A NEW CLASS OF SEQUENCES: MAPPING SEQUENCES

Guang Gong
Fondazione Ugo Bordoni

Via B. Castiglione, 59, I-00142, Roma, Italy

Abstract: A Galois field $GF(q^n)$ can be regarded as a linear vector space over $GF(q)$. The elements of $GF(q^n)$ can be represented by $m$-tuples of elements belonging to $GF(q)$. In this way, a sequence over $GF(q^n)$ becomes a sequence over $GF(q)$. We call the sequence over $GF(q)$ a mapping sequence. A change of basis of $GF(q^n)$ over $GF(q)$ can change the period, the linear span and the autocorrelation function of a mapping sequence. The aim of this work is to investigate the above properties of mapping sequences. It is shown that the sufficient and necessary conditions which guarantee the periods and the linear spans of mapping sequences reach the maximum values. The special kind of bases of $GF(q^n)$ over $GF(q)$ found is one in which the autocorrelation functions of such mapping sequences are $3$-valued. We point out that mapping sequences are of considerable theoretical importance. The result of autocorrelation functions can be used to solve the minimum distance of one kind of burst error correcting codes. The practical importance relies on the fact that the set of generalized mapping sequences contains a lot of well-known sequences (i.e., multiplexed sequences, clock controlled sequences, GMW sequences or generalized GMW sequences and No sequences).

Work carried out in the framework of the agreement between the Italian PT Administration and the Fondazione "Ugo Bordoni".
1. Definition and Algebraic Structure of Mapping Sequences

Let \( a = \{a(k)\}_{k \geq 0} \) be a periodic sequence over \( GF(q^n) \), \( \{\beta_0, \cdots, \beta_{m-1}\} \) be a basis of \( GF(q^n) \) over \( GF(q) \). Any element of \( a \) can be represented as follows:

\[
a(k) = a_0(k)\beta_0 + \cdots + a_{m-1}(k)\beta_{m-1}, \quad a_j(k) \in GF(q).
\]

We map \( a(k) \) into \( a_0(k), \cdots, a_{m-1}(k) \). This map generates the following sequence:

\[
u = a_0(0), \cdots, a_{m-1}(0), a_0(1), \cdots, a_{m-1}(1), \cdots
\]

We write \( u = \{u(k)\}_{k \geq 0} \). Notice that \( u \) is a periodic sequence over \( GF(q) \).

Definition 1: The \( q \)-ary sequence \( u \), defined by (2), is called the mapping sequence generated by the sequence \( a \) under the basis \( \{\beta_0, \cdots, \beta_{m-1}\} \) of \( GF(q^n) \) over \( GF(q) \). (we call \( u \) the mapping sequence for a short).

Let \( a_j = \{a_j(k)\}_{k \geq 0} (j = 0, \cdots, m-1) \), we call \( a_j \) the \( j \)-th component sequence of \( u \) (or \( a \)) over \( GF(q) \).

From this point on, we suppose that
- \( f(z) \) is the minimal polynomial of the sequence \( a \) over \( GF(q^n) \) (the polynomial of the lowest degree over \( GF(q^n) \) which generates the sequence \( a \));
- \( h(x) \) is the minimal polynomial of the mapping sequences \( u \) over \( GF(q) \);
- \( f_j(x) \) is the minimal polynomial of the component sequences \( a_j \) of \( u \) over \( GF(q) \) \((j=0, \cdots, m-1)\).

In this section, we will show the relationships among \( f(z) \), \( h(x) \), and \( f_j(x) (j=0, \cdots, m-1) \) and the representations of the elements of the mapping sequence \( u \).

Now we list some notations which are used throughout this paper.
- \( s^{(r)} \) represent the sequence \( s(0), s(r), s(2r), \cdots \), recalling that \( s^{(r)} \) is called a \( r \)-decimation of the sequences \( s \);
- \( L \) represent the left shift operator, i.e., \( \text{L}^k(s) = s(k), s(k+1), \cdots \); let \( g(x) = \sum_{i=0}^{r} c_i x^i \) be a polynomial over \( GF(q^n) \), then \( g(\text{L})(s) = \sum_{i=0}^{r} c_i \text{L}^i(s) \);
- \( \text{T}_{GF(q^n)/GF(q)}(z) = x + x^q + \cdots + x^{q^{t-1}}, \ x \in GF(t^t), \ t \) is a power of a prime;