Generalized BCH-theorem and linear recursive MDS-codes.  

V. Markov  
vtmarkov@mech.math.msu.su  
Moscow State University  

A. Nechaev  
nechaev@cnit.msu.ru  
Moscow State University  

Abstract. For an arbitrary monic polynomial \( f(x) \) of the degree \( m \) over the field \( P = GF(q) \) the set \( K = L_{\beta, n-1}(f) \) of all initial segments of length \( n \geq m \) of the linear recurring sequences with the characteristic polynomial \( f(x) \) is a linear \([n, m]\)-code over \( P \), called recursive. We describe some conditions sufficient for the code \( K \) to be MDS.

\(^1\)This research is supported by the President of RF grant NSh-8.2010.10 and RFBR grant 08-01-00693-a
1 Linear recursive codes

Let $P = \text{GF}(q)$. A sequence over $P$ is a function $u: \mathbb{N}_0 \to P$. We will identify: $u = (u(0), u(1), \ldots, u(i), \ldots)$.

Let us denote $P^{(1)} = \{u : \mathbb{N}_0 \to P\}$. For an arbitrary monic polynomial $f(x) = x^m - f_{m-1}x^{m-1} - \ldots - f_0 \in P[x]$

we denote $L_P(f) =$

$\{u \in P^{(1)} : u(i + m) = f_{m-1}u(i + m - 1) + \ldots + f_0u(i), i \geq 0\}$

the set of all LRS with characteristic polynomial $f(x)$.

For any $n \geq m$ and any $u \in L_P(f)$ we consider its initial segment of length $n$: $u[\overline{0, n-1}] = (u(0), \ldots, u(n - 1))$. The set $\mathcal{K} = L_P^{0, n-1}(f) = \{u[\overline{0, n-1}] : u \in L_P(f)\}$ (1)

is an $[n, m]_q$-code over $P$, called linear recursive $[n, m]$-code with characteristic polynomial $f(x)$. 


The matrix
\[
H = \begin{pmatrix}
    f_0 & f_1 & \ldots & f_{m-1} & -e & 0 & \ldots & 0 \\
    0 & f_0 & f_1 & \ldots & f_{m-1} & -e & \ldots & 0 \\
    \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
    0 & \ldots & 0 & f_0 & f_1 & \ldots & f_{m-1} & -e
\end{pmatrix}
\]
is a parity-check matrix of the code \( \mathcal{K} = L_{P,n-1}^0(f) \), and generating matrix of the linear \([n,n-m]_q\) code \( \mathcal{K}^* \) dual to \( \mathcal{K} \).

It is well known that the length \( n \), dimension \( m \) and distance \( d \) of any code satisfy the following Singleton bound [1]
\[
m + d \leq n + 1. \tag{2}
\]
Codes meeting this bound are called MDS-codes. One of the defining properties of an MDS-[\( n, m \)]-code \( \mathcal{K} \) is that \( \mathcal{K}^* \) is an MDS-code. Our aim is to describe recursive MDS-codes.
2 Generalized BCH-Theorem

There is not difficult generalization of a well-known BCH-theorem from cyclic codes to the recursive ones.

**Theorem 1.** Let a polynomial $f(x) \in P[x]$, $\deg f = m$, has in splitting field chain of $r$ roots (BCH-chain)
\[ \alpha_1, \alpha_2 = \alpha_1 \alpha, \ldots, \alpha_r = \alpha_1 \alpha^{r-1}, \ \text{ord} \alpha \geq n > m \geq r. \] (3)

Then the code $K^o$ dual to $K = L_{P}[\eta^{-1}](f)$ satisfies the condition
\[ d(K^o) \geq r + 1. \]
If $r = m = \deg f$ then both codes $K$ and $K^o$ are MDS-codes.

Note that the last condition is equivalent to the equality
\[ f(x) = (x - \alpha_1) \ldots (x - \alpha_m), \]
which in view of $f(x) \in P[x]$ is equivalent to the condition of invariance of the BCH-chain (3):
\[ \{\alpha_1^q, \ldots, \alpha_m^q\} = \{\alpha_1, \ldots, \alpha_m\}. \] (4)
3 Invariant BCH-chains. Description.

Let \( P \leq Q, \  \alpha_1, \alpha \in Q, \  t = \text{ord}(\alpha), \ m \leq t, \)

\[
B(\alpha_1, \alpha, m) = \{\alpha_1, \ \alpha_2 = \alpha_1 \alpha, \ldots, \alpha_m = \alpha_1 \alpha^{m-1}\}
\]
be a BCH-chain and

\[
f(x) = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_1).
\]

The problem of finding the recursive MDS-codes is partially reduced to that of finding invariant BCH-chains:

\[
B = B(\alpha_1^q, \alpha^q, m) = B(\alpha_1, \alpha, m),
\]
or to the problem of finding conditions of the inclusion

\[
f(x) \in P[x].
\]

It is well-known that \( B \) is invariant in the following 4 cases:
(i) $B = \{\alpha_1, \alpha_2 = \alpha_1 \alpha, \ldots, \alpha_m = \alpha_1 \alpha^{m-1}\}$
is a degenerated chain:

$B \subset P$, or $\alpha_1^{q-1} = \alpha^{q-1} = e$.

