UDK 681.5:519.7

F.E. Geche, V.M. Kotsovsky, A.V. Mitsa

SPECTRAL PROPERTIES OF DISCRETE NEURAL FUNCTIONS OVER A GALOIS FIELD

Abstract. The paper deals with the discrete functions over a Galois field. We give the necessary and sufficient condition of discrete functions decomposition in group characters. The notion of neural element over a Galois field is introduced and the criterion of discrete functions realizability on a single neuron is proved in the paper. We also propose a spectral synthesis method over a finite field.

Keywords: neuron, spectral coefficient, structure vector, group character.

Introduction

Finite fields and groups are widely spread in the automata theory and logic [1-3]. They are particularly important in the coding theory [1]. It is shown in [4] that any finite automaton is isomorphic to the linear one over some finite field. Analysis and synthesis of linear automata over an arbitrary finite field are carried out by the traditional spectral analysis. It is shown in the paper that the basic methods of spectral analysis can be successfully used for the verification of discrete functions realizability by one neural element over a Galois field.

1. Spectral analysis of discrete functions over a Galois field

Let $F = GF\left(p^m\right)$ be the Galois field containing cyclic groups

$$H_{k_1} = \langle a_1 \mid a_1^{k_1} = 1\rangle, \quad H_{k_2} = \langle a_2 \mid a_2^{k_2} = 1\rangle, \quad \ldots \quad , H_{k_n} = \langle a_n \mid a_n^{k_n} = 1\rangle$$

and $G_n = H_{k_1} \otimes H_{k_2} \otimes \ldots \otimes H_{k_n}$ be the direct product of cyclic groups H_{k_i}.

Let $F = GF\left(p^m\right)$ be the Galois field containing cyclic groups

$$H_{k_1} = \langle a_1 \mid a_1^{k_1} = 1\rangle, \; H_{k_2} = \langle a_2 \mid a_2^{k_2} = 1\rangle, \ldots, \; H_{k_n} = \langle a_n \mid a_n^{k_n} = 1\rangle$$

and $G_n = H_{k_1} \otimes H_{k_2} \otimes \ldots \otimes H_{k_n}$ be the direct product of cyclic groups H_{k_i}.

A mapping $f : G_n \to F$ is a discrete n-variable function.

It should be noted that the spectral analysis of discrete functions

 ISSN 1562-9945

$f: G_n \to C$ over complex field is always possible because complex field contains the primitive k-th root of unity, where k is the least common multiple of $k_1, k_2, \ldots, k_n$.

If $F = GF\left(p^m\right)$, then the spectral analysis of discrete functions $f: G_n \to C$ isn't always possible. It is possible when the dimension of vector space $V_F^n = \left\{ f \mid f: G_n \to GF\left(p^m\right) \right\}$ and the order of character group $X(G_n)$ over fields F are equal.

We consider the task of function $f: G_n \to F$ decomposition in characters of the G_n group over F field. If $k_1 = k_2 = \ldots = k_n = 2$ and F is the field of real numbers R, then the characters group $X\left(G_n\right)$ of the group G_n over field R is equal to Hadamard-Walsh functions system and the spectral analysis is possible.

If $k_1 = k_2 = \ldots = k_n = k\left(k > 2\right)$ and the field F is the complex field C, then the characters group $X\left(G_n\right)$ of the group G_n over field C is equal to Vilenkin-Krestenson functions system and the spectral analysis of discrete function is also possible.

Let $k = \mathrm{lcm}\left(k_1, k_2, \ldots, k_n\right)$. It's easy to show that if the field $F = GF(p^m)$ contains the primitive k-th root of unity, then $u = p^m - 1$ is multiple of k. Suppose that the field with the primitive element $\square$ contains the primitive k-root $\square$. Then the cyclic group $H_k = \left\langle \sigma \mid \sigma^k = 1 \right\rangle$ is the subgroup of field cyclic subgroup. Using the Lagrange theorem [5], we obtain that k is the divisor of number u. Let's consider $\sigma = \varepsilon^{u/k}$ and prove that $\square$ is the primitive root of unity. Since $\square$ is the primitive in F, we have [6-8] that for all $i, j, r \in \left\{1, 2, \ldots, k-1\right\}$ $\sigma^i \neq \sigma^j$, if $i \neq j$ and $\sigma^r \neq 1$. Therefore k is the least natural number that $\sigma^k = 1$. So we can conclude that the spectral analysis of discrete function $f: G_n \to F$ is possible then and only then when u is multiple of k.

