C. R. Acad. Sci. Paris, t. 315, Série I, p. 1431-1434, 1992

Informatique théorique/*Computer Science*

Indécidabilité de la théorie des entiers naturels munis d'une énumération des premiers et de la divisibilité

Patrick CEGIELSKI et Denis RICHARD

Résumé — Soient L_1 (resp. L_2) le langage logique du permier ordre ayant deux symboles propres: un de fonction noté π, l'autre de relation binaire (resp. ternaire) noté $|$ (resp. $\bullet$). Dans tout modèle $\langle M, +, \bullet \rangle$ de Peano, le symbole π sera interprété par une fonction injective de M dans l'ensemble des entiers premiers du modèle (dite *énumération de premiers*), le symbole $|$ (resp. $\bullet$) par la relation de divisibilité (resp. le graphe de la multiplication). On démontre que dans un tel modèle, une relation est L_2-définissable si, et seulement si, elle est L_1-définissable. Les relations arithmétiques ne sont pas toutes L_1-définissables (resp. L_2-définissables). Cependant il existe une structure sur M qui est L_1-définissable (donc également L_2-définissable) isomorphe à ce modèle (c'est la propriété de L_1 et L_2 dite de *ré-interprétation isomorphe*). Par suite les théories $TH(\mathbb{N}, \pi, |)$ et $TH(\mathbb{N}, \pi, \bullet)$ sont *indécidables.*

The theory of positive integers structured by a list of primes and divisibility is undecidable

Abstract — *Let L_1 (resp. L_2) be the language of first order logic which has two symbols, one of function and the other of a binary (resp. ternary) predicate. In every model of Peano's arithmetic $\langle M, +, \bullet \rangle$, the symbol π is interpreted by a one-to-one function from* M *into its set of prime integers (called* list of primes*), symbol $|$ (resp. $\bullet$) by the divisibility relation (resp. graph of multiplication). We prove that in such a model, every relation is L_2-definable if and only if it is L_1-definable. All arithmetical relations are not L_1-definable (resp. L_2-definable). However there is an L_1-definable (also L_2-definable) structure over* M *which is isomorphic to the previous model (this is precisely the* isomorphic reinterpretation property *of languages L_1 and L_2). Hence theories $TH(\mathbb{N}, \pi, |)$ and $TH(\mathbb{N}, \pi, \bullet)$ are* undecidable.

INTRODUCTION ET NOTATIONS. — On s'intéresse ci-dessous à des langages qui possèdent la propriété de coder les suites finies. Ces langages apparaissent utiles dans des questions d'informatique théorique pour coder des mots, des graphes et ramener certains problèmes dans le cadre de l'arithmétique. Par ailleurs, ces langages sont en eux-mêmes intéressants et posent des questions parfois difficiles de définissabilité.

On dira que deux sous-langages L et L′ du langage *plein* L(PA) de l'arithmétique sont *équidéfinissables dans Peano*, ou *synonymes*, ce qui se notera $L \equiv L'$, si, et seulement si, on peut prouver dans l'arithmétique de Peano (c'est-à-dire, d'après le théorème de complétude, dans n'importe quel modèle de Peano) que tout symbole de relation L-définissable est L′-définissable, et réciproquement.

On dira, par abus, que $L \subseteqq L'$ si, et seulement si, on peut prouver dans l'arithmétique de Peano que tout symbole de relation arithmétique qui est L-définissable est aussi L′-définissable. Évidemment, si $L \subseteqq L'$ et si $L' \subseteqq L$, alors $L \equiv L'$.

Un *language* $L \subseteqq L(PA)$ est dit *strict* si, et seulement si, il n'est pas synonyme de L(PA).

Les symboles de relations et fonctions sont ceux habituellement utilisés (comme pour la divisibilité) auxquels s'ajoutent $x \perp y$ pour exprimer que x et y sont premiers entre eux. Soit $x \mapsto p_x$ l'application qui à x associe le $(x+1)$-ième entier premier (ainsi $p_0 = 2$, $p_3 = 3$). On note $(x)_y = z$ la relation indiquant que l'exposant de p_y dans x est z. On notera $y \in x$ le symbole de relation $\exists z ((x)_y = z \wedge z \neq 0)$.

