Serdica J. Computing **2** (2008), 313–320

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

ON SOME GENERALIZATIONS OF A CLASS OF DISCRETE FUNCTIONS

Dimiter Stoichkov Kovachev

Abstract. In this paper we examine discrete functions that depend on their variables in a particular way, namely the H-functions. The results obtained in this work make the "construction" of these functions possible. H-functions are generalized, as well as their matrix representation by Latin hypercubes.

1. Introduction, definitions and notation. Some of the major results regarding H-functions were obtained in the works [2, 4, 6].

We will denote the set of all functions of n variables of the k-valued logic by

$$P_n^k = \{f : E_k^n \to E_k / E_k = \{0, 1, \dots, k-1\}, \quad k \geq 2\}.$$

It is proved that the matrix form of every H-function from P_n^k is a Latin hypercube and vice versa, every Latin hypercube is the matrix form of an H-function from P_n^k. Latin squares and hypercubes have their applications in coding

ACM Computing Classification System (1998): G.2.0.
Key words: k-valued logic, H-function, subfunction, range, spectrum, Latin hypercubes and hyperparallelepipeds.

theory [5, §13.1], error correcting codes [5, §13.2 ÷ 13.5], information security, decision making, statistics [5, §1.4, §12.1÷12.3], cryptography [5, §14.1÷ 14.5], conflict-free access to parallel memory systems [5, §16.3], experiment planning, tournament design [5, §1.6, §16.5], etc.

Definition 1 [3]**.** *The number $Rng(f)$ of different values of the function f is called the range of f.*

We denote the set of variables of the function $f(x_1, x_2, \ldots, x_n)$ by X_f.

Definition 2. *Every function obtained from $f(x_1, x_2, \ldots, x_n)$ by replacing the variables of M, $M \subseteq X_f$, $0 \le |M| \le n$, with constants is called a subfunction of f with respect to M.*

The notation $g \longrightarrow\!\!\!\prec f$ ($g \overset{M}{\longrightarrow\!\!\!\prec} f$) means that g is a subfunction of f (with respect to M).

Definition 3 [3]**.** *If M is the set of variables of the function f and $G = \{g : g \overset{X_f \backslash M}{\longrightarrow\!\!\!\prec} f\}$ is the set of all subfunctions of f with respect to $X_f \backslash M$, then the set $Spr(M, f) = \bigcup\limits_{g \in G} \{Rng(g)\}$ is called the spectrum of the set M for the function f.*

Definition 4 [2]**.** *We say that $f(x_1, x_2, \ldots, x_n)$ is an H-function if for every variable x_i, $1 \le i \le n$, $n \ge 2$ and for every $n+1$ constants $\alpha_1, \ldots, \alpha_{i-1}$, α', α'', α_{i+1}, $\ldots$, $\alpha_n \in E_k$ with $\alpha' \ne \alpha''$ we have*

$$f(\alpha_1, \ldots, \alpha_{i-1}, \alpha', \alpha_{i+1}, \ldots, \alpha_n) \ne f(\alpha_1, \ldots, \alpha_{i-1}, \alpha'', \alpha i+1, \ldots, \alpha_n).$$

In [4], it is proven that a function $f(x_1, x_2, \ldots, x_n) \in P_n^k$ is an H-function if and only if for every variable x_i, $i = 1, 2, \ldots, n$ the following equality holds: $Spr(x_i, f) = \{k\}$.

The examined class of $H[m; q]$-functions is a generalization of the H-functions in P_n^k.

Definition 5 [4]**.** *We say that the function $f(x_1, x_2, \ldots, x_n) \in P_n^k$ is an $H[m; q]$-function if for every set M of m elements, $M \subseteq X_f$, of variables of the function f we have $Spr(M, f) = \{q\}$.*

When $m = 1$ and $q = k$, the set of $H[1; k]$-functions of P_n^k is equal to the set of H-functions of P_n^k.

