There are exactly two nonequivalent [20,5,12;3]-codes

Noboru Hamada, Tor Helleseth, and Øyvind Ytrehus

1. Introduction

Abstract — Hill and Newton showed that there exists a $[20,5,12;3]$*-code, and that the weight distribution of a* $[20,5,12;3]$*-code is unique. However, it is unknown whether or not a code with these parameters is unique. Recently, Hamada and Helleseth showed that a* $[19,4,12;3]$*-code is unique up to equivalence, and characterized this code using a characterization of* $\{21,6;3,3\}$*-minihypers. The purpose of this paper is to show, using the geometrical structure of the* $[19,4,12;3]$*-code, that exactly two non-isomorphic* $[20,5,12;3]$*-codes exist.*

Let $V(n;q)$ be an n-dimensional vector space over $GF(q)$. If C is a k-dimensional subspace in $V(n;q)$ such that every nonzero vector in C has a Hamming weight (i. e., number of nonzero coordinates) of at least d, then C is denoted an $[n,k,d;q]$-code. The well-known Griesmer bound [Griesmer, 1960, Solomon and Stiffler, 1965] states that

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \tag{1.1}$$

where $\lceil x \rceil$ denotes the smallest integer $\geq x$.

A coding theory problem that has been the subject of considerable research is the following:

Main Problem. *Characterize all* $[n,k,d;q]$*-codes meeting bound (1.1) with equality.*

Hill and Newton recently described a $[20,5,12;3]$-code. In this paper we show that, up to equivalence, there are two types of $[20,5,12;3]$-codes.

2. Preliminary results

It is easy to show that if an $[n,k,d \leq q^{k-1};q]$-code meets bound (1.1) with equality, then any two column vectors of a generator matrix of the code must be linearly independent over $GF(q)$. Thus, in this case, it can be convenient to think of the set of columns of a generator matrix as a set of points in the finite projective geometry $PG(k-1,q)$. Each column vector $(c_0,\ldots,c_{k-1})^T$ represents a point P,

$$(c_0,\ldots,c_{k-1})^T \leftrightarrow P = \left(\sum_{i=0}^{k-1} c_i \nu_i\right) \tag{2.1}$$

where $(\nu_0),\ldots,(\nu_{k-1})$ are k linearly independent, arbitrarily chosen points in $PG(k-1,q)$.

Since the point $(a\gamma)$ is equal to (γ) for any nonzero element $a \in GF(q)$, we need to consider as potential generator matrix columns only those vectors $(c_0,\ldots,c_{k-1})^T$ that have "1" as its last nonzero entry, i. e. that satisfy

$$\exists i : 0 \le i \le k-1 : \begin{cases} c_j = 0, & i < j \le k-1 \\ c_i = 1 \end{cases} \tag{2.2}$$

Let $S_{k,q}$ be the set of vectors $(c_0,\ldots,c_{k-1})$ that satisfy (2.2). Clearly $S_{k,q}$ is isomorphic to $PG(k-1,q)$. When we, in the sequel, use the term "point", it will also refer to a point in $PG(k-1,q)$ as well as to the corresponding vector in $S_{k,q}$.

Define $v_l = (q^l-1)/(q-1)$, which is the number of points in a finite projective geometry $PG(l-1,q)$ (or in an $(l-1)$-flat in $PG(k-1,q)$). A set F of f points in a finite projective geometry $PG(t,q)$ is an $\{f,m;t,q\}$-minihyper (also known as a min·hyper) if $m(\ge 0)$ is the largest integer such that all hyperplanes in $PG(t,q)$ contain at least m points in F.

Proposition 2.1. *[Hamada, 1987]. Let F be a set of f points in $S_{k,q}$, and let C be the subspace of $V(n;q)$ generated by a $k \times n$ matrix (denoted by $\mathbf{G}$) whose column vectors are all the vectors in $S_{k,q} \setminus F$, where $n = v_k - f$, $1 \le f < v_k - 1$.*

(1) Let $H_z = \{\mathbf{y} \in S_{k,q} \mid \mathbf{z} \cdot \mathbf{y} = 0 \text{ over } GF(q)\}$ for any nonzero vector $\mathbf{z}$ in $S_{k,q}$. Then H_z is a hyperplane in $PG(k-1,q)$, and the weight of the code vector $\mathbf{zG}$ is equal to

$$|F \cap H_z| + q^{k-1} - f.$$

(2) In the case $k \ge 3$ and $1 \le d < q^{k-1}$, C is an $[n,k,d;q]$-code meeting the Griesmer bound if and only if F is a $\{v_k - n, v_{k-1} - n + d; k-1, q\}$-minihyper.

