Projective Codes Which Satisfy the Chain Condition

S. ENCHEVA
Stord/Haugesund College
Børsnesg. 45, 5528 Haugesund, Norway

G. D. COHEN
Department of Inf., ENST and CNRS
46 rue Barrault, 75634 Paris, France

(Received November 1998; revised and accepted March 1999)

Abstract—Binary linear codes with length at most one above the Griesmer bound were proven to satisfy the chain condition by Helleseth et al. [1]. Binary linear projective codes with length two above the Griesmer bound which satisfy the chain condition are found. Necessary conditions for binary linear codes for which the two-way chain condition holds are derived. © 2000 Elsevier Science Ltd. All rights reserved.

Keywords—Linear codes, Chain condition, Two-way chain condition.

1. INTRODUCTION

Let $C$ be an $[n, k]$ binary linear code.

It is called projective if any two of its coordinates are linearly independent, i.e., if the dual code $C^\perp$ has minimum distance $d^\perp \geq 3$.

For any subcode $D$ of $C$, the support of $D$, supp $(D)$, is the set of positions where not all the codewords of $D$ are zero, and it is denoted by $\chi(D)$. The support of a binary vector is the set of its nonzero coordinates. The minimum support weight, $d_r$, of a code $C$ is the size of the smallest support of any $r$-dimensional subcode of $C$. In particular, $d_1 = d$. The weight hierarchy of $C$ is $\{d_1, d_2, \ldots, d_k\}$.

The concepts of chain condition (CC) and two-way chain condition (TCC) were introduced by Wei and Yang [2] and Forney [3], respectively; our definitions are slightly different. The TCC implies that the code possesses an efficient coordinate ordering, a highly desirable feature for trellis decoding (see [3]).

DEFINITION 1. An $[n, k]$ code $C$ satisfies the chain condition if it is equivalent to a code \( \hat{C} \) such that there exists a chain of subcodes of $\hat{C}$, $D_1 \subset D_2 \subset \cdots \subset D_k = \hat{C}$, where for $1 \leq r \leq k$, we have $\dim(D_r) = r$, and $\chi(D_r) = \{1, 2, \ldots, d_r\}$.

DEFINITION 2. An $[n, k]$ code $C$ satisfies the two-way chain condition if it is equivalent to a code $\hat{C}$ with the following property: there exist two chains of subcodes of $\hat{C}$, the left chain $D^L_1 \subset \ldots \subset D^L_k = \hat{C}$ and the right chain $D^R_1 \subset \ldots \subset D^R_k = \hat{C}$.
$D^L_k \subset \ldots \subset D^L_1 = \mathcal{C}$, and the right chain $D^R_k \subset D^R_2 \subset \ldots \subset D^R_1 = \mathcal{C}$, where, for $1 \leq r \leq k$, we have $\dim(D^L_r) = \dim(D^R_r) = r$, $\chi(D^L_r) = \{1, 2, \ldots, d_r\}$, and $\chi(D^R_r) = \{n - d_r + 1, n - d_r + 2, \ldots, n\}$.

In Definition 2, the chain of subcodes $D^L_i$ is actually the chain $D_i$ from Definition 1. The chain of subcodes $D^R_i$ is similar to the chain $D_i$ but the order of coordinates is counted from the right to the left.

**Theorem 1.** (See [1].) A code $C$ of length $n = g(k, d) + 1$ satisfies the chain condition.

**Theorem 2.** (Duality) (See [4].) Let $C$ be an $[n, k]$ code and $C^\perp$ be its dual code. Then $\{d_r : 1 \leq r \leq k\} = \{1, 2, \ldots, n\} \setminus \{n + 1 - d_r : 1 \leq r \leq n - k\}$.

From now on, $C$ is a binary linear projective code.

The rest of this letter is organized as follows. In Section 2, we study conditions under which codes of length 2 above the Griesmer bound satisfy the chain condition. In Section 3, we give necessary and sufficient conditions for codes to satisfy the two-way chain condition.

