A Relation Between the Characteristic Generators of a Linear Code and its Dual

Haibin Kan, *Member, IEEE,* and Hong Shen

***Abstract*—It was conjectured by Koetter and Vardy that if the k characteristic generators of a linear code C are linearly independent, then the corresponding $n - k$ characteristic generators of the dual code $C^{\perp}$ are also linearly independent. In this correspondence, we prove that the conjecture is true for self-dual codes and cyclic codes.**

***Index Terms*—Characteristic generators, characteristic matrices, conventional trellises, cyclic codes, tailbiting trellises.**

I. Introduction

Trellis representations of linear block codes not only illustrate code structure, but also often lead to efficient trellis-based decoding algorithms. For any linear block code, there exists a unique, up to isomorphism, minimal conventional trellis. Furthermore, we can efficiently construct the minimal conventional trellis for any linear code from its generator matrix or parity-check matrix by several methods, such as Bahl–Cocke–Jelinek–Raviv (BCJR), Massey, Forney, and Kschischang–Sorokine constructions [7]. Hence, the theory on conventional trellis is well developed. However, much less is known about tailbiting trellises. Many examples show that the complexity of tailbiting trellis can be much lower than the complexity of the best possible conventional trellis. Thus, people try to find the minimal tailbiting trellises for some special codes ([1], [6]). Recently, Koetter and Vardy discussed the general theory on tailbiting trellises in [2] and [3]. They proved that any linear tailbiting trellis for a linear code could be constructed as a product of some elementary tailbiting trellises. So to construct the minimal linear tailbiting trellis for a linear code is reduced to searching the minimal linear tailbiting trellis among the product trellises of some elementary trellises. It was proved in [3] that any minimal linear tailbiting trellis for a linear code C can be constructed from its characteristic generators, and that the sum of span matrices of C and its dual $C^{\perp}$ is the constant matrix whose elements are all one. It was also conjectured that if the k characteristic generators of C are linearly independent then the corresponding $n - k$ characteristic generators of $C^{\perp}$ are linearly independent as well.

In this correspondence, we prove the conjecture in [3] is true for self-dual codes and cyclic codes. Section II introduces some preliminaries and background. Section III presents our main result on cyclic codes.

II. Preliminaries

We first introduce some basic notions on tailbiting trellises for block codes, which we borrow from [2] and [3]. For more details, the readers can refer to the two references.

An edge-labeled directed graph is a triple (V, E, A), consisting of a set V of vertices, a finite set A called the alphabet, and a set E of ordered triples (v, a, v'), with $v, v' \in V$ and $a \in A$, called edges. We say that an edge (v, a, v') begins at v, and ends at v', and has label a. We only give the definition of a tailbiting trellis, and omit the definition of a conventional trellis, which is similar to the definition of a tailbiting trellis.

Definition 1: A tailbiting trellis $T = (V, E, A)$ of depth n is an edge-labeled directed graph with the following property: the vertex set V can be partitioned as

$$V = V_0 \cup V_1 \cup \cdots \cup V_{n-1} \tag{1}$$

such that every edge in T begins at a vertex of V_i and ends at a vertex of V_{i+1}, for some $i = 0, 1, \ldots, n-2$, or begins at a vertex of V_{n-1} and ends at a vertex of V_0. The set E of edges is partitioned in a natural way as $E = E_0 \cup E_1 \cup \cdots \cup E_{n-1}$, where E_i is the set of all edges beginning at a vertex of V_i. The sets $V_0, V_1, \ldots, V_{n-1}$ are called the vertex class of T. The ordered index set $I = \{0, 1, \ldots, n-1\}$ induced by the partition in (1) is called the time axis for T. The ordered sequence $\Theta(T) = (|V_0|, |V_1|, \ldots, |V_{n-1}|)$ is called the state profile of T.

A cycle of length n in a tailbiting trellis T is a closed path in T through n distinct vertices. Clearly, any cycle in T contains exactly one vertex in each vertex class. A tailbiting trellis T is reduced if any vertex and edge belong to at least one cycle. The set of edge labels along a cycle in T is an n-tuple $(a_0, a_1, \ldots, a_{n-1})$ over the label alphabet A. Postulating that all cycles in T start at a vertex of V_0, every cycle defines a vector $(a_0, a_1, \ldots, a_{n-1}) \in A^n$, which is called an edge-label sequence in T. Let $C(T)$ denote the the set of all edge-label sequences in T. Then $C(T)$ is called the edge-label **code** of T. T is a tailbiting trellis for the block code C over A if $C(T) = C$.