Definition 2.2. Two $[n,k,d;q]$-codes C_1 and C_2 are said to be C-equivalent if there exists generator matrices $\mathbf{G}_i$ for C_i, $i = 1,2$, such that $\mathbf{G}_2 = \mathbf{G}_1\mathbf{DP}$ (or $\mathbf{G}_2 = \mathbf{G}_1\mathbf{PD}$) for some permutation matrix $\mathbf{P}$ and some nonsingular diagonal matrix $\mathbf{D}$ with entries from $GF(q)$.

Remark 2.3. (1) There is a one-to-one correspondence between the set of all nonequivalent $[19, 4, 12; 3]$-codes meeting the Griesmer bound and the set of all $\{21, 6; 3, 3\}$-minihypers.

(2) There is a one-to-one correspondence between the set of all nonequivalent $[20, 5, 12; 3]$-codes meeting the Griesmer bound and the set of all $\{101, 32; 4, 3\}$-minihypers.

Let $R \oplus S$ denote the 1–flat in $PG(t, 3)$ that contains two points R and S.

Definition 2.4. Let $\overline{\mathcal{F}}(1, 1, 2; t, 3)$, $t \geq 3$, denote the family of all sets K in $PG(t, 3)$ such that

$$K = (V \backslash \{Q\}) \cup \left(\bigcup_{i=1}^{3} (R_i \oplus S_i) \right) \tag{2.3}$$

for some points $Q, R_1, R_2, R_3, S_1, S_2, S_3$ and some 2–flat $V \subset PG(t, 3)$ such that (a) $\{Q, R_1, R_2, R_3\}$ is a 1–flat in V and (b) $\{S_0, S_1, S_2, S_3\}$ is a 1–flat in $PG(t, 3)$ such that $V \cap \{S_0, S_1, S_2, S_3\} = \{S_0\}$ and $S_0 \notin \{Q, R_1, R_2, R_3\}$.

Remark 2.5. For $i = 1, 2, 3$, let T_{i2} and T_{i3} be two points such that $R_i \oplus S_i = \{R_i, S_i, T_{i2}, T_{i3}\}$. Then K in (2.3) can also be expressed in the form

$$K = (V \backslash \{Q\}) \cup \{(S_1 =) T_{11}, T_{12}, T_{13}, (S_2 =) T_{21}, T_{22}, T_{23}, (S_3 =) T_{31}, T_{32}, T_{33}\}. \tag{2.4}$$

Proposition 2.6. [Hamada and Helleseth, 1990]. F is a $\{21, 6; 3, 3\}$-minihyper if and only if $F \in \overline{\mathcal{F}}(1, 1, 2; 3, 3)$. Equivalently, any $[19, 4, 12; 3]$-code must be generated by a matrix on the form $S_{4,3} \setminus F$ with $F \in \overline{\mathcal{F}}(1, 1, 2; 3, 3)$.

Let $Q, R_1, R_2, R_3, S_0, S_1, S_2, S_3$ be the points corresponding to the following column vectors:

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 2 \\ 1 \end{pmatrix}.$$

Then V is the 2–flat in $PG(3, 3)$ generated by points Q, R_1, and S_0. We can assume without loss of generality (w. l. o. g.) that the six points $T_{12}, T_{13}, T_{22}, T_{23}, T_{32}, T_{33}$ can be represented by the following vectors:

$$\begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 2 \\ 1 \end{pmatrix}.$$

Thus, any $[19, 4, 12; 3]$-code is C-equivalent to the code generated by the matrix

$$\mathbf{G}_4 = \begin{pmatrix} 1 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 & 1 & 2 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 & 2 & 2 & 0 & 0 & 1 & 1 & 2 & 2 & 0 & 0 & 1 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{2.5}$$

We shall employ the following fact:

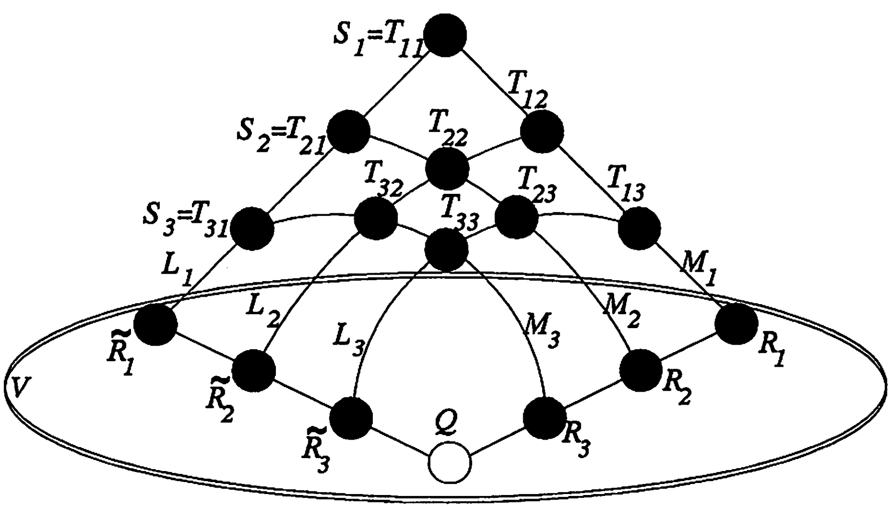
Proposition 2.7. Let F be a $\{21, 6; 3, 3\}$-minihyper as defined by (2.4). There exist six lines $L_1, L_2, L_3, M_1, M_2, M_3$, satisfying the following conditions:

