On the nonexistence of triple-error-correcting perfect binary linear codes with a crown poset structure

Hyun Kwang Kim, Dong Yeol Oh

Department of Mathematics, Pohang University of Science and Technology, Pohang 790-784, Republic of Korea

Received 12 April 2004; received in revised form 19 February 2005; accepted 1 March 2005

Abstract

Ahn et al. [Discrete Math. 268 (2003) 21–30] characterized completely the parameters of single- and error-correcting perfect linear codes with a crown poset structure by solving Ramanujan–Nagell-type Diophantine equation. In this paper, we give a shorter proof for the same result by analyzing a generator matrix of a perfect linear code. Furthermore, we combine our method with the Johnson bound in coding theory to prove that there are no triple-error-correcting perfect binary codes with a crown poset structure.

© 2005 Elsevier B.V. All rights reserved.

Keywords: Crown poset; Johnson bound; Perfect poset code

1. Introduction

A code is called perfect if the spheres of the same radius centered at the codewords cover the whole space without overlapping. The problem of classifying all perfect codes is one of the basic problems in coding theory, and it still has not been completely solved. Let \( \mathbb{F}_q \) be the finite field with \( q \) elements and \( \mathbb{F}_q^n \) be the vector space of \( n \)-tuples of \( \mathbb{F}_q \). Coding theory may be viewed as the study of \( \mathbb{F}_q^n \) when \( \mathbb{F}_q^n \) is endowed with the Hamming metric.

Since the late 1980s, several attempts have been made to generalize classical problems of coding theory by introducing a new non-Hamming metric on \( \mathbb{F}_q^n \) (cf. [6–8]). This idea...
was fully applied by Brualdi et al. in 1995 to the concept of poset codes. We first introduce basic notions on posets and poset codes which will be needed in our study. We refer to [2] for details.

Let $F^n_\mathbb{F}$ be the vector space of $n$-tuples over a finite field $F_\mathbb{F}$ with $q$ elements. Let $P$ be a partially ordered set, which will be abbreviated as a poset in the sequel, on the underlying set $[n] = \{1, 2, \ldots, n\}$ of coordinate positions of vectors in $F^n_\mathbb{F}$ with the partial order relation denoted by $\leq$ as usual. For $x = (x_1, x_2, \ldots, x_n) \in F^n_\mathbb{F}$, the support of $x$ and $P$-weight of $x$ are defined to be

$$\text{supp}(x) = \{i \mid x_i \neq 0\} \quad \text{and} \quad w_P(x) = |\langle \text{supp}(x) \rangle|,$$

where $\langle \text{supp}(x) \rangle$ is the smallest ideal (recall that a subset $I$ of $P$ is an ideal if $a \in I$ and $b \leq a$, then $b \in I$) containing the support of $x$. It is well known that for any $x, y \in F^n_\mathbb{F}$, $d_P(x, y) = w_P(x - y)$ defines a metric on $F^n_\mathbb{F}$. The metric $d_P$ is called the $P$-metric on $F^n_\mathbb{F}$.

We remark that $d_P$ becomes the classical Hamming metric if $P$ is an antichain. Let $F^n_\mathbb{F}$ be endowed with the $P$-metric. Then a (linear) code $C \subseteq F^n_\mathbb{F}$ is called a (linear) $P$-code of length $n$. For a vector $x$ in $F^n_\mathbb{F}$ and a nonnegative integer $r$, the $P$-sphere with center $x$ and radius $r$ is defined as the set

$$S_P(x; r) = \{y \in F^n_\mathbb{F} \mid d_P(x, y) \leq r\}$$

of all vectors in $F^n_\mathbb{F}$ whose $P$-distance from $x$ is less than or equal to $r$. The number of vectors in $F^n_\mathbb{F}$ whose distance from the zero vector is exactly $i$ equals

$$\sum_{j=1}^{i} (q - 1)^{j-q^{-1}} \Omega_j(i) \quad \text{if} \quad i > 0,$$

where $\Omega_j(i)$ denotes the number of ideals of $P$ with cardinality $i$ having exactly $j$ maximal elements. Hence we obtain the following equation:

$$|S_P(x; r)| = 1 + \sum_{i=1}^{r} \sum_{j=1}^{i} (q - 1)^{j-q^{-1}} \Omega_j(i). \quad (1)$$