## 2. PROJECTIVE CODES AND THE CHAIN CONDITION

For the description of generator matrices of projective codes, we need some further notations. A column in this description represents a sequence of columns in the generator matrix and the number of columns in the sequence is written above the column. Thus, a generator matrix of $C$ can be written in the form

\[
\begin{array}{cccccccc}
\multicolumn{8}{c}{a} \\
0 & 0 & \ldots & 0 & 0 \\
G_0 & 0 & 0 & \ldots & 0 \\
\ast \ast \ast & 1 & 0 & \ldots & 0 \\
\ast \ast \ast & \ast & 1 & \ldots & 0 \\
\ast \ast \ast & \ast & \ast & \ldots & 1 \\
\end{array}
\]

For given $k$ and $d$, there exists an $[n, k, d]$ code where $n(k, d) \geq g(k, d)$: $= \sum_{i=0}^{k-1} \lfloor \frac{d_i}{2^i} \rfloor$, $\lfloor x \rfloor$ being the least integer not smaller than $x$; this is known as the Griesmer bound.

**Lemma 1.** Let $C$ be an $[n = g(k, d) + 2, k, d]$ code such that $d_1 = 3, d_2 = 5$. Then $C$ satisfies the CC.

**Proof.** From Theorem 2 and conditions $d_1 = 3, d_2 = 5$ it follows that the weight hierarchy of $C$ is $d_i = g(i, d)$ for $1 \leq i \leq k - 3, d_{k-2} = g(k - 2, d) + 1$, and $d_i = g(i, d) + 2$, for $i = k - 1, k$.

Since $d \leq 2^{k-2}$, $d_{k-2} = g(k - 2, d) + 1$ and $d_2 = 5$, then $d_{k-3} = g(k - 3, d)$. By Theorem 2, the highest $d_i$'s are $d_k = n, d_{k-1} = n - 1, d_{k-2} = n - 3, d_{k-3} = n - 5$. Since $d_1 = 3$, a generator matrix of $C$ can be written in the form (1) with $s = k - 2, a = 2$, where $G_{k-2}$ generates an $[n - 3 = g(k - 2, d) + 1, k - 2, d]$ code $C_{k-2}$. The code $C_{k-2}$ generated by the first $k - 2$ rows has length $n - 3 = g(k - 2, d) + 1$, and according to Theorem 1 satisfies the CC. From $d_{k-3} = g(k - 3, d)$, it follows that the weight hierarchy of $C_{k-2}$ coincides with the first $k - 2$ elements of the weight hierarchy of $C$, completing the proof.

**Definition 3.** Let $c$ be a nonzero codeword of $C$ and $G$ a generator matrix for $C$, with $c$ as first row. The code generated by the restriction of $G$ to the columns in which $c$ has zero coordinates is called the residual code of $C$ with respect to $c$ and denoted by $\text{Res}(C, c)$.

**Theorem 3.** A necessary and sufficient condition for an $[n = g(k, d) + 2, k, d]$ code $C$ with weight hierarchy $\{d_1, d_2, \ldots, d_k\}$ to satisfy the chain condition is that there exists an $[n - d, k - 1, d'_1 = d_2 - d]$ code $C' = \text{Res}(C, c)$ with weight hierarchy $d'_1, d'_2 = d_3 - d, \ldots, d'_{k-1} = d_k - d$ which satisfies the CC.
PROOF. Let $C$ be a code as described in the theorem and satisfies the CC. W.l.o.g. its generator matrix $G$ can be written in the form (1) in such a way that its rows display the chain of subcodes of Definition 1. Let $c$ be the first row in $G$. Now, we should prove that $C' = \text{Res}(C, c)$ satisfies the CC.