If every vertex in each vertex class V_i, $0 \le i \le n-1$, is labeled by a sequence of length ι_i over A, where $\iota_i \ge \lceil \log_{|A|} |V_i| \rceil$, then this kind of trellis is called a labeled trellis. Here, we require all vertex labels within the same vertex class are distinct. Let $\iota = \iota_0 + \iota_1 + \cdots + \iota_{n-1}$. Then every cycle Γ in a labeled tailbiting defines an ordered sequence of length $n + \iota$ over A, consisting of the labels of edges and vertices in Γ. We refer to such a sequence as a label sequence in T. Let $S(T)$ denote the set of all such label sequences. $S(T)$ is called the label code of T.

For tailbiting trellises $T = (V, E, A)$ and $T' = (V', E', A')$, if

$$\Theta(T) \le \Theta(T'), i.e., |V_i| \le |V_i'| \text{ for all } 0 \le i \le n-1 \tag{2}$$

we say that T is smaller than T' under $\preceq_{\Theta}$, and denote it by $T \preceq_{\Theta} T'$, where $V = V_0 \cup V_1 \cup \cdots \cup V_{n-1}$, $V' = V_0' \cup V_1' \cup \cdots \cup V_{n-1}'$. If, moreover, equality does not hold in (2) for at least one i, we say that T is strictly smaller than T' and write it by $T \prec_{\Theta} T'$. T is a minimal tailbiting trellis for a block code C if there is no a tailbiting trellis T' for C such that $T \prec_{\Theta} T'$.

All above notions for conventional trellises can be defined in completely similar way. Henceforth, trellis means "conventional trellis" or "tailbiting trellis" when there is no adjective "conventional" or "tailbiting" in front of it. We always assume that the alphabet set A is a finite field F_q. A labeled trellis $T = (V, E, F_q)$ is linear over F_q if T is reduced and $S(T)$ is a linear code over F_q. An unlabeled trellis T is said to be linear if there exists a vertex labeling of T such that the resulting labeled trellis is linear.

For $i, j \in I = \{0, 1, \ldots, n-1\}$, define closed cyclic interval $[i, j]$ as follows:

$$[i, j] = \begin{cases} \{i, i+1, \ldots, j\}, & \text{if } i \le j \\ \{i, i+1, \ldots, n-1, 0, \ldots j\}, & \text{if } i > j. \end{cases}$$

We also define the semi-open cyclic interval $(i, j]$ as $[i, j] \setminus \{i\}$.

Manuscript received September 19, 2003; revised October 26, 2004. This work was supported by the National Science Foundation of China under Grants 60003007 and 60472038 and by the Japan Society for Promotion of Science (JSPS) under Research Grant 14380139.

H. Kan is with the Department of Computer Science and Engineering, Fudan University, Shanghai, China and with the Graduate School and Information Science, Japan Advanced Institute of Science and Technology, Ishikawa, 923-1292, Japan (e-mail: haibin@jaist.ac.jp).

H. Shen is with Graduate School and Information Science, Japan Advanced Institute of Science and Technology, Ishikawa, 923-1292, Japan (e-mail: shen@jaist.ac.jp).

Communicated by A. E. Ashikhmin, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2004.842740