Let's find the analytic view of group G_n characters over the field $F = GF\left(p^m\right)$. Let $k = \mathrm{lcm}\left(k_1, k_2, \ldots, k_n\right)$, $\square$ be the primitive element of field $F = GF\left(p^m\right)$, $H_k = \left\langle a \mid a^k = 1 \right\rangle$ is the cyclic group of the order k, and k is

the divisor of the number u. Then for all $h_i \in H_{k_i}$ exists number $j_{k_i} \in \{0,1,\ldots,k_i-1\}$ such that $h_i = a_i^{j_{k_i}}$, where $a_i = a^{k/k_i}$ is the generating element of group $H_{k_i}\,(i=1,2,\ldots,n)$. The characters χ_{r_i} of the group H_{k_i} over the field $F = GF(p^m)$ may be written as

$$\chi_{r_i}(h_i) = \sigma_i^{r_i j_{k_i}}, \tag{1}$$

where $\sigma_i = \varepsilon^{u/k_i}$, $r_i \in \{0,1,\ldots,k_i-1\}$.

Since the group G_n is the direct product of cyclic groups $H_{k_1},\ldots,H_{k_n}$, for all $\mathbf{g} \in G_n$ there exist numbers $j_i \in \{0,1,\ldots,k_i-1\}, i=1,2,\ldots,n$ such that $\mathbf{g} = \left(a_1^{j_1},\ldots,a_n^{j_n}\right) = \left(a^{kj_1/k_1},\ldots,a^{kj_n/k_n}\right)$.

The next formula follows from the multiplicative property of characters [6] and (1) concerning the general form of characters:

$$\chi_{(r_1,\ldots,r_n)}(\mathbf{g}) = \sigma^{t_1 r_1 j_1 + \ldots + t_n r_n j_n}, \tag{2}$$

where $\sigma = \varepsilon^{u/k}$, $t_i = \dfrac{k}{k_i}$, $r_i \in \{0,1,\ldots,k_i-1\}$, $i=1,2,\ldots,n$. It's possible to define the character product on the group G_n as follows:

$$\forall \mathbf{g} \in G_n \quad \chi_{(r_1,\ldots,r_n)}(\mathbf{g}) \cdot \chi_{(q_1,\ldots,q_n)}(\mathbf{g}) = \chi_{(r_1 \oplus_1 q_1,\ldots,r_n \oplus_n q_n)}(\mathbf{g}),$$

where $\oplus_i$ is the k_i-addition. Thus we obtain the multiplicative character group $X(G_n)$. We have the next consequence from (2): the number of different characters of group G_n over the field F is equal to the order of group G_n. Then from the orthogonality of characters [6, 9] and from $\left|X(G_n)\right| = \dim_F V_F^n = k_1 k_2 \ldots k_n$ we obtain that $X(G_n)$ is the orthogonal basis of the space V_F^n. Thus, an arbitrary $f \in V_F^n$ can be uniquely written as follows:

$$f(\mathbf{g}) = \sum_{r_1=0}^{k_1-1} \ldots \sum_{r_n=0}^{k_n-1} s_{(r_1,\ldots r_n)} \chi_{(r_1,\ldots,r_n)}(\mathbf{g}), \tag{3}$$

where addition and multiplication are considering in the field F.

The decomposition (3) is called the spectral decomposition of discrete function $f: G_n \to F$ in characters of G_n over the field F.

