A New Proof of a Theorem by Ginsburg and Spanier

Marcus Kracht

[Kra02]

Emmanuel Cornet
École normale supérieure

Cours de Théorie des automates – MPRI

18 février 2005

Plan

Ensembles linéaires et semilinéaires

Définition

Un sous-ensemble non vide de $\mathbb{N}^n$ est dit **linéaire** s'il s'écrit sous la forme

$$\overrightarrow{v_0} + \mathbb{N}\,\overrightarrow{v_1} + \mathbb{N}\,\overrightarrow{v_2} + \cdots + \mathbb{N}\,\overrightarrow{v_m}$$

pour un certain $m \in \mathbb{N}$ et où $\forall i \in \{1, \ldots, n\} \quad \overrightarrow{v_i} \in \mathbb{N}^n$.

Définition

Un sous-ensemble de $\mathbb{N}^n, \mathbb{Z}^n$ ou $\mathbb{Q}^n$ est dit **semilinéaire** s'il est l'union finie d'ensembles linéaires.

Exemples

- L'ensemble des nombres pairs est linéaire.
- L'ensemble $\{2^n; n \geq 0\}$ n'est pas semilinéaire.

Quelques propriétés

Quelques propriétés (dont certaines démontrées dans l'article) :

Propositions

- *Si un sous-espace affine $M \subset \mathbb{Q}^n$, alors $M \cap \mathbb{N}^n$ est un sous-ensemble semilinéaire de $\mathbb{N}^n$.*
- *Les ensembles semilinéaires sont clos par produit cartésien, union, somme, intersection et projection sur les composantes.*

Arithmétique de Presburger

Définition

L'**arithmétique de Presburger** est la théorie du premier ordre sur la structure

$$\underline{\mathbb{Z}} = \langle \mathbb{Z}, 0, 1, +, <, \langle \equiv_m, m \in \mathbb{N}^* \rangle \rangle$$

L'arithmétique de Presburger est moins puissante que celle de Peano (pas de multiplication), mais elle possède beaucoup de vertus (complétude, décidabilité...).

On peut éliminer la négation :

$$\begin{array}{lcl} \neg(x = y) & \leftrightarrow & x < y \vee y < x \\ \neg(x < y) & \leftrightarrow & x = y \vee y < x \\ \neg(a \equiv_m b) & \leftrightarrow & \bigwedge_{0<i<m} a \equiv_m b + \underline{i} \end{array}$$

où $\underline{i}$ est défini par $\underline{0} = 0$ et $\underline{n+1} = \underline{n} + 1$.

Presburger-définissabilité

Définition

Un sous-ensemble de $\mathbb{Z}^n$ est **Presburger-définissable** s'il existe une formule de l'arithmétique de Presburger que les éléments de S (et eux seuls) vérifient.

Le théorème de Ginsburg & Spanier

Théorème

Un sous-ensemble de $\mathbb{N}^n$ est semilinéaire si, et seulement si, il est Presburger-définissable.

Théorème intermédiaire : élimination des quantificateurs

Définition

On dit qu'une théorie T admet l'élimination des quantificateurs si toute formule est équivalente dans T à une formule sans quantificateurs.

Théorème

L'arithmétique de Presburger admet l'élimination des quantificateurs.

Démonstration du théorème intermédiaire (1/3)

Démonstration.

Il suffit de montrer que pour toute formule $\exists x\ \varphi(\overrightarrow{y}, x)$ où $\varphi(\overrightarrow{y}, x)$ est sans quantificateurs, il existe une formule sans quantificateur $\chi(\overrightarrow{y})$ telle que

$$\mathbb{Z} \models \forall \overrightarrow{y}\ \exists x \quad \varphi(\overrightarrow{y}, x) \leftrightarrow \chi(\overrightarrow{y})$$

On simplifie le problème car on peut :

- éliminer la négation ;
- éliminer la disjonction : $\exists x\ (\alpha \vee \beta) \leftrightarrow (\exists x\ \alpha) \vee (\exists x\ \beta)$;
- supposer que toutes les conjonctions contiennent x : si α ne contient pas d'occurrence libre de x, $\exists x\ \alpha \wedge \beta \leftrightarrow \alpha \wedge \exists x\ \beta$.

Démonstration du théorème intermédiaire (2/3)

Démonstration.