A code $C$ is called an $r$-error-correcting perfect $P$-code if the $P$-spheres of radius $r$ centered at the codewords of $C$ cover the whole space $F^n_\mathbb{F}$ without overlapping. In [1–4], perfect $P$-codes are studied for several posets $P$. One interesting feature of the theory of poset codes is that it gives us a new type of problem on perfect poset codes. We can consider problems of classifying perfect $P$-codes when a poset $P$ is given as well as problems of classifying posets which admit a given code to be a perfect code. For example, in [1], they characterized the parameters of single- and double-error-correcting perfect $P$-codes, where $P$ is a crown poset, and in [3], they classified all poset structures which admit the extended binary Hamming code to be a double- or triple-error-correcting perfect code. Recall that the crown is a poset with elements $\{1, 2, \ldots, 2m\}$, $m \geq 2$, in which $i < m + i$, $i + 1 < m + i$ for each $i = 1, 2, \ldots, m - 1$ and $1 < 2m, m < 2m$ and these are the only possible strict comparabilities.
Let \( P \) be a crown poset. In this paper, we present two results on perfect linear \( P \)-codes. We first give a simple new proof for the characterization of parameters of single- and double-error-correcting perfect linear \( P \)-codes which was done by other means in [1]. Our new method is intrinsic and uses an analysis of a generator matrix of a linear code. Next, we combine our method with the Johnson bound in coding theory to prove the nonexistence of triple-error-correcting perfect binary linear \( P \)-codes.

In the sequel, \( P \) will denote the crown on \( \{1, 2, \ldots, 2m\} \) unless otherwise specified. We will use the following notation: for a vector \( x \in \mathbb{F}_q^m \), \( x_L \) (resp. \( x_R \)) denotes the vector in \( \mathbb{F}_q^m \) consisting of the left (resp. right) half of \( x \). Sometimes we will write \( x = (x_L, x_R) \).

2. The single- and double-error-correcting perfect linear \( P \)-codes

In [1], the authors characterized completely the parameters of single- and double-error-correcting perfect linear \( P \)-codes, where \( P \) runs over the crown posets. They derived a Ramanujan–Nagell type Diophantine equation from the sphere-packing condition, and solved the equation to characterize the parameters of single- and double-error-correcting perfect \( P \)-codes. This method is quite long and complicated but also works for nonlinear \( P \)-codes. In this section, we give a shorter and simpler proof for the same result which works only for linear \( P \)-codes.

**Proposition 2.1.** Let \( \mathcal{C} \) be a linear \( P \)-code and \( r = 1 \) or 2. If \( \mathcal{C} \) is an \( r \)-error-correcting perfect \( P \)-code with a generator matrix \( G \), then \( G \) (up to equivalence) is of the form:

\[
\begin{pmatrix}
* & I_m \\
G_m & 0
\end{pmatrix},
\]

(2)

where \( I_m \) denotes the \( m \times m \) identity matrix and \( G_m \) is a generator matrix of an \( r \)-error-correcting perfect linear code of length \( m \) with the Hamming metric.

**Proof.** Let \( \mathcal{C} \) be an \( r \)-error-correcting perfect \( P \)-code, where \( r = 1 \) or 2 and the poset \( P \) is the crown on \( \{1, 2, \ldots, 2m\} \). We claim that, for each \( m + 1 \leq i \leq 2m \), there exists a codeword \( c = (c_L, c_R) \in \mathcal{C} \) such that \( \text{supp}(c_R) = \{i\} \).