Let C be any linear code with length n over the finite field F_q, i.e., $C \subseteq F_q^n$. For a nonzero element $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, a cyclic interval $(i, j]$ is called a span of c if $[i, j]$ contains all nonzero elements of c, and denoted by $[c] = (i, j]$. Clearly, c can have different spans. Let $\triangleleft(c)$ denote the smallest integer i such that $c_i \neq 0$, and let $\triangleright(c)$ the largest integer j such that $c_j \neq 0$. Obviously, $[\triangleleft(c), \triangleright(c)]$ contains all nonzero elements of c. We call $(\triangleleft(c), \triangleright(c)]$ the atomic span of c. Given $c = (c_0, c_1, \ldots, c_{n-1})$ and its span $[c] = (i, j]$, the corresponding elementary labeled trellis T_c can be easily constructed [3]. A basis $X = \{x_1, x_2, \ldots, x_k\}$ for C is said to be in minimal span form if $\triangleleft(x_1), \triangleleft(x_2), \ldots, \triangleleft(x_k)$ are distinct and $\triangleright(x_1), \triangleright(x_2), \ldots, \triangleright(x_k)$ are distinct. Kschischang and Sorokine [5] proved that $T = T_{x_1} \times T_{x_2} \times \cdots \times T_{x_k}$ is a minimal conventional trellis for C if and only if the basis $\{x_1, x_2, \ldots, x_k\}$ is in minimal span form. For convenience of notations, we impose a lexicographic order on the set of vectors in F_q^n. Though bases for C in minimal form are not unique, the lexicographically first basis for C in minimal span form is unique.

For $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, define

$$\sigma_i(c) = (c_i, \ldots, c_{n-1}, c_0, \ldots, c_{i-1})$$

i.e., σ_i is a map of cyclic shift to the left i times. So

$$\sigma_i(C) = \{(c_i, \ldots, c_{n-1}, c_0, \ldots, c_{i-1}) | (c_0, c_1, \ldots, c_{n-1}) \in C\},$$

Similarly, for $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, define

$$\rho_i(c) = (c_{n-i}, \ldots, c_{n-1}, c_0, c_1, \ldots, c_{n-i-1})$$

i.e., cyclic shift to the right i times.

A characteristic generator for C is a pair consisting of a codeword $(x_0, x_1, \ldots, x_{n-1}) \in C$ and its span $[x] = (a, b]$ such that x_a and x_b are nonzero. The set of all the characteristic generators for C is given by

$$\begin{aligned} X &= X_0 \cup X_1 \cup \cdots \cup X_{n-1} \\ &= X_0^* \cup \rho_1(X_1^*) \cup \cdots \cup \rho_{n-1}(X_{n-1}^*) \end{aligned} \tag{3}$$

with the understanding that $[x] = (\triangleleft(x^*) + j, \triangleright(x^*) + j]$ for each $x \in X_j$, where X_i^* is the lexicographically first basis for $\sigma_i(C)$ in minimal span form, and $x^* = \sigma_j(x)$. The characteristic matrix for C is the matrix having the elements of X as its rows. It is easy to verify that there exists at most one different element between $\rho_i(X_i^*)$ and $\rho_{i+1}(X_{i+1}^*)$ for $i = 0, 1, \ldots, n-2$. Let

$$\chi(C) = \{i | \text{there exists } (x_0, x_1, \ldots, x_{n-1}) \in C \text{ such that } x_i \neq 0\}$$

and call $\chi(C)$ the support set of C. It was proven that $|X| = |\chi(C)|$ in [3]. Without loss of generality, we assume $|\chi(C)| = n$. Thus, the characteristic matrix is an $n \times n$ matrix. Koetter and Vardy [3] showed that the spans of any two generators in X start at distinct positions and end at distinct positions, and that any minimal linear trellis for the code C with dimension k can be constructed as the product of k elementary trellises from the n characteristic generators of C.

There is close relation between the characteristic generators of C and that of $C^\perp$, the dual of C. Let X and $X^\perp$ be the sets of characteristic generators of C and $C^\perp$, respectively. Let φ be a map from X to $X^\perp$ defined as follows:

$$\varphi : (x, [x]) \mapsto (x', [x']) \tag{4}$$

where $[x] = (i, j]$ and $[x'] = (j, i]$ for some $i, j \in \{0, 1, \ldots, n-1\}$. Since characteristic generators start at different positions and also end at different positions, φ is a one-to-one correspondence from X to $X^\perp$. For convenience, we write