C-1. *Three lines L_1, L_2, L_3 are parallel and $V \cap L_j = \{\widetilde{R_j}\}$ for $j = 1, 2, 3$.*
C-2. *Three other lines M_1, M_2, M_3 are parallel and $V \cap M_i = \{R_i\}$ for $i = 1, 2, 3$.*
C-3. *There is a unique point T_{ij} such that $M_i \cap L_j = \{T_{ij}\}$ for $i, j \in \{1, 2, 3\}$.*
C-4. *The sets $\{Q, R_1, R_2, R_3\}$ and $\{Q, \widetilde{R_1}, \widetilde{R_2}, \widetilde{R_3}\}$ are two lines in V.*

Further, three points $T_{\alpha 1}, T_{\beta 2}, T_{\gamma 3}$ (or $T_{1\alpha}, T_{2\beta}, T_{3\gamma}$) are collinear if and only if $\alpha = \beta = \gamma$.

This structure is described by Figure 1.

Figure 1. $\overline{\mathcal{F}}(1, 1, 2; 3, 3)$



Proof. We can assume w. l. o. g. that the points $Q, R_1, S_0, S_1, S_2, S_3$ correspond to the vectors

$$\begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\end{pmatrix}, \begin{pmatrix}0\\0\\1\\1\end{pmatrix}, \begin{pmatrix}0\\0\\2\\1\end{pmatrix},$$

where the vector notation still is defined by (2.1). We can further assume that $R_2 = (\nu_0 + \nu_1), R_3 = (2\nu_0 + \nu_1)$ (since the case of $R_2 = (2\nu_0 + \nu_1), R_3 = (\nu_0 + \nu_1)$ can be linearly transformed into the assumed one). Also, $\{T_{12}, T_{13}\} = \{(\nu_1 + \nu_3), (2\nu_1 + \nu_3)\}$ and we can assume w. l. o. g. that $T_{12} = (\nu_1 + \nu_3)$ and $T_{13} = (2\nu_1 + \nu_3)$.
It follows that $\{T_{22}, T_{23}\} = \{(\nu_0 + \nu_1 + \nu_2 + \nu_3), (2\nu_0 + 2\nu_1 + \nu_2 + \nu_3)\}$, and $\{T_{32}, T_{33}\} = \{(2\nu_0 + \nu_1 + 2\nu_2 + \nu_3), (\nu_0 + 2\nu_1 + 2\nu_2 + \nu_3)\}$.
Let $T_{22} = (\nu_0+\nu_1+\nu_2+\nu_3), T_{23} = (2\nu_0+2\nu_1+\nu_2+\nu_3), T_{32} = (2\nu_0+\nu_1+2\nu_2+\nu_3), T_{33} = (\nu_0+2\nu_1+2\nu_2+\nu_3)$, and let $L_j = \{\widetilde{R_j}, T_{1j}, T_{2j}, T_{3j}\}, j = 1, 2, 3$, and $M_i = R_i \oplus S_i = \{R_i, T_{i1}, T_{i2}, T_{i3}\}, i = 1, 2, 3$, where $\widetilde{R_1} = S_0, \widetilde{R_2} = (\nu_0 + \nu_2)$ and $\widetilde{R_3} = (2\nu_0 + \nu_2)$.
$\{M_i | i = 1, 2, 3\} \cup \{L_j | j = 1, 2, 3\}$ are sets of lines that satisfy conditions C-1, C-2, C-3, and C-4. The final statement of the theorem is obvious (see Figure 1). □

Definition 2.8. Let $\mathbf{G} \subset PG(t, q)$. Alternatively, the points of $\mathbf{G}$ can be viewed as the columns of a generator matrix (also denoted $\mathbf{G}$) with $t + 1$ rows of a q-ary linear block code. Let $\mathcal{L}(\mathbf{G})$ be the set of lines in $PG(t, q)$ that contain at least two points in $\mathbf{G}$. For each point $P \in PG(t, q)$, let $l(P, \mathbf{G})$ be the number of lines in $\mathcal{L}(\mathbf{G})$ that contain P. Finally, let the *line incidence distribution* $\{l_i(\mathbf{G})\}$ be defined by

