Acta Cybernetica **17** (2006) 513–519.

On a Class of Discrete Functions

Dimiter Stoichkov Kovachev*

Abstract

We consider classes of functions which depend in a certain way on their variables. The relation between the number of *H-functions* of n variables of the *k-valued logic* and the number of *n-dimensional Latin hypercubes* of order k is found. We have shown how from an arbitrary *Latin hypercube* we can "construct" (present in table form) an *H-function* and vice versa - how every *H-function* can be represented as a *Latin hypercube*. We extend the concepts of *H-function* and *Latin hypercube*.

Keywords: H-function, subfunction, range, spectrum, Latin hypercube.

1 Introduction

In the paper we interpret the *H-function* as Latin squares or Latin hypercubes. On the other side the Latin squares and Latin hypercubes are well known combinatorial structures which are widely used in different areas of mathematics and its applications, in theoretical and applied computer science, etc. They are very important in Statistics, Coding Theory, Cryptography, Tournament Design, etc. ([3], see §1.4, §12.1 - 12.4; §1.5, §13.1 - 13.5; §14.1 - 14.4; §1.6, §16.5, respectively), Design Experiment, Security of Information, Decision Making, etc.

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

Definition 1. *[1] We say that $f(x_1,\ x_2, ...,\ x_n)$ is* H-function *if for every variable x_i, $1 \leq i \leq n$, $n \geq 2$ and for every $a_1, ..., a_{i-1}, a', a'', a_{i+1}, ..., a_n \in E_k$ for $a' \neq a''$ we have $f(a_1, ..., a_{i-1}, a', a_{i+1}, ..., a_n) \neq f(a_1, ..., a_{i-1}, a'', a_{i+1}, ..., a_n)$.*

Definition 2. *[4] The number $Rng(f)$ of different values of the function f is called* range *of f.*

Denote by X_f and $P_n^{k,q}$ respectively, the set of variables of function f, and the set of all functions of P_n^k with range q, $1 \leq q \leq k$.

Definition 3. *[2] The function h is called a* subfunction *of the function $f(x_1,\ x_2, ...,\ x_n)$ with respect to the set of variables $R = \{x_{j_1},\ x_{j_2}, ...,\ x_{j_r}\}$,*

*Department of computer science, South-West University "N. Rilski", 2700 Blagoevgrad, P.O.79, E-mail: dkovach@aix.swu.bg and dkovach@abv.bg

$R \subseteq X_f$, if h is obtained from f by replacement the variables from R respectively by values c_1, $c_2, \ldots$, c_r. We will denote the subfunction h in one of the following ways $h \overset{R}{\prec} f$ or $h = f(x_{j_1} = c_1,\ x_{j_2} = c_2, \ldots,\ x_{j_r} = c_r)$.

Let M, $M \subseteq X_f$, be a set of variables and G be the set of all subfunctions of f with respect to $X_f \backslash M$, i.e. $G = G(M, f) = \{g : g \overset{X_f \backslash M}{\prec} f\}$.

Definition 4. *[4] The set $Spr(M, f) = \bigcup_{g \in G}\{Rng(g)\}$ is called* spectrum *of the set M for the function f.*

A matrix B with m rows and m columns is denoted by $B = (b_{ij})_1^m$. Matrix $A = (a_{j_1 j_2 \ldots j_n})_1^k$ is an n-dimensional matrix of order k.

Definition 5. *Latin n-dimensional hypercube of order k based on the set E_k is defined as every matrix $A = (a_{j_1\, j_2 \,\ldots\, j_n})_1^k$, such that for every s , s=1, 2,..., n we have*

$$\{a_{i_1 \ldots i_{s-1}\ 1\ i_{s+1} \ldots i_n}\} \bigcup \{a_{i_1 \ldots i_{s-1}\ 2\ i_{s+1} \ldots i_n}\} \bigcup \cdots \bigcup \{a_{i_1 \ldots i_{s-1}\ \mathrm{k}\ i_{s+1} \ldots i_n}\} = E_k,$$

i.e.

$$|\bigcup_{j=1}^{k}\{a_{i_1 \ldots i_{s-1}\ \mathrm{j}\ i_{s+1} \ldots i_n}\}| = |E_k| = k. \tag{1}$$

The set of all Latin n-dimensional hypercubes of order k will be denoted by LHC_n^k.

