Some Properties of H–functions

Ivan Mirchev* Borislav Yurukov*

1 Introduction

Some basic results in the theory of separable and c–separable sets were obtained in [1]-[7]. In this paper some problems concerning with separable and c–separable sets for k–valued functions are considered.

We investingate the properties of k–valued functions when some of their variables are replaced with constants. The investigations of properties of H–functions are connected with separability and c–separability of functions.

2 Definitions and Notations

Definition 1 [1] A function $f(x_1, ..., x_n)$ on $A(|A| \geq 2)$ *depends essentially on the variable* x_i, $1 \leq i \leq n$ if there exist $n-1$ constants $c_1, ..., c_{i-1}, c_{i+1}, ..., c_n$ such that the unary function $f(c_1, ..., c_{i-1}, x, c_{i+1}, ..., c_n)$ takes on at least two different values.

Ess(f) denotes the set of all variables which f depends essentially on.

$\mathbf{F_n}$ denotes the set of all functions which depend essentially exactly on n variables.

Definition 2 [1] A function f and the functions obtained from f by replacing some of its variables with constants are called subfunctions of f ($g \longrightarrow\!\!\!< f$ denotes that g is a subfunction of f).

Definition 3 [4] The variable x_i, $1 \leq i \leq n$, $n \geq 1$ is a *H–variable* for a function $f \in F_n$ if for any two tuples of constants differing only in the i^{-th} component, the function has different values.

Definition 4 [4] The function f is a H–function if all its essential variables are H–variables.

$\mathbf{H^k_{f_n}}$ denotes the set of all k–valued H–functions from F_n. $\mathbf{H^k_f}$ denotes the set of all k–valued H–functions.

*Faculty of Mathematics and Natural Sciences "Neofit Rilski" South-West University 66 "Al. Velichkov" Str., 2700 Blagoevgrad, Bulgaria Fax. 00359/73/29325, Tel. 00359/73/26174, 20767

3 Basic Results

The following assertion is obvious.

Statement 1 *A function $f \in F_n$, $n \geq 2$ is a H-function if and only if all of its subfunctions from F_k, $1 \leq k < n$ are H-functions too.*

Theorem 1 *Let $p \geq 3$ be a prime number and let $f \in F_n$, $n \geq 2$, be a non-linear p-valued function. If there exists f_1, $f_1 \longrightarrow\!\!\!< f$, $|Ess(f_1)| = 1$ which as polynomial mod p is of degree $p-1$ then $f \notin H^k_{f_n}$.*

Proof. By Statement 1 it is sufficient to prove that every polynomial

$$f_1(x) = a_0 + a_1 x + ... + a_{p-1} x^{p-1} \pmod p, \ a_{p-1} \neq 0$$

cannot take on all values from the set $\{0, 1, ..., p-1\}$. Consider the polynomial

$$g(x) = a_1 x + a_2 x^2 + ... + a_{p-1} x^{p-1} \pmod p, \ a_{p-1} \neq 0.$$

Let us assume that

$$g(i) = b_i, \ i = 1, 2, ..., p-1, \ b_i \neq b_j \text{ when } i \neq j \text{ and } b_i \neq 0, \text{ if } i \neq 0.$$

The determinant of the system

$$a_1 i + a_2 i^2 + ... + a_{p-1} i^{p-1} = b_i, \ i = 1, 2, ..., p-1$$

is

$$\Delta = \begin{vmatrix} 1 & 1^2 & ... & 1^{p-1} \\ 2 & 2^2 & ... & 2^{p-1} \\ 3 & 3^2 & ... & 3^{p-1} \\ . & . & . & . \\ (p-1) & (p-1)^2 & ... & (p-1)^{p-1} \end{vmatrix} = 1.2...(p-1).W(1, 2, ..., p-1).$$

Using the facts that

$$W(c_1, ..., c_k) = \prod_{k \geq i \geq j \geq 1} (c_i - c_j)$$

and

$$(p-1)! + 1 \equiv 0 \pmod p, \quad \text{we have} \quad \Delta \neq 0.$$

Consequently the system has only one solution. As we know $a_{p-1} = \frac{\Delta_{p-1}}{\Delta}$, where

$$\Delta_{p-1} = \begin{vmatrix} 1 & 1^2 & ... & 1^{p-2} & b_1 \\ 2 & 2^2 & ... & 2^{p-2} & b_2 \\ 3 & 3^2 & ... & 3^{p-2} & b_3 \\ . & . & . & . & . \\ (p-1) & (p-1)^2 & ... & (p-1)^{p-1} & b_{p-1} \end{vmatrix}.$$