$$X = \{(x_1, [x_1]), (x_2, [x_2]), \ldots, (x_n, [x_n])\}$$

and let $(y_i, [y_i]) = \varphi((x_i, [x_i]))$ for $1 \leq i \leq n$. Then

$$X^\perp = \{(y_1, [y_1]), (y_2, [y_2]), \ldots, (y_n, [y_n])\}.$$

For any permutation $(i_1, i_2, \ldots, i_n)$ of $(0, 1, \ldots, n-1)$, k characteristic generators $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$ of C, and $n-k$ characteristic generators $y_{i_{k+1}}, y_{i_{k+2}}, \ldots, y_{i_n}$ of $C^\perp$, it was proved [3] that the trellises $T = T_{x_1} \times T_{x_2} \times \cdots \times T_{x_k}$ and $T' = T_{y_{k+1}} \times T_{y_{k+2}} \times \cdots \times T_{y_n}$ have the same state complexity profile. Koetter and Vardy conjectured that if $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$ are linearly independent characteristic generators of C, then corresponding $n-k$ characteristic generators $y_{i_{k+1}}, y_{i_{k+2}}, \ldots, y_{i_n}$ of $C^\perp$ are also linearly independent. We call it Koetter–Vardy conjecture on characteristic generators, or simply, *Koetter–Vardy conjecture*.

III. A Relation Between Characteristic Matrices of a Linear Code and its Dual

In this section, we prove that Koetter–Vardy conjecture on characteristic generators [3] is true for cyclic codes and self-dual codes. All the linear codes in the sequel are over the finite field F_q

It is easy to prove that *Koetter–Vardy conjecture* is true for self-dual codes. A linear code C is self-dual if $C = C^\perp$, i.e., the generator matrix of C is the same as the parity-check matrix of C.

Theorem 1: Koetter–Vardy conjecture is true for self-dual codes.

Proof: Let C be a self-dual code with length n and dimension k. Let X and $X^\perp$ be the sets of characteristic generators of C and $C^\perp$, respectively. Since C is self-dual, $n = 2k$ and $X = X^\perp$. Let $X = X^\perp = \{x_1, x_2, \ldots, x_n\}$. For any k linearly independent characteristic generators $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$ of C, since $X = X^\perp$, $\{x_{i_1}, x_{i_2}, \ldots, x_{i_k}\}$ corresponds to the remaining k characteristic generators of $X^\perp$ under the map φ in (4). Therefore, *Koetter–Vardyb conjecture* is true for self-dual codes. □

However, it is by no means trivial to prove *Koetter–Vardy conjecture* is true for cyclic codes. A linear code of length n is cyclic if it has the following property: if $(c_0, c_1, \ldots, c_{n-1}) \in C$, then $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$. In other words, let

$$C \subseteq \left\{ \sum_{i=0}^{n-1} c_i x^i | c_i \in F_q, 0 \leq i \leq n-1 \right\}.$$

Then C is a cyclic code if and only if C is an ideal of the quotient ring $R_n = F_q[x]/\langle x^n - 1 \rangle$. Since R_n is a principal ideal ring, the cyclic code C with dimension k has a generator $g(x)$ with degree $n-k$ and $g(x) | (x^n - 1)$. Denote $C = \langle g(x) \rangle$. Let $x^n - 1 = g(x)h(x), h'(x) = x^k h(x^{-1})$, and $g'(x) = x^{n-k} g(x^{-1})$. Then $1 - x^n = g'(x)h'(x)$ and $C^\perp = \langle h'(x) \rangle$.

For any element $u(x)g(x) \in C$, we always view $u(x)g(x)$ as $u(x)g(x) \mod (x^n - 1)$. For the span $(i, j]$ of a element in C, if $i \geq n$ or $j \geq n$, then we always view $(i, j]$ as $(i \mod n, j \mod n]$. For example, $(2n-5, n+3] = (n-5, 3]$.

Lemma 2: Let $C = \langle g(x) \rangle$ be a cyclic code of dimension k, where $g(x) = \sum_{i=0}^{n-k} g_i x^i$ and $g(x) | (x^n - 1)$. Then the set of characteristic generators of C is

$$\{(x^i g(x), (i, n-k+i]) | i = 0, 1, \ldots, n-1\}.$$

Proof: Clearly, $\{g(x), xg(x), \ldots, x^{k-1} g(x)\}$ are the lexicographically first basis for C in minimal span form. Since C is cyclic, $C = \sigma_i(C)$, where σ_i is the cyclic shift to the left i times, $i = 0, 1, \ldots, n-1$. So $\{g(x), xg(x), \ldots, x^{k-1} g(x)\}$ is also the lexicographically first basis for $\sigma_i(C)$ in minimal span form. Let ρ_i be the cyclic shift to the right i times. Obviously

$$\begin{aligned} &\rho_i(\{g(x), xg(x), \ldots, x^{k-1} g(x)\}) \\ &\qquad = \{x^i g(x), x^{i+1} g(x), \ldots, x^{i+k-1} g(x)\}. \end{aligned}$$

