MDS CODES FROM POLYCYCLIC CODES OVER FINITE FIELDS

Mehmet Özen, Halit İnce

Sakarya University, Department of Mathematics, Sakarya- Turkey

ozen@sakarya.edu.tr, ince@sakarya.edu.tr

Abstract: In this work, we construct polycyclic codes over finite fields by using linear algebraic methods. After the construction, we perform an exhaustive search by using polycyclic codes to obtain MDS codes over finite fields which have many applications in cryptography. The computer search results are presented at the end of the paper.

Keywords: Polycyclic Codes, MDS Codes, Finite Fields

Introduction

Polycyclic codes are the generalization of cyclic and constacyclic codes and were studied in (William, 1972) for the first time. In (Radkova, 2009) Radkova et al. studied the cyclic and constacyclic codes from a linear algebraic point of view. In this work, we construct polycyclic codes over finite fields by using same methods.Then we perform an exhaustive search by using polycyclic codes to obtain MDS codes over finite fields which have many applications in cryptography. The computer search results are presented at the end of the paper.

Polycyclic Codes

Polycyclic codes are the generalization of cyclic and constacyclic codes. We give the definition of polycyclic code.

Definition 2.1: A linear code C with length n over a finite field F is called polycyclic code induced by the polynomial $v(x) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1} \in F[x]$ such that if $c = (c_0, c_1, \cdots, c_{n-1}) \in C$ then its $v-vector$ shift $(0, c_0, c_1, \cdots, c_{n-2}) + c_{n-1}(v_0, v_1, \cdots, v_{n-1}) \in C.$

Let $F = GF(q)$ and let F^n be the n-dimensiomal vector space over F with standard basis $e_1 = (1,0,\ldots,0), e_2 = (0,1,\ldots,0), \ldots, e_n = (0,0,\ldots,n).$
Then polycyclic shift with respect to a vector v is the following transformation:

$$\begin{array}{rccc} \tau_v : & F^n & \to & F^n \\ & (c_0, c_1, \cdots, c_{n-1}) & \mapsto & (v_0 c_{n-1} + v_1 c_{n-1}, \cdots, c_{n-2} + v_{n-1} c_{n-1}). \end{array}$$

Then it has the following matrix

$$T_v = \begin{pmatrix} 0 & \cdots & \cdots & 0 & v_0 \\ 1 & 0 & \cdots & 0 & v_1 \\ 0 & 1 & & \vdots & \vdots \\ \vdots & & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & v_{n-1} \end{pmatrix}$$

with respect to tstansard basis. Note that the characteristic polynomial of T_v is $f(x) = x^n - v(x)$.

Let $gcd(n,q) = 1$. Assume that $f(x) = x^n - v(x) = f_1(x) f_2(x) \ldots f_t(x)$ be the factorization of $f(x)$ into monic irreducible factors over F. Cayley-Hamilton Theorem states that the matrix T_v satisfies $f(T_v) = 0$.

Now we consider the set of homogeneous equations

$$f_i(T_v)x = 0, \quad x \in F^n \text{ for } i = 1,\ldots,t.$$

Let U_i be the solution space of $f_i(T_v)x = 0, \quad x \in F^n$. We denote $U_i = Kerf_i(\tau_v)$. Then each U_i is a subspace of F^n.

Then we have the following theorem:

Theorem 2.2: The following statements hold for the subspaces U_i of F^n:

(1) U_i is τ_v-invariant subspace of F^n;

(2) If W is a τ_v-invariant subspace of F^n and $W_i \cap W = U_i$ for $i = 1,2,\ldots,t$, then W_i is free τ_v-invariant and $W = W_1 \oplus \ldots \oplus W_t$;

(3) $F^n = U_1 \oplus \ldots \oplus U_t$;

(4) $dim_F(U_i) = deg(f_i) =: k_i$;

(5) $f_i(x)$ is the minimal polynomial of τ_v over U_i;

(6) U_i is the minimal τ_v-invariant subspace of F^n;

(7) For any subspace U of F^n, U is the direct sum of some of minimal τ_v-invariant subspaces U_i of F^n.

Then the following theorem is clear from the definition:

Theorem 2.3: A linear code C with length n over F is a polycyclic code with respect to some $v(x) \in F[x]$ if and only if C is a τ_v-invariant subspace of F^n.

Theorem 2.4: Let C be a linear polycyclic code with length n over F with respect to some $v(x) \in F[x]$. Then the following statements hold:

(1) $C = U_{i_1} \oplus U_{i_2} \oplus \ldots \oplus U_{i_s}$ for some minimal τ_v-invariant subspaces of R^n and $k := dim(C) = k_{i_1} + \ldots + k_{i_s}$, where $k_{i_j} = dim(U_{i_j}), \quad j = 1,\ldots,s$;

(2) $h(x) = f_{i_1}(x)\ldots f_{i_s}(x)$ is the minimal polynomial of τ_v over C;

(3) $dim(h(T)) = n - k$;\

(4) $c \in C$ if and only if $h(T)c = 0$.

Then we have the following result which explains how we construct pollcyclic codes over finite fields.

