TAMKANG JOURNAL OF MATHEMATICS
Volume 36, Number 1, 17-31, Spring 2005

THE CONSTRUCTION OF A 4EC-AUED CODE

HOW GUAN AUN AND KEAN KIM LEONG

Abstract. In this paper, we construct a constant weight code based on the idea of Bose and Rao [2] and M. C. Lin [6]. This code can be used for correcting 4 symmetric errrors and simultaneously detecting all unidirectional errors. The code has size 70 and the information rate is 0.27.

1. Introduction

Error correcting/detecting codes are essential in most devices that store digital information and they have been extensively discussed for improving the reliability in devices such as computer systems and communication networks [1]-[3], [5]-[8]. Different systems may be vulnerable to different types of error and a lot has been written to deal with them. We classified them as symmetric, asymmetric and unidirectional errors. A transition of $0 \to 1$ will be referred as 0-error and a transition of $1 \to 0$ as 1-error.

Through research, it was found that many types of VLSI circuits exhibit a high incidence of unidirectional errors, while the number of random faults or symmetric errors caused by internal failure is usually limited. For that reason, it is useful to have codes that are capable of correcting a relatively small number of random errors and detecting any number of unidirectional errors. Considerable attention was paid to this problem [1]-[2], [5]-[8]. In this paper, we will construct a 4EC-AUED code.

2. The Construction of a 4EC-AUED Code

In this section, we will discuss the method of encoding a message word into a codeword. Messages are digitized into message words which are sequences of '0's and '1's. We consider the set $\boldsymbol{A}$ of all message words of length 8 and weight 4. $\boldsymbol{A}$ has minimum distance 2.

Each of the message word $\bar{\boldsymbol{a}}$ is encoded into a codeword $\bar{\boldsymbol{c}}$ of the form $\bar{\boldsymbol{c}} = [\bar{\boldsymbol{a}} \mid \bar{\boldsymbol{w}} \mid \bar{\boldsymbol{v}} \mid \bar{\boldsymbol{a}}]$ where $\bar{\boldsymbol{w}}$ and $\bar{\boldsymbol{v}}$ are the parity check part added to it. First, let us explain how to obtain $\bar{\boldsymbol{w}}$ and $\bar{\boldsymbol{v}}$.

Received May 15, 2003.
2000 *Mathematics Subject Classification*. 94B60.
Key words and phrases. Error correcting code, all unidirectional errors detecting code.

2.1. Method of obtaining $\bar{\boldsymbol{w}}$

Let $\boldsymbol{W}^*$ be the extended Hamming codes generated by

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \quad \text{with parity check matrix} \quad \boldsymbol{H} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then from $\boldsymbol{W}^*$, whose minimum distance is 4, we choose any 8 words to form $\boldsymbol{W}$.

Let $\boldsymbol{W} = \left\{ \begin{matrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{matrix} \right\}$. Next, we defined a one-to-one function $\boldsymbol{g}$ which maps $j = \{0,1,2,3,4,5,6,7\}$ to $\boldsymbol{W}$.

The 1-1 mapping chosen is:-

$$\begin{aligned} \boldsymbol{g}(0) &= 11101000 & \boldsymbol{g}(4) = 11010100 \\ \boldsymbol{g}(1) &= 01110001 & \boldsymbol{g}(5) = 10100101 \\ \boldsymbol{g}(2) &= 10110010 & \boldsymbol{g}(6) = 01100110 \\ \boldsymbol{g}(3) &= 11000011 & \boldsymbol{g}(7) = 00010111 \end{aligned}$$

Then, $\forall \bar{\boldsymbol{a}} = (a_0a_1a_2a_3a_4a_5a_6a_7) \in \boldsymbol{A}$ and $\bar{\boldsymbol{w}}$ is defined as $\bar{\boldsymbol{w}} = \boldsymbol{g}[\sum_{i=0}^{7} \boldsymbol{a}_i \cdot i (\mathrm{mod}\, 8)]$.

Example 1. Let's obtain $\bar{\boldsymbol{w}}$ from the message word $\bar{\boldsymbol{a}} = 10010110$.

$$\sum_{i=0}^{7} \mathbf{a}_i \cdot i = 0 + 3 + 5 + 6 \equiv 6 \bmod 8, \quad \text{so } \bar{\boldsymbol{w}} = \boldsymbol{g}(6) = 01100110.$$

2.2. Method of obtaining $\bar{\boldsymbol{v}}$

Let $\boldsymbol{V}=\left\{\begin{array}{cccccc} 0&0&0&1&1&1\\ 0&0&1&0&1&1\\ 0&0&1&1&0&1\\ 0&0&1&1&1&0\\ 0&1&0&0&1&1\\ 0&1&0&1&0&1\\ 0&1&0&1&1&0\\ 0&1&1&0&0&1\\ 0&1&1&0&1&0\\ 0&1&1&1&0&0\\ 1&0&0&0&1&1\\ 1&0&0&1&0&1\\ 1&0&0&1&1&0\\ 1&0&1&0&0&1\\ 1&0&1&0&1&0\\ 1&0&1&1&0&0\\ 1&1&0&0&0&1 \end{array}\right\}$. Note that $\boldsymbol{V}$ contains words of length 6 and weight 3 and we define $\boldsymbol{h}$ as a one-to-one function from $\boldsymbol{K} = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\}$ to $\boldsymbol{V}$.

The 1-1 mapping chosen is:-

$$\begin{array}{lll} \boldsymbol{h}(0) = 000111 & \boldsymbol{h}(6) = 010110 & \boldsymbol{h}(12) = 100110 \\ \boldsymbol{h}(1) = 001011 & \boldsymbol{h}(7) = 011001 & \boldsymbol{h}(13) = 101001 \\ \boldsymbol{h}(2) = 001101 & \boldsymbol{h}(8) = 011010 & \boldsymbol{h}(14) = 101010 \\ \boldsymbol{h}(3) = 001110 & \boldsymbol{h}(9) = 011100 & \boldsymbol{h}(15) = 101100 \\ \boldsymbol{h}(4) = 010011 & \boldsymbol{h}(10) = 100011 & \boldsymbol{h}(16) = 110001 \\ \boldsymbol{h}(5) = 010101 & \boldsymbol{h}(11) = 100101 & \end{array}$$

Then, $\forall\bar{\boldsymbol{a}} = (a_0a_1a_2a_3a_4a_5a_6a_7) \in \boldsymbol{A}$ and $\bar{\boldsymbol{v}}$ is defined as $\bar{\boldsymbol{v}} = \boldsymbol{h}[\sum_{i=0}^{7} a_i \cdot 2^i (\mathrm{mod}\, 17)]$

Example 2. Let's obtain $\bar{\boldsymbol{v}}$ from the message word $\bar{\boldsymbol{a}} = 10010110$.

$$\sum_{i=0}^{7} \boldsymbol{a}_i \cdot 2^i = 2^0 + 2^3 + 2^5 + 2^6 \equiv 3 \mathrm{mod}\, 17, \quad \text{so } \bar{\boldsymbol{v}} = \boldsymbol{h}(3) = 001110.$$

Since the codeword takes the form of $\bar{\boldsymbol{c}} = [\bar{\boldsymbol{a}} \mid \bar{\boldsymbol{w}} \mid \bar{\boldsymbol{v}} \mid \bar{\boldsymbol{a}}]$, therefore from example 1 and 2, the message word $\bar{a} = 10010110$, will be the encoded into codeword $\bar{\boldsymbol{c}} = [10010110\ 01100110\ 001110\ 10010110]$.

3. Minimal Distance of the Code

Before we calculate the minimal distance of the code obtained, let us take a look at the following theorems.