One of the results for H-functions in [7] is expanded with the proof that a function $f \in P_n^k$ is an $H[m; q]$-function if and only if each of its subfunctions that depends on at least m variables is an $H[m; q]$-function [4].

2. Main results. Let $F_n^k(\mathbb{K}) = \{f : \mathbb{K} \to E_k\}$, where $\mathbb{K} = K_1 \times K_2 \times \cdots \times K_n$, and $K_i = \{0, 1, \ldots, k_i - 1\}$, $k_i \geq 2$, $i = 1, 2, \ldots, n$ be finite sets. It is obvious that $P_n^k = F_n^k(E_k^n)$. Let us denote by $P_n^{k,q}(F_n^{k,q}(\mathbb{K}))$ the set of all functions belonging to $P_n^k(F_n^k(\mathbb{K}))$, which have a range q. By $A = \|a_{ij}\|_{m,n}$ we denote the matrix with m rows and n columns, which is called a 2-dimensional matrix of $m \times n$ size. By $B = \|b_{i_1 i_2 \ldots i_n}\|_{k_1, k_2, \ldots, k_n}$ we denote the n-dimensional matrix of size $k_1 \times k_2 \times \cdots \times k_n$. In the special case when $k_1 = k_2 = \cdots = k_n = k$, the matrix $C = \|c_{i_1 i_2 \ldots i_n}\|_{k_1, k_2, \ldots, k_n}$ is denoted by $C = \|c_{i_1 i_2 \ldots i_n}\|_1^k$ and is called an n-dimensional matrix of order k.

Each function $f(x_1, x_2, \ldots, x_n)$ from $P_n^k(F_n^k(\mathbb{K}))$ can be represented in matrix form $\|a_{i_1 i_2 \ldots i_n}\|_1^k(\|a_{i_1 i_2 \ldots i_n}\|_{k_1, k_2, \ldots, k_n})$, where for each element of the corresponding matrix, the equality $a_{i_1 i_2 \ldots i_n} = f(x_1 = i_1 - 1, x_2 = i_2 - 1, \ldots, x_n = i_n - 1)$ holds.

Definition 6. *We will call a Latin n-dimensional hyperparallelepiped (hypercube when $k_1 = k_2 = \ldots = k_n = k$) of size $k_1 \times k_2 \times \cdots \times k_n$ based on the set $E_k = \{0, 1, \ldots, k-1\}$ every n-dimensional matrix $A = \|a_{i_1 i_2 \ldots i_n}\|_{k_1, k_2, \ldots, k_n}$ of size $k_1 \times k_2 \times \cdots \times k_n$, the elements of which belong to E_k and for every s, $s = 1, 2, \ldots, n$, the following relation holds:*

$$\left| \bigcup_{j=1}^{k_s} \left\{ a_{i_1 \ldots i_{s-1} j \, i_{s+1} \ldots i_n} \right\} \right| = k_s.$$

A function f is injective if for every α, β from $\alpha \neq \beta$ it follows that $f(\alpha) \neq f(\beta)$.

Taking into account Definition 1, Definition 4 and the properties of injective functions, we have:

Proposition 1. *A function is an H-function if each of its subfunctions of one variable is injective.*

The question of the existence of H-functions among the set of discrete functions $F_n^k(\mathbb{K})$ arises naturally.

If Y and Z are finite sets and the function $h : Y \to Z$ is injective, then $|Y| \leq |Z|$ and $Rng(h) = |Y|$. In addition, taking into account Proposition 1, we have:

Proposition 2. *A necessary condition for the function $f(x_1, x_2, \ldots, x_n) \in F_n^k(\mathbb{K})$ to be an H-function is $|K_i| = k_i \leq k = |E_k|$ for every i, $1 \leq i \leq n$.*

If there exists i, $1 \leq i \leq n$, such that $|K_i| = k_i > k = |E_k|$, then the number of H-functions of the set $F_n^k(\mathbb{K})$ is zero. For the functions of P_n^k, from

$K_i = E_k$, $1 \leq i \leq n$, it follows that the necessary condition for the existence of H-functions holds.

