Sur un problème de la logique à n valeurs

par

W. Sierpiński (Warszawa)

Dans la logique à n valeurs chaque proposition admet une des n valeurs $0, 1, 2, \ldots, n-1$ et chaque fonction logique d'un nombre fini k de propositions peut être déterminée par une fonction $f(x_1, x_2, \ldots, x_k)$ de k variables, définie pour $x_i = 0, 1, \ldots, n-1$ $(i = 1, 2, \ldots, k)$ et ne prenant que les valeurs $0, 1, \ldots, n-1$. Désignons par $\varphi(x, y)$ et $\psi(x, y)$ des fonctions de deux variables, définies pour $x = 0, 1, \ldots, n-1$, $y = 0, 1, \ldots, n-1$ comme il suit: $\varphi(x, y)$, resp. $\psi(x, y)$ est le reste de la division du nombre $x+y$, resp. xy par le nombre n. (Pour $n = 2$ ces fonctions déterminent la somme et le produit logique.)

Le but de cette Note est de trouver quel doit être le nombre naturel $n > 1$ pour que toute fonction logique d'un nombre fini de propositions dans la logique à n valeurs se réduise (par superpositions) aux trois fonctions

(1) $$1\ (^1),\ \varphi(x, y) \text{ et } \psi(x, y).$$

Je démontrerai notamment que, pour qu'il en soit ainsi, il faut et il suffit que n soit un nombre premier.

En langage mathématique ce théorème peut être exprimé comme il suit:

THÉORÈME. *Pour que toute fonction d'un nombre fini de variables, définie pour les valeurs* $0, 1, \ldots, n-1$ *de ces variables, où* n *est un nombre naturel* > 1, *et ne prenant que les valeurs* $0, 1, \ldots, n-1$, *puisse être exprimée (par superpositions) à l'aide des fonctions* (1), *il faut et il suffit que* n *soit un nombre premier.*

Démonstration. Soit n un nombre premier. Désignons par $F_k^{(n)}$ la famille de toutes les fonctions $f(x_1, x_2, \ldots, x_k)$ de k variables définies pour $x_i = 0, 1, \ldots, n-1$ $(i = 1, 2, \ldots, k)$ et ne prenant que les valeurs $0, 1, \ldots, n-1$. La famille $F_k^{(n)}$ est évidemment formée de n^{n^k} fonctions distinctes. D'autre part soit $P_k^{(n)}$ la famille de tous les polynômes en

(1) C'est-à-dire la fonction dont la valeur est le nombre 1 pour $x = 0, 1, \ldots, n-1$.

$x_1, x_2, \ldots, x_k$ à coefficients $0, 1, \ldots, n-1$, dont les degrés en chacune des variables $x_1, x_2, \ldots, x_k$ sont $< n$. On voit sans peine qu'il y a n^{n^k} tels polynômes. Tout polynôme de la famille $P_k^{(n)}$, lorsqu'on remplace sa valeur par son reste modulo n, détermine évidemment une fonction de la famille $F_k^{(n)}$. Je dis que deux polynômes distincts de la famille $P_k^{(n)}$ déterminent deux fonctions distinctes de la famille $F_k^{(n)}$.

Pour le démontrer il suffit de prouver que, $f(x_1, x_2, \ldots, x_k)$ et $g(x_1, x_2, \ldots, x_k)$ étant deux polynômes de la famille $P_k^{(n)}$, on a $f(x_1, x_2, \ldots, x_k) \equiv g(x_1, x_2, \ldots, x_k) \pmod n$ pour $x_1, x_2, \ldots, x_k$ entiers seulement dans le cas où les polynômes f et g sont identiques.

Pour $k = 1$ cela résulte tout de suite du théorème de Lagrange sur le nombre des racines d'une congruence au module premier, et pour k naturel quelconque on en déduit sans peine notre proposition par induction (en considérant $f(x_1, \ldots, x_{k+1})$ et $g(x_1, \ldots, x_{k+1})$ comme des polynômes en x_{k+1}).

La famille $P_k^{(n)}$ donne ainsi n^{n^k} fonctions distinctes de la famille $F_k^{(n)}$, donc toutes les fonctions de cette famille.