Theorem 3.1. *If $\bar{\boldsymbol{c}} = [\bar{\boldsymbol{a}} \mid \bar{\boldsymbol{w}} \mid \bar{\boldsymbol{v}} \mid \bar{\boldsymbol{a}}]$ and $\bar{\boldsymbol{c}}' = [\bar{\boldsymbol{a}}' \mid \bar{\boldsymbol{w}}' \mid \bar{\boldsymbol{v}}' \mid \bar{\boldsymbol{a}}']$ are two different codewords and $\bar{\boldsymbol{w}} = \bar{\boldsymbol{w}}'$, then $d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}') \geq 4$.*

Proof. We claimed that $d(\bar{a}, \bar{a}') \geq 4$. If $d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}' < 4$, then $d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}') = 2$. Assume that $\bar{\boldsymbol{a}}$ and $\bar{\boldsymbol{a}}'$ disagree at coordinate i and j. $\bar{\boldsymbol{w}} = \bar{\boldsymbol{w}}'$ implies $\sum_{i=0}^{7}(\boldsymbol{a}_i \cdot i) \equiv \sum_{i=0}^{7}(\boldsymbol{a}'_i \cdot i) \equiv \bmod 8$. This means $\boldsymbol{i} \equiv j \bmod 8$ which leads to a contradiction since $i - j$ lies between -7 and 7. (8 is the minimum positive integer that makes it works.) We conclude that $d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}') \geq 4$

Theorem 3.2. *If $\bar{\boldsymbol{c}} = [\bar{\boldsymbol{a}} \mid \bar{\boldsymbol{w}} \mid \bar{\boldsymbol{v}} \mid \bar{\boldsymbol{a}}]$ and $\bar{\boldsymbol{c}}' = [\bar{\boldsymbol{a}}' \mid \bar{\boldsymbol{w}}' \mid \bar{\boldsymbol{v}}' \mid \bar{\boldsymbol{a}}']$ are two different codewords and $\bar{\boldsymbol{v}} = \bar{\boldsymbol{v}}'$, then $d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}') \geq 4$.*

Proof. We claimed that $d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}') \geq 4$. If $d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}') < 4$, then $d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}') = 2$. Assume that $\bar{\boldsymbol{a}}$ and $\bar{\boldsymbol{a}}'$ disagree at coordinate i and j. $\bar{\boldsymbol{v}} = \bar{\boldsymbol{v}}'$ implies $\sum_{i=0}^{7}(\boldsymbol{a}_i \cdot 2^i) \equiv \sum_{i=0}^{7}(\boldsymbol{a}'_i \cdot 2^i) \equiv \bmod 17$. This means $2^i \equiv 2^j \bmod 17$ which leads to a contradiction since $2^i - 2^j = \begin{cases} 2^i(1 - 2^{j-i}), & \text{for } j > i, \\ 2^j(2^{i-j} - 1), & \text{for } i > j, \end{cases}$ and $0 \leq i, j \leq 7$. We conclude that $d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}') \geq 4$.

Theorem 3.3. *If $\bar{\boldsymbol{c}} = [\bar{\boldsymbol{a}} \mid \bar{\boldsymbol{w}} \mid \bar{\boldsymbol{v}} \mid \bar{\boldsymbol{a}}]$ and $\bar{\boldsymbol{c}}' = [\bar{\boldsymbol{a}}' \mid \bar{\boldsymbol{w}}' \mid \bar{\boldsymbol{v}}' \mid \bar{\boldsymbol{a}}']$ are two different codewords and if $\bar{\boldsymbol{v}} = \bar{\boldsymbol{v}}'$ and $\bar{\boldsymbol{w}} = \bar{\boldsymbol{w}}'$, then $d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}') \geq 6$.*

Proof. $\bar{\boldsymbol{w}} = \bar{\boldsymbol{w}}'$ implies $d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}') \geq 4$ (from Theorem 3.2). Assume $d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}') = 4$ and that $\bar{\boldsymbol{a}}$ and $\bar{\boldsymbol{a}}'$ disagree at coordinate i, j, l and m. Then $\bar{\boldsymbol{w}} = \bar{\boldsymbol{w}}'$ implies $\sum_{i=0}^{7}(a_i \cdot i) \equiv \sum_{i=0}^{7}(\boldsymbol{a}'_i \cdot i) \bmod 8$ and thus $i + j \equiv (l + m) \bmod 8$ (1)
and $\bar{\boldsymbol{v}} = \bar{\boldsymbol{v}}'$ implies $\sum_{i=0}^{7}(\boldsymbol{a}_i \cdot 2^i) \equiv \sum_{i=0}^{7}(\boldsymbol{a}'_i \cdot 2^i) \bmod 17$ and thus we have

$$2^i + 2^j \equiv (2^l + 2^m) \bmod 17 \tag{2}$$

The choice of mod 8 and mod 17 ensures that the congruence equation (1) and (2) has no solution. Therefore, we conclude that $d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}') \geq 6$.

Now, we will use the thereoms mentioned above to calculate the minimal distance of the code obtained. Note that $d(\bar{\boldsymbol{c}}, \bar{\boldsymbol{c}}') = d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}') + d(\bar{\boldsymbol{w}}, \bar{\boldsymbol{w}}') + d(\bar{\boldsymbol{v}}, \bar{\boldsymbol{v}}') + d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}')$.

Case 1. $\bar{\boldsymbol{w}} \neq \bar{\boldsymbol{w}}'$ and $\bar{\boldsymbol{v}} \neq \bar{\boldsymbol{v}}'$.
$\bar{\boldsymbol{w}} \neq \bar{\boldsymbol{w}}'$ implies $d(\bar{\boldsymbol{w}}, \bar{\boldsymbol{w}}') \geq 4$ and $\bar{\boldsymbol{v}} \neq \bar{\boldsymbol{v}}'$ implies $d(\bar{\boldsymbol{v}}, \bar{\boldsymbol{v}}') \geq 2$. Thus $d(\bar{\boldsymbol{c}}, \bar{\boldsymbol{c}}') \geq 10$.

Case 2. $\bar{\boldsymbol{w}} \neq \bar{\boldsymbol{w}}'$ and $\bar{\boldsymbol{v}} \neq \bar{\boldsymbol{v}}'$.
From Theorem 3.1, $\bar{\boldsymbol{w}} = \bar{\boldsymbol{w}}'$ implies $d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}') \geq 4$. $\bar{\boldsymbol{v}} \neq \bar{\boldsymbol{v}}'$ implies $d(\bar{\boldsymbol{v}}, \bar{\boldsymbol{v}}') \geq 2$ and thus $d(\bar{\boldsymbol{c}}, \bar{\boldsymbol{c}}') \geq 10$.

Case 3. $\bar{\boldsymbol{w}} \neq \bar{\boldsymbol{w}}'$ and $\bar{\boldsymbol{v}} \neq \bar{\boldsymbol{v}}'$.

From Theorem 3.2, $\bar{\boldsymbol{v}} = \bar{\boldsymbol{v}}'$ implies $d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}') \geq 4$. $\bar{\boldsymbol{w}} \neq \bar{\boldsymbol{w}}'$ implies $d(\bar{\boldsymbol{w}}, \bar{\boldsymbol{w}}') \geq 4$ and thus $d(\bar{\boldsymbol{c}}, \bar{\boldsymbol{c}}') \geq 12$.

Case 4. $\bar{\boldsymbol{w}} = \bar{\boldsymbol{w}}'$ and $\bar{\boldsymbol{v}} \neq \bar{\boldsymbol{v}}'$.
From Theorem 3.3, $\bar{\boldsymbol{w}} = \bar{\boldsymbol{w}}'$ and $\bar{\boldsymbol{v}} = \bar{\boldsymbol{v}}'$ implies $d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}') \geq 6$. Thus $d(\bar{\boldsymbol{c}}, \bar{\boldsymbol{c}}') \geq 12$.

Exhausting all possible cases, we see that C is of minimal distance 10. Bose and Rao [2] have shown that constant weight code with minimum distance $2t + 2$ is tEC-AUED code. Thus C is a 4EC-AUED code.

4. Decoding Algorithm

A received word may be error-corrupted due to interference or noises. The decoding procedure for error correction can be implemented as described in the following. Let $\bar{\boldsymbol{c}}^* = \lfloor \bar{\boldsymbol{a}}^* \mid \bar{\boldsymbol{w}}^* \mid \bar{\boldsymbol{v}}^* \mid \bar{\boldsymbol{b}}^* \rfloor$ be a received word. We first compute $\boldsymbol{S}_{\bar{a}^*w} = \sum_{i=0}^{7} \boldsymbol{a}_i^* \cdot i$, $\boldsymbol{S}_{\bar{a}^*v} = \sum_{i=0}^{7} \boldsymbol{a}_i^* \cdot 2^i$, $\boldsymbol{S}_{\bar{b}^*w} = \sum_{i=0}^{7} \boldsymbol{b}_i^* \cdot i$, $\boldsymbol{S}_{\bar{b}^*v} = \sum_{i=0}^{7} \boldsymbol{b}_i^* \cdot 2^i$

Decoding Algorithm: We will split the received word into 2 parts. The first part is $\lfloor \bar{\boldsymbol{a}}^* \mid \bar{\boldsymbol{w}}^* \mid \bar{\boldsymbol{v}}^* \rfloor$ and the second part is $\lfloor \bar{\boldsymbol{b}}^* \mid \bar{\boldsymbol{w}}^* \mid \bar{\boldsymbol{v}}^* \rfloor$.

