Liet. matem. rink., T. 43, spec. nr., 75–78

On the concatenated structure of quasi-cyclic codes

Gintaras SKERSYS
e-mail: gintaras.skersys@maf.vu.lt

Introduction

The algebric structure of quasi-cyclic codes has been studied using a module structure over an infinite ring [1], Gröbner bases [2], the discrete Fourier transform and chain rings [3, 4]. In this paper, we study the algebraic structure of quasi-cyclic codes using concatenated codes. We show that every quasi-cyclic code can be expressed as a concatenation of an inner linear code and an outer $\mathbf{F}_q$-cyclic code (i.e., $\mathbf{F}_q$-linear code over $\mathbf{F}_{q^m}$ invariant under cyclic shift) and we study their properties.

1. Preliminaries

See [5, 8] for more details on error-correcting codes.

Let q be a power of a prime number, let m be a positive integer. Let's denote $\mathbf{F}_{q^m}$ the finite field of cardinality q^m.

Let $\mathbf{F}$ be any finite field, and let $\mathbf{K}$ be its subfield. Let n be a positive integer. A *code of length n over* $\mathbf{F}$ is a non-empty subset of the vector space $\mathbf{F}^n$. The vectors of a code are called *codewords*. If a code over $\mathbf{F}$ is a linear space over $\mathbf{K}$, it is called $\mathbf{K}$-*linear*. $\mathbf{F}$-linear code over $\mathbf{F}$ is called simply *linear*. If a linear code is of length n and of dimension k it will be said that it is a $[n, k]$ linear code. A $\mathbf{K}$-linear code C over $\mathbf{F}$ is called $\mathbf{K}$-*cyclic* if any cyclic shift of a codeword is also a codeword, i.e., whenever $(c_0, c_1, \ldots, c_{n-1})$ is in C then so is $(c_{n-1}, c_0, \ldots, c_{n-2})$. A $\mathbf{F}$-cyclic code over $\mathbf{F}$ is called simply *cyclic*. A linear code C is called *quasi-cyclic* if there is some integer s such that every cyclic shift of a codeword by s places is again a codeword. The smallest such s is called the *index* of C. The index of C divides the length of C.

Let C be a code of length n over $\mathbf{F}$, let $J = \{j_1, j_2, \ldots, j_t\}$ be a subset of the index set $\{0, 1, \ldots, n-1\}$. Then the code C *restricted to* J is the code

$$C|_J = \{(c_{j_1}, c_{j_2}, \ldots, c_{j_t}) \mid (c_1, c_2, \ldots, c_n) \in C\}.$$

If C is linear, $C|_J$ is linear too. Let C be a $[n, k]$ linear code over $\mathbf{F}$. A set J of cardinality k is called an *information set* of C if $C|_J = \mathbf{F}^k$, i.e., if we get all possible vectors of length k.

Let B be a $[n_B, k_B]$ linear code over $\mathbf{F}_q$. Then B and $\mathbf{F}_{q^{k_B}}$ are isomorphic as linear spaces over $\mathbf{F}_q$. Let $\theta : \mathbf{F}_{q^{k_B}} \to B$ be an isomorphism. θ allows to replace any element of

$\mathbf{F}_{q^{k_B}}$ by a codeword of B, and vice versa. Let n_E be a positive integer. Define a $\mathbf{F}_q$-linear application Θ by

$$\begin{array}{rccl} \Theta: & \mathbf{F}_{q^{k_B}}^{n_E} & \longrightarrow & B^{n_E} \\ & x = (x_1, \ldots, x_{n_E}) & \longmapsto & \Theta(x) = \left(\theta\left(x_1\right), \ldots, \theta\left(x_{n_E}\right)\right), \end{array} \tag{1}$$

where $\Theta(x)$ may be considered as a vector of length $n_B n_E$ made from the coordinates of vectors $\theta\left(x_1\right)$, $\theta\left(x_2\right)$, etc., in that order. Let E be a $\mathbf{F}_q$-linear code of length n_E over $\mathbf{F}_{q^{k_B}}$. The *concatenated code* of B and E is the code C composed of the codewords of E in which the elements of $\mathbf{F}_{q^{k_B}}$ are replaced by the codewords of B by means of θ, i.e., $C = \Theta(E) = \{\Theta(x) \mid x \in E\}$. The codes B and E are called respectively the *inner* and *outer* codes of C. We will denote $C = B\square_\theta E$. It is evident that C is a $[n_B n_E, k]$ linear code over $\mathbf{F}_q$ where k is the dimension of E as a vector space over $\mathbf{F}_q$. The concatenated codes were extensively studied by Sendrier [6, 7].

