International Journal of Innovation in Science and Mathematics
Volume 3, Issue 2, ISSN (Online): 2347–9051

On |a+x|b+x|a+b+x| Construction of Extended Binary Golay Codes

Nidhi Nijhawan
Dept. of Operational Research, University of Delhi
email: nijhawan.nidhi82@gmail.com

Vikas Dhaka
Miranda House, University of Delhi
email: vdhaka84@gmail.com

Jatin Anand
Miranda House, University of Delhi
email: jatin.msf@gmail.com

Abstract: **This paper presents the construction for such suitable (8, 4, 4) codes which together with the given systematic (8, 4, 4) linear block code (l.b.c.) generate (24, 12, 8) binary Golay code employing |a+x|b+x|a+b+x| construction. We uncover that there do exist some (8, 4, 4) codes which although devised from the construction provided in [6] but fail to generate Golay code. The modification of previously existing construction is proposed.**

Keywords: **Extended Binary Golay Code, Linear Block Codes (L.B.C), Self Dual Codes, 2-And-2 Codeword's, Generator Matrices**

I. Introduction

Up to equivalence there exists exactly one (24, 12, 8) linear code: the so called extended Golay binary code C_{24} [1], [2]. This code has been widely investigated and several interesting constructions have been provided using different techniques [7], [8]. An interesting and useful realization for C_{24} is the one originally due to Turyn [3], in which the code is realized from two suitably chosen (8, 4, 4) codes C_1, C_2 via the $|a+x|b+x|a+b+x|$ construction. Further, the construction is utilized by Sloane, Reddy, Chen [4], Forney [5],[10] and Vinocha and Dhaka[11],[12].

Peng and Farrell [6] presents a construction of the (24, 12, 8) Golay code based on the direct sum of two array codes [9]. It was discovered that given an (8, 4, 4) code in systematic form, there exist eight different (8, 4, 4) codes obtained either through proper row permutation on the parity sub matrix of the generator matrix of the first (8, 4, 4) code or by applying a set of construction rules. These nine (8, 4, 4) codes (the original plus the eight others) are of the same isomorphism type (with the same length, dimension and weight distribution), but represent different code subspaces. Using the given (8, 4, 4) code, together with any one of the eight (8, 4, 4) codes obtained leads to the construction of the (24, 12, 8) Golay code. Brief construction is outlined as:

Let C_1 be an (8, 4, 4) systematic code (an [8, 4, 4] code is systematic if, and only if, the leftmost 4×4 minor of its generator matrix has rank 4). The generator matrix of C_1 can be expressed as

$$G_1 = (I_4 \ P) \tag{1}$$

Here I_4 is the 4×4 identity matrix and P is a 4×4 parity sub matrix of G_1. The elements of P are row vectors, i.e.

$P = (P_1, P_2, P_3, P_4)^T$, where P_i $(i = 1,2,3,4)$ are chosen uniquely from the set S = {(1110); (1101); (1011); (0111)} in any order. S contains all 4-tuples with Hamming weight 3, and the weight distribution of the code is $\{N(0)=1, N(4)=14, N(8)=1\}$, where $N(x)$ represents the number of the codeword's of weight x.

It was shown that for a given generator matrix G_1 of systematic (8, 4, 4) code C_1 there exist eight different G_i' $(1 \le i \le 8)$, all leading to the construction of C_{24} when applying them to

$$G_{24} = \begin{pmatrix} G_1 & 0 & G_1 \\ 0 & G_1 & G_1 \\ G_i' & G_i' & G_i' \end{pmatrix}. \tag{2}$$

Here G_{24} is the generator matrix of Golay code, G_i' $(i = 1,2,...,6)$ are generator matrices for systematic (8, 4, 4) codes viz. C_i' $(i = 1,2,...,6)$, obtained through proper row permutation on the parity sub matrix of G_1 while G_7' and G_8' are the generator matrices of such (8, 4, 4) codes which contain the codeword's (1111 0000) and (0000 1111) constructed by applying a set of construction rules. Henceforth we denote such codes by C_7' and C_8'.

In this paper, we reveal the rebuttal of the construction rules for C_7' and C_8' given by Peng and Farrell [6] in the sense that there exist some (8, 4, 4) codes whose generator matrices although devised by the construction rules but could not form Golay code. The general forms of such matrices are provided. To unravel the problem we propose the modified construction Rules. We also set the general form of matrices constructed by these modified Rules which when used as G_i' will produce Golay code.

