A general method of constructing error correcting binary group codes is obtained. A binary group code with k information places and n places is called an \( (n,k) \) code. Explicit method of constructing \( t \)-error correcting \( (n,k) \) codes are given for \( n = 2^m - 1 \) and \( k = 2^m - 1 - mt \) for general \( t \). An example is worked out to illustrate the method of construction.
ON A CLASS OF ERROR CORRECTING BINARY GROUP CODES*

by R. C. Bose and D. K. Ray-Chaudhuri
University of North Carolina and Case Institute of Technology

1. Introduction. Consider a binary channel which can transmit either of two symbols 0 or 1. However, due to the presence of 'noise' a transmitted zero may sometimes be received as 1, and a transmitted 1 may sometimes be received as 0. When this happens we say that there is an error in transmitting the symbol. The symbols successively presented to the channel for transmission constitute the 'input' and the symbols received constitute the 'output'.

A v-letter n-place binary signalling alphabet $A_n$ may be defined as a set of $v$ distinct sequences $\alpha_0, \alpha_1, \ldots, \alpha_{v-1}$ of $n$ binary digits. The individual sequences may be called the letters of the alphabet. Given a set of $v$ distinct messages, we get an encoder $E_{n,v}$ by setting up a (1,1) correspondence between the messages and the letters of the alphabet. To transmit a message over the channel the $n$ individual symbols of the corresponding letter of the alphabet are presented to the channel in succession. The output is then an n-place binary sequence belonging to the set $B_n$ of all possible binary sequences. A decoder $D_{n,v}$ is obtained by partitioning $B_n$ into $v$ disjoint sets $S_1, S_2, \ldots, S_v$ and setting up a correspondence between these subsets and the letters of the alphabet so that if a sequence belonging to $S_i$ is received as an output, it is read as the letter $\alpha_i$ and interpreted as the corresponding message. The encoder $E_{n,v}$ together with the decoder $D_{n,v}$ constitute a binary n-place code.

* This research was supported by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command, under Contract No. AF 49(638)-213. Reproduction in whole or in part is permitted for any purpose of the United States Government.
Each sequence of $B_n$ can be regarded as an $n$-vector with elements from the Galois field $GF(2)$. The addition of these vectors may then be defined in the usual manner, the sum of two vectors being obtained by adding the corresponding elements (mod 2). For example, if $n = 6$ and $\gamma_1 = (110011)$ and $\gamma_2 = (101001)$ then $\gamma_1 + \gamma_2 = (011010)$. Clearly the set $B_n$ of all binary $n$-place sequences forms a group under vector addition. The weight $w(\gamma)$ of any sequence is defined as the number of units in the sequence. Thus in the example considered $w(\gamma_1) = 4$, $w(\gamma_2) = 3$.

The Hamming distance $d(\gamma_1, \gamma_2)$ between two sequences $\gamma_1$ and $\gamma_2$ is defined as the number of places in which $\gamma_1$ and $\gamma_2$ do not match (Hamming, 1950). Clearly $d(\gamma_1, \gamma_2) = w(\gamma_1 + \gamma_2)$. In the example $d(\gamma_1, \gamma_2) = 3 = w(\gamma_1 + \gamma_2)$.

The Hamming distance satisfies the three conditions for a metric, viz.

(i) $d(\gamma) = 0$ if and only if $\gamma$ is the null vector,

(ii) $d(\gamma_1, \gamma_2) = d(\gamma_2, \gamma_1),$

(iii) $d(\gamma_1, \gamma_2) + d(\gamma_2, \gamma_3) \geq d(\gamma_1, \gamma_3)$.

Let the letter $\alpha_i$ of the alphabet $A_n$ be transmitted over the channel. Let $\epsilon_i$ be the vector which has units in those places, where an error occurs in transmitting a symbol of $\alpha_i$. Then $\epsilon_i$ is the noise vector. The output received is the sequence $\alpha_i + \epsilon_i$, and the number of errors is $w(\epsilon_i)$. The code is said to be $t$-error correcting if $\alpha_i + \epsilon_i$ belongs to $S_i$ whenever $w(\epsilon_i) \leq t$ ($i = 1, 2, \ldots, v$). It is clear that under these circumstances if there are $t$ or a lesser number of errors in transmitting a letter $\alpha_i$, the received message will be correctly interpreted.