 ISSN 1562-9945

Multiplying the both sides of (3) in $\chi^{-1}_{(q_1,\ldots,q_n)}$ and summarizing by all elements of G_n, we obtain the following equality

$$\sum_{\mathbf{g}\in G_n} f(\mathbf{g})\chi^{-1}_{(q_1,\ldots,q_n)}(\mathbf{g}) = \sum_{\mathbf{g}\in G_n}\left(\sum_{r_1=0}^{k_1-1}\cdots\sum_{r_n=0}^{k_n-1} s_{(r_1,\ldots,r_n)}\chi_{(r_1,\ldots,r_n)}(\mathbf{g})\right)\chi^{-1}_{(q_1,\ldots,q_n)}(\mathbf{g}).$$

Subject to the orthogonality of characters the right side of last equality can be written as follows:

$$\sum_{\mathbf{g}\in G_n}\left(\sum_{r_1=0}^{k_1-1}\cdots\sum_{r_n=0}^{k_n-1} s_{(r_1,\ldots,r_n)}\chi_{(r_1,\ldots,r_n)}(\mathbf{g})\right)\chi^{-1}_{(q_1,\ldots,q_n)}(\mathbf{g}) =$$

$$= \sum_{r_1=0}^{k_1-1}\cdots\sum_{r_n=0}^{k_n-1} s_{(r_1,\ldots,r_n)}\left(\sum_{\mathbf{g}\in G_n}\chi_{(r_1,\ldots,r_n)}(\mathbf{g})\chi^{-1}_{(q_1,\ldots,q_n)}(\mathbf{g})\right) = s_{(q_1,\ldots,q_n)}|G_n|.$$

Therefore, the spectral coefficients of the function can be obtained with following formula

$$s_{(q_1,\ldots,q_n)} = |G_n|^{-1}\sum_{\mathbf{g}\in G_n} f(\mathbf{g})\chi^{-1}_{(q_1,\ldots,q_n)}(\mathbf{g}), \qquad (4)$$

where $q_i \in \{0,1,\ldots,k_i-1\}$ $(i\in\{1,2,\ldots,n\})$.

Note. The calculation of spectral coefficients $s_{(r_1,\ldots r_n)}$ of discrete function $f\in V_F^n$ can be done by using the quick algorithms issuing from matrices factorization method [10] and the well-known theorem of the theory of representations [9]: if $G_n = H_{k_1}\otimes H_{k_2}\otimes\ldots\otimes H_{k_n}$ and $|G_n|$ is the divisor of p^m-1, then $X(G_n) = X(H_{k_1})\otimes X(H_{k_2})\otimes\ldots\otimes X(H_{k_n})$ over $GF(p^m)$ field.

2. Discrete neural functions over a Galois field

In this section we introduce the notion of neuron over field $GF(p^m)$ and give the criterion of discrete functions realizability by single neuron over a Galois field.

Let $k_1,k_2,\ldots,k_n,q$ be natural numbers $(k_i\geq 2, i=1,\ldots\ldots,n, q\geq 2)$ and $k=\mathrm{lcm}(k_1,k_2,\ldots,k_n,q)$. We consider only finite fields $F=GF(p^m)$ satisfy-

ing the following condition: $p^m - 1$ is exactly divided by k. It means that field $F = GF\left(p^m\right)$ contains cyclic groups H_{k_i}, H_q with respective group generators $\sigma_i = \varepsilon^{u/k_i}$ $\left(i = 1,2,\ldots,n\right)$, $\sigma = \varepsilon^{u/q}$, where ε is the primitive element of field F, $u = p^m - 1$.

Define the function $\mathrm{Fsign}\xi$ on $F \setminus \{0\}$ as follows:

$$\forall \xi \in F \setminus \{0\} \quad \mathrm{Fsign}\xi = \sigma^j, \text{ if } \frac{ju}{q} \le \deg \xi < \frac{(j+1)u}{q},$$

where $\deg \xi$ is the degree of element $\xi\left(\xi = \varepsilon^{\deg \xi}\right)$, $j \in \{0,1,\ldots,q-1\}$.