Theorem 1. *If the functions* $f_j\ (x_j) \in F_1^k(K_j)$ *are injective, i.e.* $f_j(x_j) \in F_1^{k,k_j}(K_j)$, $j = 1, \ldots, n$, *then the function* $f(x_1, x_2, \ldots, x_n) = [f_1(x_1) + f_2(x_2) + \ldots + f_n(x_n)] \mod k$, *is an* H*-function belonging to the set* $F_n^k(\mathbb{K})$.

P r o o f. Let x_i, $1 \leq i \leq n$, $n \geq 2$, be an arbitrary variable, α' and α'' $(\alpha' \neq \alpha'')$ be two arbitrary constants of the set K_i, and $\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n$ be an arbitrary set of constants such that $\alpha_s \in K_s$, $s \in \{1, 2, \ldots, n\}\backslash\{i\}$. From $\alpha' \neq \alpha''$ and $f_i(x_i)$ being an injective function, it follows that $f_i(\alpha') \neq f_i(\alpha'')$, and therefore $Q + f_i(\alpha') \neq Q + f_i(\alpha'')$. The latter inequality, when $Q = f_1(\alpha_1) + \cdots + f_{i-1}(\alpha_{i-1}) + f_{i+1}(\alpha_{i+1}) + \cdots + f_n(\alpha_n)$, allows us to conclude that

$$f(\alpha_1, \ldots, \alpha_{i-1}, \alpha', \alpha_{i+1}, \ldots, \alpha_n) \neq f(\alpha_1, \ldots, \alpha_{i-1}, \alpha'', \alpha_{i+1}, \ldots, \alpha_n).$$

The variable x_i and the constants $\alpha_1, \ldots, \alpha_{i-1}, \alpha', \alpha'', \alpha_{i+1}, \ldots, \alpha_n$ were chosen arbitrarily. Therefore, the function $f(x_1, x_2, \ldots, x_n)$ is an H-function of the set $F_n^k(\mathbb{K})$. $\square$

The following question remains open: Do injective functions $g_j(x_j) \in F_1^k(K_j)$, $j = 1, \ldots, n$, exist for every H-function $g \in F_n^k(\mathbb{K})$, such that $g(x_1, \ldots, x_n) = [g_1(x_1) + g_2(x_2) + \cdots + g_n(x_n)] \mod k$?

From Theorem 1, we arrive at the following corollaries:

Corollary 1. *If the condition* $2 \leq |K_i| = k_i \leq k = |E_k|$ *holds for every* i, $1 \leq i \leq n$, *then for every* n *and* k *there exists an* H*-function which belongs to the set of functions* $F_n^k(\mathbb{K})$.

Corollary 2 [4]**.** *If the functions* $f_j(x_j) \in P_1^k$ *are bijective, i.e.* $f_j(x_j) \in P_1^{k,k}$, $j = 1, 2, \ldots, n$, *then the function* $f(x_1, x_2, \ldots, x_n) = [f_1(x_1) + f_2(x_2) + \cdots + f_n(x_n)] \mod k$, *is an* H*-function belonging to the set* P_n^k.

Corollary 3. *For every* n *and* k, $n \geq 1$, $k \geq 2$, *there exists an* H*-function belonging to the set* P_n^k, *i.e., there exists an* n*-dimensional Latin hypercube of order* k.

Theorem 1 allows us to "construct" H-functions of the set $F_n^k(\mathbb{K})$. We will show this in the following example.