$$l_i(\mathbf{G}) = |\{P \in PG(t, q) \mid l(P, \mathbf{G}) = i\}|.$$

Lemma 2.9. Let $\mathbf{G}$ be a matrix containing as columns three linearly dependent points of $PG(t, q)$,

$$P_1 = \begin{pmatrix} p_{10} \\ \vdots \\ p_{1i} \\ \vdots \\ p_{1t} \end{pmatrix}, P_2 = \begin{pmatrix} p_{20} \\ \vdots \\ p_{2i} \\ \vdots \\ p_{2t} \end{pmatrix}, P_3 = \begin{pmatrix} p_{30} = \alpha p_{10} + \beta p_{20} \\ \vdots \\ p_{3i} = \alpha p_{1i} + \beta p_{2i} \\ \vdots \\ p_{3t} = \alpha p_{1t} + \beta p_{2t} \end{pmatrix}.$$

Then a row operation on $\mathbf{G}$ transforms P_1, P_2, P_3 into three points P_1^*, P_2^*, P_3^* that are also linearly dependent.

Proof. Suppose a multiple of the i^{th} row is added to the top row. Then

$$P_1^* = \begin{pmatrix} p_{10}^* = p_{10} + \gamma p_{1i} \\ \vdots \\ p_{1i} \\ \vdots \\ p_{1t} \end{pmatrix}, P_2^* = \begin{pmatrix} p_{20}^* = p_{20} + \gamma p_{2i} \\ \vdots \\ p_{2i} \\ \vdots \\ p_{2t} \end{pmatrix}$$

while

$$P_3^* = \begin{pmatrix} p_{30}^* = (\alpha p_{10} + \beta p_{20}) + \gamma(\alpha p_{1i} + \beta p_{2i}) \\ \vdots \\ p_{3i} = \alpha p_{1i} + \beta p_{2i} \\ \vdots \\ p_{3t} = \alpha p_{1t} + \beta p_{2t} \end{pmatrix} = \begin{pmatrix} \alpha p_{10}^* + \beta p_{20}^* \\ \vdots \\ \alpha p_{1i} + \beta p_{2i} \\ \vdots \\ \alpha p_{1t} + \beta p_{2t} \end{pmatrix}.$$

□

Corollary 2.10. Let $\mathbf{G}_1$ *and* $\mathbf{G}_2$ *be generator matrices of C-equivalent codes. Then the line incidence distributions* $\{l_i(\mathbf{G}_1)\}$ *and* $\{l_i(\mathbf{G}_2)\}$ *coincide.*

Proof. This follows from Definition 2.2 and Lemma 2.9.

□

Remark 2.11. From Corollary 2.10, the line incidence is specific to a code rather than to a generator matrix for the code. Thus we shall also refer to the line incidence of a code C, $\{l_i(C)\} = \{l_i(\mathbf{G})\}$, where $\mathbf{G}$ is any generator matrix for C.

3. The [20,5,12;3]-codes.

Hill and Newton recently gave an example of a $[20, 5, 12; 3]$-code. In this section we show that codes with these parameters are *not* unique up to C-equivalence. We shall let C and $\mathbf{G}$ denote a $[20, 5, 12; 3]$-code and some generator matrix for C, respectively.

Definition 3.1. Given a linear block code, let $\{A_i\}$ and $\{B_i\}$ denote the weight distribution of the code and its dual, respectively.

Proposition 3.2. [Hill and Newton, 1988]The weight distribution of a $[20, 5, 12; 3]$*-code is*

$$A_0 = 1, A_{12} = 150, A_{15} = 72, A_{20} = 20,$$

and in particular $B_1 = B_2 = B_3 = 0$. *Hence, for any generator matrix* $\mathbf{G}$ *of a* $[20, 5, 12; 3]$*-code, it holds that any three points corresponding to columns of* $\mathbf{G}$ *are linearly independent.*

Proposition 3.3. *Let C be the code described by Hill and Newton. The line incidence distribution of C is*

$$l_2(C) = 10,\ l_3(C) = 40,\ l_4(C) = 20,\ l_5(C) = 26,\ l_6(C) = 5,\ l_{19}(C) = 20. \tag{3.1}$$

Proof. This follows by tedious but straightforward enumeration. □

In order to characterize all nonisomorphic $[20, 5, 12; 3]$-codes, we shall use Proposition 2.6 as follows: Let $Q = (\nu_0), R_1 = (\nu_1), R_2 = (\nu_0 + \nu_1), R_3 = (2\nu_0 + \nu_1), S_0 = (\nu_2), S_1 = (\nu_3), S_2 = (\nu_2 + \nu_3), S_3 = (2\nu_2 + \nu_3)$, where $(\nu_0), (\nu_1), (\nu_2), (\nu_3)$ are linearly independent points in $PG(3, 3)$. We shall in the following consider the points as column vectors as defined by (2.1).

