DVT (2) : Décidabilité de l'arithmétique de Presburger

L'arithmétique de Presburger = PA où on interdit l'usage de la multiplication

On procède ainsi : (i) On définit un langage $\mathcal{L}$ tel que admet l'élimination des quantificateurs

(ii) A chaque proposition de $\{0, S, +, =\}$ (← dans $\mathbb{N}$) on associe une proposition de $\mathcal{L}$ dans $\mathbb{Z}$

(i) $\mathcal{L} = \{0, 1, +, -, \leq, \text{Mult}_n\}$. Mq $\mathcal{L}$ admet l'élimination des quantificateurs

(a) On va mq $\forall$ A sans quantificateur $\exists$ B sans quantificateur, $\exists x A \Leftrightarrow B$ est valide dans $\mathbb{Z}$

dém.

* $C \Rightarrow D \rightsquigarrow \neg C \vee D$
* $\neg T \rightsquigarrow \bot$; $\neg \bot \rightsquigarrow T$; $\neg(C \wedge D) \rightsquigarrow \neg C \vee \neg D$; $\neg(C \vee D) \rightsquigarrow \neg C \wedge \neg D$; $\neg\neg C \rightsquigarrow C$; $\neg t \leq u \rightsquigarrow u+1 \leq t$; $\neg \text{Mult}_n(t) \rightsquigarrow \text{Mult}_n(t+1) \vee \dots \vee \text{Mult}_n(t+n-1)$
* dans chaque inéquation, on met les x du même côté
* On remplace $t \leq u$ par $kt \leq ku$ et $\text{Mult}_n(t)$ par $\text{Mult}_{kn}(kt)$ de façon à avoir le même coefficient devant x : sx
* On introduit $x' = sx$ et on rajoute $\text{Mult}_s(x')$ $\rightsquigarrow A'$, $\exists x A \Leftrightarrow \exists x' A'$
* Soit r un multiple commun des n tels que $\text{Mult}_n(x+t) \in A'$
* $E := \{t, x' \leq t \in A'\}$
* $A'' := A'[x' \leq t \rightsquigarrow \bot, t \leq x' \rightsquigarrow T]$
* $B := \bigvee_{i=0}^{r-1} A''[i/x'] \vee \bigvee_{t \in E} \bigvee_{j=0}^{r-1} A'[t-j/x']$

exple $A := 1 \leq \exists x \wedge x \leq y - x$

* —
* —
* $1 \leq 3x \wedge 2x \leq y$
* $2 \leq 6x \wedge 6x \leq 3y$
* $A' := 2 \leq x' \wedge x' \leq 3y \wedge \text{Mult}_6(x')$
* $r := 6$
* $E := \{3y\}$
* $A'' := T \wedge \bot \wedge \text{Mult}_6(x') = \bot$
* $B := A'[3y/x'] \vee A'[3y-1/x'] \vee \dots \vee A'[3y-5/x']$

□ Supposons que $\exists p \in \mathbb{Z}$, $A'[q_1, \dots q_n, p]$ soit valide (ie $\exists x' A'$ valide)

→ Si $\forall r$ $A'[q_1, \dots, q_n, p+rr]$ est valide alors pour p' assez grand on a :

$A'[q_1, \dots q_n, p'] \leftrightarrow A''[q_1, \dots, q_n, p']$. Donc $A''[q_1 \dots q_n, p']$ valide

Or $\forall p$ $A''[q_1, \dots q_n, p] \leftrightarrow A''[q_1, \dots q_n, p-r]$ donc $\exists i \in [0, r-1]$, $A''[i/x']$ valide

Donc $B[q_1, \dots q_n]$ valide

→ Sinon $\exists p'$ $\begin{cases} A'[q_1, \dots q_n, p'] \text{ valide} \\ A'(q_1 \dots q_n, p'+r] \text{ non valide} \end{cases}$

$\exists t, x' \le t \in E,\ p' \le t[q_1, \dots q_n],\ \neg(p'+r \le t(q_1, \dots q_n])$.

⇒ $\exists j \in [0, r-1],\ p' = t[q_1 \dots q_n] - j$. Donc $B[q_1 \dots q_n]$ valide.

□ Réciproquement si $B[q_1, \dots q_p]$ est valide.

→ Soit $\exists i \in [0, r-1]$, $A''[q_1, \dots q_n, i]$ soit valide.

Comme $A''[q_1, \dots q_n, p] \Leftrightarrow A'(q_1 \dots q_n, p+r]$ $\forall p$ et que pour p assez gd $A''[q_1, \dots q_n, p] \leftrightarrow A'[q_1 \dots q_n, p]$ on obtient $\exists p,\ A'[q_1, \dots q_n, p]$ valide.