Theorem 6. *Each matrix $A = (a_{j_1\, j_2 \,\ldots\, j_n})_1^k$, for which*

$$a_{j_1\, j_2 \,\ldots\, j_n} = [\, \sum_{r=1}^{n} f_r(j_r - 1) + c \,]\ mod\ k,$$

where $f_r \in P_1^{k,k}$, c is a natural number, belongs to LHC_n^k.

Proof. Each function $h \in P_1^{k,k}$, is of the form $h = \begin{pmatrix} 0 & 1 & \ldots & k-1 \\ l_1 & l_2 & \ldots & l_k \end{pmatrix}$, where l_1, $l_2, \ldots$, l_k is a permutation of the numbers 0, $1, \ldots$, $k-1$, and $h(t) = l_{t+1}$, $t = 0,\ 1, \ldots,\ k-1$. Assume that the matrix $A \notin LHC_n^k$ and there exists s, $s \in \{1,\ 2, \ldots,\ n\}$, such that $|\bigcup_{j=1}^k\{a_{i_1 \ldots i_{s-1}\ \mathrm{j}\ i_{s+1} \ldots i_n}\}| \neq E_k$. Therefore there exist α, β, $\alpha \neq \beta$, such that $a_{i_1 \ldots i_{s-1}\ \alpha\ i_{s+1} \ldots i_n} = a_{i_1 \ldots i_{s-1}\ \beta\ i_{s+1} \ldots i_n}$. From the last equality it follows that $f_s(\alpha - 1) = f_s(\beta - 1)$ and from $f_s \in P_1^{k,k}$, we have $\alpha = \beta$: a contradiction. Therefore $A \in LHC_n^k$. □

Function $h_1(x) = (ax + b)\ mod\ k$, where a, b are natural numbers, $(a, k) = 1$ belongs to $P_1^{k,k}$. As a corollary of Theorem 6 we obtain that matrix $B = (b_{j_1\, j_2 \,\ldots\, j_n})_1^k$, for which $b_{j_1\, j_2 \,\ldots\, j_n} = (a_1 j_1 + a_2 j_2 + \ldots + a_n j_n + c)\ mod\ k$, for $(a_i, k) = 1$, $i = 1,\ 2, \ldots,\ n$ belongs to LHC_n^k.

Each function from $P_1^{k,k}$ can be represented by a table or by interpolating polynomial and, based on Theorem 6, can be used for "constructing" elements of LHC_n^k.

Example 7. Construct Latin 2-dimensional hypercube of order 4 and Latin 3-dimensional hypercube of order 3.

Let $f_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 2 & 1 \end{pmatrix}$ and $f_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 1 & 0 \end{pmatrix}$, be arbitrary functions from $P_1^{4,4}$. Let matrix $C = (c_{ij})_1^4$ be such that $c_{ij} = [f_1(i-1) + f_2(j-1)]\ mod\ k$. Then $c_{11} = [f_1(1-1) + f_2(1-1)]\ mod\ 4 = [3+2]\ mod\ 4 = 1$. Similarly we obtain the remaining elements of matrix C. So we have

$$C = (c_{ij})_1^4 = \begin{pmatrix} 1 & 2 & 0 & 3 \\ 2 & 3 & 1 & 0 \\ 0 & 1 & 3 & 2 \\ 3 & 0 & 2 & 1 \end{pmatrix} \in LHC_2^4;\ D = (d_{ijl})_1^3,\ D \in LHC_3^3,$$

where $d_{ijl} = (2i + j + 2l + 1)\ mod\ 3$.

2 Spectrum of H-functions and Latin Hypercubes

Theorem 8. *The function $f(x_1,\ x_2, \ldots,\ x_n) \in P_n^k$ is H-function if and only if for each variable $x_i,\ i = 1,\ 2, \ldots,\ n$ we have $Spr(x_i,\ f) = \{k\}$.*

Proof. (Necessity) Let f be H-function, x_i be arbitrary variable of f. Then for every set of constants $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ we have

$$f(a_1, \ldots,\ a_{i-1},\ r,\ a_{i+1}, \ldots,\ a_n) \neq f(a_1, \ldots,\ a_{i-1},\ t,\ a_{i+1}, \ldots,\ a_n) \tag{2}$$

for each r and t for which $r \neq t,\ r, t \in E_k$.