W. l. o. g., $\mathbf{G}$ has a "1" in the first position of the first row, and "0" in the remaining positions of the first column. Deleting the first row and the first column, we obtain a generator matrix for a $[19, 4, 12; 3]$-code, which w. l. o. g. can be assumed to be on the form of (2.5):

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & a_1 & a_2 & b_1 & b_2 & c_1 & c_2 & d_1 & d_2 & e_1 & e_2 & f_1 & f_2 & g_1 & g_2 & h_1 & h_2 & i_1 & i_2 \\ 0 & 1 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 & 1 & 2 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 0 & 0 & 1 & 1 & 2 & 2 & 0 & 0 & 1 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{3.2}$$

Since $B_3 = 0$, we note that certain restrictions apply on $a_1, a_2, b_1, \ldots, i_2$. For instance, the sum of two times the second column, two times the third column and the fourth column must be nonzero, hence $2a_1 + a_2 \not\equiv 0 (mod\ 3)$. Similar arguments lead to a set of 39 restrictions on $a_1, a_2, b_1, \ldots, i_2$:

$$\begin{array}{ccc}
a_1 + 2a_2 \not\equiv 0 & a_1 + b_1 + c_1 \not\equiv 0 & a_1 + d_1 + g_1 \not\equiv 0 \\
a_1 + e_1 + i_2 \not\equiv 0 & a_1 + e_2 + i_1 \not\equiv 0 & a_1 + f_2 + h_2 \not\equiv 0 \\
a_2 + b_2 + c_2 \not\equiv 0 & a_2 + d_2 + g_2 \not\equiv 0 & a_2 + e_2 + i_2 \not\equiv 0 \\
a_2 + f_1 + h_2 \not\equiv 0 & a_2 + f_2 + h_1 \not\equiv 0 & b_1 + 2b_2 \not\equiv 0 \\
b_1 + d_2 + i_1 \not\equiv 0 & b_1 + e_2 + h_1 \not\equiv 0 & b_1 + f_1 + g_2 \not\equiv 0 \\
b_1 + f_2 + g_1 \not\equiv 0 & b_2 + d_1 + i_1 \not\equiv 0 & b_2 + d_2 + i_2 \not\equiv 0 \\
b_2 + e_1 + h_2 \not\equiv 0 & b_2 + f_1 + g_1 \not\equiv 0 & c_1 + 2c_2 \not\equiv 0 \\
c_1 + d_1 + h_2 \not\equiv 0 & c_1 + d_2 + h_1 \not\equiv 0 & c_1 + e_1 + g_2 \not\equiv 0 \\
c_1 + f_1 + i_2 \not\equiv 0 & c_2 + d_1 + h_1 \not\equiv 0 & c_2 + e_1 + g_1 \not\equiv 0 \\
c_2 + e_2 + g_2 \not\equiv 0 & c_2 + f_2 + i_1 \not\equiv 0 & d_1 + 2d_2 \not\equiv 0 \\
d_1 + e_2 + f_1 \not\equiv 0 & d_2 + e_1 + f_2 \not\equiv 0 & e_1 + 2e_2 \not\equiv 0 \\
f_1 + 2f_2 \not\equiv 0 & g_1 + 2g_2 \not\equiv 0 & g_1 + h_1 + i_2 \not\equiv 0 \\
g_2 + h_2 + i_1 \not\equiv 0 & h_1 + 2h_2 \not\equiv 0 & i_1 + 2i_2 \not\equiv 0
\end{array} \tag{3.3}$$

Observe that by deleting the second row and second column of $\mathbf{G}$, we obtain the matrix

$$\widetilde{\mathbf{G}_4} = \begin{pmatrix} 1 & a_1 & a_2 & b_1 & b_2 & c_1 & c_2 & d_1 & d_2 & e_1 & e_2 & f_1 & f_2 & g_1 & g_2 & h_1 & h_2 & i_1 & i_2 \\ 0 & 0 & 0 & 1 & 1 & 2 & 2 & 0 & 0 & 1 & 1 & 2 & 2 & 0 & 0 & 1 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{3.4}$$

which generates a $[19, 4, 12; 3]$-code. Hence, the set of columns of $S_{4,3} \backslash \widetilde{\mathbf{G}_4}$ must equal a set F constructed according to Definition 2.4, where each column $(u_0, u_1, u_2, u_3)^T$ corresponds to the point $\left(\sum_{i=0}^{3} u_i \mu_i\right)$, for some linearly independent points $(\mu_0), (\mu_1), (\mu_2), (\mu_3)$.

From Propositions 2.1 and 2.6, and from (3.4), we see that $Q = (1, 0, 0, 0) = (\mu_0)$, and V is the 2–flat generated by $(\mu_0), (\mu_1)$, and (μ_2).