On peut donc considérer que φ se met sous la forme :

$$\exists x \left(\bigwedge_{i<p} n_i x = t_i\right) \wedge \left(\bigwedge_{i<q} n'_i x < t'_i\right) \wedge \left(\bigwedge_{i<r} n''_i x > t''_i\right) \wedge \left(\bigwedge_{i<s} n'''_i x \equiv_m t'''_i\right)$$

mais $s\mathcal{R}t \leftrightarrow n\,s\mathcal{R}n\,t$:

$$\exists x \left(\bigwedge_{i<p} \nu x = \tau_i\right) \wedge \left(\bigwedge_{i<q} \nu x < \tau'_i\right) \wedge \left(\bigwedge_{i<r} \nu x > \tau''_i\right) \wedge \left(\bigwedge_{i<s} \nu x \equiv_m \tau'''_i\right)$$

puis :

$$\exists x \left(x \equiv_\nu 0\right) \wedge \left(\bigwedge_{i<p} x = \tau_i\right) \wedge \left(\bigwedge_{i<q} x < \tau'_i\right) \wedge \left(\bigwedge_{i<r} x > \tau''_i\right) \wedge \left(\bigwedge_{i<s} x \equiv_m \tau'''_i\right)$$

On peut considérer que :

- $p = 0$: $\bigwedge_{i<j<p} \tau_i = \tau_j \wedge x = \tau_0$ (occurrences de $x \rightsquigarrow \tau_0$) ;
- $q \leq 1, r \leq 1$:
  $(x < \sigma \wedge x < \tau) \leftrightarrow \big((x < \sigma \wedge \sigma \leq \tau) \vee (x < \tau \wedge \tau < \sigma)\big)$
- $s \leq 1$: *(petit raisonnement à base de pgcd)*.

Démonstration du théorème intermédiaire (3/3)

Démonstration.

$$\exists x \left(\bigwedge_{i<q} x < \tau_i'\right) \wedge \left(\bigwedge_{i<r} x > \tau_i''\right) \wedge \left(\bigwedge_{i<s} x \equiv_m \tau_i'''\right)$$

Il ne reste plus que 8 possibilités ($q, r, s \in \{0; 1\}$).

- Si $r = 0$ ou $q = 0$ (4 possibilités) : φ est équivalente à `true` ;
- $(\exists x \quad x < \tau \wedge v < x) \leftrightarrow (v + 1 < \tau)$
- $(\exists x \quad x < \tau \wedge v < x \wedge x \equiv_m \xi) \leftrightarrow$
  $\left(\bigvee_{i<m} (\tau + 1 + i < v \wedge \tau + 1 + i \equiv_m \xi)\right)$

□

Démonstration du théorème principal

Théorème

$M \subset \mathbb{N}^n$ semilinéaire $\Leftrightarrow$ M est Presburger-définissable.

Démonstration.

$\boxed{\Rightarrow}$ Il suffit de montrer que les ensembles *linéaires* sont définissables. Soit $M' = \overrightarrow{v} + \mathbb{N}\overrightarrow{v_0} + \cdots + \mathbb{N}\overrightarrow{v_{m-1}}$. La formule suivante définit M :

$$\varphi(\overrightarrow{x}) = \exists y_0 \ldots \exists y_{m-1} \quad \left(\bigwedge_{i<m} 0 \leq y_i \wedge \bigwedge_{i<n} \left(\overrightarrow{v}(i) + \sum_{j<m} y_i \, \overrightarrow{v}(i)_j = x_i \right) \right)$$

$\boxed{\Leftarrow}$ Soit $\varphi(\overrightarrow{x})$ une formule qui définit S. Alors il existe $\chi(\overrightarrow{x})$ sans quantificateurs qui définit S, et sans négation. χ est donc une disjonction de conjonctions de formules atomiques. Les sous-ensembles semilinéaires de $\mathbb{N}^n$ étant clos par intersection et par union, il suffit de vérifier que les formules atomiques définissent des ensembles semilinéaires, ce qui est facile. $\square$

Bibliographie

- L'article étudié :

  [Kra02] Marcus Kracht, A New Proof of a Theorem by Ginsburg and Spanier, manuscript, UCLA, December 2002 (published in *The Mathematics of Language*)

Retrouvez les documents sur le Web

Cette présentation est disponible au format PDF à l'adresse

`www.eleves.ens.fr/home/cornet/Presburger_presentation.pdf`