Chaque fonction de $F_k^{(n)}$ peut donc être représentée par un polynôme de $P_k^{(n)}$ pris modulo n. Or, on voit sans peine que tout polynôme en $x_1, x_2, \ldots, x_k$ à coefficients entiers est modulo n une superposition des trois fonctions (1).

Par exemple $x = (x, 1)$ pour x entiers, $0 \equiv \Big(x, \big(x, \big(x \ldots, (x, x)\big)\big)\ldots\Big) \pmod n$ pour x entiers.

Chaque fonction de la famille $F = F_1^{(n)} + F_2^{(n)} + F_3^{(n)} + \ldots$ est ainsi (pour les valeurs $0, 1, \ldots, n-1$ des variables) congruente modulo n à une superposition des trois fonctions (1), donc égale à une telle superposition, puisque deux fonctions de la famille F (en tant que fonctions qui prenent seulement les valeurs $0, 1, \ldots, n-1$) ne sont congruentes modulo n (pour toutes les valeurs de variables) que dans le cas où elles sont identiques. La condition de notre théorème est donc suffisante.

Soit maintenant n un nombre composé et soit p un diviseur de n: on a donc $p < n$. Soit $f(x, y)$ la fonction définie comme il suit: $f(p, 0) = 1$ et $f(x, y) = 0$ pour tous les systèmes x, y autres que le système $p, 0$. Je dis que la fonction $f(x, y)$ (considérée pour $x = 0, 1, \ldots, n-1$, $y = 0, 1, \ldots, n-1$) ne peut pas être exprimée par superpositions à l'aide des fonctions (1).

En effet, soit Φ la famille de toutes les fonctions de la famille $F_2^{(n)}$ qui sont des superpositions des fonctions (1). On voit sans peine que toute fonction de Φ est représentable modulo n par un polynôme à coefficients entiers. Cela résulte tout de suite du fait que si l'on a pour $x = 0, 1, \ldots, n-1$, $y = 0, 1, \ldots, n-1$, $f(x, y) \equiv f_1(x, y) \pmod n$ et $g(x, y) \equiv g_1(x, y) \pmod n$, où f, et g, sont des polynômes, alors

$$\varphi\big(f(x, y), g(x, y)\big) \equiv f_1(x, y) + g_1(x, y) \pmod n,$$

$$\psi\big(f(x, y), g(x, y)\big) \equiv f_1(x, y) \cdot g_1(x, y) \pmod n$$

pour $x = 0, 1, \ldots, n-1$, $y = 0, 1, \ldots, n-1$.

Il suffira donc de démontrer que la fonction f n'est pas représentable modulo n par un polynôme en x, y à coefficients entiers. En effet, si c'était le cas, le terme constant de ce polynôme $g(x, y)$ devrait être divisible par n, puisque $f(0, 0) = 0$, donc le nombre $g(p, 0)$ serait divisible par p, par suite $g(p, 0) \equiv 0 \pmod p$, tandis que $f(p, 0) = 1$, d'où $f(p, 0) \equiv 1 \pmod p$ et $f(p, 0) \not\equiv g(p, 0) \pmod p$, ce qui donne à plus forte raison $f(p, 0) \not\equiv g(p, 0) \pmod n$ (puisque p est un diviseur de n). Par conséquent la fonction f n'appartient pas à la famille Φ.

La condition de notre théorème est donc nésessaire.

Notre théorème est ainsi démontré. Nous en déduirons maintenant ce corollaire:

COROLLAIRE. *Si $n > 2$, les trois fonctions* (1) *peuvent être remplacées dans notre théorème par les deux fonctions*

$$\theta(x, y) \quad \text{et} \quad \psi(x, y), \tag{2}$$

où $\theta(x, y)$ est (pour $x = 0, 1, \ldots, n-1$, $y = 0, 1, \ldots, n-1$) le reste de la division du nombre $x+y+1$ par n (2).