2. The concatenated structure of quasi-cyclic codes

Let C be a $[n, k]$ quasi-cyclic code of index n_B over $\mathbf{F}_q$. We know that n_B divides n. Denote $n_E = n/n_B$. Let

$$J_i = \{in_B, in_B + 1, in_B + 2, \ldots, (i+1)n_B - 1\}, \quad 0 \leqslant i \leqslant n_E - 1.$$

$\{J_i\}_{0 \leqslant i \leqslant n_E - 1}$ is a partition of $\{0, 1, \ldots, n-1\}$. Denote

$$B_i = C|_{J_i}, \quad 0 \leqslant i \leqslant n_E - 1,$$

the code C restricted to J_i. The codes B_i are linear. Using the fact that C is quasi-cyclic, we prove the following property:

PROPOSITION 1. $B_i = B_j \quad \forall\, 0 \leqslant i, j \leqslant n_E - 1.$

Since all B_i are equal, we will denote them by B, i.e.,

$$B = B_0. \tag{2}$$

Let k_B be the dimension of B.

Let $\theta : \mathbf{F}_{q^{k_B}} \to B$ be a $\mathbf{F}_q$-linear isomorphism. Let Θ be defined by (1). Then

$$\begin{array}{rccl} \Theta^{-1}: & B^{n_E} & \longrightarrow & \mathbf{F}_{q^{k_B}}^{n_E} \\ & x = (x_1, \ldots, x_{n_E}) & \longmapsto & \Theta^{-1}(x) = \left(\theta^{-1}\left(x_1\right), \ldots, \theta^{-1}\left(x_{n_E}\right)\right), \end{array}$$

where $x_i \in B \ \forall\, 0 \leqslant i \leqslant n_E - 1$, is a $\mathbf{F}_q$-linear isomorphism too. Let

$$E = \Theta^{-1}(C). \tag{3}$$

Then we have:

PROPOSITION 2. E is a $\mathbf{F}_q$-cyclic code over $\mathbf{F}_{q^{k_B}}$ of length n_E. The dimension of E as a vector space over $\mathbf{F}_q$ is k, the dimension of C.

From the definition of concatenated code we get:

Theorem 1. *Any quasi-cyclic code C can be expressed as a concatenated code of B and E, i.e., $C = B\Box_\theta E$, where B and E are defined respectively by* (2) *and* (3)*, and $\theta : \mathbf{F}_{q^{k_B}} \to B$ is any $\mathbf{F}_q$-linear isomorphism, where k_B is the dimension of B. Conversely, if B is a $[n_B, k_B]$ linear code over $\mathbf{F}_q$, E is a $\mathbf{F}_q$-cyclic code over $\mathbf{F}_{q^{k_B}}$ of length n_E, $\theta : \mathbf{F}_{q^{k_B}} \to B$ is any $\mathbf{F}_q$-linear isomorphism, then $C = B\Box_\theta E = \Theta(E)$ is a $[n_B n_E, k]$ quasi-cyclic code of index n_B, where Θ is defined by* (1)*, and k is the dimension of E as a vector space over $\mathbf{F}_q$.*

3. The study of restricted codes

The proofs of the results of this section are rather technical and are omitted for lack of space. They will be given in the extended version of this paper.

Let C be a $[n, k]$ quasi-cyclic code of index n_B over $\mathbf{F}_q$. Denote $n_E = n/n_B$. Let

$$I_i = \{i, n_B + i, 2n_B + i, \ldots, (n_E - 1)\, n_B + i\}, \quad 0 \leqslant i \leqslant n_B - 1.$$

$\{I_i\}_{0 \leqslant i \leqslant n_B - 1}$ is a partition of $\{0, 1, \ldots, n-1\}$. Denote

$$C_i = C|_{I_i}, \quad 0 \leqslant i \leqslant n_B - 1,$$

the code C restricted to I_i. The codes C_i are linear. Using the fact that C is quasi-cyclic, we prove the following property:

PROPOSITION 3. C_i is a cyclic code for all $0 \leqslant i \leqslant n_B - 1$.