A neuron over field $F = GF\left(p^m\right)$ is a logical unit with $n+1$ inputs $x_1,\ldots,x_n; x_0$ $\left(n \ge 1\right)$ taking values respectively from cycling group H_{k_i} $(i = 1,\ldots,n)$ and $H_0 = \{1\}$, and a single output taking value from the group H_q. Weights ω_i from the field F correspond to respective inputs x_i. The output of unit is obtained as the result of sign-function $\mathrm{Fsign}\xi$ on "weighted sum" $\omega_1 x_1 + \ldots + \omega_n x_n + \omega_0$ of inputs as Fig. 1 illustrates.

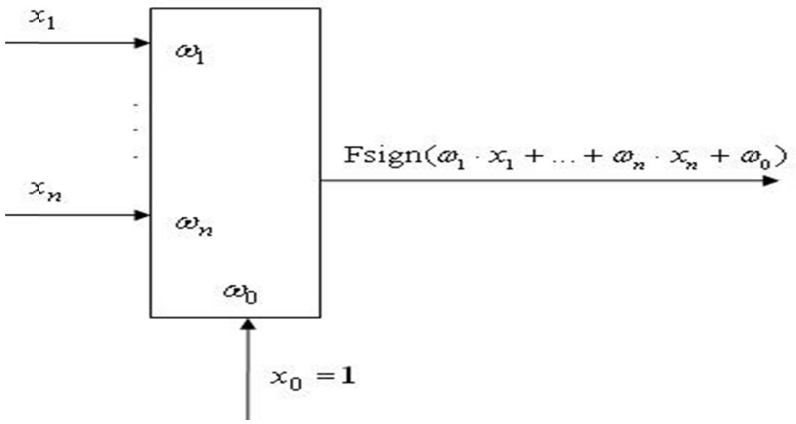

Fig. 1. A representation of neuron over a Galois field

The vector $\mathbf{w} = \left(\omega_1,\ldots,\omega_n;\omega_0\right)$ is called the structure vector of neuron over a Galois field $\left(\omega_i \in GF\left(p^m\right)\right)$.

Let $G_n = H_{k_1} \otimes H_{k_2} \otimes \ldots \otimes H_{k_n}$ be a direct product of cyclic groups H_{k_i}. A discrete function $f : G_n \to H_q$ is realizable by a single neuron over field $F = GF\left(p^m\right)$ if exists $(n+1)$-dimensional vector $\mathbf{w} = \left(\omega_1,\ldots,\omega_n;\omega_0\right)$

such that for all $\mathbf{g}=(\gamma_1,\ldots,\gamma_n)\in G_n$ $f(\mathbf{g})=\mathrm{Fsign}\,\mathrm{w}(\mathbf{g})$, where $\mathrm{w}(\mathbf{g})=\omega_1\gamma_1+\ldots+\omega_n\gamma_n+\omega_0$. A discrete function $f:G_n\to H_q$ realizable on a single neuron over field F is called a neural function over F.

Let $f:G_n\to H_q$ be an arbitrary discrete function. The question arises about realizability of f by a single neuron over filed $F=GF(p^m)$ and synthesis of structure vector $\mathbf{w}=(\omega_1,\ldots,\omega_n;\omega_0)$ of a corresponding neuron.

Let $X^*(G_n)=\left\{\chi_{(0,0,\ldots,0,0)},\chi_{(1,0,\ldots,0,0)},\chi_{(0,1,\ldots,0,0)},\ldots,\chi_{(0,0,\ldots,1,0)},\chi_{(0,0,\ldots,0,1)}\right\}$.