Suppose that there are no such codewords for some \( i, m + 1 \leq i \leq 2m \). Without loss of generality, we may assume that for all \( x = (x_L, x_R) \in \mathbb{F}_q^{2m} \) with \( \text{supp}(x_R) = \{m + 1\} \), \( x \) does not belong to \( \mathcal{C} \). Since \( \mathcal{C} \) is an \( r \)-error-correcting perfect \( P \)-code, for each \( x = (x_L, x_R) \in \mathbb{F}_q^{2m} \) with \( \text{supp}(x_R) = \{m + 1\} \), there exists a unique codeword \( c_x \in \mathcal{C} \) such that \( x \in \text{Sp}(c_x : r) \). By our hypothesis, \( \text{supp}(c_{x_R}) \neq \{m + 1\} \). Since \( P \) is a crown poset, \( d_P(x, c_x) \geq 3 \). This is a contradiction, and this proves our claim. We pick a generator matrix \( G \) of \( \mathcal{C} \) whose \( i \)th row consists of a codeword \( c = (c_L, c_R) \) such that \( \text{supp}(c_R) = \{i\} \). Then \( G \) is a matrix of the form described by Eq. (2). Finally, we show that \( G_m \) is a generator matrix of an \( r \)-error-correcting perfect linear code of length \( m \) with the Hamming metric.

Let \( \mathcal{C}_1 = \{c | c = (c_L, 0) \in \mathcal{C}\} \). Then \( G_m \) is a generator matrix of \( \mathcal{C}_1 \). Let \( x_L \in \mathbb{F}_q^m \). We denote the vector \( (x_L, 0) \in \mathbb{F}_q^{2m} \) by \( x \). Since \( \mathcal{C} \) is an \( r \)-error-correcting perfect \( P \)-code, there exists a unique codeword \( c_x \in \mathcal{C} \) such that \( x \in \text{Sp}(c_x : r) \), where \( r = 1 \) or 2. Since \( P \) is a crown poset, \( \text{supp}(c_{x_R}) = \emptyset \). Hence, \( c_x = (c_{x_L}, 0) \in \mathcal{C}_1 \). Therefore \( x_L \in \text{Sp}(c_{x_L} :
It is well known that the single-error-correcting perfect linear codes over $\mathbb{F}_q$ are the Hamming codes. Therefore we obtain the following theorem (which is the same as Theorem 1 in [1]) from Proposition 2.1:

**Theorem 2.2.** Let $P$ be the crown on $\{1, 2, \ldots, 2m\}$. Then every single-error-correcting perfect linear $P$-code over $\mathbb{F}_q$ has parameters $[2m, 2m - l]$, where $m = (q^l - 1)/(q - 1)$, and $l \geq 2$. Furthermore, for $l \geq 2$, there exists a single-error-correcting perfect linear $P$-code over $\mathbb{F}_q$ with the parameter $[2m, 2m - l, 3]$.

For double-error-correcting perfect linear codes over $\mathbb{F}_q$, the following facts are well known (see [5] for details):

(a) There are only two trivial double-error-correcting perfect linear codes over $\mathbb{F}_2$, namely, $C_1 = \{(0, 0)\}$ and $C_2 = \{(0, 0, 0, 0, 0, 0, 0, 0), (1, 1, 1, 1, 1, 1)\}$.

(b) There are no nontrivial double-error-correcting perfect linear codes over $\mathbb{F}_2$.

(c) There is only one trivial double-error-correcting perfect linear code over $\mathbb{F}_q$, $q > 2$, namely, $C = \{(0, 0)\}$.

(d) The only possible parameters for a nontrivial double-error-correcting perfect code over $\mathbb{F}_q$, $q > 2$ is the parameter of the ternary [11, 6, 5] Golay code.

