C. R. Acad. Sci. Paris, t. 331, Série I, p. 107–110, 2000
Logique/*Logic*

La théorie élémentaire de la fonction de couplage de Cantor des entiers naturels est décidable

Patrick CÉGIELSKI [a], Serge GRIGORIEFF [b], Denis RICHARD [c]

[a] **LACL, Université Paris-12–IUT, route forestière Hurtault, 77300 Fontainebleau, France**
Courriel : cegielski@univ-paris12.fr
[b] **LLAIC 1, Université Paris-7, 2, place Jussieu, 75251 Paris cedex 05, France**
Courriel : seg@ufr-info-p7.jussieu.fr
[c] **LLAIC 1, IUT informatique des Cézeaux, B.P. 86, 63172 Aubière cedex, France**
Courriel : richard@llaic.u-clermont1.fr

(Reçu le 5 mai 2000, accepté le 22 mai 2000)

Résumé. La fonction de couplage de Cantor, notée C, est définie de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$ par $C(x, y) = (1/2)\,(x + y)(x + y + 1) + y$. La théorie du premier ordre des entiers naturels munis de la fonction de Cantor est décidable. © 2000 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS

The elementary theory of the Cantor pairing function is decidable

Abstract. *The Cantor pairing function C from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{N}$ is defined by $C(x, y) = (1/2)\,(x + y)(x + y + 1) + y$. The first order theory of natural integers equipped with the Cantor pairing function is decidable.* © 2000 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS

Introduction

En 1873, Georg Cantor [1,2] a montré que les ensembles $\mathbb{N}^2$ et $\mathbb{N}$ sont équipotents, où $\mathbb{N}$ est l'ensemble des entiers naturels, en exhibant la bijection définie par :

$$C(x, y) = (1/2)\,(x + y)(x + y + 1) + y.$$

Il existe bien d'autres bijections et injections de $\mathbb{N}^2$ dans $\mathbb{N}$. On appelle *fonction de couplage* (en Anglais *pairing function*) toute injection J de $\mathbb{N}^2$ dans $\mathbb{N}$.

Il est intéressant d'étudier la théorie élémentaire, c'est-à-dire la théorie du premier ordre, des structures $(\mathbb{N}, J)$, d'abord parce que c'est une structure naturelle, ensuite parce que cela permet de répondre à des questions pour lesquelles la réponse n'est pas claire si on ne se restreint pas à un cadre logique bien déterminé. L'étude de la théorie élémentaire nous a permis, par exemple, de bien faire la différence entre les n-uplets et les listes (*voir* [3]).

Nous avons donné, dans l'article cité ci-dessus, d'une part un exemple de fonction de couplage J telle que la théorie de $(\mathbb{N}, J)$ soit décidable et, d'autre part, un exemple de fonction (récursive) telle que la théorie de

Note présentée par Gérard HUET.

S0764-4442(00)00517-6/FLA

$(\mathbb{N}, J)$ soit indécidable. Aucun résultat n'était connu en ce qui concerne les fonctions de couplage naturelles bien connues, en particulier la fonction de Cantor définie ci-dessus, pour laquelle il existe de nombreux problèmes ouverts : $C(x,y)$ et $C(y,x)$ sont les seuls polynômes du second degré, à coefficients dans $\mathbb{R}$, à établir une bijection entre $\mathbb{N}^2$ et $\mathbb{N}$ (*voir* [9], p. 24) mais on ne sait pas ce qu'il en est si on enlève la condition sur le degré.

Il existe un résultat général de complexité [5] : *si f est une fonction injective de $\mathbb{N}^2$ dans $\mathbb{N}$ alors la complexité algorithmique de la théorie de la structure $(\mathbb{N}, f, =)$ a une borne inférieure dans*

$$\mathrm{NTime}\big(\exp_\infty\big(\mathrm{O}(n)\big)\big),$$

où $\exp_\infty(n)$ est une tour d'exponentielle $2^{2^{\cdot^{\cdot^{2}}}}$ de hauteur n.

