Liet. matem. rink., **44**, *spec. nr.*, 2004, 101–104

On quasi-cyclic codes and traces of codes

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

Introduction

In [6] we show that any quasi-cyclic code C can be expressed as a concatenated code, we study the properties of the inner, outer and restricted codes of C. In this paper we continue to study the concatenated structure of quasi-cyclic codes. We show that there exists the relationship between restricted codes of C and the trace of the outer code of C.

The trace mapping allows to get a code over a small field from a code over a big field. This mapping is useful in the study of so-called subfield subcodes (see [1]). We show that it also plays a part in the study of quasi-cyclic codes.

In order to present our main results (see Section 3), we give some definitions and recall some results from [6].

1. Preliminaries

See [2,5] for more details on error-correcting codes.

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*. A $\mathbf{F}$-linear code over $\mathbf{F}$ is called simply *linear*. A linear code of length n and of dimension k will be denoted by $[n,k]$. 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, i.e., whenever $(c_0, c_1, \ldots, c_{n-1})$ is in C then so is $(c_{n-s}, c_{n-s+1}, \ldots, c_{n-1}, c_0, \ldots, c_{n-s-1})$. 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, 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

$$C|_J = \left\{ \left(c_{j_1}, c_{j_2}, \ldots, c_{j_t}\right) \,\middle|\, \left(c_0, c_1, \ldots, c_{n-1}\right) \in C \right\}.$$

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. The *support* of a code C is the set of coordinates where at least one codeword of C 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

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

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 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 θ: $\mathbf{F}_{q^{k_B}} \to B$ 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

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

where $\Theta(x)$ is a vector of length $n_B n_E$ made from the coordinates of vectors $\theta(x_1)$, $\theta(x_2)$, 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 [3,4].

2. The concatenated structure of quasi-cyclic codes

Let C be a $[n, k]$ quasi-cyclic code over $\mathbf{F}_q$. Denote n_B the index of C. 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. From [6] we have that $B_i = B_j$ for all $0 \leqslant i, j \leqslant n_E - 1$. 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 θ: $\mathbf{F}_{q^{k_B}} \to B$ be a $\mathbf{F}_q$-linear isomorphism. Let Θ be defined by (1). Then

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

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

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

From [6] we have that E is a $\mathbf{F}_q$-linear code over $\mathbf{F}_{q^{k_B}}$ of length n_E. Moreover (see [6]) any quasi-cyclic code C can be expressed as a concatenated code of B and E, i.e., $C = B\square_\theta E$, where B and E are defined respectively by (2) and (3), and θ: $\mathbf{F}_{q^{k_B}} \to B$ is any $\mathbf{F}_q$-linear isomorphism, where k_B is the dimension of B.

3. Restricted codes and trace of outer code

In this section we present our new results. 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.

The sum

$$\mathbf{T}_q(x) = x + x^q + x^{q^2} + x^{q^3} + \cdots + x^{q^{m-1}} = \sum_{i=0}^{m-1} x^{q^i}$$

is called the *trace* of $x \in \mathbf{F}_{q^m}$. It can be shown that $\mathbf{T}_q(x) \in \mathbf{F}_q$.

If A is a code over $\mathbf{F}_{q^m}$, let's denote

$$\mathbf{T}_q(A) = \left\{ \left(\mathbf{T}_q(c_0), \mathbf{T}_q(c_1), \ldots, \mathbf{T}_q(c_{n-1})\right) \mid (c_0, c_1, \ldots, c_{n-1}) \in A \right\}.$$

Then $\mathbf{T}_q(A)$ is a code over $\mathbf{F}_q$. If A is a $\mathbf{F}_q$-linear code, $\mathbf{T}_q(A)$ is a linear code.

Let C, B, E be as in Section 2. Let

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

$\{I_i\}_{0 \leqslant i \leqslant n_B - 1}$ 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.

THEOREM 1. *Let J be an information set of B. Then*

$$\mathbf{T}_q(E) \subset \sum_{j \in J} C_j.$$

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., verifies a stronger condition, we can say more.

THEOREM 2. *Let E be linear. Then $\mathbf{T}_q(E) = C_i$ for all i, $0 \leqslant i \leqslant n_B - 1$, belonging to the support of B.*

Even if E is not linear, there can exist i, $0 \leqslant i \leqslant n_B - 1$, such that $\mathbf{T}_q(E) = C_i$.

Acknowledgment

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

References

1. P. Delsarte, On subfield subcodes of Reed-Solomon codes, *IEEE Trans. Inform. Theory*, **21**, 575–576 (1975).
2. F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam (1978).
3. N. Sendrier, *Codes Correcteurs d'Erreurs à Haut Pouvoir de Correction*, PhD Thesis, Université Paris VI (1991).
4. N. Sendrier, On the concatenated structure of a linear code, *AAECC*, **9**(3), 221–242 (1998).
5. G. Skersys, Computing permutation groups of error-correcting codes, *Liet. matem. rink.*, **40** (spec. issue), 320–328 (2000).
6. G. Skersys, On the concatenated structure of quasi-cyclic codes, *Liet. matem. rink.*, **43** (spec. issue), 75–78 (2003).

REZIUMĖ

G. Skersys. Ryšys tarp kvaziciklinių kodų ir sankabos kodų pėdsakų

Parodome, koks egzistuoja ryšys tarp kvaziciklinio kodo, apriboto tam tikra aibe, ir jo išorinio kodo pėdsako.