A particularly important class of codes has been studied by Slepian (1956). For this class $v = 2^k$ and the letters of the alphabet $A_n$ form a
The null sequence is the unit element of $B_n$, and must also belong to $A_n$. We shall suppose without loss of generality that $\alpha_0 = (0,0,\ldots,0)$. Slepian's decoder may be described as follows: If $r = n-k$, then the group $B_n$ can be partitioned into $2^r$ cosets with respect to the subgroup $A_n$. The coset containing a particular sequence $\beta$ consists of the sequences

$$\alpha_0 + \beta, \alpha_1 + \beta, \ldots, \alpha_{v-1} + \beta.$$ 

In the $j$-th coset we can choose a sequence $\beta_j$ whose weight does not exceed the weight of any other sequence in the coset, and call it the coset leader. Let $\beta_0, \beta_1, \ldots, \beta_{u-1}, (u = 2^r)$ be the coset leaders, where $\beta_0 = \alpha_0$ is the null sequence and leader of the 0-th coset $A_n$. Let $S_j$ be the set of sequences $\alpha_j + \beta_0, \alpha_j + \beta_1, \ldots, \alpha_j + \beta_{u-1} (j = 0,1,\ldots,v-1)$. Then the decoder is obtained by partitioning $B_n$ into $S_0, S_1, \ldots, S_{v-1}$ and setting up the rule that if the sequence received as an output belongs to $S_j$, it is read as the letter $\alpha_j$. The code thus obtained may be called an $(n,k)$ binary group code. It is clear that a transmitted message will be correctly interpreted if and only if the error vector happens to be a coset leader. Hence a necessary and sufficient condition for the code to be $t$-error correcting is that if $\beta$ is any $n$-place binary sequence for which $w(\beta) \leq t$, then $\beta$ is a coset leader. The following lemma is then easy to deduce.

**Lemma 1.** The necessary and sufficient condition for an $(n,k)$ binary group code to be $t$-error correcting is that each letter of the alphabet except the null letter has weight $2t+1$ or more.

**Proof:** Let $\alpha_0, \alpha_1, \ldots, \alpha_{v-1}$ be the letters of the alphabet. Let $\beta$ be any $n$-place sequence for which $w(\beta) \leq t$. Let $(\alpha_j, \beta)$ denote the
number of positions simultaneously occupied by unities in both $\alpha_1$ and $\beta$. Then

$$\alpha_1, \beta \leq w(\beta) \leq t$$

(1.1)

and

$$d(\alpha_1, \beta) = w(\alpha_1, \beta) = w(\alpha_1) + w(\beta) - 2(\alpha_1, \beta).$$

Hence

$$w(\alpha_1, \beta) - w(\beta) \geq w(\alpha_1) - 2t.$$  

(1.3)

The necessary and sufficient condition for $\beta$ to be the leader of the coset in which it occurs is that the left hand side of (1.3) is non-zero positive for $i = 0, 1, \ldots, v-1$. The lemma follows.

Since the $v = 2^k$ messages can be transmitted by a $k$-place binary code if there is no possibility of error, the number $r = n-k$ is called the redundancy for an $(n, k)$ binary group code. In constructing a $t$-error correcting $(n, k)$ binary group code for given $n$ and $t$ one would like to maximize $k$ (i.e., maximize the number of different messages that it is possible to transmit). Varšemov (1957) has shown that if $k$ satisfies the inequality

$$2^{2t-1} + (2t-2) + \ldots + (2t-2) + (2t-1) + (2t-1) < 2^r$$

(1.4)

where

$$\sum_{r=1}^{q} \binom{r}{1}, \binom{r}{2}, \ldots, \binom{r}{q}$$

(1.5)

then a $t$-error correcting $(n, k)$ group code exists.

The main result of the present paper is the following: If $n = 2^m - 1$, then there exists a $t$-error correcting $(n, k)$ binary group code with $k \geq 2^m - 1 - mt$.

The method of proof is constructive and is illustrated by considering the case $n = 15$, $t = 3$, for which a 3-error correcting $(15, 5)$ binary group code is explicitly obtained.
As an example of comparison between Varşamov's result and our theorem consider the case \( n = 31 \). Varşamov's result then shows that a 2-error correcting binary group code can be obtained with \( k = 18 \), and a 3-error correcting binary group code can be obtained with \( k = 13 \) but is inconclusive for larger values of \( k \). Our method, however, gives an explicit construction for a 2-error correcting binary group code with \( k = 21 \), and a 3-error correcting binary group code with \( k = 16 \).

The following table gives some of the values of \( n, k \) and \( t \) for which a \( t \)-error correcting \((n,k)\) binary group code can be constructed by our method. The transmission rate \( R = k/n \) is also given.