1. Compute $\bar{\boldsymbol{w}}^* \boldsymbol{H}$.
   a) $\bar{\boldsymbol{w}} \boldsymbol{H} = 0$, let $\bar{\boldsymbol{w}}^{\#} = \bar{\boldsymbol{w}}^*$ and proceed to Step 2.
   b) $\bar{\boldsymbol{w}}^* \boldsymbol{H} = i^{\text{th}}$ row of $\boldsymbol{H}$, then correct the i^{th} coordinate of $\bar{\boldsymbol{w}}^*$ to get $\bar{\boldsymbol{w}}^{\beta}$. If $wt(\bar{\boldsymbol{w}}^{\beta}) = 4$, then let $\bar{\boldsymbol{w}}^{\#} = \bar{\boldsymbol{w}}^{\beta}$ and proceed to Step 2.
   If $wt(\bar{\boldsymbol{w}}^{\beta}) \neq 4$, then $\bar{\boldsymbol{w}}^{\#}$ is not obtained and proceed to Step 3.
   c) $\bar{\boldsymbol{w}}^* \boldsymbol{H} \neq i^{\text{th}}$ row of $\boldsymbol{H}$, $\bar{\boldsymbol{w}}^{\#}$ is not obtained and proceed to Step 3.
2. (a) $\boldsymbol{wt}(\bar{\boldsymbol{a}}^*) = 4$
   If $\boldsymbol{w}t(\boldsymbol{g}(\boldsymbol{S}_{\bar{a}*w} \bmod 8) + \bar{\boldsymbol{w}}^{\#}) \leq 1$, then we let $\bar{\boldsymbol{a}}_w^* = \bar{\boldsymbol{a}}^*$.
   Proceed to Step 3.
   (b) $\boldsymbol{wt}(\bar{\boldsymbol{a}}^*) = 3$
   Let $\boldsymbol{m} \equiv (\boldsymbol{g}^{-1}(\bar{\boldsymbol{w}}^{\#}) - \boldsymbol{S}_{\bar{a}^*w}) \bmod 8$. If the m^{th} coordinate of $\bar{\boldsymbol{a}}^*$ is 0, then correct the m^{th} coordinate to get $\bar{\boldsymbol{a}}_w^*$.
   Proceed to Step 3.
   (c) $\boldsymbol{wt}(\bar{\boldsymbol{a}}^*) = 5$
   Let $m \equiv (\boldsymbol{S}_{\bar{a}^*w} - \boldsymbol{g}^{-1}(\bar{\boldsymbol{w}}^{\#})) \bmod 8$. If the m^{th} coordinate of $\bar{\boldsymbol{a}}^*$ is 1, then correct the m^{th} coordinate to get $\bar{\boldsymbol{a}}_w^*$.
   Proceed to Step 3.
   (d) Proceed to Step 3.
3. (a) If $\boldsymbol{wt}(\bar{\boldsymbol{a}}^*) = 4$
   If $\boldsymbol{wt}(\boldsymbol{g}(\boldsymbol{S}_{\bar{a}*v} \bmod 17) + \bar{\boldsymbol{v}}^*) \leq 1$, then we let $\bar{\boldsymbol{a}}_v^* = \bar{\boldsymbol{a}}^*$.
   Proceed to Step 4.
   (b) If $\boldsymbol{wt}(\bar{\boldsymbol{a}}^*) \in \{3, 5\}$ and $\bar{\boldsymbol{v}}^* \in \boldsymbol{V}$.
      (i) $\boldsymbol{wt}(\bar{\boldsymbol{a}}^*) = 3$
      Let $2^m \equiv (\boldsymbol{h}^{-1}(\bar{\boldsymbol{v}}^*) - \boldsymbol{S}_{\bar{a}^*v}) \bmod 17$. If the m^{th} coordinate of $\bar{\boldsymbol{a}}^*$ is 0, then correct the m^{th} coordinate to get $\bar{\boldsymbol{a}}_v^*$.
      Proceed to Step 4.

(ii) $\boldsymbol{wt}(\bar{\boldsymbol{a}}^*) = 5$
Let $2^m \equiv (\boldsymbol{S}_{\bar{a}^*\boldsymbol{v}} - \boldsymbol{h}^{-1}(\bar{\boldsymbol{v}}^*)) \bmod 17$. If the m^{th} coordinate of $\bar{\boldsymbol{a}}^*$ is 1, then correct the m^{th} coordinate to get $\bar{\boldsymbol{a}}^*_v$.
Proceed to Step 4.

(c) Proceed to Step 4.

4. (a) If $\bar{\boldsymbol{a}}^*_w$ is obtained but not $\bar{\boldsymbol{a}}^*_v$: Let $\bar{\boldsymbol{a}}^{**} = \bar{\boldsymbol{a}}^*_w$ and proceed to Step 5.
(b) If $\bar{\boldsymbol{a}}^*_v$ is obtained but not $\bar{\boldsymbol{a}}^*_w$: Let $\bar{\boldsymbol{a}}^{**} = \bar{\boldsymbol{a}}^*_v$ and proceed to Step 5.
(c) If $\bar{\boldsymbol{a}}^*_w = \bar{\boldsymbol{a}}^*_v$: Let $\bar{\boldsymbol{a}}^{**} = \bar{\boldsymbol{a}}^*_w$ and proceed to Step 5.
(d) If $\bar{\boldsymbol{w}}^{\#}$ is obtained, $\boldsymbol{wt}(\bar{\boldsymbol{a}}^*) \in \{2, 4, 6\}$ and $\bar{\boldsymbol{v}}^* \in \boldsymbol{V}$.

(i) $wt(\bar{\boldsymbol{a}}^*) = 2$
Let $m + n \equiv (\boldsymbol{g}^{-1}(\bar{\boldsymbol{w}}^{\#}) - \boldsymbol{S}_{\bar{a}^*w}) \bmod 8$ (1)
and $2^m + 2^n \equiv (\boldsymbol{h}^{-1}(\bar{\boldsymbol{v}}^*) - \boldsymbol{S}_{\bar{a}^*\boldsymbol{v}}) \bmod 17$ (2)
By solving (1) and (2) simultaneously, a value of m and n can be obtained. If the m^{th} and n^{th} coordinate of $\bar{\boldsymbol{a}}^*$ are 0, then correct the m^{th} and n^{th} coordinate to get $\bar{\boldsymbol{a}}^{**}$ and then proceed to Step 5. Otherwise, proceed to Step 6.

(ii) $wt(\bar{\boldsymbol{a}}^*) = 4$
Let $m - n \equiv (\boldsymbol{g}^{-1}(\bar{\boldsymbol{w}}^{\#}) - \boldsymbol{S}_{\bar{a}^*w}) \bmod 8$ (1)
and $2^m - 2^n \equiv (\boldsymbol{h}^{-1}(\bar{\boldsymbol{v}}^*) - \boldsymbol{S}_{\bar{a}^*\boldsymbol{v}}) \bmod 17$ (2)
By solving (1) and (2) simultaneously, a value of m and n can be obtained. If the m^{th} coordinate of $\bar{\boldsymbol{a}}^*$ is 0 and the n^{th} coordinate is 1, then correct the m^{th} and n^{th} coordinate to get $\bar{\boldsymbol{a}}^{**}$ and then proceed to Step 5. Otherwise, proceed to Step 6.

(iii) $\boldsymbol{wt}(\bar{\boldsymbol{a}}^*) = 6$
Let $m + n \equiv (\boldsymbol{S}_{\bar{a}^*w} - \boldsymbol{g}^{-1}(\bar{\boldsymbol{w}}^{\#})) \bmod 8$ (1)
and $2^m + 2^n \equiv (\boldsymbol{S}_{\bar{a}^*v} - \boldsymbol{h}^{-1}(\bar{\boldsymbol{v}}^*)) \bmod 17$ (2)
By solving (1) and (2) simultaneously, a value of m and n can be obtained. If the m^{th} and n^{th} coordinate of $\bar{\boldsymbol{a}}^*$ are 1, then correct the m^{th} and n^{th} coordinate to get $\bar{\boldsymbol{a}}^{**}$ and then proceed to Step 5. Otherwise, proceed to Step 6.

Note: (1) and (2) give rise to a unique solution m and n due to the choice of $\bmod 8$ and $\bmod 17$.

(e) Proceed to Step 6.

5. Encode $\bar{\boldsymbol{a}}^{**}$ obtained to $\bar{\boldsymbol{c}}^{**}[\bar{\boldsymbol{a}}^{**} \mid \bar{\boldsymbol{w}}^{**} \mid \bar{\boldsymbol{v}}^{**} \mid \bar{\boldsymbol{a}}^{**}]$. If $d(\bar{\boldsymbol{c}}^*, \bar{\boldsymbol{c}}^{**}) \leq 4$, we decode the message word to be $\bar{\boldsymbol{a}}^{**}$ and if $d(\bar{\boldsymbol{c}}^*, \bar{\boldsymbol{c}}^{**}) > 4$, proceed to Step 6.