Let B and E be defined respectively by (2) and (3), and let $\theta : \mathbf{F}_{q^{k_B}} \to B$ be a $\mathbf{F}_q$-linear isomorphism, where k_B is the dimension of B. The *support* of a code A is the set of coordinates where at least one codeword of A is nonzero. If $A_1, A_2, \ldots, A_t$ are codes of the same length over the same finite field, then the code $\sum_{i=1}^t A_i$ is defined by

$$\sum_{i=1}^{t} A_i = \Big\{ \sum_{i=1}^{t} a_i \mid a_i \in A_i \ \forall i \Big\}.$$

We study the properties of C_i.

PROPOSITION 4.

- If i does not belong to the support of B, then $C_i = \{0\}$, where 0 is the zero vector.
- Let J be an information set of B. Then $C_i \subset \sum_{j \in J} C_j$ for all $0 \leqslant i \leqslant n_B - 1$.

We know that the outer code E is a $\mathbf{F}_q$-linear code over $\mathbf{F}_{q^{k_B}}$. When E is linear, i.e., satisfies a stronger condition, we can say more.

PROPOSITION 5. Let E be linear. Then $C_i = C_j$ for all $0 \leqslant i, j \leqslant n_B - 1$ belonging to the support of B.

The linearity of the outer code E is not a necessary condition to have $C_i = C_j$ for all $0 \leqslant i, j \leqslant n_B - 1$ belonging to the support of B, because there are some instances where this is satisfied with E only $\mathbf{F}_q$-linear.

When E is linear, we can say even more. Let B be a $[n_B, k_B]$ linear code over $\mathbf{F}_q$, let E be a $\mathbf{F}_q$-cyclic code over $\mathbf{F}_{q^{k_B}}$ of length n_E, let $\theta', \theta'' : \mathbf{F}_{q^{k_B}} \to B$ be $\mathbf{F}_q$-linear isomorphisms, denote $C' = B\Box_{\theta'}E$, $C'' = B\Box_{\theta''}E$, $C'_i = C'|_{I_i}$, $C''_i = C''|_{I_i}$ for all $0 \leqslant i \leqslant n_B - 1$.

PROPOSITION 6. Let E be linear. Then $C'_i = C''_j$ for all $0 \leqslant i, j \leqslant n_B - 1$ belonging to the support of B.

Acknowledgment

Author wishes to thank T. Berger and N. Sendrier for many valuable suggestions.

References

[1] J. Conan, C. Séguin, Structural properties and enumeration of quasi-cyclic codes, *AAECC*, **4**, 25–39 (1993).

[2] K. Lally, P. Fitzpatrick, Algebraic structure of quasi-cyclic codes, *Discrete Applied Mathematics*, **111**(1–2), 157–175 (2001).

[3] S. Ling, P. Solé, Decomposing quasi-cyclic codes, in: *Proceedings of WCC'2001*, D. Augot and C. Carlet (Eds.), INRIA, Paris (2001), pp. 507–517.

[4] S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes I: Finite fields, *IEEE Trans. Inform. Theory*, **47**, 2751–2760 (2001).

[5] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North–Holland, Amsterdam (1978).

[6] N. Sendrier, *Codes correcteurs d'erreurs à haut pouvoir de correction*, PhD Thesis, Université Paris VI (1991).

[7] N. Sendrier, On the concatenated structure of a linear code, *AAECC*, **9**(3), 221–242 (1998).

[8] G. Skersys, Computing permutation groups of error-correcting codes, *Liet. matem. rink.* **40**(spec. nr), 320–328 (2000).

Ryšys tarp kvaziciklinių ir sankabos kodų

G. Skersys

Parodome, kad kiekvienas kvaziciklinis kodas gali būti išreikštas kaip vidinio tiesinio kodo ir išorinio $\mathbf{F}_q$-ciklinio kodo sankabos kodas, tiriame jų savybes.