Let $\mathbf{x}_i$ denote the i^{th} column of the matrix $\mathbf{G}^*$ given by

$$\mathbf{G}^* = \begin{pmatrix} a_3 & b_3 & c_3 & d_3 & e_3 & f_3 & g_3 & h_3 & i_3 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{3.5}$$

where $\{a_1, a_2, a_3\} = \{b_1, b_2, b_3\} = \cdots = \{i_1, i_2, i_3\} = \{0, 1, 2\}$. Then it follows from Propositions 2.1 and 2.6, and from (3.4), that $\{T_{11}, T_{12}, T_{13}, T_{21}, T_{22}, T_{23}, T_{31}, T_{32}, T_{33}\} = \{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_9\}$.

Let $\mathbf{z}_i$, for $i = 1, 2, \ldots, 9$, denote the vector obtained from $\mathbf{x}_i$ by deleting the first component. Then it can be shown that there are exactly 12 subsets of $\{\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_9\}$, each consisting of three vectors which are linearly dependent over $GF(3)$. These subsets are:

$\{\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3\}$	$\{\mathbf{z}_1, \mathbf{z}_4, \mathbf{z}_7\}$	$\{\mathbf{z}_1, \mathbf{z}_5, \mathbf{z}_9\}$	$\{\mathbf{z}_1, \mathbf{z}_6, \mathbf{z}_8\}$
$\{\mathbf{z}_2, \mathbf{z}_4, \mathbf{z}_9\}$	$\{\mathbf{z}_2, \mathbf{z}_5, \mathbf{z}_8\}$	$\{\mathbf{z}_2, \mathbf{z}_6, \mathbf{z}_7\}$	$\{\mathbf{z}_3, \mathbf{z}_4, \mathbf{z}_8\}$
$\{\mathbf{z}_3, \mathbf{z}_5, \mathbf{z}_7\}$	$\{\mathbf{z}_3, \mathbf{z}_6, \mathbf{z}_9\}$	$\{\mathbf{z}_4, \mathbf{z}_5, \mathbf{z}_6\}$	$\{\mathbf{z}_7, \mathbf{z}_8, \mathbf{z}_9\}$

In order to find the correspondence between the set $\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_9\}$ and the set $\{T_{ij}\}$ in Figure 1, we consider all 3×3 arrays that satisfy the following conditions:

1. Each array consists of 9 vectors $\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_9$.
2. Each row consists of three vectors that are linearly dependent.
3. Each column consists of three vectors that are linearly dependent.

There are exactly six (nonequivalent) arrays that satisfy these three conditions. These are:

$$\mathbf{A}_1 = \begin{pmatrix} z_1 & z_2 & z_3 \\ z_4 & z_5 & z_6 \\ z_7 & z_8 & z_9 \end{pmatrix} \quad \mathbf{A}_2 = \begin{pmatrix} z_1 & z_2 & z_3 \\ z_5 & z_6 & z_4 \\ z_9 & z_7 & z_8 \end{pmatrix} \quad \mathbf{A}_3 = \begin{pmatrix} z_1 & z_2 & z_3 \\ z_6 & z_4 & z_5 \\ z_8 & z_9 & z_7 \end{pmatrix}$$

$$\mathbf{A}_4 = \begin{pmatrix} z_1 & z_4 & z_7 \\ z_5 & z_8 & z_2 \\ z_9 & z_3 & z_6 \end{pmatrix} \quad \mathbf{A}_5 = \begin{pmatrix} z_1 & z_4 & z_7 \\ z_6 & z_9 & z_3 \\ z_8 & z_2 & z_5 \end{pmatrix} \quad \mathbf{A}_6 = \begin{pmatrix} z_1 & z_5 & z_9 \\ z_6 & z_7 & z_2 \\ z_8 & z_3 & z_4 \end{pmatrix}$$

Observe that each of these arrays represents a set of six equations (of rank five). The solutions of these equation sets can be expressed in terms of four parameters, say, $\alpha, \beta, \gamma, \delta$. For example, the solutions to the first equation set be expressed as

$$\mathbf{A}_1 = \begin{pmatrix} \alpha & \beta & 2\alpha + 2\beta \\ \gamma & \delta & 2\gamma + 2\delta \\ 2\alpha + 2\gamma & 2\beta + 2\delta & \alpha + \beta + \gamma + \delta \end{pmatrix}.$$

Since this set of solutions also represents the ordered set $(a_3, b_3, \dots, i_3)$, we can assume (by performing suitable row operations on the matrix $\mathbf{G}^*$ in (3.5)) that $\alpha = \beta = \gamma = 0$. Thus, the solution of the first equation set is simplified to

$$\mathbf{A}_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & \delta & 2\delta \\ 0 & 2\delta & \delta \end{pmatrix}.$$

Further, by multiplying the first row of $\mathbf{G}^*$ in (3.5) by δ, we can assume that $\delta = 1$ (since we are only interested in nonzero solutions).

