Some notes on the theory of fuzzy code

K. P. Shum.

(Dept. of Math., The Chinese University of Hong Kong, Hong Kong, P.R.China)

Chen De Gang

(Dept. of Math, Harbin Institute of Technology, Harbin, 150001, P.R.China)

Abstract: In this paper, the fuzzy linear code is defined by using of the theory of fuzzy linear space and the method of decode is also given. At last, the fundamental properties of fuzzy cyclic code are studied.

Keywords: Fuzzy linear space; Fuzzy linear code; Fuzzy cyclic code.

1. *Introduction*

When we study a subject, we always encode its information and decode the received information, this is what the classical code theory deal with, and the information which we handle are certain. To those uncertain information, the classical code theory has less method. Since the fuzzy mathematics has well application when deal with the fuzziness, we try to use the method of fuzzy mathematics to conduct the fuzzy information.

We assume that information is coded using an alphabet Q with q distinct symbols. A code A is called a *block code* if the coded information can be divided into blocks of n symbols which can be decoded independently. These blocks are the codewords and n is called the block length of word length. Here every codeword is certain. If the information from the information channel is uncertain, then the ordinary method of coding can not deal with it. For instance, for an information α we can not make it sure whether the subject we study have this information α, we only can estimate the degree is 0.6 which it possess the information α. Such we can make a corresponding to a number 0.6 in [0,1]. If for every information there is such a number corresponding to it, then we can get a fuzzy set A on the block code, we call it the fuzzy code.

In this paper, we mainly define the fuzzy linear code and the fuzzy cyclic code on the binary symmetric channel and study its basic properties.

2.*Preliminaries*

Definition 2.1 [1]. Let V_n be a n dim linear space on a number field K, A a fuzzy subset on V_n. If for any $x,y \in V_n$, $\alpha \in K$, we have

i) $A(x+y) \geq \min\{A(x), A(y)\}$;

ii) $A(\alpha x) \geq A(x)$,

then we call A the fuzzy linear subspace of V_n on K.

Lemma 2.2. [1] A is the fuzzy linear subspace if for any $\alpha \in [0,1]$, if $A_\alpha \neq \Phi$, A_α is a linear subspace of V_n.

Lemma 2.3 [1] A is a fuzzy linear subspace if and only if for any $\alpha, \beta \in K$, $x,y \in V_n$, we have $A(\alpha x+\beta y) \geq \min\{A(x),A(y)\}$.

Definition 2.4 Let A be a fuzzy subset on FG which is the group algebra of $\langle x \rangle$ on the finite field GF(q). If for any $a(x),b(x) \in FG$, we have

$A(a(x).b(y)) \geq \max\{A(a(x)),A(b(x))\}$;

$A(a(x)-b(y)) \geq \min\{A(a(x)),A(b(x))\}$;

then we call A is a fuzzy ideal of FG.

Lemma 2.5 A is a fuzzy ideal of FG if and only if for any $\alpha \in [0,1]$, if $A_\alpha \neq \Phi$, A_α is an ideal of FG.

3. *Fuzzy linear code*

In case of the length of this paper, we omit the fundamentul preliminalies of the coding theory which can be indexed in [2,3]

Definition 3.1 Let GF(2) be a binary symmetric channel, then the fuzzy linear subspace A of V_n is called a fuzzy linear code where V_n is the n dim linear spcace on GF(2).

Proposition 3.2 A is a fuzzy linear code iff for any $\alpha \in [0,1]$, if $A_\alpha \neq \phi$, then A_α is a linear code

Since V_n is a finite set, we know Im(A)=$\{A(x);x \in V_n\}$ is finite. Assume there are *m* elements in Im(A): $\alpha_1 > \alpha_1 > \cdots > \alpha_m$, by Proposition 3.2 we know m≤n. Let the generator matrix of A_{α_k} is G_{α_k}, then A can be determined by m-1 matrixes $G_{\alpha_1}, G_{\alpha_2}, \ldots, G_{\alpha_{m-1}}$ and G_{α_i} is the submatrixes of G_{α_j}, $i<j$.