Since $g(x)|(x^n-1)$ and $\deg(g(x))=n-k$, the span of $x^ig(x)$ is $(i,n-k+i]$. Therefore, the set of characteristic generators of C is $\{(x^ig(x),(i,n-k+i])|i=0,1,\ldots,n-1\}$. □

Therefore, the characteristic matrix of C is

$$\begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & \cdots & 0 \\ & & \ddots & & & & \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \\ g_{n-k} & 0 & \cdots & 0 & g_0 & \cdots & g_{n-k-1} \\ & & & & \ddots & & \\ g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 & g_0 \end{pmatrix}.$$

Corollary 3: Let $C=\langle g(x)\rangle$ be a cyclic code of dimension k, and $x^n-1=g(x)h(x)$. Then the set of characteristic generators of $C^\perp$ is $\{(x^ih'(x),(i,k+i])|i=0,1,\ldots,n-1\}$, where $h'(x)=x^kh(x^{-1})$.

Lemma 4: Let $C=\langle g(x)\rangle$ be a cyclic code of dimension k and $x^n-1=g(x)h(x)$. For $0\le i_1<i_2<\cdots<i_k\le n-1$, the k characteristic generators $x^{i_1}g(x),x^{i_2}g(x),\ldots,x^{i_k}g(x)$ are linearly dependent if and only if there exist no all-zero $\alpha_1,\alpha_2,\ldots,\alpha_k\in F_q$ such that $h(x)|(\alpha_1x^{i_1}+\alpha_2x^{i_2}+\cdots+\alpha_kx^{i_k})$.

Proof: Clearly

$$\alpha_1x^{i_1}g(x)+\alpha_2x^{i_2}g(x)+\cdots+\alpha_kx^{i_k}g(x)=0$$

in C if and only if

$$(x^n-1)|(\alpha_1x^{i_1}g(x)+\alpha_2x^{i_2}g(x)+\cdots+\alpha_kx^{i_k}g(x)).$$

Since $x^n-1=g(x)h(x)$,

$$(x^n-1)|(\alpha_1x^{i_1}g(x)+\alpha_2x^{i_2}g(x)+\cdots+\alpha_kx^{i_k}g(x))$$

if and only if

$$h(x)|(\alpha_1x^{i_1}+\alpha_2x^{i_2}+\cdots+\alpha_kx^{i_k}).$$ □

By Lemma 2 and Corollary 3, the sets of characteristic generators of C and $C^\perp$ are

$$\{(x^ig(x),(i,n-k+i])|i=0,1,\ldots,n-1\}$$

and

$$\{(x^ih'(x),(i,k+i])|i=0,1,\ldots,n-1\}$$

respectively. Let φ be the map defined in (4). Then

$$\varphi(x^ig(x))=x^{n-k+i}h'(x),\qquad \text{for } i=0,1,\ldots,n-1.$$

The following lemma is crucial.

Lemma 5: Let $C=\langle g(x)\rangle$ be a cyclic code with dimension k over the field F_q and $x^n-1=g(x)h(x)$. Assume that the greatest common divisor of n and q is 1, i.e., $\gcd(n,q)=1$. Let $g'(x)=x^{n-k}g(x^{-1})$ and $h'(x)=x^kh(x^{-1})$. Let $(i_1,i_2,\ldots,i_n)$ be a permutation of $(0,1,\ldots,n-1)$. Then $x^{i_1}g(x),x^{i_2}g(x),\ldots,x^{i_k}g(x)$ are linearly independent characteristic generators of C if and only if $x^{i_{k+1}}h'(x),x^{i_{k+2}}h'(x),\ldots,x^{i_n}h'(x)$ are linearly independent characteristic generators of $C^\perp$.