Since $C$ is a code with length $n$ above the Griesmer bound, there are integers $0 < m < p < k$ such that $d_1 = d, d_2 = g(2, d), \ldots, d_m = g(m, d), d_{m+1} = g(m+1, d) + 1, d_{p+1} = g(p+1, d) + 2, \ldots, d_k$. Now, we prove that $m \neq p$. Suppose that there exists a code $C$ with parameters as described in the theorem and an integer $s$ such that $0 < s < k$, $B_j = 0, j = 1, 2, \ldots, k - s - 2$ and $B_k-s-1 > 0$, with furthermore $d_i = g(i, d)$ for $1 \leq i \leq s$, $d_i = g(i, d) + 2$ for $s + 1 \leq i \leq k$. In other words, suppose that $l = p = s$. Assuming w.l.o.g. that a codeword of $C'$ has for support the last $k - s$ positions. Then a generator matrix of $C$ can be written in the form (1) where $G_s$ generate a subcode of length $n - (k - s)$ and dimension $s$ and $n = 3$.

The last $k - s - 2$ columns in (1) are linear independent. The second column after $G_s, (h_2)$, is a linear combination of all $k - s - 2$ columns on its right since $B_k - s - 1 > 0$. The first column after $C_s$ differs from $h_2$ by the projectivity assumption. Therefore, it can be a linear combination of at most $k - s - 3$ columns chosen among the last $k - s - 2$. This contradicts the assumption that $B_j = 0, j = 1, 2, \ldots, k - s - 2$. Hence, $m \neq p$.

Let us calculate $d_{i-1}'$ and $d_i'$: $d_{i-1}' = d_l - d = g(l - 1, d'_1), d_i' = d_{i+1} - d = g(l, d'_1) + 1$. The same relations are valid between $d_p, d_{p-1}'$ and $d_p+1, d_p'$. Therefore, $C'$ has weight hierarchy $d_1' = d_2 - d, d_2' = d_3 - d, \ldots, d_{k-1}' = d_k - d$ and satisfies the CC.

Conversely, let $C$ be an $[n = g(k, d) + 2, k, d]$ code with weight hierarchy $\{d_1 = d, d_2, \ldots, d_k\}$ and such that there exists an $[n - d, k - 1, d'_1 = d_2 - d]$ code $C' = \text{Res}(C, c)$ with weight hierarchy $\{d_1', d_2' = d_3 - d, \ldots, d_{k-1}' = d_k - d\}$ satisfying the CC. From the definition of a residual code, it follows that $C$ satisfies the CC.

PROPOSITION 1. If $C$ is an $[n = g(k, d) + 2, k, d \leq 2^{k-l+1}]$ code with $d_1^l = l \geq 3$ containing an $[n - l, k - l + 1, d]$ subcode, then $C$ satisfies the CC.

PROOF. Since $C$ is projective, its generator matrix can be written in the form (1) where $G_s$ spans an $[n - l, k - l + 1, d]$ code $C_{k-l+1}$.

From Theorem 1, it follows that $C_{k-l+1}$ code satisfies the CC because $n - l = g(k, d) + 2 - l = g(k-l+1, d) + 1$.

3. CODES AND THE TWO-WAY CHAIN CONDITION

Delsarte [5] has shown that the weights of a two-weight code $C$ are of the form

$$w_1 = u2^t, \quad w_2 = (u + 1)2^t$$

for suitable integers $u$ and $t$, $u \geq 1, t \geq 0$.

According to Klove [6], if a binary linear code $C$ satisfies the TCC, then it contains two codewords with minimum weight and disjoint supports. Thus, $w_2 = 2w_1$. Using equation (2), we get $(u + 1)2^t = 2u2^t$, i.e., $u = 1$, proving the following lemma.

LEMMA 2. If $C$ is a two-weight code which satisfies the TCC, then its weights are of the form $w_1 = 2^t, w_2 = 2^{t+1}, t \geq 0$.

PROPOSITION 2. If $C$ is an $[n, k, 2^t]$ two-weight code with $t = k - 1 + j, j \geq 0$, which satisfies the TCC, then $n \geq 2^t + 2^j$.

PROOF. By Griesmer bound $g(k, 2^t) = \sum_{i=0}^{k-1} \binom{2^t}{2^i} = 2^{t+1} - 2^j$, if $t = k - 1 + j$. But we know that $n \geq w_2 = 2^{t+1}$. ■
LEMMA 3. If \( C \) is a self-complementary two-weight code, then it satisfies the TCC.