Theorem 1. *A discrete function $f:G_n\to H_q$ is realizable by a single neuron over field $F=GF(p^m)$ with the structure vector $\mathbf{w}=(\omega_1,\ldots,\omega_n;\omega_0)$ if and only if there exists $r:G_n\to F\setminus\{0\}$ such that*

$$0\le\deg r(\mathbf{x})<\frac{u}{q}, \tag{5}$$

and

$$\left(r(\mathbf{x})f(\mathbf{x}),\chi^{-1}(\mathbf{x})\right)=0, \tag{6}$$

for all $\chi\in X(G_n)\setminus X^*(G_n)$, where $(\mathbf{a},\mathbf{b})$ is the standard inner product of vectors **a** *and* **b**.

Proof. At first we shall prove the necessity of the conditions. A discrete function $f:G_n\to H_q$ is realizable over F by a single neuron with the structure $\mathbf{w}=(\omega_1,\ldots,\omega_n;\omega_0)$. That is

$$\forall\mathbf{g}\in G_n\quad f(\mathbf{g})=\mathrm{Fsign}\,\mathrm{w}(\mathbf{g}). \tag{7}$$

Construct the function $r(\mathbf{g})$ in the following way: for all $\mathbf{g}\in G_n$ assume

$$\deg r(\mathbf{g})=\deg \mathrm{w}(\mathbf{g})-\deg f(\mathbf{g}). \tag{8}$$

Then $\deg \mathrm{w}(\mathbf{g})=\deg r(\mathbf{g})+\deg f(\mathbf{g})$ and for an arbitrary $\mathbf{g}\in G_n$

$$f(\mathbf{g})r(\mathbf{g})=\omega_0+\omega_1x_1(\mathbf{g})+\cdots+\omega_nx_n(\mathbf{g}). \tag{9}$$

Suppose that the value of f on an arbitrary fixed element $\mathbf{g} \in G_n$ is σ^j. Then from (7) follows

$$\frac{ju}{q} \le \deg \mathrm{w}(\mathbf{g}) < \frac{(j+1)u}{q}. \tag{10}$$

The inequality (10) can be written as follows:

$$\frac{ju}{q} - \deg f(\mathbf{g}) \le \deg \mathrm{w}(\mathbf{g}) - \deg f(\mathbf{g}) < \frac{(j+1)u}{q} - \deg f(\mathbf{g}).$$

From the last inequality, (8) and

$$\deg f(\mathbf{g}) = \frac{ju}{q},$$

$\left(f(\mathbf{g}) = \sigma^j = \varepsilon^{ju/q}\right)$ follows $0 \le \deg r(\mathbf{g}) < \frac{u}{q}$.

Now we give the proof of the sufficiency of the theorem condition. Let us assume that for $f: G_n \to H_q$ exists a function $r: G_n \to F \setminus \{0\}$ satisfying conditions (5) and (6). We can expand the function $r(\mathbf{x}) f(\mathbf{x}) \in V_F^n$ in characters of group G_n over field F. In consideration of (6) and $\forall \chi \in \chi(G_n) \setminus \chi^*(G_n)$ $s_\chi = =\mid G_n \mid^{-1} \left(r(\mathbf{x}) f(\mathbf{x}), \chi^{-1}(\mathbf{x})\right)$ we have $s_\chi = 0$. It means

$$r(\mathbf{x}) f(\mathbf{x}) = \sum_{\chi \in \chi^*(G_n)} s_\chi \chi(\mathbf{x}). \tag{11}$$

The equality (11) can be written as follows:

$$r(\mathbf{x}) f(\mathbf{x}) = s_{(0,\cdots,0)} \chi_{(0,\cdots,0)}(\mathbf{x}) + s_{(1,\cdots,0)} \chi_{(1,\cdots,0)}(\mathbf{x}) + \cdots + s_{(0,\cdots,1)} \chi_{(0,\cdots,1)}(\mathbf{x}),$$

or

$$r(\mathbf{x}) f(\mathbf{x}) = \omega_0 + \omega_1 \chi_{(1,\cdots,0)}(\mathbf{x}) + \cdots + \omega_n \chi_{(0,\cdots,1)}(\mathbf{x}). \tag{12}$$