<table>
<thead>
<tr>
<th>( t )</th>
<th>( n )</th>
<th>( k )</th>
<th>( R )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>11</td>
<td>4</td>
<td>.36</td>
</tr>
<tr>
<td>2</td>
<td>15</td>
<td>7</td>
<td>.47</td>
</tr>
<tr>
<td>2</td>
<td>31</td>
<td>21</td>
<td>.68</td>
</tr>
<tr>
<td>2</td>
<td>63</td>
<td>51</td>
<td>.81</td>
</tr>
<tr>
<td>2</td>
<td>127</td>
<td>113</td>
<td>.89</td>
</tr>
<tr>
<td>3</td>
<td>15</td>
<td>5</td>
<td>.33</td>
</tr>
<tr>
<td>3</td>
<td>31</td>
<td>16</td>
<td>.52</td>
</tr>
<tr>
<td>3</td>
<td>63</td>
<td>45</td>
<td>.71</td>
</tr>
<tr>
<td>3</td>
<td>127</td>
<td>106</td>
<td>.83</td>
</tr>
<tr>
<td>4</td>
<td>63</td>
<td>39</td>
<td>.64</td>
</tr>
<tr>
<td>4</td>
<td>127</td>
<td>99</td>
<td>.78</td>
</tr>
<tr>
<td>5</td>
<td>127</td>
<td>92</td>
<td>.72</td>
</tr>
</tbody>
</table>

2. We shall now prove a theorem which gives a necessary and sufficient condition for the existence of a \( t \)-error correcting \((n,k)\) group code.
Theorem 1. The necessary and sufficient condition for the existence of a $t$-error correcting $(n,k)$ binary group code is the existence of a matrix $A$ of order $nxr$ and rank $r = n-k$ with elements from $GF(2)$, such that any set of $2t$ row vectors from $A$ are independent.

Proof of sufficiency. The matrix $A$ has the property $(P_{2t})$ that any $2t$ row vectors of $A$ are independent. Clearly $r \geq 2t$. The property $(P_{2t})$ is invariant under the following operations: (i) interchange of two rows or columns and (ii) replacement of the $i$-th column by the sum of $i$-th and $j$-th column, $i \neq j$. By these operations $A$ can be transformed to the matrix

$$A^* = \begin{bmatrix} I_r \\ C \end{bmatrix}$$

where $A^*$ has the property $(P_{2t})$, $I_r$ is the unit matrix of order $r$, and $C$ is a matrix of order $kxr$. Consider the matrix

$$C^* = \left[ C, I_k \right].$$

Then $C^*$ is of order $kxm$. We shall show that the $k$ rows of $C$ (under vector addition (mod 2)) are generators of a group $G$ of order $2^k$ such that if $\alpha$ is any arbitrary (non-null) element of $G$, then $w(\alpha) \geq 2t+1$. Let $\alpha$ be the sum of any $d$ row vectors of $C^*$, $d \leq k$. We can write $\alpha = (\gamma, \epsilon)$, where $\gamma$ is the part coming from $C$ and $\epsilon$ the part coming from $I_k$. Now $w(\alpha) = w(\gamma) + w(\epsilon) = w(\gamma) + d$. Hence $w(\alpha) \geq 2t+1$ if $d > 2t$. Suppose $d \leq 2t$. If $w(\alpha) < 2t+1$, then $w(\gamma) \leq 2t-d$. Let $w(\gamma) = c$. There are exactly $c$ positions in $\gamma$ which are occupied by unity. Corresponding to each such position we can find a row vector of $I_r$ which has unity in this position (and zero in all other positions). Then these $c$ vectors of $I_r$ together with the $d$ row vectors of $C$ whose sum is $\gamma$, constitute a
set of c+d vectors which are dependent. Since c+d ≤ 2t, this contradicts the fact that A* has the property \((P_{2t})\). Thus the weight of any nonnull element of G is greater than or equal to 2t+1. It follows from Lemma 1 that the sequences of the subgroup generated by the k rows of C* form the alphabet of a t-error correcting \((n,k)\) group code.