B. Decode $\lfloor \bar{\boldsymbol{b}}^* \mid \bar{\boldsymbol{w}}^* \mid \bar{\boldsymbol{v}}^* \rfloor$

6. (a) $\boldsymbol{wt}(\bar{\boldsymbol{b}}^*) = 4$
If $\boldsymbol{wt}(\boldsymbol{g}(\boldsymbol{S}_{\bar{b}^*w} \bmod 8) + \bar{\boldsymbol{w}}^{\#}) \leq 1$, then we let $\bar{\boldsymbol{b}}^*_w = \bar{\boldsymbol{b}}^*$.
Proceed to Step 7.
(b) If $\bar{\boldsymbol{w}}^{\#}$ has not been obtained, proceed to Step 7. Otherwise,

(i) $\boldsymbol{wt}(\bar{\boldsymbol{b}}^*) = 3$
Let $m \equiv (\boldsymbol{g}^{-1}(\bar{\boldsymbol{w}}^{\#}) - \boldsymbol{S}_{\bar{b}^*w}) \bmod 8$. If the m^{th} coordinate of $\bar{\boldsymbol{b}}^*$ is 0, then correct the m^{th} coordinate to get $\bar{\boldsymbol{b}}^*_w$.

Proceed to Step 7.

(ii) $\boldsymbol{wt}(\bar{\boldsymbol{b}}^*) = 5$

Let $m \equiv (\boldsymbol{S}_{\bar{b}^*w} - \boldsymbol{g}^{-1}(\bar{\boldsymbol{w}}^{\#}))\bmod 8$. If the m^{th} coordinate of $\bar{b}^*$ is 1, then correct the m^{th} coordinate to get $\bar{\boldsymbol{b}}^*_w$.

Proceed to Step 7.

(iii) Proceed to Step 7.

7. (a) $\boldsymbol{wt}(\bar{\boldsymbol{b}}^*) = 4$

If $\boldsymbol{wt}(\boldsymbol{h}(\boldsymbol{S}_{\bar{b}^*v}\bmod 17) + \bar{\boldsymbol{w}}^*) \leq 1$, then we let $\bar{\boldsymbol{b}}^*_v = \bar{\boldsymbol{b}}^*$.

Proceed to Step 8.

(b) If $\boldsymbol{wt}(\bar{\boldsymbol{b}}^*) \in \{3, 5\}$ and $\bar{\boldsymbol{v}}^* \in \boldsymbol{V}$.

(i) $\boldsymbol{wt}(\bar{\boldsymbol{b}}^*) = 3$

Let $2^m \equiv (\boldsymbol{h}^{-1}(\bar{\boldsymbol{v}}^{\#}) - \boldsymbol{S}_{\bar{b}^*v})\bmod 17$. If the m^{th} coordinate of $\bar{\boldsymbol{b}}^*$ is 0, then correct the m^{th} coordinate to get $\bar{\boldsymbol{b}}^*_v$.

Proceed to Step 8.

(ii) $\boldsymbol{wt}(\bar{\boldsymbol{b}}^*) = 5$

Let $m \equiv (\boldsymbol{S}_{\bar{b}^*w} - \boldsymbol{h}^{-1}(\bar{\boldsymbol{w}}^{\#}))\bmod 17$. If the m^{th} coordinate of $\bar{\boldsymbol{b}}^*$ is 1, then correct the m^{th} coordinate to get $\bar{\boldsymbol{b}}^*_w$.

Proceed to Step 8.

(c) Proceed to Step 8.

8. (a) If $\bar{\boldsymbol{b}}^*_w$ is obtained but not $\bar{\boldsymbol{b}}^*_v$: Let $\bar{\boldsymbol{b}}^{**} = \bar{\boldsymbol{b}}^*_w$ and proceed to Step 9.

(b) If $\bar{\boldsymbol{b}}^*_w$ is obtained but not $\bar{\boldsymbol{b}}^*_w$: Let $\bar{\boldsymbol{b}}^{**} = \bar{\boldsymbol{b}}^*_v$ and proceed to Step 9.

(c) If $\bar{\boldsymbol{b}}^*_w = \bar{\boldsymbol{b}}^*_v$: Let $\bar{\boldsymbol{b}}^{**} = \bar{\boldsymbol{b}}^*_w$ and proceed to Step 9.

(d) If $\bar{\boldsymbol{w}}^{\#}$ is obtained, $\boldsymbol{wt}(\bar{\boldsymbol{b}}) \in \{2, 4, 6\}$ and $\bar{\boldsymbol{v}}^* \in \boldsymbol{V}$.

(i) $wt(\bar{\boldsymbol{b}}^*) = 2$

Let $m + n \equiv (\boldsymbol{g}^{-1}(\bar{\boldsymbol{w}}^{\#}) - \boldsymbol{S}_{\bar{b}^*w})\bmod 8$ (1)

and $2^m + 2^n \equiv (\boldsymbol{h}^{-1}(\bar{\boldsymbol{v}}^*) - \boldsymbol{S}_{\bar{b}^*\boldsymbol{v}})\bmod 17$ (2)

By solving (1) and (2) simultaneously, a value of m and n can be obtained. If the m^{th} and n^{th} coordinate of $\bar{\boldsymbol{b}}^*$ are 0, then correct the m^{th} and n^{th} coordinate to get $\bar{\boldsymbol{b}}^{**}$ and then proceed to Step 9. If not, stop here as there are more than 4 errors in the received word.

(ii) $\boldsymbol{wt}(\bar{\boldsymbol{b}}^*) = 4$

Let $m - n \equiv (\boldsymbol{g}^{-1}(\bar{\boldsymbol{w}}^{\#}) - \boldsymbol{S}_{\bar{b}^*w})\bmod 8$ (1)

and $2^m - 2^n \equiv (\boldsymbol{h}^{-1}(\bar{\boldsymbol{v}}^*) - \boldsymbol{S}_{\bar{b}^*\boldsymbol{v}})\bmod 17$ (2)

By solving (1) and (2) simultaneously, a value of m and n can be obtained. If the m^{th} coordinate of $\bar{\boldsymbol{b}}^*$ is 0 and the n^{th} coordinate is 1, then correct the m^{th} and n^{th} coordinate to get $\bar{\boldsymbol{b}}^{**}$ and then proceed to Step 9. If not, stop here as there are more than 4 errors in the received word.

(iii) $\boldsymbol{wt}(\bar{\boldsymbol{b}}^*) = 6$

Let $m + n \equiv (\boldsymbol{S}_{\bar{b}^*w} - \boldsymbol{g}^{-1}(\bar{\boldsymbol{w}}^{\#}))\bmod 8$ (1)

and $2^m + 2^n \equiv (\boldsymbol{S}_{\bar{b}^*v} - \boldsymbol{h}^{-1}(\bar{\boldsymbol{v}}^*))\bmod 17$ (2)

By solving (1) and (2) simultaneously, a value of m and n can be obtained. If the m^{th} and n^{th} coordinate of $\bar{\boldsymbol{b}}^*$ are 1, then correct the m^{th} and n^{th} coordinate to get $\bar{\boldsymbol{b}}^{**}$ and then proceed to Step 9. If not, stop here as there are more than 4 errors in the received word.

(e) If $\bar{\boldsymbol{b}}^*_w$ and $\bar{\boldsymbol{b}}^*_v$ is not obtained but $\bar{\boldsymbol{a}}^* = \bar{\boldsymbol{b}}^*$ and $\boldsymbol{wt}(\bar{\boldsymbol{b}}^*) = 4$, let $\bar{\boldsymbol{b}}^{**} = \bar{\boldsymbol{b}}^*$ and proceed to Step 9.
(f) If $\bar{\boldsymbol{a}}^*_w \neq \bar{\boldsymbol{a}}^*_v$ and $\bar{\boldsymbol{b}}^*_w \neq \bar{\boldsymbol{b}}^*_v$, but $\bar{\boldsymbol{a}}^*_w = \bar{\boldsymbol{b}}^*_w$, let $\bar{\boldsymbol{b}}^{**} = \bar{\boldsymbol{b}}^*_w$ and proceed to Step 9.
(g) Stop here as there are more than 4 errors in the received word.

9. Let $\bar{\boldsymbol{a}}^{**} = \bar{\boldsymbol{b}}^{**}$ and encode $\bar{\boldsymbol{a}}^{**}$ to $\bar{\boldsymbol{c}}^{**} = [\bar{\boldsymbol{a}}^{**} \mid \bar{\boldsymbol{w}}^{**} \mid \bar{\boldsymbol{v}}^{**} \mid \bar{\boldsymbol{a}}^{**}]$. If $d(\bar{\boldsymbol{c}}^*, \bar{\boldsymbol{c}}^{**}) \leq 4$, we decode the message word to be $\bar{\boldsymbol{b}}^{**}$ and if $d(\bar{\boldsymbol{c}}^*, \bar{\boldsymbol{c}}^{**}) > 4$, we conclude that the received word has more than 4 errors.