Following we discuss the decode of fuzzy linear code. When we sent the information by the channel, not only the information can be set wrong, but also the membership of the information to the fuzzy linear code can also be sent wrong. The purpose of decode is to translate both the information and the membership clearly and certainly. For an information α, firstly we must find out the tangible linear code it may belong to by its possible membership, then we decode it by the original method. Since the kinds of error of membership are so many that it certainly has many method to deal with it. Here we give a basic method by assuming A(x)≥A*(y), here x is the information from the information source; A(x) is the membership of x to the fuzzy linear code A; y is the received information and A*(y) is the received membership.

1) Let α=A*(y), then we can get the tangible linear subspace A_α;

2) Let A_α be the linear code, then use the decoding method in [3] to decode y.

4. *Fuzzy cyclic code*

Let GF(*q*) be a finite field which has *q* elements, V_n be a *n*-dim vector space on GF(*q*), then V_n is isomorphic to the group algebra FG of <x> on GF(*q*). Following we express the vectors in V_n by these two structurce of V_n and we always assume (*n*,*q*)=1.

Definition 4.1 A fuzzy linear subspace A of V_n is called a fuzzy cyclic code if for any $(a_0, a_1, \ldots, a_{n-1}) \in V_n$, we have $A((a_{n-1}, a_0, \ldots, a_{n-2})) \geq A((a_0, a_1, \ldots, a_{n-1}))$.

Proposition 4.1 A is a fuzzy cyclic code iff for any $\alpha \in [0,1]$,. if $A_\alpha \neq \phi$, then A_α is a cyclic code.

Proof $\Rightarrow$ Let A be a fuzzy cyclic code, for any $\alpha \in [0,1]$, if $A_\alpha \neq \phi$, then for any $(a_0, a_1, \ldots, a_{n-1}) \in A_\alpha$, we know $A((a_0, a_1, \ldots, a_{n-1})) \geqslant \alpha$, hence $(a_{n-1}, a_0, \ldots, a_{n-2}) \in A_\alpha$.

$\Leftarrow$ For any $\alpha \in [0,1]$ $A_\alpha \neq \phi$ and A_α is a cyclic code. If there exist $(a_0, a_1, \ldots, a_{n-1}) \in V_n$ such that $A((a_{n-1}, a_0, \ldots, a_{n-2})) < A((a_0, a_1, \ldots, a_{n-1}))$. Let $\lambda = A((a_0, a_1, \ldots, a_{n-1}))$, then $(a_0, a_1, \ldots, a_{n-1}) \in A_\lambda$, hence $A_\lambda \neq \phi$, A_λ is a cyclic code, but $(a_{n-1}, a_0, \ldots, a_{n-2}) \notin A_\lambda$, this is a contradiction.

Propostion 4.3 A is a fuzzy cyclic code of V_n iff for any $(a_0, a_1, \ldots, a_{n-1}) \in V_n$, we have $A((a_0, \ldots, a_{n-1})) = A((a_{n-1}, a_0, \ldots, a_{n-2})) = \cdots = A((a_1, a_2, \ldots, a_{n-1}, a_0))$.

Proof: $\Leftarrow$ by Definition 4.1 it is clear.

$\Rightarrow$ if A is a fuzzy cyclic code, then .

$A((a_0, a_1, \ldots, a_{n-1})) \leqslant A((a_{n-1}, a_0, \ldots, a_{n-2})) \leqslant \cdots \leqslant A((a_1, a_2, \ldots, a_{n-1}, a_0)) \leqslant A((a_0, a_1, \ldots, a_{n-1}))$.

Theorem 4.4 A is a fuzzy cyclic code iff A is a fuzzy ideal of the group algebra FG.