Note présentée par Maurice NIVAT.

0764-4442/92/03151431 $ 2.00

Soit π un symbole fonctionnel dont l'interprétation (dans $\langle \mathbb{N}, +, \bullet \rangle$) sera une injection de $\mathbb{N}$ dans l'ensemble $\mathbb{P}$ des premiers.

PROBLÈMES ET RÉSULTATS. — On considère les langages suivants: $L_0 = \{x \in y\}$; $L_0' = \{x \mapsto p_x, \perp\}$; $L_1 = \{x \mapsto p_x, |\}$; $L_2 = \{x \mapsto p_x, \bullet\}$; $L_3 = \{(x)_y = z\}$; $L(PA) = \{+, \bullet\}$. Il est clair que l'on a la suite d'inclusions suivante:

$$L_0 \subseteq L_0' \subseteq L_1 \subseteq L_2 \subseteq L_3 \subseteq L(PA).$$

La question est de savoir si elles sont strictes ou non. Il est facile de voir que $L_0 \equiv L_0'$. Il est démontré en ([1], p. IV-25 à 32) que $L(PA) \equiv L_3$, et que $L_0 \not\equiv L_1$. Nous allons prouver ici que $L_1 \equiv L_2$ et que $L_3 \not\equiv L_1$. Il en résulte que les théories des interprétations naturelles dans $\mathbb{N}$ des langages L_1 et L_2 sont strictement plus faibles que l'arithmétique de Peano. Pour qu'elles puissent modéliser valablement les problèmes de codages de suites finies, il faut qu'elles soient indécidables, puisque la théorie d'une seule relation binaire (par exemple la théorie des graphes) est elle-même indécidable, et en effet nous montrerons l'indécidabilité de $TH(\mathbb{N}, \pi, |)$ et $TH(\mathbb{N}, \pi, \bullet)$. On constatera dans certaines preuves que l'énumération naturelle des premiers peut être remplacée par une fonction injective quelconque (pas nécessairement surjective) de l'ensemble des entiers dans l'ensemble des premiers.

Plus précisément, nous démontrerons le théorème suivant:

THÉORÈME. — *Soient, dans un modèle* M *quelconque de Peano,* π *une énumération d'un sous-ensemble des premiers et* $x \mapsto p_x$ *l'énumération des entiers premiers. On considère les deux langages* $L_1' = \{\pi, |\}$ *et* $L_2' = \{\pi, \bullet\}$.

(i) *Pour toute énumération* π, *toutes les relations définissables dans le réduit* $(M, \pi, \bullet)$ *le sont dans* $(M, \pi, |)$ *(et réciproquement), et donc les langages* L_1' *et* L_2' *sont équidéfinissables dans l'arithmétique de Peano; en particulier les théories* $TH(\mathbb{N}, \pi, |)$ *et* $TH(\mathbb{N}, \pi, \bullet)$ *sont extensions par définition l'une de l'autre;*

(ii) L_1 *(donc également* L_2*) ne sont pas synonymes du langage plein* $L(PA)$ *de l'arithmétique;*

(iii) *Les langages* L_1 *et* L_2 *possèdent la propriété de ré-interprétation isomorphe, de sorte que* $TH(\mathbb{N}, x \mapsto p_x, |)$ *et* $TH(\mathbb{N}, x \mapsto p_x, \bullet)$ *sont indécidables.*

Pour obtenir (i) on démontre les trois lemmes suivants, le premier étant classique.

LEMME 1 (Premières notions définissables dans le langage de la divisibilité). — *Dans l'arithmétique de Peano sont* $\{|\}$*-définissables les symboles de relations suivantes:*

[x est premier] *noté* PREM (x);

[u est une puissance non nulle du premier p] *noté* PRIM (p, u);

[u est primaire] *noté* PRIM (u);

[u est le primaire de plus grand exposant qui divise x (*appelé* composante p-adique de x)] *noté* COMP (x, p, u);

[d est le pgcd de x et y] *noté* PGCD (x, y, d);

[m est le ppcm de x et y] *noté* PPCM (x, y, m);

Les symboles de relations usuelles $[x = y]$, $[x = 0]$, $[x = 1]$ *respectivement notés de la même façon;*

[x et y sont premiers entre eux] *noté* $x \perp y$;

[p est premier et $u = p^2$] *noté* $\square(p, u)$;

[x est premier ou est produit de premiers distincts (*c'est-à-dire* est un nombre de Poulet)] *noté* POUL (x).