5. Justification of the Decoding Algorithm

The decoding algorithm given above is capable of correcting t errors if $t \leq 4$. Assuming that the codeword $\bar{\boldsymbol{c}} = [\bar{\boldsymbol{a}} \mid \bar{\boldsymbol{w}} \mid \bar{\boldsymbol{v}} \mid \bar{\boldsymbol{a}}]$ is transmitted and the received word is $\bar{\boldsymbol{c}}^* = [\bar{\boldsymbol{a}}^* \mid \bar{\boldsymbol{w}}^* \mid \bar{\boldsymbol{v}}^* \mid \bar{\boldsymbol{b}}^*]$. Now, let us study a few facts about the error pattern. Assume that the number of error occurred is ≤ 4. Let the error distribution be displayed in the boxes.

F1

	$\bar{\boldsymbol{a}}^*$	$\bar{\boldsymbol{w}}^*$
No. of errors	≤ 1	≤ 1

We conclude that $\bar{\boldsymbol{w}}^{\#} = \bar{\boldsymbol{w}}$ in Step 1 and $\bar{\boldsymbol{a}}^*_w = \bar{\boldsymbol{a}}$ in Step 2.

F2

	$\bar{\boldsymbol{a}}^*$	$\bar{\boldsymbol{v}}^*$
No. of errors	0	≤ 1

We conclude that $\bar{\boldsymbol{a}}^*_v = \bar{\boldsymbol{a}}^* = \bar{\boldsymbol{a}}$ in Step 3(a).

F3

	$\bar{\boldsymbol{a}}^*$	$\bar{\boldsymbol{v}}^*$
No. of errors	1	0

We conclude that $\bar{\boldsymbol{a}}^*_v = \bar{\boldsymbol{a}}$ in Step 3(b).

F4

	$\bar{\boldsymbol{a}}^*$	$\bar{\boldsymbol{v}}^*$
No. of errors	1	1

$\boldsymbol{wt}(\bar{\boldsymbol{a}})^* = 3$ or 5 and $\bar{\boldsymbol{v}}^* \notin \boldsymbol{V}$. We conclude that $\bar{\boldsymbol{a}}^*_v$ will not be obtained in Step 3(b).

F5

	$\bar{\boldsymbol{a}}^*$	$\bar{\boldsymbol{v}}^*$
No. of errors	0	2

$\boldsymbol{h}(\boldsymbol{S}_{\bar{a}^* v} \bmod 17) = \bar{\boldsymbol{v}}$. We conclude that $\boldsymbol{wt}(\bar{\boldsymbol{v}} + \bar{\boldsymbol{v}}^*) > 1$ and $\bar{\boldsymbol{a}}^*_v$ will not be obtained in Step 3.

F6

	$\bar{\boldsymbol{a}}^*$	$\bar{\boldsymbol{w}}^*$
No. of errors	≤ 2	2

We conclude that $\bar{\boldsymbol{w}}^{\#}$ will not be obtained in Step 1 and $\bar{\boldsymbol{a}}^*_w$ will not be obtained in Step 2.

F7

	$\bar{\boldsymbol{a}}^*$	$\bar{\boldsymbol{w}}^*$
No. of errors	2	≤ 1

We conclude that $\bar{\boldsymbol{w}}^{\#} = \bar{\boldsymbol{w}}$ We conclude that $\boldsymbol{wt}(\bar{\boldsymbol{w}} + \bar{\boldsymbol{w}}^{\#}) > 2$ and $\bar{\boldsymbol{a}}_w^*$ will not be obtained in Step 2.

F8

	$\bar{\boldsymbol{a}}^*$	$\bar{\boldsymbol{v}}^*$
No. of errors	2	0

We conclude that $\boldsymbol{wt}(\bar{\boldsymbol{v}}^* + \bar{\boldsymbol{v}}') > 2$ and $\bar{\boldsymbol{a}}_v^*$ will not be obtained in Step 3.

F9

	$\bar{\boldsymbol{a}}^*$	$\bar{\boldsymbol{w}}^*$
No. of errors	0	3

We conclude that $\bar{\boldsymbol{w}}^{\#} = \bar{\boldsymbol{w}}$ in Step 1 and $\boldsymbol{wt}(\bar{\boldsymbol{w}}^{\#} + \bar{\boldsymbol{w}}) > 1$ and $\bar{\boldsymbol{a}}_w^*$ will not be obtained in Step 2.

(i) **Considering the case where $\bar{\boldsymbol{c}}^*$ has no error.**

From fact F1 and F2, $\bar{\boldsymbol{a}}_w^* = \bar{\boldsymbol{a}}$ and $\bar{\boldsymbol{a}}_v^* = \bar{\boldsymbol{a}}$ will be obtained and hence in Step 4(c), $\bar{\boldsymbol{a}}^{**} = \bar{\boldsymbol{a}}_w^*$ is obtained as $\bar{\boldsymbol{a}}_w^* = \bar{\boldsymbol{a}}_v^*$. Then in Step 5, $\bar{\boldsymbol{c}}_w^*$ will be decoded to $\bar{\boldsymbol{a}}_w^{**}$ and this will give us the correct message word.

(ii) **Considering the case where $\bar{\boldsymbol{c}}^*$ has 1 error.** (Distributions of errors are listed in the box).

Case	$\bar{\boldsymbol{a}}^*$	$\bar{\boldsymbol{w}}^*$	$\bar{\boldsymbol{v}}^*$	$\bar{\boldsymbol{b}}^*$
1	0	1	0	0
2	0	0	1	0
3	0	0	0	1
4	1	0	0	0

For cases 1, 2 and 3, we conclude from F1 and F2 that $\bar{\boldsymbol{a}}_w^* = \bar{\boldsymbol{a}}$ and $\bar{\boldsymbol{a}}_v^* = \bar{\boldsymbol{a}}$ are obtained in Step 2 and in Step 3. $\bar{\boldsymbol{a}}^{**} = \bar{\boldsymbol{a}}_w^*$ is obtained in Step 4(c) as $\bar{\boldsymbol{a}}_w^* = \bar{\boldsymbol{a}}_v^*$ and subsequently the correct message word will be obtained in Step 5.

For case 4, we conclude from F1 and F3 that $\bar{\boldsymbol{a}}_w^* = \bar{\boldsymbol{a}}$ will be obtained in Step 2 and $\bar{\boldsymbol{a}}_v^* = \bar{\boldsymbol{a}}$ in Step 3(c). In Step 4(c), $\bar{\boldsymbol{a}}^{**} = \bar{\boldsymbol{a}}_w^*$ will be obtained and in Step 5, the correct message word will be obtained.

(iii) **Considering the case where $\bar{\boldsymbol{c}}^*$ has 2 errors.**

Case	$\bar{\boldsymbol{a}}^*$	$\bar{\boldsymbol{w}}^*$	$\bar{\boldsymbol{v}}^*$	$\bar{\boldsymbol{b}}^*$
1	0	0	0	2
2	0	0	1	1
3	0	1	0	1
4	0	1	1	0
5	1	0	0	1
6	1	1	0	0
7	1	0	1	0
8	0	0	2	0
9	0	2	0	0
10	2	0	0	0

Cases 1−6 are similar to cases discussed earlier where $\bar{\boldsymbol{c}}^*$ has ≤ 1 error.

For case 7, we conclude from F1 and F4 that $\bar{\boldsymbol{a}}^*_w = \bar{\boldsymbol{a}}$ is obtained in Step 2 but $\bar{\boldsymbol{a}}^*_v$ is not obtained in Step 3. In Step 4(a), $\bar{\boldsymbol{a}}^{**} = \bar{\boldsymbol{a}}^*_w$ is obtained and thus obtained the correct message word in Step 5.

For case 8, we conclude from F1 and F5 that $\bar{\boldsymbol{a}}^*_w = \bar{\boldsymbol{a}}$ is obtained in Step 2 but $\bar{\boldsymbol{a}}^*_v$ is not obtained in Step 3. In Step 4(a), $\bar{\boldsymbol{a}}^{**} = \bar{\boldsymbol{a}}^*_w$ is obtained and thus the correct message word is obtained in Step 5.

For case 9, we conclude from F2and F6 that $\bar{\boldsymbol{a}}^*_w$ is not obtained in Step 2 but $\bar{\boldsymbol{a}}^*_v$ is obtained in Step 3. In Step 4(b), $\bar{\boldsymbol{a}}^{**} = \bar{\boldsymbol{a}}^*_v$ is obtained and thus the correct message word is obtained in Step 5.

For case 10, we conclude from F7and F8 that $\bar{\boldsymbol{a}}^*_w$ and $\bar{\boldsymbol{a}}^*_v$ are not obtained in Step 2 and in Step 3. In Step 4(d), the errors in $\bar{\boldsymbol{a}}^*$ will be corrected and $\bar{\boldsymbol{a}}^{**}$ is obtained. Subsequently, in Step 5, the correct message word is obtained.

