Note

Indecomposability of cyclic codes

Yoshimi Kashiwagi\(^a\)*, Isao Kikumasa\(^b\)

\(^a\)Department of Mathematics, Faculty of Liberal Arts, Yamaguchi University, Yamaguchi, 753 Japan
\(^b\)Department of Mathematical Sciences, Faculty of Science, Yamaguchi University, Yamaguchi, 753 Japan

Received 6 December 1995; revised 19 January 1997; accepted 17 February 1997

Abstract

It is stated in Montpetit (1987) that cyclic codes are indecomposable, but it is not true in general. In this paper we will give a necessary and sufficient condition for a cyclic code to be indecomposable, using its generator polynomial. © 1999 Elsevier Science B.V. All rights reserved

1. Introduction

All codes in this paper are linear block codes over the field GF\(q\) of \(q\) elements. A matrix whose rows form a basis of a code is called a *generator matrix* of the code. If a generator matrix of a code of length \(n\) is in a form \((I_k A)\) where \(I_k\) is the \(k \times k\) identity matrix and \(A\) is a \(k \times (n - k)\) matrix, it is said to be in a *standard form*. Let \(C\) be a code of length \(n\) and \(x = (x_1, \ldots, x_n) \in C\). Then \(\text{supp } x = \{i: x_i \neq 0\}\) is called the *support of \(x\)* and for a subset \(S\) of \(C\) \(\text{supp } S = \bigcup_{x \in S} \text{supp } x\) is called the *support of \(S\)*. A non-zero element of \(C\) which has a minimal support is called an *elementary element*. A code is called *decomposable* if it is a direct sum of two non-zero codes whose supports are disjoint and is called *indecomposable* otherwise. If every cyclic shift of an element of a code \(C\) is in \(C\), \(C\) is called a *cyclic code*. A cyclic code of length \(n\) can be regarded as an ideal of the quotient ring of the polynomial ring in one variable \(x\) by the ideal generated by \(x^n - 1\). A cyclic code can be characterized by its *generator polynomial* (see [1, Ch. 7]).

In this paper we will characterize the indecomposability of a code by its support (Proposition 4) and give a necessary and sufficient condition for a cyclic code to be indecomposable, using its generator polynomial (Theorem 8).

* Corresponding author. E-mail: kashi@po.yb.cc.yamaguchi-u.ac.jp.

0012-365X/99/$ - see front matter © 1999 Elsevier Science B.V. All rights reserved
PII: S0012-365X(98)00180-0
2. The main result

We define equivalence relations on the support of a code, which are suggested by Proposition 4 of [3].

**Definition 1.** Let C be a code and \( \Gamma \) be a subset of C which spans C. Two elements \( i \) and \( j \) of \( \text{supp} \ C \) are called \( \Gamma \)-equivalent, denoted by \( i \sim \Gamma j \), if there exist \( x_1, x_2, \ldots, x_m \) in \( \Gamma \) such that \( i \in \text{supp} \ x_1, j \in \text{supp} \ x_m \) and \( \text{supp} \ x_\ell \cap \text{supp} \ x_{\ell+1} \neq \emptyset \) for \( \ell = 1, 2, \ldots, m - 1 \).

It is easy to see that the \( \Gamma \)-equivalence is an equivalence relation on \( \text{supp} \ C \). The number of \( \Gamma \)-equivalence classes is denoted by \( |\text{supp} \ C/\sim \Gamma| \).

**Lemma 2.** Let C be a code and \( \Gamma \) be a subset of C which spans C. If C is indecomposable, then \( |\text{supp} \ C/\sim \Gamma| = 1 \).

**Proof.** Assume that \( |\text{supp} \ C/\sim \Gamma| \geq 2 \). Then we have \( \text{supp} \ C = S_1 \cup S_2 \), where \( S_i \) is a union of equivalence classes \( (i = 1, 2) \) and \( S_1 \cap S_2 = \emptyset \). Let \( x \in \Gamma \). Since two elements of \( \text{supp} \ x \) are \( \Gamma \)-equivalent, we have that \( \text{supp} \ x \subset S_1 \) or \( \text{supp} \ x \subset S_2 \). Put \( \Gamma_i = \{ x \in \Gamma: \text{supp} \ x \subset S_i \}(i = 1, 2) \). Then \( \Gamma = \Gamma_1 \cup \Gamma_2 \) and \( \text{supp} \ \Gamma_1 \cap \text{supp} \ \Gamma_2 = \emptyset \). Assume that \( \text{supp} \ \Gamma_1 = \emptyset \). Then \( \text{supp} \ \Gamma \subset S_2 \). Since \( \Gamma \) spans C, \( \text{supp} \ \Gamma = \text{supp} \ C \) and so \( \text{supp} \ C \subset S_2 \). This is a contradiction. Hence \( \text{supp} \ \Gamma_1 \neq \emptyset \). In the same way we have \( \text{supp} \ \Gamma_2 \neq \emptyset \). This means the decomposability of C. \( \square \)

**Remark 3.** Let \( C = \text{GF}(2)^2 \) and \( \Gamma = \{(1,0), (1,1)\} \). It is easy to see that \( |\text{supp} \ C/\sim \Gamma| = 1 \) and C is decomposable. Hence the converse of Lemma 2 does not hold in general.

By Lemma 2 and [3, Proposition 4] we have the following

**Proposition 4.** Let C be a code and \( \Gamma \) be a subset of C which spans C and consists of elementary elements. Then C is indecomposable if and only if \( |\text{supp} \ C/\sim \Gamma| = 1 \).

It follows by [3, Proposition 3] that the set of elementary elements of C is an example of \( \Gamma \) in Proposition 4. The following proposition gives another example of \( \Gamma \) as well as another proof for [3, Proposition 3].