Nous allons démontrer ici que la théorie $\mathrm{Th}(\mathbb{N}, C)$ est décidable en utilisant un résultat de Maltsev sur les algèbres libres. Notons que nous avons, depuis, amélioré ce résultat en démontrant que la théorie de la structure $(\mathbb{N}, C, S)$, où S est la fonction successeur, est également décidable (*voir* [4]) par une méthode totalement différente et dont la démonstration est fort longue.

THÉORÈME. – *La théorie élémentaire de la structure $(\mathbb{N}, C)$, où $\mathbb{N}$ est l'ensemble des entiers naturels et C la fonction de couplage de Cantor, est décidable.*

1. Rappels sur les algèbres libres

Nous renvoyons, par exemple, à [6] pour une introduction à la logique du premier ordre ainsi que pour les notations classiques utilisées dans ce domaine.

DÉFINITION 1. – Une structure du premier ordre (A, L) est une *algèbre* si, et seulement si, son langage L ne contient pas de prédicat autre que l'égalité (et donc uniquement des symboles de fonctions ; les constantes sont considérées comme des symboles de fonctions 0-aires).

DÉFINITION 2. – Une algèbre (A, L) est *localement libre* si, et seulement si, elle vérifie tous les axiomes possibles de l'une des trois formes suivantes :

$$\begin{aligned} f\big(\vec{x}\big) &\neq g\big(\vec{y}\big), \\ f(x_1,\dots,x_n) = f(y_1,\dots,y_n) &\longrightarrow (x_1 = y_1 \wedge \cdots \wedge x_n = y_n), \\ t(x_1,\dots,x_n) &\neq x_i. \end{aligned}$$

Pour le premier type d'axiomes, f et g sont deux symboles de fonctions différents de L, et $\vec{x}$ et $\vec{y}$ des uplets de variables, de longueurs égales aux arités de f et de g respectivement.

Pour le deuxième type d'axiomes, f est un symbole de fonctions de L d'arité n, et $x_1,\dots,x_n$, $y_1,\dots,y_n$ des variables, toutes différentes.

Pour le troisième type d'axiomes, t est un terme de L d'arité n, $x_1,\dots,x_n$ des variables et $1 \leqslant i \leqslant n$.

PROPOSITION 1 (Anatole Maltsev, [7]). – *Toute algèbre localement libre a une théorie élémentaire décidable.*

2. Démonstration du résultat

Introduction. – La démonstration repose sur la remarque fondamentale selon laquelle l'algèbre de termes sur le langage $(C, 0, 1)$ engendre $\mathbb{N}$ mais n'est pas libre, puisqu'on a $C(0,0) = 0$ et $C(1,0) = 1$. Cependant, l'algèbre de termes sur le langage comprenant C, $2 = C(0,1)$, $4 = C(1,1)$ et quelques fonctions auxiliaires est libre er engendre $\mathbb{N} \setminus \{0,1\}$.

Remarque 1. – Les constantes 0 et 1 sont définissables dans l'algèbre $(\mathbb{N}, C)$, de la façon suivante :

$$x = 0 \leftrightarrow C(x,x) = x,$$
$$x = 1 \leftrightarrow \big(x \neq 0 \wedge C(x,0) = x\big).$$

Notations. – Notons L_0, L_1, R_0 et R_1 les applications de $\mathbb{N}$ dans $\mathbb{N}$ définies de la façon suivante :

$$L_0(x) = C(0,x), \quad L_1(x) = C(1,x), \quad R_0(x) = C(x,0), \quad R_1(x) = C(x,1).$$

LEMME 1. – *L'algèbre* $(\mathbb{N} \setminus \{0,1\}, 2, 4, C, L_0, L_1, R_0, R_1)$ *est libre.*

Démonstration. – Résulte immédiatement des deux faits suivants :

$$C(x,y) = C(u,v) \longrightarrow (x = u \wedge y = v),$$
$$C(x,y) > x \quad \text{et} \quad C(x,y) > y \quad \text{pour } (x,y) \neq (0,0),\ (1,0).$$

COROLLAIRE 1. – *La théorie* $\mathrm{Th}\,(\mathbb{N} \setminus \{0,1\}, 2, 4, C, L_0, L_1, R_0, R_1)$ *est décidable.*

LEMME 2. – *Tout terme* $t(x_1, \ldots, x_n, 0, 1)$ *du langage* $\{C, 0, 1\}$*, non équivalent à* 0 *ou à* 1*, est équivalent à un terme du langage* $\{2, 4, C, L_0, L_1, R_0, R_1\}$*, ayant le même ensemble de variables.*

L'équivalence signifie qu'ils prennent la même valeur dans le modèle standard dont l'ensemble de base est $\mathbb{N}$.