(iv) **Considering the case where has 3 errors.**

Case	$\bar{\boldsymbol{a}}^*$	$\bar{\boldsymbol{w}}^*$	$\bar{\boldsymbol{v}}^*$	$\bar{\boldsymbol{b}}^*$
1	0	1	1	1
2	0	0	1	2
3	0	1	0	2
4	0	0	0	3
5	1	0	1	1
6	1	1	1	0
7	1	0	0	2
8	1	1	0	1
9	0	0	2	1
10	0	1	2	0
11	0	2	1	0
12	0	2	0	1
13	2	1	0	0
14	2	0	0	1
15	1	2	0	0
16	2	0	1	0
17	1	0	2	0
18	0	0	3	0
19	0	3	0	0
20	3	0	0	0

Cases 1−14 are similar to cases discussed earlier where $\bar{\boldsymbol{c}}^*$ has ≤ 2 errors.

For case 15, we conclude from F3 and F6 that $\bar{\boldsymbol{a}}^*_w$ is not obtained in Step 2 but $\bar{\boldsymbol{a}}^*_v = \bar{\boldsymbol{a}}$ is obtained in Step 3. In Step 4(b), $\bar{\boldsymbol{a}}^{**} = \bar{\boldsymbol{a}}^*_v$ is obtained and in Step 5 the correct message word is thus obtained.

For case 16, $\bar{\boldsymbol{w}}^{\#} = \bar{\boldsymbol{w}}^*$ is obtained in Step 1 and we conclude from F7 that $\bar{\boldsymbol{a}}^*_w$ is not obtained in Step 2. Since $d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}^*) = 2$ and $d(\bar{\boldsymbol{v}}, \bar{\boldsymbol{a}}^*) = 1$, $\bar{\boldsymbol{a}}^*_v$ will not be obtained. $\bar{\boldsymbol{b}}^*_w = \bar{\boldsymbol{a}}$ and $\bar{\boldsymbol{b}}^*_v = \bar{\boldsymbol{a}}$ are obtained in Step 6 and Step 7. In Step 8(c), $\bar{\boldsymbol{b}}^{**} = \bar{\boldsymbol{b}}^*_w$ is obtained and subsequently the correct message word is obtained in Step 9.

For case 17, we conclude from fact F1 that $\bar{\boldsymbol{a}}_w^* = \bar{\boldsymbol{a}}$ is obtained in Step 2. Since $d(\bar{\boldsymbol{a}}, \bar{\boldsymbol{a}}^*) = 1$ and $d(\bar{\boldsymbol{v}}, \bar{\boldsymbol{v}}^*) = 2$, $\bar{\boldsymbol{a}}_v^*$ may be obtained in Step 3(b). If $\bar{\boldsymbol{a}}_v^*$ is not obtained, $\bar{\boldsymbol{a}}^{**}$ is obtained in Step 4 and thus the correct message word is obtained in Step 5. If $\bar{\boldsymbol{a}}_v^*$ is obtained in Step 3, $\bar{\boldsymbol{a}}^{**}$ will not be obtained in Step 4 as $\bar{\boldsymbol{a}}_w^* \neq \bar{\boldsymbol{a}}_v^*$. In Step 6, $\bar{\boldsymbol{b}}_w^* = \bar{\boldsymbol{a}}$ is obtained and $\bar{\boldsymbol{b}}_v^* = \bar{\boldsymbol{a}}$ is obtained in Step 7. In Step 8(c), $\bar{\boldsymbol{b}}^{**} = \bar{\boldsymbol{b}}_w^*$ is obtained and thus the correct message word is obtained in Step 9.

For case 18, in Step 1, $\bar{\boldsymbol{w}}^{\#} = \bar{\boldsymbol{w}}$ and we conclude from fact F1 that $\bar{\boldsymbol{a}}_w^* = \bar{\boldsymbol{a}}$ will be obtained in Step 2 and in Step 3, $\bar{\boldsymbol{a}}_w^*$ will not be obtained as $\boldsymbol{wt}\bar{\boldsymbol{v}} + \bar{\boldsymbol{v}}^* > 1$. In Step 4(a), $\bar{\boldsymbol{a}}^{**} = \bar{\boldsymbol{a}}_w^*$ is obtained and thus in Step 5, the correct message word will be obtained.

For case 19, $\bar{\boldsymbol{w}}^{\#} \neq \bar{\boldsymbol{w}}$ is obtained in Step 1. $\bar{\boldsymbol{a}}_w^*$ will not be obtained in Step 2 as $\boldsymbol{wt}(\bar{\boldsymbol{w}} + \bar{\boldsymbol{w}}^{\#}) > 1$. But from fact F5, conclude that $\bar{\boldsymbol{a}}_v^* = \bar{\boldsymbol{a}}$ is obtained in Step 3 and thus in Step 4 and subsequently in Step 5, the correct message word will be obtained.

For case 20, $\bar{\boldsymbol{w}}^{\#}$ obtained in Step 1 is $\bar{\boldsymbol{w}}$. In Step 2, $\bar{\boldsymbol{a}}_w^* = \bar{\boldsymbol{a}}$ will not be obtained and $\bar{\boldsymbol{a}}_v^* = \bar{\boldsymbol{a}}$ will not be obtained in Step 3. Since both $\bar{\boldsymbol{a}}_w^* = \bar{\boldsymbol{a}}$ and $\bar{\boldsymbol{a}}_v^* = \bar{\boldsymbol{a}}$ will not be obtained the algorithm will proceed to Step 6. In Step 6, $\bar{\boldsymbol{b}}_v^* = \bar{\boldsymbol{a}}$ is obtained and $\bar{\boldsymbol{b}}_v^* = \bar{\boldsymbol{a}}$ is also obtained in Step 7. In Step 8(c), $\bar{\boldsymbol{b}}^{**} = \bar{\boldsymbol{b}}_w^*$ is obtained and thus the correct message word will be obtained in Step 9.

(v) **Considering the case where $\bar{\boldsymbol{c}}^*$ has 4 errors.**

For cases where 4 errors exist in $\bar{\boldsymbol{c}}^*$, we have 35 different combinations of errors and they are shown in the table below.

After doing a detail study of the each case listed above, we found that almost all the cases are similar to cases with errors in $\bar{\boldsymbol{c}}^*3$ but except cases 34 and 35 and we will discuss them now.

For case 34, we conclude that in Step 1, $\bar{\boldsymbol{w}}^{\#} = \bar{\boldsymbol{w}}$ is obtained and from fact F1, $\bar{\boldsymbol{a}}_w^* = \bar{\boldsymbol{a}}$ is obtained in Step 2. In Step 3, $\bar{\boldsymbol{a}}_v^* \neq \bar{\boldsymbol{a}}$ may be obtained or $\bar{\boldsymbol{a}}_v^*$ will not be obtained. If $\bar{\boldsymbol{a}}_v^*$ is not obtained, then in Step 4(a), $\bar{\boldsymbol{a}}^{**} = \bar{\boldsymbol{a}}_w^*$ will be obtained and thus in Step 5, the correct message word will be obtained. If $\bar{\boldsymbol{a}}_v^*$ is obtained, in Step 4, $\bar{\boldsymbol{a}}^{**}$ will not be obtained as $\bar{\boldsymbol{a}}_w^* \neq \bar{\boldsymbol{a}}_v^*$ and proceed to Step 6. The no. of errors in $\lfloor \bar{\boldsymbol{a}}^* \mid \bar{\boldsymbol{w}}^* \mid \bar{\boldsymbol{v}}^* \rfloor$ and $\lfloor \bar{\boldsymbol{b}}^* \mid \bar{\boldsymbol{w}}^* \mid \bar{\boldsymbol{v}}^* \rfloor$ are symmetrical and $\bar{\boldsymbol{b}}_w^* = \bar{\boldsymbol{a}}$ is obtained in Step 6 and $\bar{\boldsymbol{b}}_v^* = \bar{\boldsymbol{a}}$ may be obtained in Step 7. If $\bar{\boldsymbol{b}}_v^*$ is not obtained, in Step 8, $\bar{\boldsymbol{b}}^{**} = \bar{\boldsymbol{b}}_w^* = \bar{\boldsymbol{a}}$ is obtained and thus the correct message word will be obtained in Step 9. If $\bar{\boldsymbol{b}}_v^*$ is obtained, we will have $\bar{\boldsymbol{b}}_w^* \neq \bar{\boldsymbol{b}}_v^*$ and in Step 8(f), $\bar{\boldsymbol{b}}^{**} = \bar{\boldsymbol{a}}_w^*$ is obtained as $\bar{\boldsymbol{a}}_w^* = \bar{\boldsymbol{b}}_w^*$. Subsequently, in Step 9, we will obtained the correct message word.