**Proof of necessity.** Suppose there exists a t-error correcting \((n,k)\) binary group code. We can then find a set of \(k\) \(n\)-place binary sequences, or \(n\)-vectors with elements from \(GF(2)\), which under addition generate the group of sequences which constitute the letters of the alphabet. By Lemma 1 if \(\alpha\) is a sequence of this group \(w(\alpha) ≥ 2t+1\). Consider the \(k \times m\) matrix \(C^*\) whose row vectors are given by these sequences. If we interchange any two rows or columns of \(C^*\), or replace the \(i\)-th row of \(C^*\) by the sum of the \(i\)-th and the \(j\)-th row \((i ≠ j)\), the transformed matrix still retains the property that its rows generate under addition a group, each sequence of which has weight \(2t+1\) or more. Hence we can without loss of generality take \(C^*\) in the canonical form \((2.2)\) where \(C\) is of order \(r \times k\) and \(I_k\) is the unit matrix of order \(k\). By retracing the arguments used in proving the first part of the theorem, we see that the matrix \(A^*\) of order \(n \times r\), given by \((2.1)\), has the property that any two \(2t\) row vectors are independent. This proves that the condition of the theorem is necessary.

**Corollary 1.** The existence of a t-error correcting \((n,k)\) binary group code implies the existence of a t-error correcting \((n-c, k-c)\) binary group code, \(0 < c < k\).

If in the matrix \(C^*\) given by \((2.2)\) we delete the last \(c\) rows and the last \(c\) columns, we get a matrix
of order (k-c) x (n-c), the rows of which generate a group for which each nonnull element is of weight 2t+1 or more. The rows of $C^*_1$ generate the alphabet of the required code.

Let $V_r$ denote the vector space of all r-vectors whose elements belong to $GF(2)$. One may then ask the following question. What is the maximum number of vectors in a set $E$ chosen from $V_r$, such that any 2t distinct vectors from $E$ are independent. This number may be denoted $n_{2t}(r)$, and the problem of finding the set $E$ may be called the packing problem (of order 2t) for $V_r$. For a given $t$, $n_{2t}(r)$ is a monotonically increasing function of $r$.

Let $k = k_t(n)$ denote the maximum value of $k$ such that a $t$-error correcting $(n, k)$ binary group code for given $t$ and $n$ exists. We can then state the following.

**Theorem 2.** If $n_{2t}(r) > n > n_{2t}(r-1)$, then $k_t(n) = n - r$.

From Theorem 1 there exists a $t$-error correcting $(n_{2t}(r), n_{2t}(r) - r$ binary group code. Taking $c = n_{2t}(r) - n$ in Corollary 1, there exists a $t$-error correcting $(n, n-r)$ group code. But a $t$-error correcting $(n, n-r+1)$ binary group code cannot exist, since from Theorem 1 its existence would imply that $n_{2t}(r-1) > n$. Hence $k_t(n) = n - r$ is the maximum value of $k$ for which a $t$-error correcting $(n, k)$ binary group code exists.

Thus the problem of finding a $t$-error correcting n-place binary group code, with the maximum transmission rate $k/n$, is equivalent to determining the smallest $r$ for which there exists a set of $n$ or more distinct vectors of $V_r$, such that any 2t distinct vectors from the set are independent.
3. The theorem to be proved in the next section depends upon the following lemma.

**Lemma 2.** If \( x_1, x_2, \ldots, x_{\ell} \) are different non-zero elements of the Galois field \( \text{GF}(2^m) \), then the equations

\[
(3.1) \quad x_1^{2i-1} + x_2^{2i-1} + \ldots + x_{\ell}^{2i-1} = 0, \quad i = 1, 2, \ldots, t
\]

cannot simultaneously hold if \( \ell \leq 2t \).

Suppose if possible the equations (3.1) simultaneously hold. Let

\[
(3.2) \quad x^{\ell} + p_1 x^{\ell-1} + p_2 x^{\ell-2} + \ldots + p_{\ell} = 0
\]

be the algebraic equation whose roots are \( x_1, x_2, \ldots, x_{\ell} \). Then \( p_j \) belongs to \( \text{GF}(2^m) \) and is the sum of the products of the roots taken \( j \) at a time \( (j = 1, 2, \ldots, \ell) \). We define \( s_j \) as the sum of the \( j \)-th powers of the roots. For a field of characteristic 2 the well known relations between the symmetric functions \( s_j \) and \( p_j \) become (Levi, 1942, p. 147),

\[
(3.3) \begin{align*}
& s_1 + \delta_1 p_1 = 0 \\
& s_2 + p_1 s_1 + \delta_2 p_2 = 0 \\
& s_3 + p_1 s_2 + p_2 s_1 + \delta_3 p_3 = 0 \\
& \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \\
& s_{\ell} + p_1 s_{\ell-1} + p_2 s_{\ell-2} + \cdots + \delta_{\ell} p_{\ell} = 0
\end{align*}
\]

where \( \delta_i = 0 \) or 1 according as \( i \) is even or odd. From equations (3.1) \( s_j = 0 \) when \( j \) is odd \((j < 2t)\). It then follows from (3.3) that \( s_j = 0 \) if \( j \) is even \((j \leq \ell)\) and \( p_j = 0 \) if \( j \) is odd \((j \leq \ell)\).