According to our definition $\chi_{(1,\cdots,0)}(\mathbf{x}) = x_1(\mathbf{x}), \cdots, \chi_{(0,\cdots,1)}(\mathbf{x}) = x_n(\mathbf{x})$. Thus,

$$r(\mathbf{x}) f(\mathbf{x}) = w(\mathbf{x}). \tag{13}$$

The direct consequence from (13) is the fact that for all $\mathbf{g} \in G_n$

$$\deg r(\mathbf{g}) = \deg \mathrm{w}(\mathbf{g}) - \deg f(\mathbf{g}).$$

Condition (5) implies that

$$0 \le \deg \mathrm{w}(\mathbf{g}) - \deg f(\mathbf{g}) < \frac{u}{q}. \qquad (14)$$

Let $\mathbf{g}$ is an arbitrary element in G_n and $f(\mathbf{g}) = \sigma^j$. Then

$$\deg f(\mathbf{g}) = \frac{uj}{q}$$

and from (14) follows

$$\frac{uj}{q} \le \deg \mathrm{w}(\mathbf{g}) < \frac{u(j+1)}{q}.$$

So, for all $\mathbf{g}$ in G_n $f(\mathbf{g}) = \mathrm{Fsign}\,\mathrm{w}(\mathbf{g})$, that proves the sufficiency of theorem conditions.

If a discrete function $f: G_n \to H_q$ satisfies all conditions of theorem 1, then the coordinates of the structure vector $\mathbf{w} = (\omega_1, \ldots, \omega_m; \omega_0)$ of the neuron, realizing f over field F, can be found as follows:

$$\omega_0 = |G_n|^{-1} \left(r(\mathbf{x}) f(\mathbf{x}), \chi^{-1}_{(0,\ldots,0)}(\mathbf{x}) \right),$$

$$\omega_1 = |G_n|^{-1} \left(r(\mathbf{x}) f(\mathbf{x}), \chi^{-1}_{(1,0,\ldots,0)}(\mathbf{x}) \right), \qquad (15)$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\omega_n = |G_n|^{-1} \left(r(\mathbf{x}) f(\mathbf{x}), \chi^{-1}_{(0,\ldots,0,1)}(\mathbf{x}) \right).$$

Example. Let $n = 2, k_1 = 2, k_2 = q = 3$ i $G_2 = H_2 \otimes H_3$. Then $k = \mathrm{lcm}(2,3,3)$. So, we can use $GF(13)$ as F with 2 as the primitive element of F, that is $GF(13) \setminus \{0\} = \{2^j \mid j = 0,1,\ldots,11\}$. The group generators of groups H_2, H_3 over F are correspondently $\sigma_1 = 2^{12/2} = 12$ and $\sigma_2 = 2^{12/3} = 3$, and the range of values of function $f: G_n \to H_q$ is the set $\{1,3,9\}$. Table 1 can be used for value assignment of functions $f: G_n \to H_q$, $r: G_n \to F \setminus \{0\}$ and the character group $X(G_2)$ of group G_2 over F:

Table 1.

Values of f, r and characters from $\chi(G_2)$

x_1	x_2	f	r	$\chi_{(0,0)}$	$\chi_{(0,1)}$	$\chi_{(0,2)}$	$\chi_{(1,0)}$	$\chi_{(1,1)}$	$\chi_{(1,2)}$
1	1	1	r_0	1	1	1	1	1	1
1	3	1	r_1	1	3	9	1	3	9
1	9	3	r_2	1	9	3	1	9	3
12	1	3	r_3	1	1	1	12	12	12
12	3	9	r_4	1	3	9	12	10	4
12	9	9	r_5	1	9	3	12	4	10

On the basis of theorem 1 and table 1 we can write the following linear equation system over F:

$$\begin{cases} r_0 + 3r_1 + r_2 + 3r_3 + r_4 + 3r_5 = 0, \\ r_0 + 9r_1 + 9r_2 + 10r_3 + 10r_4 + 12r_5 = 0, \\ r_0 + 3r_1 + r_2 + 10r_3 + 12r_4 + 10r_5 = 0, \end{cases}$$

