DEMONSTRATIO MATHEMATICA
Vol. XI No 4 1978

A. O. Uziembło, L. Żurawska

DEFINABILITY OF FUNCTIONS ON A FINITE SET BY MEANS OF COMPOSITIONS OF ADDITION AND MULTIPLICATION MODULO SOME PRIME NUMBERS

The aim of this paper is to show that every function defined on a finite set of cardinality Q may be represented as a composition of addition and multiplication modulo prime numbers which divide Q and usual addition and multiplication. A.W. Kuzniecow [1] showed that if n is prime, then every function defined on $N_n = \{0,1,\ldots,n-1\}$ and with values in this set may be represented as a composition of addition and multiplication modulo n. In this paper we generalize Kuzniecow's theorem to sets of cardinality, which is not prime. Let $Q = q_1\ldots q_r$, where $q_1,\ldots,q_r$ is a non-decreasing r - termed sequence of primes. We define a sequence $Q_0,\ldots,Q_r$ of natural numbers by

$$Q_0 = Q,\ldots,Q_{s+1} = \frac{Q_s}{Q_{s+1}} \quad \text{for} \quad s < r.$$

The following theorem holds.

T h e o r e m 1. If $q_1,\ldots,q_r$ is a non-decreasing r-termed sequence of primes and $Q = q_1\ldots q_r$, then for every natural number $z < Q$ there exists exactly one sequence $z_1,\ldots,z_r$ of natural numbers, such that

$$(i) \qquad z = z_1Q_1 + \ldots + z_rQ_r$$

and

(ii) $0 \leq z_s < q_s$ for $s = 1,\dots,r$.

P r o o f : It suffices to remark that if $0 < z < Q$, then there exists $s < r$ such that $Q_{s+1} \leq z < Q_s$ and $\frac{z}{Q_{s+1}} < q_{s+1}$.

If $z = 0$, then let $z_1 = \dots = z_r = 0$.

The theorem proved above allows us to give the following definition.

D e f i n i t i o n . For any natural numbers $Q > 1$ and $0 \leq z < Q$ the sequence $z_1,\dots,z_r$ is the expansion of z for the base Q, in symbols $z = (z_1,\dots,z_r)_Q$ iff the sequence $z_1,\dots,z_r$ satisfies conditions (i) and (ii) from Theorem 1.

Let $Q = q_1 \dots q_r$, where $(q_i)_{i=1}^{r}$ be a non-decreasing sequence of primes and $x_i \in N_Q$, for $i = 1,\dots,m$.

According to the above definition we have:

$$x_1 = (\overset{1}{x}_1,\dots,\overset{1}{x}_r)_Q$$

$$\vdots$$

$$x_m = (\overset{m}{x}_1,\dots,\overset{m}{x}_r)_Q.$$

Let us denote $(\tilde{x}) = \langle x_1,\dots,x_m \rangle$ and let $a_1,\dots,a_m \in N_Q$. We define a function $c_{(\tilde{a})} : N_Q^m \to \{0,1\}$ in the following way

$$c_{(\tilde{a})}(\tilde{x}) = \begin{cases} 1 & \text{if } (\tilde{x}) = (\tilde{a}) \\ 0 & \text{if } (\tilde{x}) \neq (\tilde{a}). \end{cases}$$

Then we have the following lemma.

L e m m a 1.

$$c_{(\tilde{a})}(\tilde{x}) = \prod_{i=1}^{m} \prod_{j=1}^{r} \left[\left(1 - (\overset{i}{x}_j - \overset{i}{a}_j)^{q_j - 1} \right) (\mathrm{mod}\ q_j) \right].$$

P r o o f . Let $(\tilde{x}) = (\tilde{a})$. Then we obviously have

$$c_{(\tilde{a})}(\tilde{a}) = \prod_{i=1}^{m} \prod_{j=1}^{r} \left[1 - (\overset{i}{a}_j - \overset{i}{a}_j)^{q_j-1} \pmod{q_j}\right] = 1.$$

Let $(\tilde{x}) \neq (\tilde{a})$. There are indices i,j, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant r$ such that $\overset{i}{x}_j \neq \overset{i}{a}_j$. By the Fermat theorem we have $(\overset{i}{x}_j - \overset{i}{a}_j)^{q_j-1} = 1 \pmod{q_j}$, hence $\left(1 - (\overset{i}{x}_j - \overset{i}{a}_j)^{q_j-1}\right) = 0 \pmod{q_j}$. Hence, for $(\tilde{x}) \neq (\tilde{a})$ we have $c_{(\tilde{a})}(\tilde{x}) = 0$. Q.E.D.

J. Słupecki [4] gives an example of a function f, such that every function defined on $Z_Q = \{1,\dots,Q\}$, where $Q \in N$, and with values in Z_Q may be represented as a composition of f. This function f is defined by

$$f^Q(x,y) = \begin{cases} 1 & \text{if } x \neq y \text{ or } x = y = Q \\ x + 1 & \text{if } x = y \text{ and } x < Q \end{cases}$$

for any $x, y \in Z_Q$.

From this it easily follows that each function $h : N_Q^m \longrightarrow N_Q$ is a composition of $g^Q : N_Q \times N_Q \longrightarrow N_Q$ defined in the following way

$$(*) \qquad g^Q(x,y) = \begin{cases} 0 & \text{if } x \neq y \text{ or } x = y = Q - 1 \\ x + 1 & \text{if } x = y \text{ and } x < Q - 1. \end{cases}$$

From the definition of $c_{(\tilde{a})}$ and $(*)$ we have

L e m m a 2.

$$g^Q(x,y) = \sum_{i=0}^{Q-2} c_{(i,i)}(x,y) \cdot (x + 1).$$

We omit an easy proof of Lemma 2.

From Lemmas 1 and 2 we get the following theorem.

T h e o r e m 2. If $Q = q_1 \dots q_r$, where $q_1,\dots,q_r$ is a non-decreasing sequence of prime numbers, then every function $f : N_Q^m \to N_Q$ is a composition of operations modulo q_i, $i = 1,2,\dots,r$ and usual addition and multiplication.

We would like to thank T. Prucnal for his valuable suggestions.

REFERENCES

[1] С.В. Яблонский: Функциональные построения в k-значной логике, Trudy Mat. Inst. Steklov, Moskwa 1958.

[2] E. Bałuka: O sprawdzaniu wyrażeń wielowartościowych rachunku zdań, Studia Logika 17 (1965).

[3] G. Bryll: O półpełnych systemach rachunku zdań, Studia Logika 19 (1966.

[4] J. Słupecki: O tak zwanych algebrach pełnych. Sprawozdania ze Zjazdu Matematyków Słowiańskich, Praga 1948.

INSTITUTE OF MATHEMATICS, PEDAGOGICAL UNIVERSITY, KIELCE
Received November 14, 1977.