This paper is divided into four Sections, Section I to Section IV. Section I includes the brief introduction of the paper. Section II is partitioned in two subsections (A) and (B). In (A), we have discussed the construction rules for the generator matrices of non systematic (8, 4, 4) given by Peng and Farrell [6] and in (B), we have exhibited the general form for the matrices which although satisfy the rules presented in (A) but do not form Golay code using

International Journal of Innovation in Science and Mathematics
Volume 3, Issue 2, ISSN (Online): 2347–9051

(2). In Section III, we have propounded the modified construction rules that prevail over the above problem. Section IV concludes the paper.

II. Construction Rules and Their Contradiction

A). Construction Rules for G_7' and G_8':

The design of the generator matrices G_7' and G_8' of codes C_7' and C_8' will be characterized by the feature that they have 8-tuples (11110000) and (00001111) as their codeword's. Because of this character, all weight-4 codeword's, except the above two of these codes have exact two non zero elements in each half of the 8-tuples. We call this type of weight-4 codeword a 2-and-2 codeword and all these codeword's must be distinct from the 4-weighted codeword's generated by the given G_1. Based on these conditions the two generator matrices are designed in the forms

$$G_7' = \begin{pmatrix} g_{7,1}' \\ g_{7,2}' \\ g_h \\ g_{w=8} \end{pmatrix} \quad \text{and} \quad G_8' = \begin{pmatrix} g_{8,1}' \\ g_{8,2}' \\ g_h \\ g_{w=8} \end{pmatrix} \qquad (3)$$

respectively. Here g_h is an 8-tuple with all 4 nonzero elements in its either half, i.e., (00001111) or (11110000), and $g_{w=8}$ is a weight-8 8-tuple. For $g_{7,m}'$ and $g_{8,m}'$ (m = 1, 2) they are weight-4 8-tuples or 2-and-2 codewords. So when they are divided into two equal halves, i.e., left half: $g_{7,m}'^{(L)}$ and $g_{8,m}'^{(L)}$; and right half: $g_{7,m}'^{(R)}$ and $g_{8,m}'^{(R)}$, any of these halves is a weight-2 4-tuple. The constructions of $g_{7,m}'$ and $g_{8,m}'$ follow the Rules stated below.

Rule (i) Assign

$$g_{7,1}'^{(L)} = g_{8,1}'^{(L)} = x$$
$$g_{7,2}'^{(L)} = g_{8,2}'^{(L)} = y\,.$$

Where x and y are any two different weight- 2 4 -tuple with $\overline{x} \neq y$.

($\overline{v}$ is the compliment of v)

Rule (ii)

$$g_{l,m}'^{(R)} \ (l = 7,8 \ and \ \ m = 1,2) \ must \ satisfy$$
$$g_{7,m}'^{(R)} \neq g_{8,m}'^{(R)},\ \overline{g_{7,m}'^{(R)}} \neq g_{8,m}'^{(R)} \ for \ m = 1,2$$
$$g_{l,1}'^{(R)} \neq g_{l,2}'^{(R)},\ \overline{g_{l,1}'^{(R)}} \neq g_{l,2}'^{(R)} \ for \ l = 7,8.$$

Rule (iii)

Assume that the nonzero elements of x are in its i^{th} and j^{th} positions, and the nonzero elements of y are in its i'^{th} and j'^{th} positions, where $i, j, i', j' \in \{1,2,3,4\}$. The following conditions must also be satisfied.

$$g_{l,1}'^{(R)} \neq P_i + P_j,\ \overline{g_{l,1}'^{(R)}} \neq P_i + P_j \ \ for \ l = 7,8 \text{ and}$$
$$g_{l,2}'^{(R)} \neq P_{i'} + P_{j'},\ \overline{g_{l,2}'^{(R)}} \neq P_{i'} + P_{j'} \ \ for \ l = 7,8$$

Here P_u $(1 \le u \le 4)$ are the row vectors of P in G_1.

B. The Contradiction.

Peng and Farrell claimed that the matrices G_7' and G_8' devised by the construction rules (presented in subsection (A)) generate 4-weight codeword's all distinct from that of C_1 [Theorem 2 of [6]]. Refer to "(1) and (2)" to apply G_7' and G_8' together with G_1, which in turn generate C_{24}. Our study reveals:

(1) A few such constructed matrices exist which generate some 4-weighted codeword's same as that of C_1.

(2) At the same time one of the matrices G_7' and G_8' can't constructed by the construction rules (presented in subsection (A)).