Corollary 2.5: $H = h(T_v)$ is a parity check matrix for the code C and $G = (g(T_v))^t$ is a generator matrix for the code C where $x^n - v(x) = f(x) = g(x)h(x)$. In this case, $g(x)$ is said to be the generating polynomial of the polycyclic code C.

MDS Codes

In this section we briefly explain the MDS codes and its applications in cryptography. The reader who wants more information about this topic may consult (Augot, 2014).

Definition 3.1: Let C be linear code over F_q with parameters [n,k,d]. C is said to be a MDS code if $d = n + k - 1$ is satisfied.

Definition 3.2: A matrix M is MDS if its concatenation with the identity matrix $G_M := [I_k \mid M]$ yields a generating matrix of an MDS code C.

MDS matrices are used in linear diffusion layers in cryptography. A linear diffusion layer of a block cipher is defined by an invertible matrix of size $k \times k$ over F_q. It takes $x \in F_q^n$ as a input and yields $y \in F_q^k$ as an output with $y = x \times M$.

The security of a diffusion layer is measured by its differential branch number and the linear branch number. The larger the two branch numbers are, the stronger a diffusion layer is. The diffusion layers with the optimal branch numbers are called being maximum distance separable. Optimal linear diffusion can thus obtained by using codes with largest possible minimal distance, namely MDS codes.

Several different techniques have been studied to obtain MDS matrices, a well known example being circulant matrices as used in the AES (Daemen, 1012) or FOX (Junod, 2004). Recently a new construction has been proposed: the so-called recursive MDS matrices, that were for example used in LED (Guo, 2011). These matrices have the property that they can be expressed as a power of a companion matrix C.

Definition 3.3: The companion matrix of monic polynomial $c(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} + x^n$ is defined as the square matrix

$$T_v = \begin{pmatrix} 0 & \cdots & \cdots & 0 & c_0 \\ 1 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & & \vdots & \vdots \\ \vdots & & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & c_{n-1} \end{pmatrix}$$

Recently Augot et al. in [4] propose a fast algorithm which yields $k \times k$ square matrices whose k^{th} power of its companion matrices are MDS matrices. They obtain recursive MDS matrices by using shortened BCH codes.

The Link Between Polycyclic Codes and Recursive MDS Matrices

The matrix of a linear transformation of a polycyclic shift with respect to a polynomial $v(x) = v_0 + v_1 x + \ldots + v_{n-1}x^{n-1}$ and the companion matrix of a monic polynomial $x^n + v(x)$ same and as the following:

$$T_v = \begin{pmatrix} 0 & \cdots & \cdots & 0 & v_0 \\ 1 & 0 & \cdots & 0 & v_1 \\ 0 & 1 & & \vdots & \vdots \\ \vdots & & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & v_{n-1} \end{pmatrix}$$

There is an obvious link between polycyclic codes and recursive MDS matrices. Augot et al.'s algorithm already finds the polynomials whose companion matrices are recursive MDS matrices. So we perform an algorithm as explained below:

1. Choose a field F_{2^s} and a code length n.
2. Take a polynomial $v(x)$ of degree $n-1$ form $F_{2^s}[x]$ from the previous algorithm results (Augot's Algorithm).
3. Compute the polycyclic codes with respect to $v(x)$ using the theory we just derive.
4. Decide if the polycyclic codes we obtain MDS code or not.

We run this algorithm by using computer algebra system MAGMA (Bosma, 1997) and we have seen that most of the codes we obtain is indeed MDS. We think it is worth to study on this topic deeper and more theoretical point of view. We present the result in a table.

Table 1: The Number of MDS and non-MDS Codes

s	n	Number of MDS Codes	Number of non-MDS Codes
4	4	256	0
4	6	384	0
5	10	4700	0
5	12	5610	30
6	6	7650	0
6	10	12720	0
6	14	15996	48

References

Ling, S., Xing C. (2004). Coding Theory A First Course: Cambridge University Press.

William W. P., Weldon E. J. Jr. (1972). Error Correcting codes: second edition: MIT Press (1972).

D. Radkova, A.J. Van Zanten (2009). Constacyclic codes as invariant subspaces, Linear Algebra and its Applications, 430, (pp. 855-864).

D. Augot, M. Finiasz. (2014). Direct Construction of Recursive MDS Di_usion Layers Using Shortened BCH Codes. FSE. To appear.

Daemen J., Rijmen V..(2002). The Design of Rijndael. Information Security and Cryptography: Springer.

Junod P., Vaudenay S. (2004). FOX: A new family of block ciphers. In Helena Handschuh and M. Anwar Hasan, editors, Selected Areas in Cryptography, volume 3357 of Lecture Notes in Computer Science, (pp. 114-129): Springer.

Guo J., Peyrin T., Poschmann A., and Matthew J. B. Robshaw. (2011). The LED block cipher. In Bart Preneel and Tsuyoshi Takagi, editors, CHES 2011, volume 6917 of Lecture Notes in Computer Science, (pp. 326-341): Springer.

Bosma W., Cannon J. and Playoust C., (1997.) The Magma algebra system. I. The user language, J. Symbolic Comput., 24, 235-265.