Example 1. Let us "construct" the H-function f of the set $F_3^4(\mathbb{K})$, where

$$\mathbb{K} = K_1 \times K_2 \times K_3, \quad K_1 = K_2 = \{0, 1, 2\}, \quad K_3 = E_4 = \{0, 1, 2, 3\}.$$

Let $f(x_1, x_2, x_3) = [f_1(x_1) + f_2(x_2) + f_3(x_3)] \mod 4$, where

$$f_1 = \begin{pmatrix} 0 & 1 & 2 \\ 3 & 0 & 1 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{and} \quad f_3 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 3 & 0 & 2 \end{pmatrix}$$

be injective functions defined in the sets K_1, K_2, K_3, respectively, and taking values in E_4.

Consequently we get:

$$f(0,0,0) = [f_1(0) + f_2(0) + f_3(0)] \mod 4 = [3+2+1] \mod 4 = 2;$$

$$f(0,0,1) = [f_1(0) + f_2(0) + f_3(1)] \mod 4 = [3+2+3] \mod 4 = 0$$

and so on, placing the results in Table 1 to arrive at the table representation of the function $f(x_1, x_2, x_3)$.

x_1	x_2	x_3	$f(x_1,x_2,x_3)$	a_{ijl}	x_1	x_2	x_3	$f(x_1,x_2,x_3)$	a_{ijl}	x_1	x_2	x_3	$f(x_1,x_2,x_3)$	a_{ijl}
0	0	0	**2**	a_{111}	1	0	0	**3**	a_{211}	2	0	0	**0**	a_{311}
0	0	1	**0**	a_{112}	1	0	1	**1**	a_{212}	2	0	1	**2**	a_{312}
0	0	2	**1**	a_{113}	1	0	2	**2**	a_{213}	2	0	2	**3**	a_{313}
0	0	3	**3**	a_{114}	1	0	3	**0**	a_{214}	2	0	3	**1**	a_{314}
0	1	0	**1**	a_{121}	1	1	0	**2**	a_{221}	2	1	0	**3**	a_{321}
0	1	1	**3**	a_{122}	1	1	1	**0**	a_{222}	2	1	1	**1**	a_{322}
0	1	2	**0**	a_{123}	1	1	2	**1**	a_{223}	2	1	2	**2**	a_{323}
0	1	3	**2**	a_{124}	1	1	3	**3**	a_{224}	2	1	3	**0**	a_{324}
0	2	0	**3**	a_{131}	1	2	0	**0**	a_{231}	2	2	0	**1**	a_{331}
0	2	1	**1**	a_{132}	1	2	1	**2**	a_{232}	2	2	1	**3**	a_{332}
0	2	2	**2**	a_{133}	1	2	2	**3**	a_{233}	2	2	2	**0**	a_{333}
0	2	3	**0**	a_{134}	1	2	3	**1**	a_{234}	2	2	3	**2**	a_{334}

Table 1

Every discrete function $h = \begin{pmatrix} 0 & 1 & \dots & k-1 \\ b_1 & b_2 & \dots & b_k \end{pmatrix}$, where $b_i \in E_k$, $i = 1, \dots, k$, can be written in the analytic form $y = h(x)$ by interpolating polynomial [1] or by the following determinant form

$$\begin{vmatrix} 1 & x & x^2 & \dots & x^{k-2} & x^{k-1} & y \\ 1 & 0 & 0 & \dots & 0 & 0 & b_1 \\ 1 & 1 & 1 & \dots & 1 & 1 & b_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & k-1 & (k-1)^2 & \dots & (k-1)^{k-2} & (k-1)^{k-1} & b_k \end{vmatrix} = 0.$$

Each of the functions f_1, f_2, f_3 could be expressed analytically by using the Newton form of the interpolating polynomial, and for the function $f(x_1, x_2, x_3)$ we have the following analytic form:

$$f(x_1, x_2, x_3) =$$
$$\left[2(x_1)^2 - x_1 + 3 + \frac{3(x_2)^2 - 5x_2 + 4}{2} + \frac{10(x_3)^3 - 45(x_3)^2 + 47x_3 + 6}{6}\right] \mod 4.$$