The particular case:

Let G_7' is constructed using (3) and x and y are any two different weight- 2 4 -tuple with $\overline{x} \neq y$ (Rule (i)). According to the Rule (iii), assume that the nonzero elements of x are in its i^{th} and j^{th} positions and the nonzero elements of y are in its i'^{th} and j'^{th} positions, where $i, j, i', j' \in \{1,2,3,4\}$ and we may take the following values for $g_{7,1}'^{(R)}$ and $g_{7,2}'^{(R)}$:

$$\left.\begin{aligned} g_{7,1}'^{(R)} &= \left\{P_{i'} + P_{j'} \ \ or \ \ \overline{P_{i'} + P_{j'}}\right. \\ g_{7,2}'^{(R)} &= \left\{P_i + P_j \ \ or \ \ \overline{P_i + P_j}\right. \end{aligned}\right\} \qquad (4)$$

It may be seen that these values also satisfy Rule (ii). Thus for these values of $g_{7,1}'^{(R)}$ and $g_{7,2}'^{(R)}$, G_7' becomes

$$G_7' = \begin{pmatrix} x & | & g_{7,1}'^{(R)} \\ y & | & g_{7,2}'^{(R)} \\ & g_h & \\ & g_{w=8} & \end{pmatrix} = \begin{pmatrix} x & | & P_{i'} + P_{j'} \ \ or \ \ \overline{P_{i'} + P_{j'}} \\ y & | & P_i + P_j \ \ or \ \ \overline{P_i + P_j} \\ & g_h & \\ & g_{w=8} & \end{pmatrix}. \qquad (5)$$

1st contradiction:

We'll show by an example that the matrix G_7' in (5) generates two 4 weighted codewords which are same as that of C_1.

*Example 1***:** Let the generator matrix of given systematic (8, 4, 4) code C_1 is

$$G_1 = \begin{pmatrix} 1000 & 1101 \\ 0100 & 0111 \\ 0010 & 1110 \\ 0001 & 1011 \end{pmatrix} = (I_4 \mid P) \qquad (6)$$

where $P = (P_1, P_2, P_3, P_4)^t$. This matrix G_1 generates six 2-and-2 codeword's viz.

$$\begin{aligned} cw1 &= (1100\ P_1 + P_2), & cw4 &= (0011\ P_3 + P_4), \\ cw2 &= (1010\ P_1 + P_3), & cw5 &= (0101\ P_2 + P_4), \\ cw3 &= (1001\ P_1 + P_4), & cw6 &= (0110\ P_2 + P_3). \end{aligned}$$

or

$$\begin{aligned} cw1 &= (1100\ 1010), & cw4 &= (0011\ 0101), \\ cw2 &= (1010\ 0011), & cw5 &= (0101\ 1100), \\ cw3 &= (1001\ 0110), & cw6 &= (0110\ 1001). \end{aligned}$$

Suppose G_7' is of the form (3) and ${g'_{7,1}}^{(L)} = x = 1100$ and ${g'_{7,2}}^{(L)} = y = 1010$. Here $x \neq y$ and $\bar{x} \neq y$ (Rule (i) is satisfied). Let us take the values of ${g'_{7,1}}^{(R)}$ and ${g'_{7,2}}^{(R)}$ using (4) (which satisfy the Rules (ii) and (iii)) viz. ${g'_{7,1}}^{(R)} = 0011$ and ${g'_{7,2}}^{(R)} = 1010$. For these values of x, y, ${g'_{7,1}}^{(R)}$ and ${g'_{7,2}}^{(R)}$ the matrix G_7' becomes

$$G_7' = \begin{pmatrix} 1100 & P_1 + P_3 \\ 1010 & P_1 + P_2 \\ 1111 & 0000 \\ 1111 & 1111 \end{pmatrix} = \begin{pmatrix} 1100 & 0011 \\ 1010 & 1010 \\ 1111 & 0000 \\ 1111 & 1111 \end{pmatrix}. \qquad (7)$$

This matrix generates two 4 weighted codewords (0110 1001) and (1001 0110) (by adding first two rows and 1st, 2nd and 4th rows respectively) which are same as $cw6$ and $cw3$ (4 weighted codeword's of C_1).

Before presenting the second contradiction we prove that a very useful fact based on the 1st contradiction in the following theorem 1.

Theorem 1: The matrix G_7', together with G_1 (defined in (5) and (1) respectively) do not generate Golay code C_{24} when applying them to (2).

Proof: Every word generated by G_{24} in (2) is of the form $(a + x \mid b + x \mid a + b + x)$ where $a, b \in C_1$ and $x \in C_7'$. As we have shown in 1st contradiction that some of the 4 weighted codeword's generated by both the matrices G_1 and G_7' are same. If we take $a = b = x$, the weight of the word $(a + x \mid b + x \mid a + b + x)$ is four which is less than eight. Thus the minimum weight of a non zero codeword generated by G_{24} is less than eight. This contradict the minimum distance of (24, 12, 8) Golay code.