PROOF. Let \( C[n, k, 2^t] \) be such a code, with generator matrix \( G \). One has \( w_1 = 2^t, w_2 = 2^{t+1} = n \), since the code is self-complementary.

W.l.o.g. assume that the first row of \( G \) has support in the first \( 2^t \) positions; call it \( c_1 \). Since \( n = 2^{t+1} \), its complement \( c_1^t \) has its support in the last \( 2^t \) positions.

Let \( c_2 \) be any codeword not in \( \{c_1, c_1^t, 1\} \). Since wt\((c_1 + c_2) = 2^t \), we get \( d_2 = 3.2^{t-1} - 1 \) and \( d_2 - d_1 = 2^{t-1} \). Consider the union of the supports of \( c_1 \) and \( c_2 \) \( u_s(c_1, c_2) \) where wt\((c_1) = wt(c_1^t) = wt(c_1 + c_2) = 2^t \). Therefore, \( u(c_1, c_2) = 3.2^{t-1} - 1 \). Continuing in the same way, we see that \( u_s(c_1, c_2, c_3) = u_s(c_1^t, c_2, c_3) \) and so on. Hence, \( C \) satisfies the TCC.

PROPOSITION 3. MacDonald codes \([2^k - 2^u + 1, k, 2^k - 2^u] \) satisfy the TCC only for \( u = k - 2 \).

PROOF. MacDonald codes \([2^k - 2^u + 1, k, 2^k - 2^u] \) are two-weight codes with \( w_1 = 2^k - 2^u \) and \( w_2 = 2^{k-1} \). By Lemmas 2 and 3, we conclude that these codes satisfy the TCC only for \( u = k - 2 \).

LEMMA 4. A necessary condition for a code \( C \) to satisfy the two-way chain condition is that \( B_1 \geq 2 \), where \( d_1^l = l \geq 3 \).

PROOF. By Definition 2 (now we need only the left chain of subcodes of \( C \)) and the fact that \( C \) is projective, its generator matrix can be written written in the form \( \begin{array}{c} \end{array} \) with \( s = k - l + 1, a = 2, G_{k-l+1} \) spans the \([n - l - 1, k - l + 1, d + 1, k - l - 1, d] \) code \( C_{k-l+1} \). In other words, \( B_1 \geq 1 \). From the existence of the right chain in Definition 2, we conclude that \( B_1 \geq 2 \).

PROPOSITION 4. Subcodes of the extended \([24, 12, 8] \) Golay code with parameters \([24-p, 12-p, 8], 1 \leq p \leq 6 \) do not satisfy the TCC.

PROOF. All codes described in Proposition 4 are enumerated in [7].

By [7], there are exactly two \([18, 6, 8] \) codes. The first one has weight distribution

\[
A_0 = 1, \quad A_8 = 45, \quad A_{12} = 18.
\]

There is no codeword of weight 16, hence by Lemma 5, the code does not satisfy the TCC. The second one has \( B_2 = 1 \), thus does not satisfy the TCC by Lemma 6. Let \( C \) be a \([19, 7, 8] \) code.

If \( C \) satisfies the TCC, there must exist three codewords as follows:

\[
1111111100000000000 \\
0000011111110000000 \\
0000000000011111111.
\]

To see this, note that [6] for the TCC to hold, we need two codewords with minimum weight and disjoint supports; for the left chain, we need a two-dimensional subcode with weight hierarchy 8,12. They lead to a codeword of weight 14, which does not belong to the code since by [7], the unique \([19, 7, 8] \) code has weight distribution

\[
A_0 = 1, \quad A_8 = 78, \quad A_{12} = 48, \quad A_{16} = 1.
\]

Therefore, \( C \) does not not satisfy the TCC. Similar considerations complete the proof for the other five codes of lengths 20,21,22,23, and 24, respectively.

REFERENCES

