Publication of Little Lion Scientific R&D, Islamabad PAKISTAN
Journal of Theoretical and Applied Information Technology
15th March 2011. Vol. 25 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CYCLICITY AND DECODING OF LINEAR ERROR-BLOCK CODES

RABII DARITI, EL MAMOUN SOUIDI
Laboratoire Mathématiques informatique et Applications,
Faculty of Science, B.P 1014, RABAT - MOROCCO
E-mail: rabiedariti@yahoo.fr, souidi@fsr.ac.ma

ABSTRACT

Linear error-block codes (LEBC) were introduced in [1]. They are a natural generalization of linear error correcting codes. In this paper, we introduce a notion of cyclic LEBC. In order to allow application in cryptography, especially in a McEliece-like cryptosystem [3], a method of decoding this kind of codes is presented. There exist linear error-block codes with fast decoding algorithms.

Keywords: *Linear error-block codes, Cyclic and quasi-cyclic error-block codes, Decoding linear error-block codes*

1. INTRODUCTION

A composition π of a positive integer n is given by $n = l_1m_1 + l_2m_2 + \dots + l_rm_r$, where $r, l_1, l_2, \dots, l_r, m_1, m_2, \dots, m_r$ are integers ≥ 1, and is denoted

$$\pi = [m_1]^{l_1}[m_2]^{l_2}\dots[m_r]^{l_r}$$

If moreover $m_1 > m_2 > \dots > m_r \geq 1$ then π is called a partition.

Let q be a prime power and F_q be the finite field with q elements. Let $s, n_1, n_2, \dots, n_s$ be the non negative integers given by a partition π as

$$s = l_1 + \dots + l_r,$$

$$n_1 = n_2 = \dots = n_{l_1} = m_1$$

$$n_{l_1+1} = n_{l_1+2} = \dots = n_{l_1+l_2} = m_2$$

□

$$n_{l_1+\dots+l_{r-1}+1} = n_{l_1+\dots+l_{r-1}+2} = \dots = n_s = m_r$$

Let $V_i = F_q^{n_i}$ $(1 \leq i \leq s)$ and $V = V_1 \oplus V_2 \oplus \dots \oplus V_s = F_q^n$. Each vector in V can be written uniquely as $v = (v_1,\dots,v_s)$, $v_i \in V_i$ $(1 \leq i \leq s)$. For any $u = (u_1,\dots,u_s)$ and $v = (v_1,\dots,v_s)$ in V, the π-weight $w_\pi(u)$ of u and the π-distance $d_\pi(u, v)$ of u and v are defined by

$$w_\pi(u) = \#\{i / 1 \leq i \leq s, u_i \neq 0 \in V_i\} \text{ and}$$

$$d_\pi(u, v) = w_\pi(u - v) = \#\{i / 1 \leq i \leq s, u_i \neq v_i\}.$$

An F_q-linear subspace C of V is called an $[n, k, d]_q$ linear error-block code over F_q of type π, where $k = dim_{F_q}(C)$ and $d = d_\pi(C)$ is the minimum π-distance of C, which is defined as

$$d = min\{d_\pi(c, c')/c, c' \in C, c \neq c'\}$$
$$= min\{w_\pi(c)/0 \neq c \in C\}.$$

A classical linear error correcting code is a linear error-block code of type $\pi = [1]^n$.

A linear error-block code with a composition type is equivalent to some linear error-block code with a partition type.

Some algebraic aspects and fields of application of linear error-block codes are given in [1], and in its concluding section, a few open problems are stated. Answering some of those problems, new constructions and bounds are given in [2].

Application in cryptography is an interesting extension of coding theory. In 1978, Robert J. McEliece found [3] a reliable approach to apply linear error correcting codes in a cryptographic scheme. His idea still resists cryptanalysis until today. This paper is devoted to generalize, to the error-block case, properties of classical error correcting codes that allow or improve their application in cryptography. For instance, notions of cyclic and quasi-cyclic linear error-block codes are introduced. The advantage of these codes is that they are presentable by less information than usual. We also introduce a method for decoding linear error-block codes inspired from the standard array classical method. Though it is slow and not practical to correct errors rising from transmission throw a binary noisy channel, this method allows

Publication of Little Lion Scientific R&D, Islamabad PAKISTAN
Journal of Theoretical and Applied Information Technology
15th March 2011. Vol. 25 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

application in a McEliece-like cryptosystem. Nevertheless, we take advantage of classical codes with fast decoding algorithms to construct families of linear error-block codes which also admit a fast decoding algorithm.