**Case I.** If \( \ell \) is odd then \( p_{\ell} = x_1 x_2 \ldots x_{\ell} \neq 0 \), since \( x_1, x_2, \ldots, x_{\ell} \) are non-zero. This is a contradiction.

**Case II.** If \( \ell \) is even, say \( \ell = 2c \), the equation (3.2) becomes

\[
(3.4) \quad x^{2c} + p_2 x^{2c-2} + \ldots + p_{2c} = 0
\]
(3.5) \[ (x^0 + q_1 x^{c-1} + \ldots + q_c)^2 = 0 \]

where \( q_j \) is the unique square root of \( p_{2j} \) in \( GF(2^m) \). Hence (3.2) cannot have more than \( c \) distinct roots, which again is a contradiction, since \( x_1, x_2, \ldots, x_f \) are distinct by hypothesis.

Hence the lemma is true whether \( f \) is odd or even.

4. Let \( V_m \) be the vector space of \( m \)-vectors with elements from \( GF(2) \). We can institute a correspondence between the vector \( \alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) \) of \( V_m \) and the element \( a_0 + a_1 x + \ldots + a_{m-1} x^{m-1} \) of \( GF(2^m) \), where \( x \) is a given primitive element of the field. This is a (1,1) correspondence in which the null vector \( \alpha_0 \) of \( V_m \) corresponds to the null element of \( GF(2^m) \), and the sum of any two vectors of \( V_m \) corresponds to the sum of the corresponding elements of \( V_m \). We can therefore identify the vector \( \alpha \) of \( V_m \) and the corresponding element of \( GF(2^m) \).

This in effect defines a multiplication of the vectors of \( V_m \) and converts it into a field. In particular we can speak of powers of any vector.

Let \( V_{mt} \) be the vector space of all \( mt \)-vectors with elements from \( GF(2) \). To any vector \( \alpha_i \) of \( V_m \) there corresponds a unique vector \( \alpha_i^* \) of \( V_{mt} \) defined by

\[ (4.1) \quad \alpha_i^* = (\alpha_i, \alpha_i^3, \ldots, \alpha_i^{2t-1}) \]

though the converse is true.

There are \( n = 2^m - 1 \) distinct nonnull vectors in \( V_m \). Let

\[ (4.2) \quad M^* = \begin{bmatrix} \alpha_1, \alpha_1^3, \ldots, \alpha_1^{2t-1} \\ \alpha_2, \alpha_2^3, \ldots, \alpha_2^{2t-1} \\ \vdots & \vdots & \vdots \\ \alpha_n, \alpha_n^3, \ldots, \alpha_n^{2t-1} \end{bmatrix} \]
be the n×m matrix, which has for row vectors the corresponding vectors \( \alpha_1^*, \alpha_2^*, \ldots, \alpha_n^* \). We shall show that \( M^* \) has the property \((P_{2t})\) that any of \( 2t \) distinct row vectors belonging to \( M^* \) are independent. For this it is sufficient that the sum of any \( \ell \) row vectors of \( M^* \), \( \ell \leq 2t \), is nonnull. This is ensured by Lemma 2, since \( \alpha_1 \) can also be regarded as elements of \( \text{GF}(z^m) \).

Now rank \( (M^*) \leq mt \). Since there is essentially only one Galois field \( \text{GF}(z^m) \), this rank is a definite function of \( m \) and \( t \) and will be denoted by \( R(m,t) \). When \( R(m,t) < mt \), we can choose \( R(m,t) \) independent columns of \( M^* \), and delete the other columns dependent on them. The matrix \( A \) so obtained has still the property \((P_{2t})\). Using Theorem 1 we have

**Theorem 3.** If \( n = z^m - 1 \), we can obtain \( t \)-error correcting \((n,k)\) binary group code where \( k = z^m - 1 - R(m,t) \geq z^m - 1 - mt \).

\( t \)-error correcting \((n,k)\) binary group codes when \( n \) is not of the form \( z^m - 1 \) can be deduced from those obtainable from Theorem 3, by using Corollary 1 of Theorem 1. Stronger results than those which can be obtained in this way will be given in a subsequent communication.