Then of course $f(x) \in P$ and under the condition

$m < n \leq t = \text{ord} \alpha$

the code $K = L_{p,n-1}^0(f)$ is a

**recursive Reed–Solomon** $[n, m, n - m + 1]$ MDS-code

with a generating matrix

$$G = \begin{pmatrix}
e & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\
e & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\
\vdots & \cdots & \cdots & \cdots & \cdots \\
e & \alpha_m & \alpha_m^2 & \ldots & \alpha_m^{n-1}
\end{pmatrix}.$$
(ii) \( B = \{\alpha_1, \alpha_2 = \alpha_1 \alpha, \ldots, \alpha_m = \alpha_1 \alpha^{m-1}\} \) is a group chain:

\[ m = t = \text{ord} \alpha \quad \text{and} \quad B = \alpha_1 < \alpha > \]

is a coset by the cyclic subgroup \(< \alpha >\) generated by \(\alpha_1 \in Q\) with property \(\alpha_1^t \in P\). Then

\[ f(x) = x^t - \alpha_1^t \in P[x], \quad m = n = t, \]

and \(K = L_{P}^{0,n-1}(f)\) is a trivial \([n, n, 1]\)-MDS-code.
(iii) $B = \{\alpha_1, \alpha_2 = \alpha_1 \alpha, \ldots, \alpha_m = \alpha_1 \alpha^{m-1}\}$ is a shortened group chain:

$$m = t - 1 \quad \text{where} \quad t = \text{ord} \alpha, \quad \text{and}$$

$B = c(\langle \alpha \rangle \setminus \{e\}) = c\{\alpha, \ldots, \alpha^{t-1}\}$, where $c = \alpha_1 \alpha^{-1} \in P$.

Then

$$f(x) = x^{t-1} + cx^{t-2} + \ldots + c^{t-2} x + c^{t-1} \in P[x]$$

and for $n = t$ we can state that $\mathcal{K} = L_P^{0,n-1}(f)$ is a trivial $[n, n-1, 2]$-MDS code of parity check;
(iv) \( B = \{\alpha_1, \alpha_2 = \alpha_1 \alpha, \ldots, \alpha_m = \alpha_1 \alpha^{m-1}\} \)

is a Georgiades chain [2, 1982]:

\[ Q = \text{GF}(q^2), \text{ ord } \alpha = t, \ t|q+1, \ 1 < m < t, \ \alpha_1^{q-1} = \alpha^{m-1}. \]

Then

\[ \alpha_i^q = \alpha_{m-i+1}, \ i \in \overline{1, m}, \ f(x) \in P[x] \]

and \( K = L_P^{0,n-1}(f) \) is an MDS \([n, m, n - m + 1]\)-code for every \( n \in \overline{m, t}. \)
Our main result:

**Theorem 2.** Any invariant BCH-chain has one of the following types:

(i) a degenerated chain;
(ii) a group chain;
(iii) a shortened group chain;
(iv) a Georgiades chain.

The codes described in this Theorem we will call **recursive BCH-MDS-codes**.

However this result does not solve the problem of description of all recursive MDS-codes.
4 Examples and open questions

The family of recursive MDS-codes is very diverse.

1. Let $P$ be a field of characteristic $p \geq n$. Then among the recursive $[n, 2, n - 1]_P$-MDS-codes there exist Reed–Solomon codes, Georgiades codes and non BCH-codes, for example the code $K = L_P^{0,n-1}((x - e)^2)$.

2. All the recursive $[8, 4, 5]_8$-MDS-codes are BCH-codes.

3. Although there are no recursive $[10, 7, 4]_8$-BCH-codes. But there exist exactly 42 other recursive MDS-codes with these parameters. Everyone of them has characteristic polynomial of the form $f(x) = (x - a)^3 g(x)$, where $a \in P^*$ and $g(x) \in P[x]$ is an irreducible polynomial of degree 4.
4. There are no recursive $[18, 15, 4]_{16}$-BCH-codes.

For $P = GF(16)$ we could not enumerate all recursive $[18, 15, 4]_p$-MDS-codes with PC. Tveritinov (2009) has found 15 such codes. Their characteristic polynomials have decompositions over $P$ of various types. The following table presents some properties of these polynomials

<table>
<thead>
<tr>
<th>Number of polynomials</th>
<th>Number of irreducible factors</th>
<th>Number of roots in $P$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>3 (inseparable)</td>
</tr>
</tbody>
</table>

So the problem of full description of linear recursive MDS-codes remains open.

**References**