The following theorems (which are the same as Theorems 2 and 3 in [1]) follow from Proposition 2.1 and the preceding facts for the double-error-correcting case:

**Theorem 2.3.** Every double-error-correcting perfect linear $P$-code over $\mathbb{F}_2$ has parameters $[4, 2]$ or $[10, 6]$. Moreover, there is a double-error-correcting perfect linear $P$-code over $\mathbb{F}_2$ with each of the given parameters.

**Theorem 2.4.** Every double-error-correcting perfect linear $P$-code over $\mathbb{F}_3$ has parameters $[4, 2]$ or $[22, 17]$. Moreover, there is a double-error-correcting perfect linear $P$-code over $\mathbb{F}_3$ with each of the given parameters.

**Theorem 2.5.** Every double-error-correcting perfect linear $P$-code over $\mathbb{F}_q$, $q > 3$, has the parameter $[4, 2]$. Moreover, there is a double-error-correcting perfect linear $P$-code over $\mathbb{F}_q$ with the given parameter.

3. Nonexistence of triple-error-correcting perfect binary linear $P$-codes

In this section, we continue our analysis on a generator matrix of a perfect linear $P$-code and prove that there are no triple-error-correcting perfect linear $P$-codes over $\mathbb{F}_2$ by using the Johnson bound in coding theory.

We start with a proposition which gives a necessary and sufficient condition for a given code to be an $r$-error-correcting perfect $P$-code. We refer to [3] for a proof.
Proposition 3.1. Let \( C \) be an \([n, k]\) binary linear code. Then, \( C \) is an \( r \)-error-correcting perfect \( P \)-code if and only if the following two conditions are satisfied:

(i) (The sphere-packing condition) \(|S_P(0 : r)| = 2^{n-k}\).
(ii) (The partition condition) for any nonzero codeword \( c \) and any partition \( \{x, y\} \) of \( c \), either \( w_P(x) \geq r + 1 \) or \( w_P(y) \geq r + 1 \).

Here we identify a binary vector of length \( n \) with its support, and consider \( c, x, \) and \( y \) as subsets of \([n] = \{1, 2, \ldots, n\}\).

The following lemma, which is useful in the sequel, is an easy consequence of the partition condition.

Lemma 3.2. Let \( C \) be a triple-error-correcting perfect linear \( P \)-code. Then, for each \( x = (x_L, x_R) \in \mathbb{F}_2^m \),

1. if \( w_P(x) = 3, 4, \) or \( 5 \), then \( x \notin C \).
2. if \( x \in C \) and \( w_P(x) = 3 \), then \( w_P(x) \geq 7 \).
3. if \( x \in C \) and \( w_P(x_R) = 5 \) (resp. \( w_P(x_R) = 6 \)), then \( w_P(x) \geq 6 \) (resp. \( w_P(x) \geq 7 \)), and
4. if \( x \in C \) and \( x_R = 0 \), then \( w_P(x) = w_H(x) \geq 7 \).

Remark. If \( C \) is a triple-error-correcting perfect linear \( P \)-code, then \( d_P(C) \geq 6 \). Hence, we should have \( m \geq 3 \).

The following lemma gives a necessary condition for the existence of triple-error-correcting perfect \( P \)-codes.

Lemma 3.3. Let \( C \) be a triple-error-correcting perfect binary linear \( P \)-code. Then, for each \( m + 1 \leq i \leq 2m \), there exists a codeword \( c = (c_L, c_R) \in C \) such that \( \text{supp}(c_R) = \{i\} \).