This paper is organized as follows. In Section 2 we give definitions and results concerning cyclic and quasi-cyclic LEBC. In Section 3 we introduce a decoding method for LEBC which aims to allow an application in cryptography. Construction of error-block codes with fast decoding algorithms is evoked in Section 4. Perspective of this work is given in Section 5.

2. CYCLIC AND QUASI-CYCLIC LEBC

In literature, a cyclic code is a code that is invariant by a cyclic shift. That means that if the values of a codeword in each coordinate are shifted to the next coordinate, they produce another codeword of the same code. In the error-block case, and except partitions of the form $\pi = [m]^s$, the coordinates are presented by blocks with different sizes. Thus, the cyclicity of an error-block code is first of all predicted by the form of its partition. It must allow that by some cyclic shift, the sizes of the coordinates still unchanged.

Definition 1 Let π be a composition of an integer n of the form

$$\begin{aligned}\pi &= ([n_1][n_2]\dots[n_j])^l \\ &= \underbrace{[n_1][n_2]\dots[n_j]\,[n_1][n_2]\dots[n_j]\dots[n_1][n_2]\dots[n_j]}_{l \text{ times}}\end{aligned}$$

where j is the minimum integer verifying this form.

Note $V_j = \oplus_{i=1}^{j} V_i$. Each vector a $\in V$ can be written uniquely as $a=(a_1,a_2,\dots, a_l)$, $a_i \in V_j$ $(i=1,\dots,l)$.

An $[n, k, d]$ code C of type π is π-cyclic if for each a $\in C$ we have $\sigma_\pi(a) \in C$ where

$$\begin{aligned}\sigma_\pi : \underbrace{V_j \oplus \dots \oplus V_j}_{l \text{ times}} &\to \underbrace{V_j \oplus \dots \oplus V_j}_{l \text{ times}} \\ (\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_l) &\mapsto (\mathbf{a}_l, \mathbf{a}_1, \dots, \mathbf{a}_{l-1})\end{aligned}$$

σ_π is a cyclic shift of j blocks (and also of $\sum_{i=1}^{j} n_i$ bits) to the right.

Definition 2 An $[n, k, d]$ code C of type π is π-quasi-cyclic of order r if for each a $\in C$ we have $\sigma_\pi^r(a) \in C$.

Example 1 $\pi = ([2][1])^2$, $C = \{000000, 010110, 110010, 100100\}$. C is a $[6, 2, 2]$ π-cyclic code.

The next remarks are straightforward consequences of Definition 1 and Definition 2.

Remark 1 A π-cyclic error-block code is a π-quasi-cyclic code of order $r = 1$.

Remark 2 If C is a π-cyclic error-block code of $s = l_j$ blocks where j is as given in Definition 1 and l is a positive integer, then C is also π-quasi-cyclic of order r for any r which divides l.

Remark 3 If $\pi = [1]^n$ then the classical definitions are found by setting $n_i = 1$ $(i = 1,\dots,s)$, $j = 1$ and $l = s = n$.

Therefore, all the results on classical quasi-cyclic codes can be generalized to the error-block case.

Theorem 1 Each $[n,k]$ π-quasi-cyclic error-block code C is generated by a matrix of the form

$$\begin{bmatrix} A_1 & A_2 & \cdots & A_l \\ A_l & A_1 & \cdots & A_{l-1} \\ \vdots & \vdots & & \vdots \\ A_2 & A_3 & \cdots & A_1 \end{bmatrix}$$

where A_i $(i = 1,\dots,l)$ are $(\frac{k'}{l} \times j)$ matrices over F_q with $k' \geq k$ and l divides k'.