For case 35, we conclude that $\bar{\boldsymbol{w}}^{\#}$ is not obtained in Step 1 and from fact F6 and F5 , $\bar{\boldsymbol{a}}_w^*$ and $\bar{\boldsymbol{a}}_v^*$ will not be obtained. In Step 4(e), both $\bar{\boldsymbol{a}}_w^*$ and $\bar{\boldsymbol{a}}_v^*$ will not be obtained and proceed to Step 6. Since the no. of errors in $\lfloor \bar{\boldsymbol{a}}^* \mid \bar{\boldsymbol{w}}^* \mid \bar{\boldsymbol{v}}^* \rfloor$ and $\lfloor \bar{\boldsymbol{b}}^* \mid \bar{\boldsymbol{w}}^* \mid \bar{\boldsymbol{v}}^* \rfloor$ are symmetrical, both $\bar{\boldsymbol{b}}_w^*$ and $\bar{\boldsymbol{b}}_v^*$ will not be obtained. In Step 8(e), $\bar{\boldsymbol{b}}^{**} = \bar{\boldsymbol{b}}^*$ is obtained as $\bar{\boldsymbol{a}}^* = \bar{\boldsymbol{b}}^*$ and $\boldsymbol{wt}(\bar{\boldsymbol{b}}^*) = 4$. Subsequently, from Step 9, the correct message word will be obtained.

From the above discussion, it is shown that the algorithm is capable of correcting t errors if $t \leq 4$.

Case	$\bar{\boldsymbol{a}}^*$	$\bar{\boldsymbol{w}}^*$	$\bar{\boldsymbol{v}}^*$	$\bar{\boldsymbol{b}}^*$		$\bar{\boldsymbol{a}}_w^*$	$\bar{\boldsymbol{a}}_v^*$	$\bar{\boldsymbol{a}}^{**}$	$\bar{\boldsymbol{b}}_w^*$	$\bar{\boldsymbol{b}}_v^*$	$\bar{\boldsymbol{b}}^{**}$
1	0	0	0	4		$\vee$	$\vee$	$\vee$			
2	0	0	1	3		$\vee$	$\vee$	$\vee$			
3	0	1	0	3		$\vee$	$\vee$	$\vee$			
4	0	1	1	2		$\vee$	$\vee$	$\vee$			
5	1	0	0	3		$\vee$	$\vee$	$\vee$			
6	1	1	0	2		$\vee$	$\vee$	$\vee$			
7	0	0	2	2		$\vee$		$\vee$			
8	0	0	3	1		$\vee$		$\vee$			
9	0	0	4	0		$\vee$		$\vee$			
10	0	1	2	1		$\vee$		$\vee$			
11	0	1	3	0		$\vee$		$\vee$			
12	1	0	1	2		$\vee$		$\vee$			
13	1	0	3	0		$\vee$		$\vee$			
14	1	1	1	1		$\vee$		$\vee$			
15	0	2	0	2			$\vee$	$\vee$			
16	0	3	0	1			$\vee$	$\vee$			
17	0	4	0	0			$\vee$	$\vee$			
18	0	2	1	1			$\vee$	$\vee$			
19	0	3	1	0			$\vee$	$\vee$			
20	1	2	0	1			$\vee$	$\vee$			
21	2	0	0	2				$\vee$			
22	2	1	0	1				$\vee$			
23	1	2	1	0						$\vee$	$\vee$
24	2	2	0	0						$\vee$	$\vee$
25	1	1	2	0		$\vee$	$\times$	$(\vee)$	$\vee$		$\vee$
26	1	3	0	0		$\times$	$\vee$	$(\vee)$		$\vee$	$\vee$
27	3	0	0	1		$\times$	$\times$	$\times$	$\vee$	$\vee$	$\vee$
28	3	1	0	0		$\times$	$\times$	$\times$	$\vee$	$\vee$	$\vee$
29	4	0	0	0		$\times$	$\times$	$\times$	$\vee$	$\vee$	$\vee$
30	3	0	1	0		$\times$		$\times$	$\vee$	$\vee$	$\vee$
31	2	0	1	1			$\times$	$\times$	$\vee$	$\vee$	$\vee$
32	2	1	1	0			$\times$	$\times$	$\vee$	$\vee$	$\vee$
33	2	0	2	0			$\times$	$\times$	$\vee$		$\vee$
34	1	0	2	1		$\vee$	$\times$		$\vee$	$\times$	
35	0	2	2	0							

$\boxed{\vee}$ Obtained and is the same as the message word.

$\boxed{\times}$ May be obtained and if obtained, it is not the same as the message word.

$\boxed{(\vee)}$ May be obtained and if obtained, it is the same as the message word.

Let's decode some received words.

Example 3. (This example shows an error in $\bar{\boldsymbol{c}}^*$).
Let us assume that a codeword $\bar{\boldsymbol{c}}$ = [00110011 10110010 000111 00110011]
is sent and the received word is $\bar{\boldsymbol{c}}^*$ = [01110011 10110010 000111 00110011]

	$\bar{\boldsymbol{a}}^*$	$\bar{\boldsymbol{w}}^*$	$\bar{\boldsymbol{v}}^*$	$\bar{\boldsymbol{b}}^*$
No. of errors	1	0	0	0

Step 1: $\bar{\boldsymbol{w}}^*\boldsymbol{H}$ = [0000] and we let $\bar{\boldsymbol{w}}^\#$ = [10110010].

Step 2: $(\boldsymbol{S}_{\bar{a}^*,w} - \boldsymbol{g}^{-1}(\bar{\boldsymbol{w}}^\#))$ mod $8 \equiv 1$. Since $\bar{\boldsymbol{a}}_1$ is a '1', we let $\bar{\boldsymbol{a}}_w^*$ = [00110011].

Step 3: $2^m \equiv [\boldsymbol{S}_{\bar{a}^*,v} - \boldsymbol{h}^{-1}(\bar{\boldsymbol{v}}^\#)]$ mod $17 \equiv 2$ since $m = 1$ and $\boldsymbol{a}_1$ is a '1' , we let $\bar{\boldsymbol{a}}_v^*$ = [00110011].

Step 4: $\bar{\boldsymbol{a}}_w^* = \bar{\boldsymbol{a}}_v^*$, we let $\bar{\boldsymbol{a}}^{**} = \bar{\boldsymbol{a}}_w^*$ = [00110011].

Step 5: Encode $\bar{\boldsymbol{a}}^{**}$ to $\bar{\boldsymbol{c}}^{**}$ = [00110011101100100000111 00110011] and since $d(\bar{\boldsymbol{c}}^*, \bar{\boldsymbol{c}}^{**}) = 1 \leq 4$, we conclude that the message word is [00110011].

Example 4. (This example shows 2 errors in $\bar{\boldsymbol{c}}^*$).
Let us assume that a codeword $\bar{\boldsymbol{c}}$ = [01010011 01110001 101100 01010011]
is sent and the received word is $\bar{\boldsymbol{c}}^*$ = [01011001 01110001 101100 01010011]

	$\bar{\boldsymbol{a}}^*$	$\bar{\boldsymbol{w}}^*$	$\bar{\boldsymbol{v}}^*$	$\bar{\boldsymbol{b}}^*$
No. of errors	2	0	0	0

Step 1: $\bar{\boldsymbol{w}}^*\boldsymbol{H}$ = [0000] and we let $\bar{\boldsymbol{w}}^\#$ = [01110001].

Step 2: $\boldsymbol{wt}(\boldsymbol{g}(\boldsymbol{S}_{\bar{a}^*,v}$ mod 8)+$\bar{\boldsymbol{w}}^\#] = 4$ and $\bar{\boldsymbol{a}}_w^*$ is not obtained.

Step 3: $\boldsymbol{wt}(\boldsymbol{h}(\boldsymbol{S}_{\bar{a}^*,v}$ mod 17)+$\bar{\boldsymbol{v}}^*] = 4$ and $\bar{\boldsymbol{a}}_v^*$ is not obtained.

Step 4: Since $\bar{\boldsymbol{a}}_w^*$ and $\bar{\boldsymbol{a}}_v^*$ are not obtained and $\bar{\boldsymbol{v}}^* \in \boldsymbol{V}$, we will proceed to Step 4(d)(ii) and solve the following equation simultaneously to get $n = 4$ and $m = 6$.

$$m - n \equiv 2 \bmod 8 \tag{1}$$

$$2^m - 2^n \equiv 14 \bmod 17 \tag{2}$$

Since $\bar{\boldsymbol{a}}_6$ is a '0' and $\bar{\boldsymbol{a}}_4$ is a '1', we let $\bar{\boldsymbol{a}}^{**}$ = [01010011].