$r_0, r_1, r_2, r_3, r_4, r_5 \in \{1,2,4,8\}$. The last system has several solutions, one of these is $(1,8,1,1,4,2)$. This system solution may be use for finding the structure vector of the neuron, realizing the function f:

$$\omega_0 = 11 \cdot (1 + 8 + 3 + 3 + 36 + 18) = 11 \cdot 4 = 5,$$
$$\omega_1 = 11 \cdot (1 + 8 + 3 + 3 \cdot 12 + 36 \cdot 12 + 18 \cdot 12) = 11 \cdot 7 = 12,$$
$$\omega_2 = 11 \cdot (1 + 72 + 9 + 3 + 9 \cdot 9 \cdot 4 + 9 \cdot 3 \cdot 2) = 11 \cdot 8 = 10.$$

Therefore, $f(x_1, x_2) = \text{Fsign}(12x_1 + 10x_2 + 5)$.

The design of neuron synthesis methods for partially specific discrete functions is very important in practice, because this task often arises in many applications, such as pattern recognition, diagnostics and talk synthesis

Let a discrete function $f : G_n \to H_q$ be not fully defined on group G_n. We shall denote $D_n \subset G_n$ the set of elements, in which the value of the function f is well defined and let $D'_n = G_n \setminus D_n$ be the set of elements in which the function f is undefined.

 ISSN 1562-9945

The partially defined discrete function $f: G_n \to H_q$ is realizable on a single neuron over the field F if exists $(n+1)$-dimensional vector $\mathbf{w} = (\omega_1, \ldots, \omega_n; \omega_0)$ such that for all $\mathbf{g} \in D_n$ $f(\mathbf{g}) = \mathrm{Fsign}\, \mathrm{w}(\mathbf{g})$.

Theorem 2. *A partially defined discrete function* $f: G_n \to H_q$ *is realizable on a single neuron over field* $F = GF(p^m)$ *with the structure vector* $\mathbf{w}$ *if such well defined functions* $r: G_n \to F \setminus \{0\}$, $h: G_n \to H_q$ *exist, that the restriction of* h *on* D_n *coincides with* f *and for all* $\mathbf{x}$ *in* D_n *the following conditions are satisfied*

$$0 \le \deg r(\mathbf{x}) < \frac{u}{q},$$

$$\left(r(\mathbf{x}) f(\mathbf{x}), \chi^{-1}(\mathbf{x})\right) = 0,$$

where $\chi \in X(G_n) \setminus X^*(G_n)$.

The proof results from theorem 1.

The class of discrete functions realizable on a single neuron depends on selected Galois field. The computer modeling of synthesis neurons over a finite field F proves that increasing of the cardinality of the field F implies that the cardinality of the class of neural functions does not decrease. The following example confirms the last claim. Let $n = 2, k_1 = k_2 = q = 2$ i $F = GF(3)$. The number u is multiple of $k = \mathrm{lcm}(k_1, k_2, q)$, thus the spectral analysis of Boolean functions over F is possible. It is evident that $\varepsilon = 2$ is the primitive element of the field F. All Boolean neural functions of two variables over F are given in the following table.

Table 2

Neural functions over $GF(3)$

x_1	x_2	g_0	g_1	g_2	g_3	g_4	g_5
1	1	1	1	1	2	2	2
1	2	1	1	2	2	2	1
2	1	1	2	1	2	1	2
2	2	1	2	2	2	1	1

The respective structure vectors are $\mathbf{w}_{g_0} = (0,0;1)$, $\mathbf{w}_{g_1} = (1,0;0)$, $\mathbf{w}_{g_2} = (0,1;0)$, $\mathbf{w}_{g_3} = (0,0;2)$, $\mathbf{w}_{g_4} = (2,0;0)$ and $\mathbf{w}_{g_5} = (0,2;0)$. Thus, the class of Boolean neural functions of two variables over $GF(3)$ contains six functions $g_0, g_1, g_2, g_3, g_4, g_5$.