Proof The theorem is proved, like in the classical case [4], by recursion. We start by a null $(1 \times n)$ matrix G_0. We choose a random word $c = (c_1, c_2, \dots, c_s)$ of C. Then c is split into $l = s_j$ equal parts: $(c_1, c_2, \dots, c_j)$, $(c_{j+1}, c_{j+2}, \dots, c_{2j})$, $\dots$, $(c_{s-j+1}, c_{s-j+2}, \dots, c_s)$. We note

$$A_i^1 = (c_{(i-1)j+1}, c_{(i-1)j+2}, \dots, c_{ij}),$$

for $1 \leq i \leq l$, and we construct the matrix G_1 by cyclic shifts of the matrices A_i^1 :

$$G^1 = \begin{bmatrix} A_1^1 & A_2^1 & \cdots & A_l^1 \\ A_l^1 & A_1^1 & \cdots & A_{l-1}^1 \\ \vdots & \vdots & & \vdots \\ A_2^1 & A_3^1 & \cdots & A_1^1 \end{bmatrix}$$

The code generated by G_1 is either included in C or contains it. In the second case we set $G = G_1$ and the result is found, else we choose another codeword c_2 that does not belong to the code generated by G_1. We split it again into j equal parts and add them as rows to the matrices A_i^1 to obtain matrices A_i^2 :

Publication of Little Lion Scientific R&D, Islamabad PAKISTAN
Journal of Theoretical and Applied Information Technology
15th March 2011. Vol. 25 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$A_i^2 = \begin{pmatrix} c_{(i-1)j+1}, c_{(i-1)j+2}, \ldots, c_{ij} \\ c^2_{(i-1)j+1}, c^2_{(i-1)j+2}, \ldots, c^2_{ij} \end{pmatrix}$$

We repeat the same process to construct matrices G_2, G_3 and so on. Since the rank of the matrix constructed in each iteration increases, it will stop when the number of its rows k' becomes $\geq k$. The matrix then generates the code C.

Remark 4 The previous form of the generating matrix implies that it is sufficient to know the matrices $A_1, A_2, \ldots, A_l$ to derive the whole matrix G.

Remark 5 The matrix G generates the code C but is not necessarily a generator matrix of C since k' may be greater than k.

Remark 6 A quasi-cyclic code C of type π is equivalent to a code C' of type π' where π' is a permutation of the form $\pi' = [n_1]^l \ldots [n_j]^l$. Moreover, there exist a generating matrix of C' for which each l consecutive column blocks of the same size n_i define a quasi-cyclic matrix of order n_i $(i = 1,\ldots,j)$.

3. DECODING ERROR-BLOCK CODES

Let C be an $[n, k, d]_q$ code of type π. Assume that a word $x \in V$ is received. Decoding x consists of finding $c \in C$ such that

$$d_\pi(x, c) = \min_{a \in C} d_\pi(x, a).$$

The error vector $e = x - c$ must be of minimum π-weight. The block-support of a vector $x \in F_q^n$ is defined by

$$Supp_\pi(x) = \{i / 1 \leq i \leq s, 0 \neq x_i \in V_i\}$$

If $d = 2l + 1$ then the balls

$$B_\pi(c, l) = \{v \in V / d_\pi(c, v) \leq l\}$$

for $c \in C$, are pairwise disjoint. Therefore they are forming a partition of V. Hence, if a codeword c is sent and x is received with l or fewer swapped blocks, then c is the unique codeword closest to x.

If $d = 2l \geq 2$ then the sets

$$B'_\pi(c, l) = \{v \in B_\pi(c, l) / \sharp\{Supp_\pi(c - v) \cap \{2, 3, \ldots, s\}\} \leq l - 1\}$$

for $c \in C$, are pairwise disjoint. Therefore they are forming a partition of V. Note that

$$B'_\pi(c, l) = B_\pi(c, l - 1) \cup \{v \in V / d_\pi(c, v) = l \text{ and } c_1 \neq v_1\}$$

where c_1 and v_1 denote the first block of c and v respectively. Hence, if a codeword c is sent and x is received with $l - 1$ or fewer swapped blocks, then c is the unique codeword closest to x. If x has exactly l swapped blocks, then c is the unique codeword closest to x verifying $c_1 \neq x_1$.

Thus, decoding a received word x consists of finding $c \in C$ such that:

- $d_\pi(x, c) \leq l$ if $d = 2l + 1$,
- $d_\pi(x, c) \leq l - 1$, or, $d_\pi(x, c) \leq l$ and $x_1 \neq c_1$ if $d = 2l \geq 2$.

A standard table can be constructed to decode a linear error-block code up to l error blocks even if the minimum π-distance is not known. Coset leaders are words of minimum π-weight; if two words have the same π-weight we choose the one that have a non zero first block.