Step 5: Encode $\bar{\boldsymbol{a}}^{**}$ to $\bar{\boldsymbol{c}}^{**}$ = [01010011011100011011000101 0011] and since $d(\bar{\boldsymbol{c}}^*, \bar{\boldsymbol{c}}^{**}) = 2 \leq 4$, we conclude that the message word is [01010011].

Example 5. (This example shows 3 errors in $\bar{\boldsymbol{c}}^*$).
Let us assume that a codeword $\bar{\boldsymbol{c}}$ = [10010011 11101000 101010 10010011]
is sent and the received word is $\bar{\boldsymbol{c}}^*$ = [10001011 11101000 101110 10010011]

	$\bar{\boldsymbol{a}}^*$	$\bar{\boldsymbol{w}}^*$	$\bar{\boldsymbol{v}}^*$	$\bar{\boldsymbol{b}}^*$
No. of errors	2	0	1	0

Step 1: $\bar{\boldsymbol{w}}^*\boldsymbol{H} = [0000]$ and we let $\bar{\boldsymbol{w}}^{\#} = [11101000]$.

Step 2: $\boldsymbol{wt}(\boldsymbol{g}(\boldsymbol{S}_{\bar{a}^*,v} \bmod 8)+\bar{\boldsymbol{w}}^{\#}] = 3$ and $\bar{\boldsymbol{a}}_w^*$ is not obtained.

Step 3: $\boldsymbol{wt}(\boldsymbol{h}(\boldsymbol{S}_{\bar{a}^*,v} \bmod 17)+\bar{\boldsymbol{v}}^*] = 6$ and $\bar{\boldsymbol{a}}_v^*$ is not obtained.

Step 4: Since $\bar{\boldsymbol{a}}_w^*$ and $\bar{\boldsymbol{a}}_v^*$ are not obtained and $\bar{\boldsymbol{v}}^* \in \boldsymbol{V}$, we will proceed to Step 6.

Step 6: $\boldsymbol{wt}(\boldsymbol{g}(\boldsymbol{S}_{\bar{a}^*,v} \bmod 8)+\bar{\boldsymbol{w}}^{\#}] = 0$ and $\bar{\boldsymbol{b}}_w^* = [11101000]$.

Step 7: $\boldsymbol{wt}(\boldsymbol{h}(\boldsymbol{S}_{\bar{a}^*,v} \bmod 17)+\bar{\boldsymbol{v}}^*] = 2$ and $\bar{\boldsymbol{v}}_v^*$ is not obtained.

Step 8: Since $\bar{\boldsymbol{b}}_w^*$ is obtained but $\bar{\boldsymbol{b}}_v^*$ is not obtained, we let $\bar{\boldsymbol{b}}^{**} = \bar{\boldsymbol{b}}_w^*$, and proceed to Step 9.

Step 9: Let $\bar{\boldsymbol{a}}^{**} = \bar{\boldsymbol{b}}^{**}$ and encode $\bar{\boldsymbol{a}}^{**}$ to $\bar{\boldsymbol{c}}^{**} = [10010011111010001010101010010011]$ and since $d(\bar{\boldsymbol{c}}^*, \bar{\boldsymbol{c}}^{**}) = 3 \leq 4$, we conclude that the message word is [10010011].

Example 6. (This example shows 4 errors in $\bar{\boldsymbol{c}}^*$).
Let us assume that a codeword $\bar{\boldsymbol{c}}$ = [01101010 10100101 001011 01101010] is sent and the received word is $\bar{\boldsymbol{c}}^*$ = [01011010 10100101 001001 01101011]

	$\bar{\boldsymbol{a}}^*$	$\bar{\boldsymbol{w}}^*$	$\bar{\boldsymbol{v}}^*$	$\bar{\boldsymbol{b}}^*$
No. of errors	2	0	1	1

Step 1: $\bar{\boldsymbol{w}}^*\boldsymbol{H} = [0000]$ and we let $\bar{\boldsymbol{w}}^{\#} = \bar{\boldsymbol{w}}^*$.

Step 2: $\boldsymbol{wt}(\boldsymbol{g}(\boldsymbol{S}_{\bar{a}^*,v} \bmod 8)+\bar{\boldsymbol{w}}^{\#}] = 4$ and $\bar{\boldsymbol{a}}_w^*$ is not obtained.

Step 3: $\boldsymbol{wt}(\boldsymbol{h}(\boldsymbol{S}_{\bar{a}^*,v} \bmod 17)+\bar{\boldsymbol{v}}^*] = 3$ and $\bar{\boldsymbol{a}}_v^*$ is not obtained.

Step 4: Since $\bar{\boldsymbol{a}}_w^*$ and $\bar{\boldsymbol{a}}_v^*$ are not obtained and $\boldsymbol{wt}(\bar{\boldsymbol{v}}^*) \neq 3$, we will proceed to Step 6.

Step 6: $[\boldsymbol{S}_{\bar{a}^*,w} - \boldsymbol{g}^{-1}(\bar{\boldsymbol{w}}^{\#})] \bmod 8 \equiv 7$. Since $\boldsymbol{b}_7$ is a '1', we let $\bar{\boldsymbol{b}}_w^* = [01101010]$.

Step 7: Since $\boldsymbol{wt}(\bar{\boldsymbol{b}}^*) = 5$ and $\boldsymbol{wt}(\bar{\boldsymbol{v}}^*) \neq 3$, we proceed to Step 8.

Step 8: Since $\bar{\boldsymbol{b}}_w^*$ is obtained but not $\bar{\boldsymbol{b}}_v^*$, we let $\bar{\boldsymbol{b}}^{**} = \bar{\boldsymbol{b}}_w^* = [01101010]$.

Step 9: Let $\bar{\boldsymbol{a}}^{**} = \bar{\boldsymbol{b}}^{**}$ and encode $\bar{\boldsymbol{a}}^{**}$ to $\bar{\boldsymbol{c}}^{**} = [01101010101001010010110110101010]$ and since $d(\bar{\boldsymbol{c}}^*, \bar{\boldsymbol{c}}^{**} = 4 \leq 4$, we conclude that the message word is [01101010].

4. Conclusion

In this paper, a simple code is constructed by using the idea of Bose and Rao [2] and M. C. Lin [6] with some alterations in order to correct 4 errors and to detect all unidirectional errors. Here, the length of the message code is 8 and of constant weight 4 is used. Therefore, from $\binom{8}{4}$, we have a maximum of 70 message words. If we are to increase the size of the message set we can use a message word of length greater than 8. For example, if we are to increase the length of the message word to 12, from $\binom{12}{6}$, we are able to have a maximum size of 924. With the increase in message word length, a suitable length for $\bar{\boldsymbol{w}}$ and $\bar{\boldsymbol{v}}$ should be chosen as the modulus will increase in tandem. Of course, this will reduce the efficiency rate with the increase in the length of the codeword.

One weakness of this code is when checking whether $\bar{\boldsymbol{v}}^*$ is in $\boldsymbol{V}$ or not. The only way we can check is by its weight and then by sorting and if the size of $\boldsymbol{V}$ is large, then the checking will be quite time consuming.

References

[1] M. Blaum and H. C. A. Van Tilborg, *On t-error correcting/all unidirectional error detecting codes*, IEEE Trans. Comp. **C-38** (1989), 1493-1501.

[2] B. Bose and T. R. N. Rao, *Theory of unidirectional error correcting/detecting codes*, IEEE Trans. Comp. **C-31** (1982), 564-568.

[3] R. W. Hamming, *Error detecting and error correcting codes*, Bell Syst. Tech. J. **29** (1950), 147-160.

[4] D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger and J. R. Wall, Coding Theory: The Essentials, Marcel Dekker, Inc., 1991.

[5] G. A. How and M. H. Ang, *The check positions of Hamming Codes an the construction of a 2EC-AUED code*, Bull. Malaysian Math. Soc.(Second Series) **21** (1998), 63-78.

[6] M. C. Lin, *Constant weight codes for correcting symmetry errors and detecting unidirectional errors*, IEEE Trans. Comp. **C-42** (1993), 1294-1302.

[7] D. Nilolos, N. Gaitanis and G. Philokyprou, *Systematic t-error correcting/all unidirectional error detecting codes*, IEEE Trans. Comp. **C-35** (1986), 394-402.

[8] D. L. Tao, C. R. P. Hartmann and P. K. Lala, *An efficient class of unidirectional error detecting/correcting codes*, IEEE Trans. Comp. **C-37** (1988), 879-882.

School of Mathematical Sciences, Universiti Sains Malaysia, 11800 USM Pulau Pinang, Malaysia.
E-mail: gahow@cs.usm.my

School of Mathematical Sciences, Universiti Sains Malaysia, 11800 USM Pulau Pinang, Malaysia.
E-mail: victork@pc.jaring.my