Let us consider the field $F = GF(5)$. It is possible to take $\varepsilon = 2$ as a primitive element Then $\sigma = \varepsilon^{\frac{5-1}{2}} = 4$. The Boolean neural functions of two variables over $GF(5)$ are given in Table 3.

Table 3

Neural functions over $GF(5)$

x_1	x_2	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
1	1	1	1	1	1	1	1	1	1	4	4	4	4	4	4	4	4
1	4	1	1	1	1	4	4	4	4	1	1	1	1	4	4	4	4
4	1	1	1	4	4	1	1	4	4	1	1	4	4	1	1	4	4
4	4	1	4	1	4	1	4	1	4	1	4	1	4	1	4	1	4

The respective structure vectors are

$\mathbf{w}_{f_0} = (0,0;1), \mathbf{w}_{f_1} = (2,2;2), \mathbf{w}_{f_2} = (2,3;2), \mathbf{w}_{f_3} = (1,0;0), \mathbf{w}_{f_4} = (3,2;2), \mathbf{w}_{f_5} = (0,1;0),$
$\mathbf{w}_{f_6} = (1,1;4), \mathbf{w}_{f_7} = (2,2;3), \mathbf{w}_{f_8} = (3,3;2), \mathbf{w}_{f_9} = (4,4;1), \mathbf{w}_{f_{10}} = (0,4;0), \mathbf{w}_{f_{11}} = (2,3;3),$
$\mathbf{w}_{f_{12}} = (4,0;0), \mathbf{w}_{f_{13}} = (3,2;3), \mathbf{w}_{f_{14}} = (3,3;3), \mathbf{w}_{f_{15}} = (0,0;4)$.

We see that all two variable Boolean function are realizable over $GF(5)$. The field $GF(5)$ is the minimal Galois field (by cardinality) having the mentioned property.

Let $k = \text{lcm}(k_1, \ldots, k_n, q) (k_i \geq 2, q \geq 2)$ and $G_n = H_{k_1} \otimes \ldots \otimes H_{k_n}$.

Hypothesis. For any k and n there exists minimal Galois field $F_{\min}$ such that all functions $f : G_n \to H_q$ are realizable on single neuron over which.

Conclusions

The effective synthesis method of many valued neurons over a Galois field is designed on the basis of spectral analysis of discrete functions. This method can be used for solving practical problems, such as information encoding, data compression, data communication, classification, pattern recognition, etc.

 ISSN 1562-9945

REFERENCES

1. Берлекемп Э. Алгебраическая теория кодирования / Э. Берлекемп. – М.: Мир, 1971. – 477 с.
2. Кузьмин И. В. Основы теории информации и кодирования / И. В. Кузьмин, В. А. Кедрус. – К.: Вища школа, 1977. – 278 с.
3. Кларк Дж. Кодирование с исправлением ошибок в системах цифровой связи / Дж. Кларк, Дж. Кейн мл. – М.: Радио и связь, 1987. – 391 с.
4. Eichner L. Homomorphe Darstellungen endlicher Automaten in linearen Automaten / L. Eichner. – EIK. – 1973. – Т. 9. – № 10. – P. 67-76.
5. Курош А. Г. Теория групп / А. Г. Курош. – М.: Наука, 1967. – 648 с.
6. Ван дер Варден Б. Л. Алгебра / Б. Л. Ван дер Варден. – М.: Наука, 1979. – 623 с.
7. Кострикин А. И. Введение в алгебру/ А. И. Кострикин. – М.: Наука, 1977. – 495 с.
8. Постников М. М. Теория Галуа / М. М. Постников. – М.: Физматгиз, 1963. – 218 с.
9. Кертис Ч. Теория представлений конечных групп и ассоциативных алгебр / Ч. Кертис, И. Райнер. – М.: Наука, 1969. – 667 с.
10. Ярославский Л. П. Введение в цифровую обработку изображений / Л. П. Ярославский. – М.: Советское радио, 1979. – 312.