From Definition 3 and the inequality (2) it follows that every subfunction of f with respect to $X_f \backslash \{x_i\}$ assumes exactly k different values, i.e. it has a range equal to k.

For $M = \{x_i\}$, from Definition 4 it follows that $Spr(x_i,\ f) = \{k\}$.

(Sufficiency) Let for the variable x_i we have

$$Spr(x_i,\ f) = \{k\}. \tag{3}$$

From Definition 4 for $M = \{x_i\}$ and (3) it follows that every subfunction of f with respect to $X_f \backslash \{x_i\}$ has a range equal to k. This means that for an arbitrary $n-1$ tuple of values $< c_1, \ldots,\ c_{i-1},\ c_{i+1},\ \ldots,\ c_n >$, the subfunction $f(x_1 = c_1, \ldots,\ x_{i-1} = c_{i-1},\ x_i,\ x_{i+1} = c_{i+1}, \ldots,\ x_n = c_n)$ has a range k, i.e. it assumes exactly k different values. Because x_i can also assume exactly k different values, we obtain that for every $c', c'' \in E_k,\ (c' \neq c'')$, the following inequality holds $f(c_1, \ldots,\ c_{i-1},\ c',\ c_{i+1}, \ldots,\ c_n) \neq f(c_1, \ldots, c_{i-1},\ c'',\ c_{i+1}, \ldots,\ c_n)$.

Since the variable x_i and the set of values $< c_1, \ldots, c_{i-1},\ c',\ c'',\ c_{i+1},\ \ldots, c_n >$ are arbitrary, from Definition 1 it follows that f is an H-function. □

Remark 9. More that Theorem 8 can also be used as a definition of an H-function, where the restriction $n \geq 2$ can be eliminated, i.e. the definition holds for the functions of one variable as well.

Theorem 10. *The number of all H-functions of P_n^k is equal to the number of all Latin n-dimensional hypercubes of order k.*

Proof. Let $< c_{1i}, c_{2i}, ..., c_{ni} >$, i=1, 2,..., k^n be all the possible $n-$tuples of constants and $f \in P_n^k$ be an arbitrary function for which

$$f(x_1 = c_{1i}, x_2 = c_{2i}, ..., x_n = c_{ni}) = a_i, \ i = 1, 2, ..., k^n, \ a_i \in E_k. \tag{4}$$

Let the mapping $\varphi_f : E_k^{n+1} \longrightarrow E_k$ be such that it maps a_i from any equality (4) into an element of the matrix $D_1 = (d_{j_1 j_2 \dots j_n})_1^k$,

$$d_{j_{1i}j_{2i}\dots j_{ni}} = a_i = \varphi_f(c_{1i}, c_{2i}, ..., c_{ni}, a_i), \ i = 1, 2, ..., k^n, \tag{5}$$

where

$$j_{1i} = c_{1i} + 1, \ j_{2i} = c_{2i} + 1, ..., \ j_{ni} = c_{ni} + 1, \ i = 1, 2, ..., k^n. \tag{6}$$

Conversely, to every element of the matrix D_1 from (5), through the equalities (6), the constant a_i from equality (4) is assigned uniquely.

If we take into consideration Definitions 1 and 5 as well, we draw the conclusion that to each H-function of P_n^k we can assign, using φ_f, a Latin n-dimensional hypercube of order k, and vice versa. Therefore, the number of H-functions of P_n^k is equal to the number of the Latin n-dimensional hypercubes of order k. □

Using the mapping φ_f, every Latin n-dimensional hypercube of order k, which elements are in the set E_k, can be used for the "construction"(i.e. tabular representation) of an H-function of P_n^k.

Corollary 11. *Every H-function of P_n^k can be represented as Latin n-dimensional hypercube of order k and vice versa, every Latin $n-$dimensional hypercube of order k can be represented as H-function.*

In the general case, the sum of the H-functions of P_n^k can be an H-function, but this is not always true.

Example 12. Indeed, if $f_1 \in P_n^k$ is an arbitrary H-function, then $f_2 = k - 1 - f_1$ is also an H-function. However the sum $f_1 + f_2 = k - 1$ is a constant and it is not an H-function.

Example 13. Let k be an odd number and $f \in P_n^k$ be an arbitrary H-function. For every number $a \in E_k = \{0, 1, ..., k-1\}$ the function f_a, $f_a = f + a$ (mod k) is also an H-function. In addition, the sum $f + f_a = 2.f + a$ (mod k) is an H-function.