Theorem 2. *The function $f(x_1, x_2, \dots, x_n) \in F_n^k(\mathbb{K})$ is an H-function if and only if for each of its variables x_i, $i = 1, 2, \dots, n$, the following equality holds: $Spr(x_i, f) = \{k_i\}$.*

Proof. (Necessity) Let $f \in F_n^k(\mathbb{K})$ be an H-function and x_i, $i \in \{1, 2, \dots, n\}$ be an arbitrary variable of f. Then each of its subfunctions g, $g \overset{X_f \backslash x_i}{\prec} f$ is injective, i.e. $Rng(g) = k_i$ and therefore $Spr(x_i, f) = \{k_i\}$ holds for $i = 1, 2, \dots, n$.

(Sufficiency) Let $Spr(x_i, f) = \{k_i\}$ hold for every variable x_i, $i \in \{1, 2, \dots, n\}$.

This would mean that every subfunction h, $h \overset{X_f \backslash x_i}{\prec} f$, has a range equal to k_i, and therefore, h is injective. The variable x_i was chosen arbitrarily, so it follows that every subfunction of one variable of the function f is injective. Therefore f is an H-function. $\square$

Theorem 3. *Every H-function of $F_n^k(\mathbb{K})$ can be represented in matrix form as an n-dimensional Latin hyperparallelepiped of size $k_1 \times k_2 \times \dots \times k_n$ based on E_k.*

Proof. Let $f(x_1, x_2, \dots, x_n)$ be an arbitrary H-function of $F_n^k(\mathbb{K})$, let s be an arbitrary number, $s \in \{1, 2, \dots, n\}$, and let $(c_1, \dots, c_{s-1}, c_{s+1}, \dots, c_n)$ be an arbitrary set of constants, such that $c_i \in K_i$, $i \in \{1, 2, \dots, n\} \backslash \{s\}$. If B is the matrix form of the function f, then for each element of the matrix B, the following equation holds: $b_{j_1 j_2 \dots j_n} = f(x_1 = j_1 - 1, x_2 = j_2 - 1, \dots, x_n = j_n - 1) \in E_k$.

From $x_t = j_t - 1 = c_t$ it follows that $j_t = c_t + 1$, $t \in \{1, 2, \dots, n\} \backslash \{s\}$.

Since f is an H-function of $F_n^k(\mathbb{K})$, it follows that $f(c_1, \dots, c_{s-1}, \mathbf{0}, c_{s+1}, \dots, c_n)$, $f(c_1, \dots, c_{s-1}, \mathbf{1}, c_{s+1}, \dots, c_n)$, $\dots$, $f(c_1, \dots, c_{s-1}, \boldsymbol{k}_s - 1, c_{s+1}, \dots, c_n)$ assume different values and hence, $\left|\bigcup_{r=0}^{k_s - 1} \{f(c_1, \dots, c_{s-1}, \boldsymbol{r}, c_{s+1}, \dots, c_n)\}\right| = \left|\bigcup_{r=1}^{k_s} \{b_{j_1 \dots j_{s-1} r \, j_{s+1} \dots j_n}\}\right| = k_s$.

The function f, the number s and the set of constants $(c_1, \ldots, c_{s-1}, c_{s+1}, \ldots, c_n)$ were chosen arbitrarily. Consequently, the matrix B is a Latin n-dimensional hyperparallelepiped of size $k_1 \times k_2 \times \cdots \times k_n$ based on E_k. $\square$

In Table 1 of Example 1, the H–function f of the set $F_3^4(\mathbb{K})$ has been "constructed" and represented in tabular and matrix form $\|a_{ijl}\|_{3,3,4}$, by using a Latin 3-dimensional hyperparallelepiped of size $3{\times}3 \times 4$.