Thus, the vector $(a_3, b_3, \dots, i_3)$ can be assumed to be on one of the following forms:

Case	a_3	b_3	c_3	d_3	e_3	f_3	g_3	h_3	i_3
I	0	0	0	0	1	2	0	2	1
II	0	0	0	0	2	1	2	0	1
III	0	0	0	0	2	1	1	2	0
IV	0	0	2	0	2	0	0	1	1
V	0	0	2	0	1	1	0	2	0
VI	0	0	2	0	0	2	1	1	0

It is a simple matter to check these six cases against the conditions (3.3).

Applying a *simple* bactracking search, in case I we get the nine solutions $\mathbf{v}_1, \ldots, \mathbf{v}_9$, where

	a_1	a_2	b_1	b_2	c_1	c_2	d_1	d_2	e_1	e_2	f_1	f_2	g_1	g_2	h_1	h_2	i_1	i_2
$\mathbf{v}_1$:	2	1	1	2	1	2	1	2	2	0	1	0	1	2	1	0	2	0
$\mathbf{v}_2$:	1	2	2	1	2	1	1	2	2	0	1	0	2	1	0	1	0	2
$\mathbf{v}_3$:	1	2	2	1	2	1	2	1	0	2	0	1	1	2	1	0	2	0
$\mathbf{v}_4$:	2	1	1	2	2	1	2	1	0	2	1	0	1	2	1	0	0	2
$\mathbf{v}_5$:	1	2	2	1	1	2	2	1	0	2	1	0	2	1	0	1	2	0
$\mathbf{v}_6$:	2	1	1	2	2	1	1	2	2	0	0	1	2	1	0	1	2	0
$\mathbf{v}_7$:	1	2	1	2	2	1	2	1	2	0	0	1	2	1	1	0	0	2
$\mathbf{v}_8$:	2	1	2	1	1	2	1	2	0	2	1	0	2	1	1	0	0	2
$\mathbf{v}_9$:	2	1	2	1	1	2	2	1	2	0	0	1	1	2	0	1	2	0

Let $\mathbb{G}_1$ be the family of matrices on the form (3.2) with one of the vectors $\mathbf{v}_i, i = 1, \ldots, 9$ in the place of $(a_1, a_2, \ldots, i_2)$, and let $\mathbb{C}_1$ be the family of codes generated by some $\mathbf{G} \in \mathbb{G}_1$. It can be verified that all codes in $\mathbb{C}_1$ have minimum distance 12.

There are no solutions in cases II, III, IV, and V, but in case VI we get the solutions

	a_1	a_2	b_1	b_2	c_1	c_2	d_1	d_2	e_1	e_2	f_1	f_2	g_1	g_2	h_1	h_2	i_1	i_2
$\mathbf{u}_1$:	1	2	1	2	0	1	1	2	2	1	0	1	2	0	2	0	2	1
$\mathbf{u}_2$:	2	1	2	1	1	0	2	1	1	2	1	0	0	2	0	2	1	2

Let $\mathbb{G}_2$ be the family of matrices on the form (3.2) with one of the vectors $\mathbf{u}_i, i = 1, 2$ in the place of $(a_1, a_2, \ldots, i_2)$, and let $\mathbb{C}_2$ be the family of codes generated by some $\mathbf{G} \in \mathbb{G}_2$. Again, it can be verified that all codes in $\mathbb{C}_2$ have minimum distance 12.

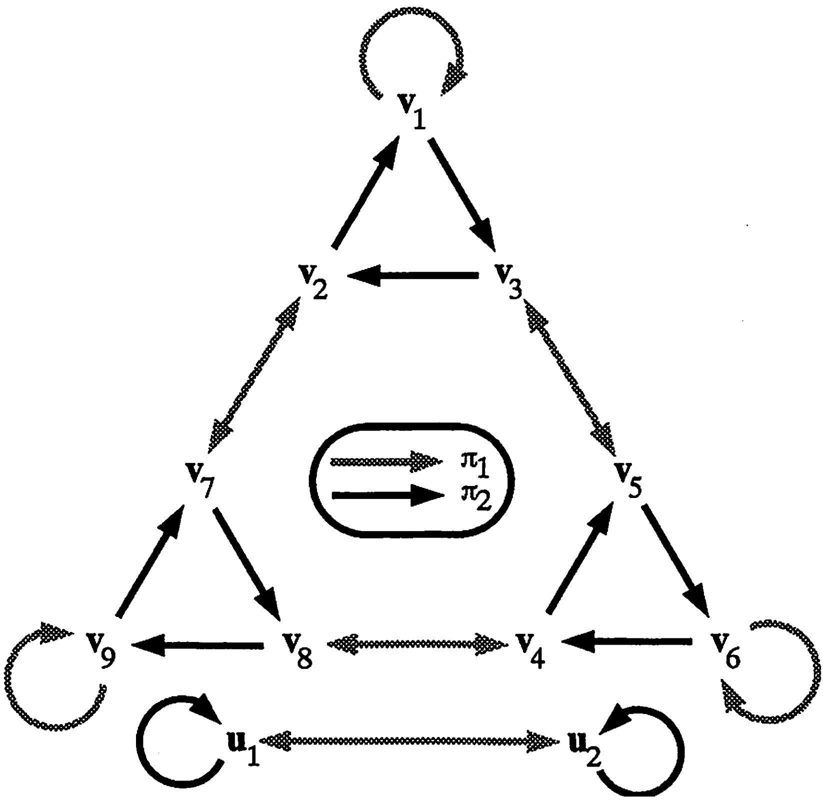
Theorem 3.4. *For $i \in \{1, 2\}$, let C_1 and C_2 be two codes in $\mathbb{C}_i$. Then C_1 and C_2 are C-equivalent.*