Proof: By Lemma 4, $x^{i_1}g(x),x^{i_2}g(x),\ldots,x^{i_k}g(x)$ are linearly dependent if and only if there exist no all-zero $\alpha_1,\alpha_2,\ldots,\alpha_k\in F_q$ such that $h(x)|(\alpha_1x^{i_1}+\alpha_2x^{i_2}+\cdots+\alpha_kx^{i_k})$. Let $\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_k$ be the roots of $h(x)$ in the splitting field F' of $x^n-1=0$ over F_q. Since $\gcd(n,q)=1$, F' is a separable extension field of F_q. So, $x^{i_1}g(x),x^{i_2}g(x),\ldots,x^{i_k}g(x)$ are linearly dependent if and only if the matrix

$$A=\begin{pmatrix} \varepsilon_1^{i_1} & \varepsilon_1^{i_2} & \cdots & \varepsilon_1^{i_k} \\ \varepsilon_2^{i_1} & \varepsilon_2^{i_2} & \cdots & \varepsilon_2^{i_k} \\ \cdots & \cdots & \cdots & \cdots \\ \varepsilon_k^{i_1} & \varepsilon_k^{i_2} & \cdots & \varepsilon_k^{i_k} \end{pmatrix}$$

is singular. Let $\varepsilon_{k+1},\varepsilon_{k+2},\ldots,\varepsilon_n$ be the roots of $g(x)$ in the splitting field F'. Thus, $\varepsilon_{k+1}^{-1},\varepsilon_{k+2}^{-1},\ldots,\varepsilon_n^{-1}$ are the roots of $g'(x)$. Similarly, $x^{i_{k+1}}h'(x),x^{i_{k+2}}h'(x),\ldots,x^{i_n}h'(x)$ are linearly dependent if and only if the matrix

$$D^*=\begin{pmatrix} \varepsilon_{k+1}^{-i_{k+1}} & \varepsilon_{k+1}^{-i_{k+2}} & \cdots & \varepsilon_{k+1}^{-i_n} \\ \varepsilon_{k+2}^{-i_{k+1}} & \varepsilon_{k+2}^{-i_{k+2}} & \cdots & \varepsilon_{k+2}^{-i_n} \\ \cdots & \cdots & \cdots & \cdots \\ \varepsilon_n^{-i_{k+1}} & \varepsilon_n^{-i_{k+2}} & \cdots & \varepsilon_n^{-i_n} \end{pmatrix}$$

is singular. Now we prove that A is invertible iff D^* is invertible. Since $x^n-1=g(x)h(x)$, $\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n$ are all roots of $x^n-1=0$. Let

$$H=\begin{pmatrix} \varepsilon_1^{i_1} & \varepsilon_1^{i_2} & \cdots & \varepsilon_1^{i_n} \\ \varepsilon_2^{i_1} & \varepsilon_2^{i_2} & \cdots & \varepsilon_2^{i_n} \\ \cdots & \cdots & \cdots & \cdots \\ \varepsilon_n^{i_1} & \varepsilon_n^{i_2} & \cdots & \varepsilon_n^{i_n} \end{pmatrix}$$

and

$$H'=\begin{pmatrix} \varepsilon_1^{-i_1} & \varepsilon_2^{-i_1} & \cdots & \varepsilon_n^{-i_1} \\ \varepsilon_1^{-i_2} & \varepsilon_2^{-i_2} & \cdots & \varepsilon_n^{-i_2} \\ \cdots & \cdots & \cdots & \cdots \\ \varepsilon_1^{-i_n} & \varepsilon_2^{-i_n} & \cdots & \varepsilon_n^{-i_n} \end{pmatrix}.$$

For any $1\le i,j\le n$, and $i\ne j$, $\varepsilon_i\varepsilon_j^{-1}$ is a root of $x^n-1=0$ and $\varepsilon_i\varepsilon_j^{-1}\ne 1$. Hence,

$$\sum_{u=0}^{n-1}\left(\varepsilon_i\varepsilon_j^{-1}\right)^u=0.$$

Since $(i_1,i_2,\ldots,i_n)$ is a permutation of $(0,1,\ldots,n-1)$, $H\cdot H'=nI_n$, where I_n is the unit matrix with order n. Set

$$H=\begin{pmatrix} A & B \\ C & D \end{pmatrix}\quad\text{and}\quad H'=\begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix}$$