The problem for finding necessary and sufficient conditions under which the sum of two H-functions is again an H-function remains open.

From Definitions 1, 2, 3 it follows that a function of P_n^k is an H-function if each of its subfunctions of one variable takes k different values, i.e. if it has a range equal to k.

3 Generalizations of H-functions

We extend the concept of H-function in two directions - increasing the number of the variables on which the function depends in a certain way (each of its subfunctions of $m \geq 2$ variables takes q, $1 \leq q \leq k$, different values, i.e. it has a range equal to q) and changing the number of different values which the function assumes in this dependence.

Let m, q be integers such that $1 \leq m \leq n$, $1 \leq q \leq k$, and M be an arbitrary set of m variables of the function $f \in P_n^k$.

Definition 14. *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, $M \subseteq X_f$, $|M| = m$, we have*

$$Spr(M, f) = \{q\}. \tag{7}$$

The set of all functions of P_n^k for which (7) holds will be denoted by $H[m;q]_n^k$. When $m = k$, the set $H[1;m]_n^k$ coincides with the set of all H-functions from P_n^k.

From Definition 14 it follows that a function of P_n^k is an $H[m;q]$ function if each of its subfunctions of m variables takes q different values, i.e. it has a range equal to q.

We will prove a necessary and sufficient condition for a function to be an $H[m;q]$ function, which generalizes Theorem 8.

Theorem 15. *A function $f \in P_n^k$ is an $H[m;q]$ function if and only if each of its subfunctions, depending on at least m variables, is an $H[m;q]$ function.*

Proof. (Necessity) Let $f \in P_n^k$ be an $H[m;q]$ function and let h be an arbitrary subfunction of f, for which $|X_h| \geq m$. We will prove that h is an $H[m;q]$ function. Let us suppose that h is not an $H[m;q]$ function. Therefore there is a set of variables M, $|M| = m$, $M \subseteq X_h$, such that

$$Spr(M, h) \neq \{q\}. \tag{8}$$

From (8) it follows that a subfunction h_1 exists, $h_1 \overset{X_h \backslash M}{\prec} h$, such that $Rng(h_1) \neq q$. Since $h_1 \overset{X_h \backslash M}{\prec} h$, $h \prec f$, it follows that $h_1 \overset{X_f \backslash M}{\prec} f$ and $Rng(h_1) \neq q$. From Definition 4 and Definition 14 it follows that $Spr(M, f) \neq \{q\}$ and f is not an $H[m;q]$ function. This is a contradiction.

(Sufficiency) Let each subfunction of f, depending on at least m variables, be an $H[m;q]$-function. We will prove that f is an $H[m;q]$-function. Let us suppose that f is not an $H[m;q]$-function, i.e. there exists a set of variables M, $|M| = m$, $M \subseteq X_f$, such that

$$Spr(M, f) \neq \{q\}. \tag{9}$$

From (9) it follows that there is a subfunction g, $g \overset{X_f \backslash M}{\prec} f$, $|X_g| = m$, for which $Rng(g) \neq q$. Therefore the subfunction g is not an $H[m;q]$-function which contradicts the given condition. The contradiction is due to the assumption that f is not an $H[m;q]$-function. $\square$

As a corollary of Theorem 15 for $m = 1$, $q = k$ we get:

Corollary 16. *A necessary and sufficient condition for the function $f \in P_n^k$ to be an H-function is that every of its subfunctions, depending on at least one variable, is an H-function.*

Definition 17. *An n-dimensional matrix $W = (w_{i_1 i_2 \dots i_n})_1^k$ of order k, the elements of which are in the set E_k, such that when we fix arbitrary $n - m$ of its indices, we get an m-dimensional matrix of order k, in which there are exactly q different elements of the set E_k, is called an n-dimensional $H[m; q]$-hypercube of order k, generated by E_k.*

The set of all n-dimensional $H[m;q]$-hypercubes of order k, generated by the set E_k, will be denoted by $HHC[m;q]_n^k$.

It is obvious that for m=1, $q = k$, $LHC_n^k = HHC[1;k]_n^k$ holds, i.e. the Latin n-dimensional hypercubes of order k are special cases of the n-dimensional $H[m;q]$-hypercubes of order k.