→ Soit $\exists t \in E, j \in [0, r-1]$, $A'[q_1, \dots, q_n, t[q_1 \dots q_n] - j]$ valide. ok.

(b) Corollaire : $\forall A \in \mathcal{F}(\mathcal{L})$ $\exists B$ sans quantificateur et close telle que $A \leftrightarrow B$ soit valide dans $\mathbb{Z}$

clém. On remplace $\forall x\, C$ par $\neg \exists x \neg C$ puis récurrence.

(ii). A de Presburger $\rightsquigarrow |A|$ de $\mathcal{L}$:

- $|0| = 0$; $|x| = x$; $|S(t)| = |t|+1$; $|t+u| = |t| + |u|$
- $|t \le u| = |t| \le |u| \wedge |u| \le |t|$
- $|\top| = \top$; $|\bot| = \bot$; $|\neg A| = \neg |A|$; $|A \wedge B| = |A| \wedge |B|$; $|A \vee B| = |A| \vee |B|$; $|A \Rightarrow B| = |A| \to |B|$
- $|\forall x A| = \forall x (0 \le x \Rightarrow |A|)$; $|\exists x A| = \exists x (0 \le x \wedge |A|)$

Ainsi Presburger admet l'élimination des quantificateurs.

Comme pour toute formule close sur $\{0, S, +, =\}$ (atomique) il est facile de décider si elle est valide ou pas dans $\mathbb{N}$ et que la théorie est récursive sur un langage fini, par les théorèmes 56 et 59, Presburger est décidable (sur $\mathbb{N}$).

Refs : Dowek, Chap 7.
(DNR, Chap 3)

DVT 3 : Indécidabilité d'une théorie permettant d'encoder les programmes

Rappel : {fonctions calculables} = le + pt ensemble contenant les projections, les fonctions nulles, le successeur, l'addition, la multiplication et $\chi_\leq$ et clos par composition et minimisation

- Props représentant un prog : f calculable. Si :

- $f = \pi_i^n$, $A := Eq[x_i, y]$
- $f = Z^n$, $A := Null[y]$
- $f = Succ$, $A := Succ[x_1, y]$
- $f = +$, $A := Plus[x_1, x_2, y]$
- $f = \times$, $A := Mult[x_1, x_2, y]$

On veut $f(x_1 \dots x_n) = y \Leftrightarrow A[x_1 \dots x_n, y]$

$Inf \leftarrow \exists z (N[z] \wedge Plus[z, x, y])$

$InfS \leftarrow \exists x' (N[x'] \wedge Succ[x, x'] \wedge Inf[x', x])$

- $f = \chi_\leq$, $A := (Inf[x_1, x_2] \wedge \exists z (Null[z] \wedge Succ[z, y]) \vee (InfS[x_2, x_1] \wedge Null[y])$
- $f = o_m^n(h, g_1, \dots g_m)$. $g_i \simeq B_i$. $h \simeq C$

  $A := \exists w_1, \dots w_m (N[w_1] \wedge \dots \wedge N[w_m] \wedge \bigwedge_{i=1}^{m} B_i[x_1, \dots x_m, w_i] \wedge C[w_1, \dots w_m, y])$
- $f = \mu^n(g)$. $g \simeq B$ $A := (\forall z (N[z] \wedge InfS[z, y] \Rightarrow \exists w w' (N[w'] \wedge Succ[w', w] \wedge B[x_1, \dots, x_n, z, w]))) \wedge (\forall w (Null[w] \rightarrow B[x_1, \dots x_n, y, w]))$

- Théorie $\mathcal{T}$: On donne à N, Null, Succ, Plus, Mult, Eq les sens usuels de $\mathbb{N}$

- Prédicat N : $\forall x (Null[x] \rightarrow N[x]) \wedge \forall xy ((N[x] \wedge Succ[x, y]) \rightarrow N[y])$
- Ice des entiers : $\exists x\, Null[x] \wedge \forall x (N[x] \rightarrow \exists y\, Succ[x, y])$
- égalité : $\forall x\, Eq[x, x] \wedge \forall xy (Null[x] \rightarrow (Null[y] \leftrightarrow Eq[x, y]) \wedge$
  $\forall xyx'y' ((N[x] \wedge Succ[x, x'] \wedge Eq[x, y]) \rightarrow (Succ[y, y'] \leftrightarrow Eq[x', y'])$
- Successeur : $\forall xyx'y' (Succ[x, x'] \wedge Succ[y, y'] \wedge Eq[x', y']) \Rightarrow Eq[x, y]) \wedge$ (A_3)
  $\forall xx' (Succ[x, x'] \rightarrow \neg Null[x']) \wedge \forall x (N[x] \rightarrow (Null[x] \vee \exists y (N[y] \wedge Succ[y, x]$ (A_1, A_2)
- addition : $\forall xyz ((Null[x] \wedge N[y]) \Rightarrow (Eq[y, z] \leftrightarrow Plus[x, y, z]) \wedge$ (A_4)
  $\forall xyzx'z' ((N[x] \wedge N[y] \wedge Plus[x, y, z] \wedge Succ[x, x']) \rightarrow (Succ[z, z'] \leftrightarrow Plus[x', y, z'])) \wedge$ (A_5)
  $\forall xyx'y' ((N[x] \wedge N[y] \wedge Succ[x, x'] \wedge Succ[z, z'] \wedge Plus[x, y, z]) \rightarrow Plus[x, y, z]) \wedge$
  $\forall xyy'z' ((N[x] \wedge N[y] \wedge N[y'] \wedge Succ[y, y'] \wedge Plus[x, y', z']) \rightarrow \exists z (Plus[x, y, z] \wedge Succ[z, z']))$