where A and A' are matrices consisting of the first k rows and k columns of H and H', respectively. Thus,

$$AA'+BC'=nI_k\quad\text{and}\quad AB'+BD'=0$$

where I_k is the $k\times k$ unit matrix. If D' is invertible, then $AB'D'^{-1}+B=0$. So $AB'D'^{-1}C'+BC'=0$. Hence,

$$AB'D'^{-1}C'-AA'=-nI_k$$

and A is invertible. Conversely, assume that A is invertible. Clearly

$$CB'+DD'=nI_{n-k}\quad\text{and}\quad AB'+BD'=0.$$

Since A is invertible, $B'+A^{-1}BD'=0$. Thus, $CB'+CA^{-1}BD'=0$. Hence, $DD'-CA^{-1}BD'=nI_{n-k}$ and D' is invertible. Consequently, A is invertible iff so is D'. Since D' is the transpose matrix of D^*, A is invertible iff so is D^*. Thus, we finish the proof. □

Now we can show *Koetter–Vardy conjecture* is true for cyclic codes. Since 0 is not a root of $x^n-1=0$

$$x^{i_{k+1}}h'(x),x^{i_{k+2}}h'(x),\ldots,x^{i_n}h'(x)$$

are linearly independent characteristic generators of $C^\perp$ if and only if

$$x^{n-k+i_{k+1}}h'(x),x^{n-k+i_{k+2}}h'(x),\ldots,x^{n-k+i_n}h'(x)$$

are also linearly independent characteristic generators of $C^\perp$. Therefore, we conclude the following main result.

Theorem 6: Koetter–Vardy conjecture is true for cyclic codes.

Proof: It follows directly from Theorem 5. □

Example 1: Let $R_6 = F_5[x]/\langle x^6-1\rangle$, $g(x) = x^3-1$ and $h(x) = x^3+1$. So $g'(x) = x^3 g(x^{-1}) = 1-x^3$, and $h'(x) = x^3 h(x^{-1}) = h(x)$. The characteristic matrix of the code $C = \langle g(x)\rangle$ is

$$G = \begin{pmatrix} -1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 \end{pmatrix}$$

and the characteristic matrix of $C^{\perp} = \langle h'(x)\rangle$ is

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

The zeroth, first, and fourth rows of G are linearly dependent, the corresponding second, third, and fifth rows of H are also linearly dependent. This can also be explained by polynomials, i.e., $g(x)$, $xg(x)$, $x^4 g(x)$ are linearly dependent characteristic generators of the cyclic code $C = \langle g(x)\rangle$ and the corresponding characteristic generators $x^2 h'(x)$, $x^3 h'(x)$, $x^5 h'(x)$ of $C^{\perp}$ are also linearly dependent. It is easy to see that the zeroth, first, and fifth rows of G are linearly independent, the corresponding second, third, and fourth rows of H are linearly independent as well.

The preceding simple example shows that there exist k linearly dependent rows and k linearly independent rows of the characteristic matrices for some cyclic codes at the same time. However, for a Reed–Solomon code C with dimension k, any k rows of its characteristic matrix must be linearly independent. Denote by $B_q(n,\delta,\omega,b)$ a q-ary Bose–Chaudhuri–Hocquenghem (BCH) code, whose generator $g(x)$ is the polynomial with minimal degree such that $g(\omega^{b+i}) = 0$ for $i = 0, 1, \ldots, \delta-2$. It is well known that the minimal distance of $B_q(n,\delta,\omega,b)$ is at least δ. If $n = q-1$, then $B_q(n,\delta,\omega,b)$ is called a Reed–Solomon code. The generator of the Reed–Solomon code $B_q(n,\delta,\omega,b)$ is $g(x) = (x-\omega^b)(x-\omega^{b+1})\cdots(x-\omega^{b+\delta-2})$, and so its dimension $k = n-\delta+1$.

Proposition 7: Let $C = B_q(n,\delta,\omega,b)$ be a Reed–Solomon code, where $n = q-1$. Then any k characteristic generators of C are linearly independent, where $k = n-\delta+1$ is the dimension of C.