But

$$\Delta_{p-1} = \begin{vmatrix} 1 & 1^2 & \dots & 1^{p-2} & b_1 \\ 2 & 2^2 & \dots & 2^{p-2} & b_2 \\ 3 & 3^2 & \dots & 3^{p-2} & b_3 \\ . & . & . & . & . \\ S_1 & S_2 & \dots & S_{p-2} & S \end{vmatrix}, \text{ where}$$

$$S_k = 1^k + 2^k + \dots + (p-1)^k, \ k = 1, 2, \dots, (p-2),$$

$$S = b_1 + b_2 + \dots + b_{p-1} = 1 + 2 + 3 + \dots + (p-1) = S_1.$$

The numbers $1, 2, \dots, p-1$ are solutions of the equation $x^{p-1} - 1 = 0 \pmod p$. Consequently for the elementary symmetric polynomials $\tau_1, \tau_2, \dots, \tau_{p-2}$ of $1, 2, \dots, p-1$ we have

$$\tau_1 = \tau_2 = \dots = \tau_{p-2} = 0.$$

On the other hand from Newton's formulas

$$S_k - \tau_1.S_{k-1} + \tau_2.S_{k-2} - \dots + (-1)^{k-1}\tau_{k-1}.S_1 + (-1)^k.k\tau_k = 0,$$

when $k \le p-1$.

If $k < p-1$, then $S_k = 0$. Consequently $\Delta_{p-1} = 0$ implies $a_{p-1} = 0$. This contradicts the condition $a_{p-1} \neq 0$.

Therefore the values of the polynomials $g(x)$ and $f_1(x)$ cannot form a whole system modulo p. This completes the proof. □

Remarks:

1. If $p = 2$, then according to Lemma 4.2 [3], Theorem 4.1 [3] and Lemma 4.10 [3] it follows that $f \in H^2_{f_n}$ if and only if f is a linear function.

2. When $p = 3$ this theorem was proved by K. Chimev in [4] and now was improved (by Mirchev and Drenski) for $p \ge 3$, where p – a prime number.

3. It is obvious that if $f \in L_p$ then $f \in H^p_f$ (L_p denotes the set of all linear p–valued functions). The converse statement is not valid and this fact is evident from the following example.

Example 1 Let $f(x_1, x_2) = x_1^3 + x_2^3 \pmod 5$. For the function f, $f \in H^5_{f_2}$ but $f \notin L_5$ (Here $x_i^3 = x_i.x_i.x_i$, $i = 1, 2$).

Now we will consider some results which give us good possibilities to construct catalogues of H–functions modulo 3.

Definition 5 We will say that $f(x_1, \dots, x_n)$ and $g(x_1, \dots, x_n)$ are *distinguishable everywhere* if for each tuple of constants $c_1, \dots, c_n$ the relation

$$f(c_1, \dots, c_n) \neq g(c_1, \dots, c_n) \text{ holds.}$$

We denote by $f <> g$ that f and g are distinguishable everywhere.

Let $j_i(x) = \begin{cases} 1, & x = i, \\ 0, & x \neq i. \end{cases}$

If $f(x_1, ..., x_n)$, $n \geq 2$, is a k–valued function then it is obvious that $\forall p (1 \leq p \leq n)$

$$f(x_1, ..., x_n) = \sum_{i=0}^{k-1} j_i(x_p).f(x_1, ..., x_{p-1}, i, x_{p+1}, ..., x_n).$$

If
$$\begin{aligned} f_1(x_1, ..., x_{n-1}) &= f(x_1, ..., x_{n-1}, 0), \\ &\vdots \\ f_k(x_1, ..., x_{n-1}) &= f(x_1, ..., x_{n-1}, k-1), \end{aligned}$$
then
$$f(x_1, ..., x_n) = \sum_{i=0}^{n} j_i(x_n) f_{i+1}(x_1, ..., x_{n-1}).$$

Theorem 2 (Theorem 1 [6]) *$f \in H^k_{f_n}$, $n \geq 2$, if and only if $f_i \in H^k_{f_{n-1}}$ and $f_i <> f_j$ for $i, j = 1, ..., k$, $i \neq j$.*

According to this result each function $f \in H^3_{f_n}$ can be derived from f_1, f_2, f_3, where for each $1 \leq i \leq 3$, $1 \leq j \leq 3$ and $i \neq j$ the relations

$$f_i \in H^3_{f_{n-1}} \text{ and } f_i <> f_j \text{ hold.}$$

We denote by $f = (f_1, f_2, f_3)$ the fact that $f \in H^3_{f_n}$ is derived from $f_1, f_2, f_3 \in H^3_{f_{n-1}}$.

Lemma 1 *Let $f = (f_1, f_2, f_3)$, $g = (g_1, g_2, g_3)$ and $f, g \in H^3_{f_n}$. Then $f <> g$ if and only if $f_1 <> g_1$, $f_2 <> g_2$ and $f_3 <> g_3$.*

Proof.