Taking into account Definition 1 and Theorem 3, we have:

Proposition 3. *If $f(x_1, x_2, \ldots, x_n)$ is an arbitrary H-function of $F_n^k(\mathbb{K})$ and the matrix A_f is its matrix form, then by fixing any $n-1$ indices of the matrix A_f we get a 1-dimensional matrix, which does not contain repeating elements.*

Directly from Theorem 1 and Theorem 3 we get:

Corollary 4. *Every matrix $A = \|a_{i_1 i_2 \ldots i_n}\|_{k_1, k_2, \ldots, k_n}$, for which $a_{i_1 i_2 \ldots i_n} = \left(\sum_{j=1}^{n} f_j(i_j - 1)\right) \mod k$, where $f_j \in F_1^{k,k_j}(K_j)$, $j = 1, 2, \ldots, n$, is an n-dimensional Latin hyperparallelepiped of size $k_1 \times k_2 \times \cdots \times k_n$ based on E_k.*

The function $h_2(x) = (ax{+}b) \mod k$, where a and b are natural numbers, $(a, k) = 1$, is injective (moreover, it is bijective). Applying Corollary 4, we get:

Corollary 5. *Every matrix $B = \|b_{j_1 j_2 \ldots j_n}\|_{k_1, k_2, \ldots, k_n}$, for which $b_{j_1 j_2 \ldots j_n} = (a_1 j_1 + a_2 j_2 + \cdots + a_n j_n + c) \mod k$, where c is a natural number, $(a_i, k) = 1$, $i = 1, 2, \ldots, n$, is a Latin n-dimensional hyperparallelepiped of size $k_1 {\times} k_2 {\times} \cdots {\times} k_n$ based on E_k.*

3. Conclusions. The author is not aware of any published papers which investigate the H-functions from the set $F_n^k(\mathbb{K})$. The present paper shows the relationship between H-functions, spectrum of a variable with respect to a function, and Latin hyperparallelepipeds.

Since $P_n^k = F_n^k(E_k^n)$, i.e. the set of functions P_n^k is a partial case of the set $F_n^k(\mathbb{K})$, then the results arrived at in this paper are also valid in P_n^k.

In Theorem 6 [2] it is proven that if the function $f(x_1, x_2, \ldots, x_n) \in P_n^3$ is an H-function, then it is a linear function. From Theorem 1 and Example 1 we conclude that for all $n \geq 1$ and $k \geq 3$ there exist H-functions from $F_n^k(\mathbb{K})$, and therefore also from P_n^k, which are not linear and can be represented in analytic form.

he paper "On a Class of Discrete Functions" published in Acta Cybernetica [4] examines the functions from P_n^k: the H-functions are generalized and the class of $H[m; q]$-functions (Definition 5) is investigated.

REFERENCES

[1] Bozhorov E. Higher Mathematics, State Publishing House TECHNICA, Sofia, Bulgaria, 1975.

[2] Chimev K. On a way some functions of P_k depend on their arguments. Annuaire Des Ecoles Techniques Superieures, Mathematique, Vol. **IV**, livre 1, 1967, 5–12.

[3] Kovachev D. On the Number of Discrete Functions with a Given Range. In: General Algebra and Applications, Proceedings of the 59th Workshop on General Algebra (Eds K. Denecke, H.-J. Vogel), Potsdam, 2000, 125–134.

[4] Kovachev D. On a Class of Discrete Functions. *Acta Cybernetica* **17**, No 3, (2006), 513–519.

[5] Laywine Ch., G. Mullen. Discrete Mathematics Using Latin Squares, John Wiley & Sons, New York, 1998.

[6] Mirchev I., B. Yurukov. Some Properties of H-functions. *Acta Cybernetica* **12**, No 2 (1995), 137–143.

[7] Mirchev I. Otdelimi i dominirashti mnojestva ot promenlivi na funkciite – disertacija [Separable and Dominating Sets of Variables of the functions – dissertation], Sofia University – Math, 1990, (in Bulgarian).

Department of Computer Science
South-West University "N. Rilski"
2700 Blagoevgrad, P.O.79, Bulgaria
e-mail: `dkovach@swu.bg`

Received October 16, 2008
Final Accepted January 8, 2009