Proof $\Leftarrow$ Let A be a fuzzy ideal, then for any $(a_0, a_1, \ldots, a_{n-1}) \in V_n$, we have $A(a_{n-1}+a_0x+\ldots+a_{n-2}x^{n-1}) = A(x(a_0+a_1x+\ldots+a_{n-1}x^{n-1})) \geqslant \max\{A(x), A(a_0+a_1x+\ldots+a_{n-1}x^{n-1})\}$, that is to say A is a fuzzy cyclic code.

$\Rightarrow$ Let A be a fuzzy cyclic code. For any $a(x)$, $b(x) \in V_n$, since A is a fuzzy linear subspace, we have $A(a(x)-b(x)) \geqslant \min\{A(a(x)), A(b(x))\}$. If $a(x) \in V_n$, then $A(xa(x)) \geqslant A(a(x))$, $A(x^2(a(x))) \geqslant A(a(x))$, $A(x^3a(x)) \geqslant A(a(x))$, so for any $p(x) = p_0+p_1x+p_{n-1}x^{n-1} \in V_n$, we have $A(p(x)a(x)) = A(p_0a(x)+\ldots+p_nx^{n-1}a(x)) \geqslant A(a(x))$, hence A is a fuzzy ideal of FG.

Since GF(g) is a finite field, then Im(A) is finite. Let Im(A)= $\{\alpha_1 > \alpha_2 > \cdots > \alpha_k\}$, then we have $A_{\alpha_1} \subseteq A_{\alpha_2} \subseteq \cdots \subseteq A_{\alpha_{k-1}} \subseteq A_{\alpha_k} = V_n$. Let $g_i(x)$ be the generator polynomial of A_{α_i}, then $g_i(x) | g_{i+1}(x)$. On the contrary, we have.

Theorem 4.5 Let g=(g_1(x), g_2(x),..., g_k(x)), $g_i(x) | g_{i+1}(x)$, i=1,..., k-1, then g can determined a fuzzy cyclic code A, and $\{(g_i(x)): i=1, \ldots, k\}$ is the family of level cyclic subcodes of A.

Proof Let A_i=(g_i(x)), then $A_i \subseteq A_{i+1}$, i=1,2,...,k-1. Take $\alpha_i \in [0,1]$, satisfying $\alpha_1 > \alpha_2 > \cdots > \alpha_k$,

Let

$$A(x) = \begin{cases} \alpha_1, x \in (g_1(x)); \\ \alpha_i, x \in (g_i(x)) - (g_{i-1}(x)); \\ 0, x \in V_n - (g_k(x)); \end{cases}$$

then A is the fuzzy cyclic code we need.

Therem 4.6 Let A_1 and A_2 be two fuzzy cyclic code, then $A_1 \bigcap A_2$ is a fuzzy cyclic code.

Theorm 4.7 Let A_1,A_2 be two fuzzy cyclic code, then A_1+A_2 is a fuzzy cyclic code.

Proof: For any $(a_0, a_1, \ldots, a_{n-1}) \in V_n$, we have

$(A_1+A_2)(x)(a_{n-1},a_0,\ldots,a_{n-2})$

$=\max \min\{A_1((b_{n-1},b_n,\ldots,b_{n-2})), A_2((c_{n-1},c_0,\ldots,c_{n-2}))\}$

$b_i+c_i=a_i$, i=1,...,n-1.

$\geq \max \min\{A_1((b_0,b_1,\ldots,b_{n-1})), A_2((c_0,c_1,\ldots,c_{n-1}))\}$

$b_i+c_i=a_i$, i=1,...,n-1.

$=(A_1+A_2)((a_0,a_1,\ldots,a_{n-1}))$

Remark The theory of fuzzy code is more complex then the original one. The above content is the most basic work about the fuzzy code. In our another papers we will study the encode and decode of fuzzy code which have a lot of difference to the original coding theory.

References

[1] S.Nanda, Fuzzy fields and fuzzy linear spaces, FSS, 191(1986)89-94.

[2] J.H.Van Lint, Introduction to coding Theory, springer-Vereag (1981).

[3] Berlekamp E.R, Algebraic Coding Theory, McGraw-Hill Book Compny, 1968.