" $\Rightarrow$ " Let $f <> g$. Then $f(x_1, ..., x_{n-1}, 0) <> g(x_1, ..., x_{n-1}, 0)$, i.e. $f_1 <> g_1$. Analogously $f_2 <> g_2$ and $f_3 <> g_3$.

" $\Leftarrow$ " Let $f_i <> g_i$, $i = 1, 2, 3$. Let us suppose that there exist $c_1, ..., c_n$ so that $f(c_1, ..., c_n) = g(c_1, ..., c_n)$.

If $c_n = 0$, then we obtain $f_1(c_1, ..., c_{n-1}) = g_1(c_1, ..., c_{n-1})$ which contradicts the condition $f_1 <> g_1$.

If $c_n = 1$ or $c_n = 2$ we obtain a contradiction with $f_2 <> g_2$ or $f_3 <> g_3$. □

Theorem 3 *If $f \in H^3_{f_n}$, $n \geq 2$ then there exist g and h, $g <> h$ and g, $h \in H^3_{f_n}$, such that $f <> g$ and $f <> h$.*

Proof.

$$\text{Let } \quad f = (f_1, f_2, f_3); \quad g = (f_2, f_3, f_1); \quad \text{and} \quad h = (f_3, f_1, f_2).$$

Since f_1, f_2, f_3 are pairwise distinguishable everywhere then according to Lemma 1, f, g and h are pairwise distinguishable everywhere too. By Theorem 2 we have

$$g \in H^3_{f_n} \text{ and } h \in H^3_{f_n}. \qquad \square$$

Theorem 4 *If $f \in H^3_{f_n}$ then there exist only two functions $g, h \in H^3_{f_n}$, such that f, g and h are pairwise distinguishable everywhere.*

Proof. We will prove the theorem by induction on the number of the variables.

The case $n = 1$ is trivial.

Let us assume that for functions from F_{n-1} the statement is true.

Let now $f \in H^3_{f_n}$. By Theorem 3, it is sufficient to prove that there exist only two functions g and h.

Let

$$f = (f_1, f_2, f_3), \text{ where } f_i <> f_j \text{ when } i \neq j;$$

$$g = (g_1, g_2, g_3), \text{ where } g_i <> g_j \text{ when } i \neq j;$$

$$h = (h_1, h_2, h_3), \text{ where } h_i <> h_j \text{ when } i \neq j;$$

$g, h \in H^3_{f_n}$, $g <> f$, $h <> f$, $g <> h$ and $f_i, g_i, h_i \in H^3_{f_{n-1}}$, $1 \leq i, j \leq 3$.

Since f, g and h are pairwise distinguishable everywhere then according to Lemma 1, f_1, g_1 and h_1 are distinguishable everywhere too.

By the induction hypothesis on f_1 there exist only two functions which are distinguishable everywhere from f_1. Therefore $\{g_1, h_1\} = \{f_2, f_3\}$.

Similarly we get:

$$\{g_2, h_2\} = \{f_1, f_3\}, \{g_3, h_3\} = \{f_1, f_2\}. \tag{1}$$

Withoutloss of generality we can assume that

$$g_1 = f_2 \text{ and } h_1 = f_3. \tag{2}$$

If we suppose $h_2 = f_3$, then from $h_1 = f_3$ we obtain $h_1 = h_2$, which contradicts the condition $h_1 <> h_2$. Therefore from (1) we obtain

$$g_2 = f_3 \text{ and } h_2 = f_1. \tag{3}$$

If we assume $g_3 = f_2$, then from $g_1 = f_2$ we obtain $g_1 = g_3$, which contradicts the condition $g_1 <> g_3$. Therefore from (1)

$$g_3 = f_1 \text{ and } h_3 = f_2. \tag{4}$$

Consequently g and h are exactly determined by f. $\square$

Theorem 5 *If $f, g, h \in H^3_{f_n}$, $g \neq h$, $f <> g$ and $f <> h$ then $g <> h$.*

Proof. We will prove the theorem by induction on the number of the variables.

Let $n = 1$. Then:

$$f(0) = a_1,\ f(1) = a_2,\ f(2) = a_3,\ g(0) = a'_1,\ g(1) = a'_2,\ g(2) = a'_3,$$

$$h(0) = a_1'',\ h(1) = a_2'',\ h(2) = a_3'', \text{ i. e.}$$
$$f = (a_1\ a_2\ a_3), \text{ where } a_i \neq a_j \text{ when } i \neq j;$$
$$g = (a_1'\ a_2'\ a_3'), \text{ where } a_i' \neq a_j' \text{ when } i \neq j;$$
$$h = (a_1''\ a_2''\ a_3''), \text{ where } a_i'' \neq a_j'' \text{ when } i \neq j.$$

Let us assume that $g <> h$ doesn't hold. Without loss of generality we may assume that $a_1' = a_1''$. Then $\{a_2', a_3'\} = \{a_2'', a_3''\}$.