LEMME 3 (Réduction). – *Pour toute formule* $F(x_1, \ldots, x_n)$ *du langage* $\{C, 0, 1\}$*, il existe une formule* $\varphi(F)(x_1, \ldots, x_n)$ *de* $\{C, L_0, L_1, R_0, R_1\}$ *telle que, pour* $a_1, \ldots, a_n \in \mathbb{N} \setminus \{0,1\}$*, on ait* :

$$(\mathbb{N}, C, 0, 1) \models F[a_1, \ldots, a_n]$$

si, et seulement si,

$$(\mathbb{N}, 2, 4, C, L_0, L_1, R_0, R_1) \models \varphi(F)[a_1, \ldots, a_n].$$

Démonstration. – Il suffit de poser :

$$\begin{aligned}
\varphi(\neg F) &:= \neg\varphi(F),\\
\varphi(F \wedge G) &:= \varphi(F) \wedge \varphi(G),\\
\varphi(\exists x F) &:= (\exists x \geqslant 2)\big(\varphi(F)\big)(x) \vee \varphi\big(F[0/x]\big) \vee \varphi\big(F[1/x]\big)
\end{aligned}$$

[en remarquant dans ce dernier que, en fait $\exists x \geqslant 2$ est équivalent à $\exists x$ dans la structure $(\mathbb{N}, 2, 4, C, L_0, L_1, R_0, R_1)$],

$$\begin{aligned}
&\varphi(0 = 0) := \varphi(1 = 1) := 4 = 4,\\
&\varphi(0 = 1) := \varphi(1 = 0) := \varphi(t = 0) := \varphi(t = 1) := \varphi(0 = t) := \varphi(1 = t) := 4 \neq 4,\\
&\varphi(t = u) := t = u
\end{aligned}$$

[pour des termes t et u non réduits à 0 ou à 1, dans les deux derniers cas]. □

On en déduit facilement la décidabilité de $\mathrm{Th}\,(\mathbb{N}, C)$.

Références bibliographiques

[1] Cantor G., 1873 in: Cantor Georg, Dedekind Richard, Briefwelrel, Hermann, Paris, 1937; traduction française in: Cavaillès J., Philosophie mathématique, Hermann, Paris, 1962, pp. 177–249.

[2] Cantor G., Uber eine Eigenschaft des Inbegroffes aller reellen algebraischen Zahlen, J. fur die Reine und Angew. Math. 77 (1874) 258–262; = Gesamm. abh., Springer, Berlin, 1930, pp. 15–118; traduction française in: Acta Math. 2 (1883) 305–310.
[3] Cegielski P., Richard D., On arithmetical first-order theories allowing encoding and decoding of lists, Theor. Comput. Sci. 222 (1999) 55–75.
[4] Cegielski P., Richard D., Decidability of the theory of the natural integers with the Cantor pairing function and the successor, Theor. Comput. Sci. (à paraître).
[5] Compton K.J., Henson C.W., A uniform method for proving lower bounds on the computational complexity of logical theories, Ann. Pure and Appl. Logic 48 (1990) 1–79.
[6] Enderton H.B., A Mathematical Introduction to Logic, Academic Press, 1972, XIII+295 p.
[7] Mal'cev A.I., On the elementary theories of locally free universal algebras, Soviet Math. Doklady (1961) 768–771.
[8] Mal'cev A.I., Axiomatizable classes of locally free algebras of various types, Sibirsk. Mat. Z. (1962) 729–743 (en russe) ; English translation in: The Metamathematics of Algebraic Systems: Collected Papers 1936–1967, North-Holland, Studies in Logic and the Found. of Math. 66 (1971) 262–281.
[9] Smorynski C., Logical Number Theory I, Springer-Verlag, Berlin, 1991, X+405 p.