P}$ homogène

Idée de la preuve (2)

- Soit $M = (A, <, \overline{P})$, où $(A, <)$ est dénombrable ou contient un intervalle de type $\pm\mathbb{N}$
- On définit $x \approx y$ ssi $[x, y]$ fini ou $[x, y]$ inclus dans un intervalle de type $\mathbb{Q}$ homogène
- $\approx$ est une condensation (toute classe est un intervalle)
- $\approx$ est définissable dans M
- A quoi ressemblent les classes d'équivalence ?
  1. intervalles finis
  2. intervalles de type $\pm\mathbb{N}$
  3. intervalle de type $\mathbb{Z}$
  4. intervalle de type $\mathbb{Q}$ où $\overline{P}$ est homogène
- Plusieurs cas :
  1. si $(A, <)$ contient un intervalle de type $\pm\mathbb{N}$, alors au moins l'une des classes est de type (1) ou (2)
  2. au moins l'une des classes est de type (4)
  3. somme dense dénombrable d'intervalles finis (cas le plus difficile)

Idée de la preuve (3) - un exemple

- Exemple : si $M = (A, <, \overline{P})$ contient au moins un intervalle de type $\mathbb{N}$, et au moins une $\approx -$classe de type $\mathbb{N}$
- On étend M en M' à l'aide d'un prédicat unaire R.
  On étend chaque $\approx -$classe de type $\mathbb{N}$ en utilisant la construction pour $(\mathbb{N}, <, \overline{P})$ (et on n'ajoute rien ailleurs)
- Notations : $M = \sum_{i \in I} M_i$ et $M' = \sum_{i \in I} M'_i$
- R non définissable ? facile
- $MSO(M')$ décidable ?
  - D'après Shelah, $MSO(M')$ se réduit à $MSO(I, <, (Q'_\tau))$ où les Q'_τ représentent les types des M'_i
  - Chaque Q'_τ peut s'exprimer à l'aide de prédicats Q_τ qui représentent les types des M_i
  - $MSO(I, <, (Q'_\tau))$ se réduit donc à $MSO(I, <, (Q_\tau))$
  - la relation $\approx$ est définissable dans M, donc $MSO(I, <, (Q_\tau))$ s'interprète dans $MSO(M)$

Idée de la preuve (4) - remarque sur l'uniformité

- On a démontré

$$MSO(M') \rightsquigarrow MSO(I,<,(Q'_\tau)) \rightsquigarrow MSO(I,<,(Q_\tau)) \rightsquigarrow MSO(M)$$

- La réduction $MSO(I,<,(Q'_\tau)) \rightsquigarrow MSO(I,<,(Q_\tau))$ vient du fait que l'on peut calculer *uniformément* le $k-$type de M'_i à partir du $g(k)-$type de M_i (g récursive), ce qui est rendu possible par le fait d'avoir étendu toutes les $\approx-$classes de type $\mathbb{N}$ (pas seulement cela).
- Peut-on se contenter d'étendre une seule $\approx-$classe de type $\mathbb{N}$?
- Ne marche pas forcément : si $M = (\mathbb{N} \times \mathbb{Z}, <, P)$ avec $MSO(M)$ décidable, et FO indécidable pour toute expansion par une constante, et qu'on étend une seule $\approx-$classe de type $\mathbb{N}$ dans M, alors R possède un plus petit élément, qui est définissable dans M', d'où $MSO(M')$ indécidable.

Pour aller plus loin

- Y. Gurevich, Monadic Second-Order Theories, dans Model-Theoretic Logics (J. Barwise and S. Feferman), 1985
- W. Thomas, Ehrenfeucht games, the composition method, and the monadic theory of ordinal words, LNCS 1997
- J.A. Makowsky, Algorithmic Uses of the Feferman-Vaught Theorem, APAL 2004