Example 18. If the elements of the matrix of an arbitrary Latin hypercube of the set LHC_n^k are taken by modulo q, then we will get the matrix of an $H[1;q]$-hypercube of the set $HHC[1;q]_n^k$. In the matrix obtained in this way there will be exactly q different elements of E_k.

Let the matrix C from Example 7 be taken by modulo 3 and the new matrix we get be denoted by C_1

$$C = \begin{pmatrix} 1 & 2 & 0 & 3 \\ 2 & 3 & 1 & 0 \\ 0 & 1 & 3 & 2 \\ 3 & 0 & 2 & 1 \end{pmatrix} \in LHC_2^4,\ C \xrightarrow[mod\ 3]{q=3} C_1 = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 2 & 1 \end{pmatrix} \in HHC[1;3]_2^4.$$

Of course, there are matrices in the set $HHC[1;q]_n^k$ which cannot be obtained from matrices of the set LHC_n^k by taking modulo q. Below in Example 20 we have shown such a matrix. The matrix B is constructed in which the number of different elements is more that $q, (q = 3)$.

Theorem 19. *Each matrix $B = (b_{j_1 j_2 \dots j_n})_1^k$, for which*

$$b_{j_1 j_2 \dots j_n} = [\sum_{r=1}^{n} g_r(j_r - 1)]\ mod\ k,$$

where $g_r \in P_1^{k,q}$, $r = 1, 2, \dots, n$, is an n-dimensional $H[1;q]$-hypercube of order k.

Proof. If $f_1 \in P_1^{k,q}$ then f_2, ($f_2 = (f_1 + c_0)\ mod\ k$, c_0 is a natural number) also belongs to $P_1^{k,q}$. By fixing any $n-1$ indices of the matrix B we will obtain a function of $P_1^{k,q}$ and according to Definition 17, $B \in HHC[1;q]_n^k$. □

Because each function $g_r \in P_1^{k,q}$, $r = 1, 2, \ldots, n$, can be chosen in $\mid P_1^{k,q} \mid$ ways it follows that $\mid HHC[1;q]_n^k \mid \leq \mid P_1^{k,q} \mid^n$.

Example 20. Construct 2-dimensional $H[1;3]$ -hypercube of order 4. Let $g_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 2 & 1 \end{pmatrix}$ and $g_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 1 & 0 & 1 \end{pmatrix}$, be arbitrary functions from $P_1^{4,3}$ Let matrix $B = (b_{ij})_1^4$ be such that $b_{ij} = [g_1(i-1) + g_2(j-1)]$ *mod* 4. We compute the elements of the matrix B and we get:

$$B = (b_{ij})_1^4 = \begin{pmatrix} 1 & 0 & 3 & 0 \\ 0 & 3 & 2 & 3 \\ 0 & 3 & 2 & 3 \\ 3 & 2 & 1 & 2 \end{pmatrix} \in HHC[1;3]_2^4,\ m = 1,\ n = 2,\ q = 3,\ k = 4.$$

Proposition 21. *The number of hypercubes of the set $HHC[m;q]_n^k$ is equal to the number of functions of the set $H[m;q]_n^k$, i.e.*

$$|HHC[m;q]_n^k| = |H[m;q]_n^k|.$$

Using Definitions 2, 3, 4, 14, 17 and the arguments from Theorem 8 we can complete the proof of Proposition 21.

Every n-dimensional $H[m;q]$-hypercube of order k generated by the set of k elements E_k can be used for the "construction"(i.e. tabular representation) of a function of the set $H[m;q]_n^k$.

References

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

[2] Chimev K. N. *Discrete Functions and Subfunctions*, Blagoevgrad, 1991, (in Bulgarian).

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

[4] Kovachev D. S. *On the Number of Some k-Valued Functions of n Variables*, Union of Bulgarian Mathematicians, Mathematics and Education in Mathematics, Proceedings of Thirtieth Spring Conference of the Union of Bulgarian Mathematicians, Borovets, pp. 176-181, April 8-11, 2001.

[5] Kovachev D. S. *On the Number of Discrete Functions with a Given Range*, General Algebra and Applications, Proceedings of "59th Workshop on General Algebra", Potsdam edited by K. Denecke and H.-J. Vogel, pp.125-134, 2000.

Received June, 2005