5. The proofs of the theorems in sections 2 and 4 are constructive in the sense that they give an actual procedure for obtaining the required codes. We shall illustrate the procedure to be followed by taking the case \( m = 4, t = 3 \). Then \( n = 15 \) and the rank \( R(m,t) \) turns out to be 10. We thus obtain a 3-error correcting \((15,5)\) group code. The roots of the equation

\[(5.1) \quad x^4 = x + 1\]
are primitive elements of $GF(2^4)$, (Carmichael, 1937, p. 262). Using (5.1) the non-zero elements of $GF(2^4)$ can be expressed in two equivalent forms (i) as powers of the primitive element $x$ or (ii) as polynomials in $x$ of degree 3 or less. We thus have the following table of the 15 non-zero elements or vectors.

$$
\begin{align*}
x^0 &= 1 & = (1,0,0,0) &= \alpha_1 \\
x &= x & = (0,1,0,0) &= \alpha_2 \\
x^2 &= x^2 & = (0,0,1,0) &= \alpha_3 \\
x^3 &= x^3 & = (0,0,0,1) &= \alpha_4 \\
x^4 &= 1 + x & = (1,1,0,0) &= \alpha_5 \\
x^5 &= x + x^2 & = (0,1,1,0) &= \alpha_6 \\
x^6 &= x^2 + x^3 & = (0,0,1,1) &= \alpha_7 \\
x^7 &= 1 + x + x^3 & = (1,1,0,1) &= \alpha_8 \\
x^8 &= 1 + x^2 & = (1,0,1,0) &= \alpha_9 \\
x^9 &= x + x^3 & = (0,1,0,1) &= \alpha_{10} \\
x^{10} &= 1 + x + x^2 & = (1,1,1,0) &= \alpha_{11} \\
x^{11} &= x + x^2 + x^3 & = (0,1,1,1) &= \alpha_{12} \\
x^{12} &= 1 + x + x^2 + x^3 & = (1,1,1,1) &= \alpha_{13} \\
x^{13} &= 1 + x^2 + x^3 & = (1,0,1,1) &= \alpha_{14} \\
x^{14} &= 1 + x^3 & = (1,0,0,1) &= \alpha_{15}
\end{align*}
$$

In obtaining the powers of the elements it should be remembered that each non-zero element of $GF(2^m)$ satisfies $x^{2^m-1} = 1$. Since $m = 4$ we have

$$x^{15} = 1.$$ 

Thus for example
\[ \alpha_7^3 = (x^6)^3 = x^{18} = x^3 = (0,0,0,1) = \alpha_4 \]
\[ \alpha_7^5 = (x^6)^5 = x^{30} = x^0 = (1,0,0,0) = \alpha_1. \]

It is now easy to calculate the matrix \( M^* \) given by (4.2). For example, the seventh row is \( (\alpha_7, \alpha_7^3, \alpha_7^5) \) or \( (0\ 0\ 1\ 1,\ 0\ 0\ 0\ 1,\ 1\ 0\ 0\ 0) \). Thus

\[
M^* = \begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0
0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0
1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0
0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0
1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0
1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0
\end{bmatrix}
\]

where the vertical divisions separate the parts coming from \( \alpha, \alpha_7^3 \) and \( \alpha_7^5 \).

From \( M^* \) we can drop the last null column and the 11-th column which is identical with the 10-th. The 10x15 matrix of rank 10 so obtained we can take as the matrix \( A \) of Theorem 1. From what has been shown in section 4, this matrix has the property \( P(6) \) that any 6 row vectors are independent. Using operations (i) and (ii) of section 2, we can then transform \( A \) to \( A^* \) where

\[
A^* = \begin{bmatrix}
I_{10} \\
\mathbf{c}
\end{bmatrix}
\]
where $I_{10}$ is the unit matrix of order 10, and $C$ is the $5 \times 10$ matrix given by

\[
C = \begin{bmatrix}
1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1
\end{bmatrix}.
\]

Taking

\[
C^* = \left[ C, I_{15} \right]
\]

we have a matrix of order $5 \times 15$ whose rows generate under vector addition (mod 2), the group of 32 sequences which constitute the letters of the alphabet of the required 3-error correcting $(15, 5)$ binary group alphabet. It is easy to verify that of the 31 nonnull sequences 15 have weight 7, 15 have weight 8 and one has weight 15, which checks with Lemma 1.

References