Proof. Let $\overline{C}_4$ be the code generated by the rightmost 18 columns of matrix $\mathbf{G}_4$ of (2.5). Let π_1 and π_2 be two permutations of 18–tuples such that

$$\pi_1 = (1\ \ 2\ \ 7\ \ 8\ \ 13\ \ 14\ \ 3\ \ 4\ \ 9\ \ 10\ \ 15\ \ 16\ \ 5\ \ 6\ \ 11\ \ 12\ \ 17\ \ 18)$$
$$\pi_2 = (13\ \ 14\ \ 15\ \ 16\ \ 18\ \ 17\ \ 1\ \ 2\ \ 4\ \ 3\ \ 5\ \ 6\ \ 7\ \ 8\ \ 10\ \ 9\ \ 12\ \ 11).$$

(For instance, π_2 maps the vector $\mathbf{v} = (v_1, v_2, v_3, \ldots, v_{18})$ into $\mathbf{v}\pi_2 = (v_{13}, v_{14}, v_{15}, \ldots, v_{11})$). It is easy to verify that π_1 and π_2 are automorphisms of $\overline{C}_4$. Applying these permutations to the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_9$ (or $\mathbf{u}_1, \mathbf{u}_2$), and adding a suitable linear combination of the three lower rows of $\mathbf{G}_4$, we find that all the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_9$ (resp. $\mathbf{u}_1, \mathbf{u}_2$) generate C-equivalent codes, as shown in Figure 2:

Figure 2. Action of the permutations π_1 and π_2.



□

Theorem 3.5. Let $C_1 \in \mathbb{C}_1$ and $C_2 \in \mathbb{C}_2$. Then C_1 and C_2 are not *C-equivalent.*

Proof. The line incidence of C_1 is given by (3.1), while the line incidence of C_2 is

$$l_1(C_2) = 10, \; l_4(C_2) = 90, \; l_{10}(C_2) = 1, \; l_{19}(C_2) = 20.$$

By Corollary 2.10, C_1 and C_2 are C-nonequivalent.

□

References

J. H. Griesmer, "A bound for error-correcting codes", *IBM Journal of Res. and Dev.*, vol. 4(5) pp.532–542, 1960.

N. Hamada and T. Helleseth, "A characterization of some $\{3v_2, 3v_1; t, q\}$-minihypers and some $\{2v_2 + v_{\gamma+1}, 2v_1 + v_\gamma; t, q\}$-minihypers ($q = 3$ or $4, 2 \leq \gamma < t$) and its applications to error-correcting codes", *Bulletin of Osaka Women's University*, vol. 27 pp.49–107, 1990.

N. Hamada, "Characterization of min·hypers in a finite projective geometry and its applications to error-correcting codes", *Bulletin of Osaka Women's University*, vol. 24 pp.1–24, 1987.

R. Hill and D. E. Newton, "Some optimal ternary codes", *ARS Combinatoria*, vol. Twenty-Five A pp.61–72, 1988.

G. Solomon and J. J. Stiffler, "Algebraically punctured cyclic codes", *Inform. Contr.*, vol. 8 pp.170–179, 1965.

N. Hamada is with Department of Applied Mathematics, Osaka Women's University, Sakai, Osaka, Japan 590. T. Helleseth (e-mail: torh@eik.ii.uib.no) and Ø. Ytrehus (e-mail: oyvind@eik.ii.uib.no) are with Department of Informatics, University of Bergen, Thormøhlensgt. 55, N-5008 Bergen, Norway.

Financial support: This research was supported partially by Grant-in-Aid for Scientific Research of the Ministry of Education, Science and Culture under Contract Numbers 403–4005–02640182, and partially by the Norwegian Research Council for Science and the Humanities (NAVF).