Proof. Suppose that there are no such codewords for some \( i, m + 1 \leq i \leq 2m \). Without loss of generality, we may assume that \( c = (c_L, c_R) \notin C \) if \( \text{supp}(c_R) = \{m + 1\} \). Consider the following subset \( A \) of \( \mathbb{F}_2^{2m} \):

\[
A = \{x = (x_L, x_R) \in \mathbb{F}_2^{2m} \mid \text{supp}(x_R) = \{m + 1\}, \text{ and } w_P(x) = 4\}.
\]

It follows from our assumption that \( x \notin C \) for every \( x \in A \). Since \( C \) is a triple-error-correcting perfect \( P \)-code, for each \( x \in A \), there exists a unique codeword \( c_x \in C \) such that \( x \in S_P(c_x : 3) \). It follows from Lemma 3.2 and the perfectness of \( C \) that \( c_x \) has one of the following forms:

\[
w_P(c_x) = 5 \quad \text{and} \quad w_P(c_x) = 6, \quad \text{(3)}
\]

\[
w_P(c_x) = 6 \quad \text{and} \quad w_P(c_x) = 7. \quad \text{(4)}
\]

For each case, \( c_x \) satisfies the following properties:

\[
\text{supp}(x_R) \subset \text{supp}(c_x) \quad \text{and} \quad \text{supp}(x_L) \nsubseteq \text{supp}(c_x). \quad \text{(5)}
\]
Furthermore, $S_{P}(c_{x} : 3)$ contains only one element, say $x$, of $A$. Since $|A| = 4(m - 2)$, there exist $4(m - 2)$ codewords $c_{x} = (c_{xL}, c_{xR}) \in \mathcal{C}$ satisfying Eq. (5). For each such codeword $c_{x}$, $m + 1 \in \text{supp}(c_{xR})$ and $|\text{supp}(c_{xR})| = 2$. By the pigeonhole principle, if $m \geq 3$, we can choose two codewords $c_{x}$ and $c_{x}'$ of $\mathcal{C}$ such that $\text{supp}(c_{xR}) = \text{supp}(c_{x'R})$. It follows from our construction that $d_{P}(c_{x}, c_{x}') = d_{H}(c_{xL}, c_{x'L}) \leq 6$. This yields a contradiction to Lemma 3.2 (4). Therefore, for each $m + 1 \leq i \leq 2m$, there exists a codeword $c = (c_{L}, c_{R}) \in \mathcal{C}$ such that $\text{supp}(c_{R}) = \{i\}$.

**Remark.** If $\mathcal{C}$ is a triple-error-correcting perfect linear binary $P$-code, then $\mathcal{C}$ has a generator matrix $G$ of the following form:

$$
\begin{pmatrix}
* & I_{m} \\
G_{m} & 0
\end{pmatrix},
$$

where $I_{m}$ denotes the $m \times m$ identity matrix.

We recall the Johnson bound and refer to [5, Chapter 17] for a proof.

**Theorem 3.4.** Let $A(n, d)$ be the maximum number of codewords in any binary code of length $n$ and minimum distance $d$ between codewords. Then we have

$$
A(n, 2\delta + 1) \left\{ 1 + \binom{n}{1} + \cdots + \binom{n}{\delta} + \frac{n}{\delta + 1} - \frac{n}{\delta + 1} \right\} \leq 2^{n}.
$$

We now give the main result of this paper.

**Theorem 3.5.** There are no triple-error-correcting perfect binary linear $P$-codes.

**Proof.** Suppose that $\mathcal{C}$ is a triple-error-correcting perfect binary linear $P$-code. By the preceding remark, $\mathcal{C}$ has a generator matrix $G$ of the following form:

$$
\begin{pmatrix}
* & I_{m} \\
G_{m} & 0
\end{pmatrix},
$$

where $I_{m}$ denotes the $m \times m$ identity matrix. By Lemma 3.2, $\mathcal{C}$ is a $[2m, m + k, d_{P} \geq 6]$-code. Let $\mathcal{C}_{1}$ be the linear code generated by $G_{m}$. Then $\mathcal{C}_{1}$ is an $[m, k, d_{H} \geq 7]$-code.

