GENERATION OF NONLINEAR RECURRENT SEQUENCES IN EXPANDED $GF(p^n)$ FIELDS BY SOFTWARE-HARDWARE METHODS

I. I. Snytkin

Izvestiya VUZ. Radioelektronika,
Vol. 33, No. 7, pp. 26-31, 1990

UDC 691.392.82

A software-hardware concept has been developed for methods and engineering solutions in the creation of means for generating expanded Galois fields $GF(p^n)$, $p > 2$; this basis has been used to develop systems of nonlinear recurrence sequences (NLRS) which exist in $GF(p^n)$. The conception given has been based on utilizing established and reducible systematic combinatorial-logic properties in the theory of $GF(p^n)$ fields and employing the rules for formulating NLRS.

Unlike the widely known linear recurrent sequences (LRS) and nonlinear recurrent sequences (NLRS) in the form of complete code rings existing in the fields $GF(2^n)$ for lengths L which respectively equal $L = 2^n - 1$ and $L = 2^n$ which are widely utilized in systems with noise-like signals (NLS), NLRS in the form of characteristic codes which exist in expanded falls $GF(p^n)$ in which any prime number $p > 2$ (see [1,2]) occupy a special place. This is associated with the fact that the given NLRS exist for a much greater number of lengths $L = p^n - 1$, have a much greater coding power (see [2]), and are stable relative to decoding and simulation (see [1]); this makes them much more preferable in the general case. However, the practical application and researched knowledge about the given NLRS is very restricted, since their construction is very complex and cumbersome and, what is very important, no methods or generation means have been developed for them as is the case for LRS and complete code rings (see [1]).

The rule for constructing NLRS in the form of characteristic codes in $GF(p^n)$ has the following form in accordance with [2]:

$$GF(p^n) = \{a_i : \Theta^i \,(\operatorname{mod} df(x), p)\}, \quad L = p^n - 1 = 4t,\ 4t+2, \quad t = 1, 2, \dots;$$
$$\begin{cases} V = \{V_i : i = 0, 1, \dots, p^n - 2\}; \\ V_i = \psi(\Theta^i + 1), \ \text{for} \ \Theta^i + 1 \not\equiv 0 \,(\operatorname{mod} df(x), p); \\ V_i = \pm 1, \ \text{for} \ \Theta^i + 1 \equiv 0 \,(\operatorname{mod} df(x), p), \end{cases} \tag{1}$$

where a_i are the elements of the field $GF(p^n)$; Θ is the primitive field element; $\psi(\cdot)$ is the two-valued character of the multiplicative group $G(p^n - 1)$:

$$\psi(a) = \exp[j2\pi u] = \begin{cases} 1 & \text{for} \ u \equiv 0 \,(\operatorname{mod} 2); \\ -1 & \text{for} \ u \not\equiv 0 \,(\operatorname{mod} 2), \end{cases} \tag{2}$$

where u is the index (Ind) of the element a if the condition

$$a \equiv \Theta^u \,(\operatorname{mod} df(x), p). \tag{3}$$

is fulfilled.

As is evident from the rule (1) and relationships (2), (3), the construction of a system of linear NLRS is associated with calculating the elements a_i of the field $GF(p^n)$ for a known primitive $f(x)$ while finding the congruences between a_i and their indices, calculating the indices Ind a_i and determining the characters $\psi(a_i)$.

The algorithmic realization of the rule (1) is very difficult, since it is associated first of all with operations

REFERENCES

1. R. K. Dickson, Broadband Systems [Russian translation], V. I. Zhuravlev (Editor), Svyaz, Moscow, 1979.
2. M. B. Sverdlik, Optimal Discrete Signals [in Russian], Sov. radio, Moscow.
3. R. Liedle and G. Niederrieter, Finite Fields [Russian translation], V. I. Nechaev (Editor), [translated from English by A. E. Zhukov and V. I. Petrov], Mir, Moscow, 1988.
4. USSR Patent Application No. 900281, MKI^3 G06F 7/49.
5. USSR Patent Application No. 1334143, MKI^4 G06F 7/52.

19 June 1989