For a row reduced echelon matrix see [2, p. 135].

**Proposition 5.** Row vectors of a generator matrix of a code in a row reduced echelon form are elementary.

**Proof.** We may assume that the generator matrix in a row reduced echelon form is in a standard form. Let C be a code with a generator matrix in a standard form, \( k = \dim \ C \) and \( x_i \) be the \( i \)th row vector of its generator matrix in a standard form
Let $u = \sum_{j=1}^{k} a_j x_j$ (where $a_j \in \text{GF}(q)$) with $\emptyset \neq \text{supp} u \subset \text{supp} x_i$. Since the only non-zero component in the first $k$ components of $u$ is the $i$th component, $u = a_i x_i$. Hence $\text{supp} u = \text{supp} x_i$. This means that $x_i$ is elementary.

From now on we will consider only cyclic codes and their codewords will be expressed by polynomials.

**Lemma 6.** Every cyclic shift of the generator polynomial of a cyclic code is elementary.

**Proof.** Let $g(x)$ be the generator polynomial and $u(x)$ be a codeword such that $\emptyset \neq \text{supp} u(x) \subset \text{supp} g(x)$. Since $\deg u(x) \leq \deg g(x)$ and $g(x)$ divides $u(x)$, there exists $a \in \text{GF}(q) \setminus \{0\}$ such that $u(x) = ag(x)$. Hence $\text{supp} u(x) = \text{supp} g(x)$ and so $g(x)$ is elementary. It is easy to see that every cyclic shift of $g(x)$ is elementary.

**Lemma 7.** Let $n$ and $l$ be positive integers and $f(x)$ be a polynomial over $\text{GF}(q)$. If $f(x^l)$ divides $x^n - 1$, then $l$ divides $n$.

**Proof.** By direct calculation.

**Theorem 8.** Let $C$ be a non-trivial code and $g(x) = \sum_{i=0}^{m} a_i x^e_i$ be the generator polynomial of $C$, where $a_i \in \text{GF}(q) \setminus \{0\}$ (i = 0, 1, ..., m) and $0 = e_0 < e_1 < \cdots < e_m$. Then $C$ is indecomposable if and only if $(e_1, \ldots, e_m)$ is the greatest common divisor for the $e_j$ (j = 1, ..., m).

**Proof.** Let $n$ be the length of $C$ and $d = (e_1, \ldots, e_m)$. We will show that $C$ is a direct sum of $d$ non-zero indecomposable subcodes. Since $C$ is a non-zero cyclic code, we may regard $\text{supp} C = \{0, 1, \ldots, n - 1\}$ as the residue group of integers modulo $n$. In this way integers can be considered elements of $\text{supp} C$. We note that $d$ divides $n$ by Lemma 7. For $s = 0, 1, \ldots, d - 1$ let $R_s$ be the set of integers whose residues modulo $d$ are $s$. $\Gamma_s = \{x^i g(x) : l \in R_s\}$ and $C_s$ be the subspace of $C$ spanned by $\Gamma_s$. Then $\text{supp} C = \bigcup_{s=0}^{d-1} R_s$, which is a disjoint union. Since $g(x)$ is the generator polynomial of $C$, we have $C = \bigcup_{s=0}^{d-1} C_s$. If $l \in R_s$, then $\text{supp} x^l g(x) \subset R_s$, since $\text{supp} x^l g(x) = \{l, l + e_1, \ldots, l + e_m\}$ and $d = (e_1, \ldots, e_m)$. Hence $\text{supp} C_s \subset R_s$ and so $\bigcup_{s=0}^{d-1} C_s$ is a direct sum. If we show that $C_s$ is indecomposable, the proof will be completed. First we note that $\text{supp} C_s = \text{supp} \Gamma_s = R_s$ and $s + Ze_1 + \cdots + Ze_m = s + Zd = R_s$. Let $l \in R_s$ and $i = 1, \ldots, m$. Then $l, l + e_i \in \text{supp} x^l g(x)$ and $l - e_i, l \in \text{supp} x^{l-e_i} g(x)$. Hence $(l - e_i, l) \sim (l, l)$. Thus two elements of $s + Ze_1 + \cdots + Ze_m$ are $\Gamma_s$-equivalent and so $|\text{supp} C_s/\sim| = 1$. It follows from Proposition 4 that $C_s$ is indecomposable.

**Corollary 9.** Let $C$ be a cyclic code and $g(x)$ be its generator polynomial. Then $C$ is decomposable if and only if $g(x)$ is a polynomial of $x^l$ for some $l \geq 2$. 
By this corollary it is easy to find a cyclic code which is decomposable. The cyclic
code of length 9 with generator polynomial $x^3 + 1$ over GF(2) is one of such examples.

**Corollary 10.** (1) A non-trivial cyclic code of prime length is indecomposable.

(2) A cyclic code whose dimension and length are relatively prime is indecomposable.

**Proof.** (1) By Corollary 9 and Lemma 7.

(2) Let $C$ be a cyclic code of length $n$ and $g(x)$ be its generator polynomial. Assume
that $C$ is decomposable. Then there exists an integer $l$ such that $l \geq 2$ and $l$ divides
both $n$ and $\deg g(x)$. Noting that $\dim C = n - \deg g(x)$, we have that $l$ is a common
divisor of $n$ and $\dim C$. This is a contradiction. \(\Box\)

**Example 11.** Let $C$ be the cyclic code of length 15 with generator polynomial
$x^5 + x^4 + x^2 + 1$ over GF(2). Then $C$ is indecomposable by Theorem 8. Since
$\dim C = 10$, we have that the dimension and the length of $C$ have a non-trivial common
divisor. This shows that the converse of (2) in Corollary 10 is not true in general.

**References**