4. LINEAR ERROR-BLOCK CODES WITH FAST DECODING ALGORITHM

Lemma 1 Let q be a prime power, $l \geq 1$ be an integer and $(\alpha_1, \alpha_2, \ldots, \alpha_l)$ be a basis of the finite field F_{q^m}. Each vector c in F_{q^m} is written $c = c_1\alpha_1 + c_2\alpha_2 + \ldots + c_m\alpha_m$ where $c_i \in F_q$, $i = 1, 2, \ldots, m$. It is known that the mapping

$$\begin{aligned} \varphi : \mathbb{F}_{q^m} &\rightarrow \mathbb{F}_q^m \\ c &\mapsto (c_1, c_2, \ldots c_m) \end{aligned}$$

is an isomorphism. Therefore, an $[l, k, d]_{q^m}$ classical error correcting code (sub-space of $\oplus_{i=1}^{l} \mathbb{F}_{q^m}$) is identified to an $[lm, km, d]_q$ linear error-block code of type $\pi = [m]^l$ (sub-space of $\oplus_{i=1}^{l} \mathbb{F}_q^m$).

This lemma implies that every q-ary error-block code with type $[m]^l$ can be decoded with the same algorithm of some q^m-ary classical error correcting code of length l. Thus, classical codes with fast decoding algorithm yield error-block codes with fast decoding algorithm with type $[m]^l$. Furthermore, we can combine these codes to construct error-block codes of different types with a fast decoding algorithm.

Example 2 (Catenation) Let $s \geq 1$ be a positive integer, and for $i = 1, 2, \ldots, s$ let C_i be an $[l_i, k_i, d_i]_{q^{m_i}}$ classical error correcting code admitting a fast decoding algorithm (GRS for example). Note $k_{max} = max(k_i)$ and G_i the generator matrix of the code C_i. Let C be the linear error-block code of generator matrix

$$G = [G'_1 G'_2 \ldots G'_s]$$

where G_i' is G_i with $k_{max} - k_i$ rows of zeros attached.

Publication of Little Lion Scientific R&D, Islamabad PAKISTAN
Journal of Theoretical and Applied Information Technology
15th March 2011. Vol. 25 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The code C has length $n = \sum_{i=1}^{s} l_i m_i$, dimension $k = k_{max} \sum_{i=1}^{s} m_i$, minimum distance $d \geq min_{i=1,...,s}(d_i)$ and is of type $\pi = [n_1]^{l_1} [n_2]^{l_2} ... [n_s]^{l_s}$. As codewords of C have the form $c = (c_1,c_2,...,c_s)$, it can be decoded block by block using the decoding algorithms of the initial codes.

Example 3 (Cartesian product) We conserve the notation of the previous example. Define the error-block code C by

$$C = C_1 \oplus C_2 \oplus ... \oplus C_s$$

$$= \{(c_1,c_2,...,c_s) / c_i \in C_i, i=1, 2,...,s\}$$

This is a $[\sum_{i=1}^{s} n_i, \sum_{i=1}^{s} k_i, \min_{i=1,2,...,s} d_i]_q$ code of type $\pi = [n_1]^{l_1} [n_2]^{l_2} ... [n_s]^{l_s}$ that is decoded by a similar technique.

5. CONCLUSION AND PERSPECTIVE

By this work, we aim to construct error-block codes with cryptographical properties. Quasi-cyclic codes are useful as they can be presented by just some lines of the generator matrix instead of the whole matrix. However we gave linear error-block codes with fast decoding algorithms, more properties are needed to claim to find codes to use in cryptography. Namely, there must be a way to hide their structure so that they look like random codes. An idea is to look for a generalization of Goppa codes. Their structure is hidden when they are permuted, and they are the best classical codes known to be used in the McEliece public key cryptosystem.

REFRENCES:

[1] K. Feng, L. Xu, F.J. Hickernell, "Linear error-block codes", *Finite Fields Appl,* Vol. 12, 2006, pp. 638-652.

[2] S. Ling, F. Ozbudak, "Constructions and bounds on linear error-block codes", *Designs, Codes and Cryptography*. Vol. 45, 2007, pp. 297-316.

[3] R.J. McEliece, "A public-key cryptosystem based on algebraic coding theory". *DSN Progress Report*. 1978, pp. 114-116.

[3] P. Gaborit, "Shorter keys for code based cryptography". *Proceedings of Workshop on Codes and Cryptography*, Bergen, 2005, pp. 81-90.

[3] J.H. van Lint, "Introduction to coding theory", third edition. *Graduate Texts in Mathematics*, Vol. 86, Springer, Berlin, 1999.