If we suppose that $a_2' = a_2''$ then we get $a_3' = a_3''$. Therefore $g = h$ which is a contradiction.

Let us now suppose that $a_2' = a_3''$ and $a_3' = a_2''$, i.e., that

$$g = (a_1'\ a_2'\ a_3') \text{ and } h = (a_1'\ a_3'\ a_2').$$

But $a_2 \notin \{a_2', a_3'\}$ and $a_3 \notin \{a_3', a_2'\}$ therefore $a_2 = a_3$. This contradicts the condition $f \in H^3_{f_1}$.

So, if $n = 1$ the statement is true.

Let us assume that the statement is true for all functions from F_{n-1}. We will prove the statement for the functions from F_n, $n \geq 2$.

Let

$$f = (f_1, f_2, f_3), \text{ where } f_i <> f_j \text{ when } i \neq j;$$
$$g = (g_1, g_2, g_3), \text{ where } g_i <> g_j \text{ when } i \neq j;$$
$$h = (h_1, h_2, h_3), \text{ where } h_i <> h_j \text{ when } i \neq j$$

and $f_i, g_i, h_i \in H^3_{f_{n-1}}$ $(1 \leq i, j \leq 3)$. As we know $f <> g$, $f <> h$ and $g \neq h$. Consequently $g_1 \neq h_1$ or $g_2 \neq h_2$ or $g_3 \neq h_3$.

Whitout loss of generality we can assume that $g_1 \neq h_1$.
From the conditions of the Theorem we obtain $f_1 <> g_1$ and $f_1 <> h_1$. But $f_1, g_1, h_1 \in H^3_{f_{n-1}}$. From this fact and our inductive supposition it follows that

$$g_1 <> h_1. \tag{5}$$

Since f_1, f_2, f_3 and f_1, g_1, h_1 are pairwise distinguishable everywhere it follows from Theorem 4 that

$$\{f_2, f_3\} = \{g_1, h_1\}.$$

Let us assume now that

$$g_1 = f_2 \text{ and } h_1 = f_3.$$

Since g_1, g_2, g_3 and f_1, f_2, f_3 are pairwise distinguishable everywhere and $g_1 = f_2$ it follows from Theorem 4 that

$$\{g_2, g_3\} = \{f_1, f_3\}.$$

Similarly as above, we have

$$\{h_2, h_3\} = \{f_1, f_2\}.$$

If we suppose that $g_2 = h_2$ or $g_2 = h_3$ then we obtain

$$g_2 \in \{f_1, f_3\} \cap \{f_1, f_2\} = \{f_1\}.$$

Therefore $g_2 = f_1$, $g_3 = f_3$, which contradicts $g_3 <> f_3$.

If we suppose that $g_3 = h_3 = f_1$ then we have $h_2 = f_2$, which contradicts $h_2 <> f_2$. Consequently $g_3 = h_2 = f_1$, $g_2 = f_3$, $h_3 = f_2$ which implies

$$g_2 <> h_2 \text{ and } g_3 <> h_3. \qquad (6)$$

From Lemma 1, (5) and (6) it follows that $g <> h$. □

Finally we note, that some algorithms, computer programs and catalogues for H–functions are given in [3].

References

[1] Chimev, K.N., Separable Sets of Arguments of Functions, MTA SZTAKI, Tanulmanyok 180/1986. 1-173 p.

[2] Chimev, K.N., Funkcii i grafi [Functions and Graphs], South-West University Publishing House, Blagoevgrad, 1983.

[3] Mirchev, I. A. Otdelimi i dominirashti mnojestva ot promenlivi - disertacija [Separable and Dominating Sets of Variables - dissertation], Sofia University - Math, 1990.

[4] Chimev, K.N., Varhu edin nachin na zavisimost na njakoi funkcii ot P_k ot tehnite argumenti [On a Dependence of Some Functions from P_k on their Variables], Year-book of the Technical Universities, Math, v. IV, book 1, 1967, 5-12 p.

[5] Shtrakov, S. V., Dominating and Annuling Sets of Variables for the Functions, Blagoevgrad, 1987, 1-179 p.

[6] Gyudjenov, I.D., B.P. Yurukov, Varhu zavisimostta na funkciite ot tehnite promenlivi po shesti nachin [On the Sixth Way's Dependence of Some Functions on their Variables], Year-book of the South-West University, Math, book 1, 1987, 5-12 p.

[7] Yablonskii, S. V., O.B. Lupanov, Diskretnaya matematika i matematicheskie voprosi kibernetiki [Discrete mathematics and mathematical tasks of cybernetics], Moscow, 1974.

Received April, 1994