En effet, soit n un nombre premier impair et soit Π la famille de toutes les fonctions qui s'experiment à l'aide de superpositions par les fonctions (2). On a, pour $x = 0, 1, \ldots, n-1$, $y = 0, 1, \ldots, n-1$: $\theta(x, y) \equiv x+y+1 \pmod n$, donc $\theta(x, x) \equiv 2x+1 \pmod n$. La fonction $2x+1$ est donc pour $x = 0, 1, \ldots, n-1$, $y = 0, 1, \ldots, n-1$ congruente modulo n à une fonction de Π. Supposons que $kx+(k-1) \equiv f(x, y) \pmod n$, où $f \in \Pi$. On aura $(k+1)x+k \equiv \theta\big(x, f(x, y)\big) \pmod n$, donc la fonction $(k+1)x+k$ est congruente modulo n à une fonction de Π. Il en résulte par induction que la fonction $nx+n-1$, donc aussi la fonction -1, est congruente modulo n à une fonction de Π, et par suite, aussi la fonction $\psi(-1, -1) = 1$, d'où il résulte tout de suite que $1 \in \Pi$. La fonction $x+2 = x+1+1 \equiv \theta(x, 1) \pmod n$ est donc congruente à une fonction de Π. On démontre le même par induction pour les fonctions $(x+2)+2 = x+4$, $(x+4)+2 = x+6, \ldots, x+(n-1)$ (puisque n est impair), donc la fonction $\varphi(x, y) \equiv x+y \equiv x+(n-1)+y+1 \equiv \theta(x+n-1, y) \pmod n$ est aussi congruente modulo n à une fonction de Π, d'où $\varphi \in \Pi$. Par conséquent on a $1 \in \Pi$, $\varphi \in \Pi$, $\psi \in \Pi$, et il résulte tout de suite de notre théorème que notre corollaire est vrai pour n premiers > 2.

(2) Pour $n = 2$ on peut démontrer que, dans notre théorème, les fonctions (1) peuvent être remplacées par une seule fonction $\tau(x, y)$, où $\tau(x, y)$ est (pour $x = 0, 1, \ldots, n-1$, $y = 0, 1, \ldots, n-1$) le reste de la division du nombre $xy+1$ par n.

Soit maintenant n un nombre composé et supposons que toute fonction de F soit une superposition des fonctions (2). Vu que $\theta(x,y) \equiv \varphi(x,y)+1 \equiv \varphi(\varphi(x+1), y) \pmod{n}$ pour $x = 0, 1, \ldots, n-1$, $y = 0, 1, \ldots, n-1$, toute fonction de F serait donc une superposition des fonctions (1), contrairement à notre théorème.

Notre corollaire est ainsi démontré.

Reçu par la Rédaction le 12. 3. 1960

Undecidable and creative theories

by

J. R. Shoenfield * (Durham, N. C.)

1. The basic method of proving that a formal system is undecidable (i. e., has an unsolvable decision problem) is the original method of Church [1], which requires that recursive functions or sets be representable in some sense in the system. Other methods are given in [9]; but in each case, it is shown that the decidability of the given system would imply the decidability of a system already seen to be undecidable by the basic method.

To formulate the precise results, we recall some definitions. By a *theory*, we shall mean a formal system, formalized within the first order predicate calculus with equality. We suppose Gödel numbers assigned to the terms and sentences (1) of each theory by one of the usual methods. We say that a theory is *decidable* if the set of (Gödel numbers of) theorems of the theory is recursive. A theory is *axiomatizable* if the set of theorems of the theory is recursively enumerable (2).

We shall suppose that in each theory T a sequence of terms

$$\overline{0}, \overline{1}, \overline{2}, \ldots$$

is fixed so that the Gödel number of $\overline{n}$ is a recursive function of n, and so that if $m \neq n$, then $\vdash_T \overline{m} \neq \overline{n}$.

Let $A(x)$ be a sentence of the theory T containing no free variable other than x. We say that $A(x)$ *strongly represents* a set K if

$$n \in K \to \vdash_T A(\overline{n})$$

and

$$n \notin K \to \vdash_T \neg A(\overline{n})$$

for all n. We say that $A(x)$ *weakly represents* K if

$$n \in K \leftrightarrow \vdash_T A(\overline{n})$$

* This research was supported by a grant from the National Science Foundation of the U.S.A.

(1) We do not require (as in [9]) that a sentence contain no free variables.

(2) This is equivalent to more usual definitions of axiomatizability by Craig's theorem.