Un deuxième groupe de notions, L_1'-définissables, sert à comparer les exposants des premiers apparaissant dans les décompositions des entiers.

LEMME 2. — (a) *Dans tout modèle de Peano, la relation, notée* INJ(x, y, j), *définie par* [x et y sont des produits de nombres premiers, sont premiers entre eux et j code une injection de l'ensemble des diviseurs de x (*dit* support *de* x *et noté* SUPP(x)) dans l'ensemble SUPP(y) des diviseurs de y] *est* L_1'*-définissable*;

(b) *Dans tout modèle de Peano, la relation, notée* BIJ(x, y), *définie par*

[x et y sont des produits de premiers, sont premiers entre eux et

$$\text{Card}(\text{SUPP}(x)) = \text{Card}(\text{SUPP}(y))]$$

est L_1'*-définissable.*

Pour définir le produit dans le langague L_1', il sera nécessaire de pouvoir y exprimer le produit de p-primaires pour un même premier p. Pour cela, nous aurons besoin de notions auxiliaires de codages de hauteur de primaires, c'est-à-dire de coder l'exposant d'un primaire donné.

LEMME 3. — *Soient, dans un modèle* M *de Peano, p et q des premiers distincts,* $u = p^\alpha$ *et* $h = \pi(p).\pi(p^2)...\pi(p^\alpha)$ *et* $k = \pi(q.p).\pi(q.p^2)...\pi(q.p^\alpha)$.

(a) *Les relations ci-dessus liant d'une part u et h et, d'autre part, u, k et q, notées* HAUT(u, h) *et* HAUTBIS(u, k, q), *sont toutes deux* L_1'*-définissables.*

(b) *La relation, notée* MULTFIBRE(p, u, v, w), *indiquant que w est le produit des primaires u et, v puissances d'un même premier p, est* L_1'*-définissable.*

PROPOSITION 4. — *Dans tout modèle de Peano, une relation arithmétique est* $\{\pi, \bullet\}$*-définissable si, et seulement si, elle est* $\{\pi, |\}$*-définissable, de sorte que* $L_1' = \{\pi, |\}$ *et* $L_2' = \{\pi, \bullet\}$ *sont synonymes.*

Cette proposition achève la preuve du point (i) du théorème. La question naturelle est alors de montrer que $\{\pi, |\}$ est un langage strict, ce qui constitue le point (ii) du théorème. Compte tenu de la proposition 4, il suffit de montrer que $\{\pi, \bullet\}$ est strict. Cela résulte de la

PROPOSITION 5. — *Le* L_2*-automorphisme* $f: \mathbb{N} \to \mathbb{N}$ *déterminé par*

$$f(0) = 0 \quad \text{et} \quad f(1) = 1,$$
$$f(p_x) = p_{f(x)} \quad \text{pour tout } x,$$
$$f(a.b) = f(a).f(b) \quad \text{lorsque } a \perp b,$$
$$f(a^n) = f(a)^n \quad \text{pour tout } a \text{ et tout } n \in \mathbb{N},$$

ne respecte pas l'ordre naturel. En conséquence, les langages L_1 *et* L_2 *sont stricts.*

La proposition 5 prouve le point (ii) du théorème et, comme L_1 et L_2 sont stricts, il est naturel de se demander s'ils ont *la propriété de ré-interprétation isomorphe*, c'est-à-dire de savoir si dans chaque modèle M de Peano, on peut définir une L_1*-structure interne* (à savoir un sous-ensemble de M muni de deux lois de composition interne, tous trois L_1-définissables) isomorphe à M. La proposition 7 donnera une réponse positive à cette question.