Proof: Let $g(x)$ be the generator of C, $x^n - 1 = g(x)h(x)$. Since C is a cyclic code, we could assume that $x^{i_1}g(x), x^{i_2}g(x), \ldots, x^{i_k}g(x)$ are any k characteristic generators by Lemma 2, where $0 \le i_1 < i_2 < \cdots < i_k \le n-1$. Since $\omega^b, \omega^{b+1}, \ldots, \omega^{b+\delta-2}$ are the all roots of $g(x)$ and $x^n - 1 = g(x)h(x)$, $\omega^{b+\delta-1}, \omega^{b+\delta}, \ldots, \omega^{n+b-1}$ are the all roots of $h(x)$. Clearly, the matrix

$$\begin{pmatrix} \omega^{i_1(b+\delta-1)} & \omega^{i_2(b+\delta-1)} & \cdots & \omega^{i_k(b+\delta-1)} \\ \omega^{i_1(b+\delta)} & \omega^{i_2(b+\delta)} & \cdots & \omega^{i_k(b+\delta)} \\ \cdots & \cdots & \cdots & \cdots \\ \omega^{i_1(n+b-1)} & \omega^{i_2(n+b-1)} & \cdots & \omega^{i_k(n+b-1)} \end{pmatrix}$$

is invertible since its determinant is a Vandermonde determinant. Therefore, $x^{i_1}g(x), x^{i_2}g(x), \ldots, x^{i_k}g(x)$ are linearly independent characteristic generators. □

ACKNOWLEDGMENT

The authors would like to thank anonymous referees for their careful reading and comments which have improved the clarity of this correspondence. They also would like to acknowledge Prof. A. E. Ashikhmin for his kind help. The first author is in debt to Mr. Jiajie Xiao for his discussion.

REFERENCES

[1] A. R. Calderbank, G. D. Forney Jr, and A. Vardy, "Minimal tailbiting trellises: The Golay code and more," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1435–1455, Jul. 1999.

[2] R. Koetter and A. Vardy, "On the theory of linear trellises," in *Information, Coding and Mathematics*, M. Blaum, Ed. Boston, MA: Kluwer, 2002, pp. 323–354.

[3] ——, "The structure of tailbiting trellises: Minimality and basic principals," *IEEE Trans. Inf. Theory*, vol. 49, no. 9, pp. 2081–2105, Sep. 2003.

[4] F. R. Kschischang, "The trellis structure of maximal fixed-cost codes," *IEEE Trans. Inf. Theory*, vol. 42, no. 6, pp. 1828–1838, Nov. 1996.

[5] F. R. Kschischang and V. Sorokine, "On the trellis structure of block codes," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1924–1937, Nov. 1995.

[6] H. Singh, B. S. Rajan, P. Shankar, and P. N. A. Kumar, "Minimal tailbiting trellises for certain MDS and cyclic codes," *IEEE Trans. Inf. Theory*, submitted for publication.

[7] A. Vardy, "Trellis structure of codes," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, pp. 1989–2118.

The Probability of Undetected Error for a Class of Asymmetric Error Detecting Codes

Torleiv Kløve, *Fellow, IEEE*, Paul Oprisan, and Bella Bose, *Fellow, IEEE*

***Abstract*—Bose and Lin introduced a class of systematic codes for the detection of asymmetric errors (or equivalently, unidirectional errors). The determination of the probability of undetected error for these codes has been an open problem for many years.**

In this correspondence, the undetectable errors are characterized and the probability of undetected error is determined. Some detailed examples are given.

***Index Terms*—Asymmetric error, Bose–Lin codes, error detection, probability of undetected error, Z-channel.**

I. The Bose–Lin Codes

Bose and Lin [2] introduced a class of systematic binary codes for the detection of asymmetric errors (or equivalently, unidirectional errors). We assume that transmission is done over the Z-channel, the channel where a sent zero is always received correctly whereas a sent

Manuscript received October 16, 2003; revised October 25, 2004. This work was supported by the National Science Foundation under Grant CCR-0105204 and by the Norwegian Research Council.

T. Kløve is with the Department of Informatics, University of Bergen, N-5020 Bergen, Norway.

P. Oprisan and B. Bose are with the School of Electrical Engineering and Computer Science, Oregon State University, Corvallis, OR 97331 USA.

Communicated by K. A. S. Abdel-Ghaffar, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2004.842757