- multiplication : $\forall x\, y\, z\ ((\mathrm{Null}(x) \wedge N(y)) \to (\mathrm{Null}(z) \leftrightarrow \mathrm{Mult}(x,y,z)))$
  $\forall x\, y\, z\, x'\, z'\ ((N(x) \wedge N(y) \wedge \mathrm{Mult}(x,y,z) \wedge \mathrm{Succ}(x,x')) \to (\mathrm{Plus}(y,z,z') \leftrightarrow \mathrm{Mult}(x',y,z')))$

- **$\mathbb{N}$-modèle** : $\mathcal{L}$ langage ar les prop N, Null, Succ, Plus, Mult, Eq. $\mathcal{N}$ $\mathbb{N}$-modèle
  - $\{a \in \mathcal{N},\ N(a) = 1\} = \mathbb{N}$
  - $\{a \in \mathbb{N},\ \mathrm{Null}(a) = 1\} = \{0\}$
  - $\{(a,b) \in \mathbb{N}^2,\ \mathrm{Succ}(a,b) = 1\} = \{(a,b) \in \mathbb{N}^2,\ b = a+1\}$
  - $\{(a,b,c) \in \mathbb{N}^3,\ \mathrm{Plus}(a,b,c) = 1\} = \{(a,b,c) \in \mathbb{N}^3,\ c = a+b\}$
  - $\{(a,b,c) \in \mathbb{N}^3,\ \mathrm{Mult}(a,b,c) = 1\} = \{(a,b,c) \in \mathbb{N}^3,\ c = a \times b\}$
  - $\{(a,b) \in \mathbb{N}^2,\ \mathrm{Eq}(a,b) = 1\} = \{(a,b) \in \mathbb{N}^2,\ a = b\}$

  Les $\mathbb{N}$-modèles sont des modèles de $\mathcal{C}_0$

- **Prop** $\mathcal{L}$ ar N, Null, Succ, Plus, Mult, Eq. $\mathcal{C} \vdash \mathcal{C}_0$ ayant un $\mathbb{N}$-modèle $\mathcal{N}$. f un programme et A la prop représentant f. Alors :
  (i) $f(p_1, \dots p_n) = q$
  ⇕
  (ii) $\mathcal{C} \vdash \forall x_1 \dots x_n\, y\ ((N_{p_1}(x_1) \wedge \dots \wedge N_{p_n}(x_n) \wedge N_q(y)) \to A(x_1, \dots x_n, y))$ — $N_a(v) := N(v) \wedge \mathrm{Eq}(a,v)$
  ⇕
  (iii) $\mathcal{N} \models$

  dém. Par rec s/ la structure de f"

- **Def** f un prog. A représente f. Alors la prop "f termine sur $p_1 \dots p_n$" est :
  $\forall x_1 \dots x_n\ ((N_{p_1}(x_1) \wedge \dots N_{p_n}(x_n)) \to \exists y\ (N(y) \wedge A(x_1, \dots, x_n, y))) = \top$

  Si $\mathcal{C}$ est décidable, on sait décider $\top$ = le problème de l'arrêt. Contradiction. Donc $\mathcal{C}$ n'est pas décidable.

- **Rq** $\mathcal{C} \vdash \mathcal{C}_0$ est une hyp. superflue.

- **Cor** PA est indécidable.

  dém.
  - $N = \top$
  - $\mathrm{Null} = (x = 0)$
  - $\mathrm{Succ} = (y = S(x))$
  - $\mathrm{Plus} = (z = x + y)$
  - $\mathrm{Mult} = (z = x \times y)$
  - $\mathrm{Eq} = (x = y)$

  Et $\mathbb{N}$ est un $\mathbb{N}$-modèle de PA.

Réf. Dowek, Chap 5.