Remarquons d'abord que $x \in 2^M$ si, et seulement si, PRIM$(2, x)$ ou $x = 1$, de sorte que l'ensemble 2^M est L_1-définissable. Soient $u = 2^x$, $v = 2^y$ et $w = 2^z$. On définit une addition sur 2^M en posant:

$$w = u \oplus v = 2^x \oplus 2^y = 2^x.2^y = 2^{x+y}.$$

On observe que $(2^x, 2^y) \mapsto 2^{x+y}$ est L_2 (et donc L_1)-définissable par une formule notée $\oplus(u, v, w)$. La fonction $\phi : \mathrm{M} \to 2^{\mathrm{M}}$ déterminée par $\phi(x) = 2^x$ est une bijection qui respecte les additions.

Comme, dans un modèle quelconque de Peano, $[z = x.y]$ équivaut à $[(x+y)^2 = x^2 + y^2 + z + z]$, la multiplication y est $\{+, x \mapsto x^2\}$-définissable. Pour étendre $\langle 2^{\mathrm{M}}, \oplus \rangle$ en un modèle $\langle 2^{\mathrm{M}}, \oplus, \otimes \rangle$ interne à M et isomorphe à celui-ci, il suffit donc de définir une application $2^x \mapsto 2^x \otimes 2^x$ de façon à ce que $\phi(x^2) = 2^{(x^2)} = 2^x \otimes 2^x$ et à ce que $\langle 2^{\mathrm{M}}, \oplus, 2^x \mapsto 2^x \otimes 2^x \rangle$ soit isomorphe à $\langle \mathrm{M}, +, x \mapsto x^2 \rangle$.

LEMME 6. — *Soient x un entier donné, $u = p_{2^x}^x$ un entier primaire et*

$$c = p_{2^x}^x . p_{2^{2^x}}^{x+1} . p_{2^{3^x}}^{x+2} \ldots p_{2^{x^2}}^{2^x}.$$

La relation entre c et u est L_1-définissable dans tout modèle de l'arithmétique de Peano par une formule notée CODCALCCAR (u, c).

PROPOSITION 7. — *Dans tout modèle de Peano, l'application*

$$u = 2^x \mapsto v = 2^{(x^2)} = 2^x \otimes 2^x$$

est L_1-définissable par une formule notée CAR (u, v).

Preuve. — Une formule de L_1 pour CAR (u, v) est la suivante :

$$\exists c \exists p \exists w \{ \mathrm{CODCALCCAR}(u, c) \wedge \mathrm{MAX}(c, p) \wedge p = p_v \}. \quad \square$$

La proposition 7 et la remarque faite avant le lemme 6 montrent que les langages L_1 et L_2 possèdent la propriété de ré-interprétation isomorphe, ce qui implique clairement l'indécidabilité de TH $(\mathbb{N}, x \mapsto p_x, |)$ et TH $(\mathbb{N}, x \mapsto p_x, \bullet)$. $\square$

Question. — Pour démontrer que L_1 et L_2 sont équivalents, on a eu besoin de définir une notion d'*équipotence*. On se pose naturellement la question de savoir s'il existe une notion d'équipotence $\{ \mid \}$-définissable. Les méthodes usuelles de définisabilité ne semblent pas fournir de preuve de la réponse naturellement conjecturée comme négative.

Note remise le 19 octobre 1992, acceptée le 2 novembre 1992.

RÉFÉRENCES BIBLIOGRAPHIQUES

[1] D. RICHARD, Définissabilité en arithmétique et méthode de codage Z.B.V. appliquée à des languages avec successeurs et coprimarité, *Thèse de doctorat d'État*, Université de Lyon-I, 1985, p. IV-25 à IV-32.

[2] P. CEGIELSKI et D. RICHARD, *Undecidability and undefinability from computational complexity within positive integers structures by a list of primes and divisibility*, preprint du LLAIC 1.

D. R. : *Laboratoire de Logique, Algorithmique et Informatique de Clermont-I (LLAIC* 1), *I.U.T.Informatique*, B. P. n° 86, 63172 *Aubière Cedex;*

P. C. : *L.I.T.P., I.B.P., U.R.A. n°* 248, *Université Paris-VII*, 55-56-119, 4, *place Jussieu*, 75252 *Paris Cedex* 05.