We consider the set $B$ of vectors $x = (x_{L}, x_{R}) \in \mathbb{F}_{2}^{2m}$ such that $x_{R} = 0$ and $x$ belongs to a sphere of radius $3$ centered at a codeword $c \in \mathcal{C}$ satisfying $|\text{supp}(c_{R})| = 1$. We identify $\mathbb{F}_{2}^{2m}$ with the left part of $\mathbb{F}_{2}^{2m}$ by the embedding $x \mapsto (x, 0)$. Then we can write $B$ as follows:

$$
B = \bigcup \left( S_{P}(c : 3) \cap \mathbb{F}_{2}^{m} \right),
$$

where $c$ runs over codewords of $\mathcal{C}$ satisfying $|\text{supp}(c_{R})| = 1$. Then we can easily verify that $|B| = 4m2^{k}$. Since $\mathcal{C}$ is a triple-error-correcting perfect $P$-code and $P$ is the crown poset, any
vector in \( \mathbb{F}_{m}^{n} \setminus B \) is uniquely covered by a sphere of radius 3 with the center at a codeword of \( C_1 \). Furthermore, since \( C_1 \) is an \([m, k, d_H \geq 7]\)-code, we have the following equation:

\[
|C_1| \left( 1 + \binom{m}{1} + \binom{m}{2} + \binom{m}{3} \right) = 2^m - 4m 2^k. \tag{7}
\]

Since \( d_H(C_1) \geq 7 \), we obtain the following inequality by the Johnson bound:

\[
|C_1| \left( 1 + \binom{m}{1} + \cdots + \binom{m}{3} + \left( \frac{m}{3} \right) \left( \frac{(m - 3)/4 - \lfloor (m - 3)/4 \rfloor}{m/4} \right) \right) \leq 2^m. \tag{8}
\]

Set \( f(m) = \left( \frac{m}{3} \right) \left( \frac{(m - 3)/4 - \lfloor (m - 3)/4 \rfloor}{m/4} \right). \) Then the following is an immediate consequence of Eqs. (7) and (8):

\[
f(m) \leq 4m. \tag{9}
\]

As \( m \geq 3 \), we can write \( m - 3 = 4l + t \), where \( l \) is a nonnegative integer and \( t = 0, 1, 2, \) or \( 3 \).

Case 1: \( m - 3 = 4l + 1 \). It follows from Eq. (9) that \( 0 \leq l \leq 6 \). Hence \( m = 4, 8, 12, 16, 20, 24 \), or \( 28 \).

Case 2: \( m - 3 = 4l + 2 \). We obtain \( m = 5, 9, \) or \( 13 \) by the same argument.

Case 3: \( m - 3 = 4l + 3 \). Then \( m = 6 \).

By the sphere-packing condition, we have

\[
|C_1||S_p(0, 3)| = |\mathbb{F}_{m}^{2^n}| = 2^{2m}. \tag{10}
\]

Therefore \( |S_p(0, 3)| = 1 + 5m + \binom{m}{2} + \binom{m}{3} \) should be a power of 2. However, \( |S_p(0 : 3)| \) is not a power of 2 for any \( m \) which are listed in Cases 1, 2, or 3.

We now consider the final case.

Case 4: \( m - 3 = 4l \). Since \( m \equiv 3 \pmod{4} \), it satisfies one of the following congruence modulo 48:

\[
m \equiv 3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47 \pmod{48}. \tag{11}
\]

By a simple calculation, it can be shown that \( |S_p(0, 3)| = 1 + 5m + \binom{m}{2} + \binom{m}{3} \) is not divisible by 8 for any \( m \) which satisfies one of the congruences in Eq. (11). For example, if \( m \equiv 3 \pmod{48} \), then we have \( |S_p(0, 3)| = 16s + 20 \) for some nonnegative integer \( s \).

From Cases 1–4, we conclude that any integer \( m \) which satisfies Eq. (9) cannot satisfy the sphere-packing condition. This completes the proof of our main result. \( \square \)

Acknowledgements

The present studies were supported by Com²MaC-KOSEF.

References