*2nd contradiction***:**

Here we'll show by an example that for the matrix G_7' (defined in (5)), we can't construct G_8' by the construction rules (presented in subsection (A)). In context of Example-1 and G_7' in (7) Rules (ii) and (iii) imply the following restrictions on ${g'_{8,1}}^{(R)}$ and ${g'_{8,2}}^{(R)}$:

$${g'_{8,1}}^{(R)} \neq {g'_{7,1}}^{(R)}, \ \overline{{g'_{8,1}}^{(R)}} \neq {g'_{7,1}}^{(R)}$$

$${g'_{8,1}}^{(R)} \neq P_1 + P_2, \ \overline{{g'_{8,1}}^{(R)}} \neq P_1 + P_2$$

and

$${g'_{8,2}}^{(R)} \neq {g'_{7,2}}^{(R)}, \ \overline{{g'_{8,2}}^{(R)}} \neq {g'_{7,2}}^{(R)}$$

$${g'_{8,2}}^{(R)} \neq {g'_{8,1}}^{(R)}, \ \overline{{g'_{8,2}}^{(R)}} \neq {g'_{7,1}}^{(R)}$$

$${g'_{8,2}}^{(R)} \neq P_1 + P_3, \ \overline{{g'_{8,2}}^{(R)}} \neq P_1 + P_3$$

With these conditions ${g'_{8,1}}^{(R)}$ can take only two values viz. 1001 or 0110 but ${g'_{8,2}}^{(R)}$ has no choices. Therefore we can't construct G_8'.

III. Modified Construction Rules for G_7' and G_8'.

Rewriting G_7' *and* G_8' as follow

$$G_7' = \begin{pmatrix} {g'_{7,1}}^{(L)} & {g'_{7,1}}^{(R)} \\ {g'_{7,2}}^{(L)} & {g'_{7,2}}^{(R)} \\ \multicolumn{2}{c}{g_h} \\ \multicolumn{2}{c}{g_{w=8}} \end{pmatrix} \text{ and } G_8' = \begin{pmatrix} {g'_{8,1}}^{(L)} & {g'_{8,1}}^{(R)} \\ {g'_{8,2}}^{(L)} & {g'_{8,2}}^{(R)} \\ \multicolumn{2}{c}{g_h} \\ \multicolumn{2}{c}{g_{w=8}} \end{pmatrix} \qquad (8)$$

Rule (i) Assign

$${g'_{7,1}}^{(L)} = {g'_{8,1}}^{(L)} = x$$
$${g'_{7,2}}^{(L)} = {g'_{8,2}}^{(L)} = y\,.$$

Where x and y are any two different weight- 2 4 -tuple with $\bar{x} \neq y$, ($\bar{v}$ is the compliment of v).

Let ${g'_{7,1}}^{(R)} = x'$, ${g'_{7,2}}^{(R)} = y'$, ${g'_{8,1}}^{(R)} = x''$, ${g'_{8,2}}^{(R)} = y''$. Now first we assign values to x' and y' (according to Rule (ii)) and then to x'' and y'' (according to Rule (iii)).

Rule (ii)

Assume that the nonzero elements of x are in its i^{th} and j^{th} positions, and the nonzero elements of y are in its i'^{th} and j'^{th} positions, where $i, j, i', j' \in \{1,2,3,4\}$. The following conditions must also be satisfied.

- $x' \neq P_i + P_j \;\; and \;\; x' \neq \overline{P_i + P_j}$,
- $y' \neq P_{i'} + P_{j'} \;\; and \;\; y' \neq \overline{P_{i'} + P_{j'}}$,
- $y' \neq x' \;\; and \;\; y' \neq \overline{x'}$
- either $x' \neq P_{i'} + P_{j'}$ and $x' \neq \overline{P_{i'} + P_{j'}}$ or $y' \neq P_i + P_j$ and $y' \neq \overline{P_i + P_j}$ not both (9)

Here P_u $(1 \le u \le 4)$ are the row vectors of P in G_1 .

Rule (iii)

After obtaining x, y, x', y' using above Rules, we find x'', y'' that must satisfy the following conditions

- $x'' \neq P_i + P_j \;\; and \;\; x'' \neq \overline{P_i + P_j}$,
- $x'' \neq x' \;\; and \;\; x'' \neq \overline{x'}$,
- $y'' \neq P_{i'} + P_{j'} \; and \;\; y'' \neq \overline{P_{i'} + P_{j'}}$,
- $y'' \neq y' \;\; and \;\; y'' \neq \overline{y'} \;\; and$
- $y'' \neq x'' \;\; and \;\; y'' \neq \overline{x''}$.

Here, we present the general form of matrices formed using the abovementioned modified construction rules.

As we know $G_1 = (I_4 \; P)$ where I_4 is the 4×4 identity matrix. Writing I_4 as $I_4 = [r_1 \; r_2 \; r_3 \; r_4]^T$ and P as $P = [P_1 \; P_2 \; P_3 \; P_4]^T$. According to **Rule (i)** if we take $x = r_1 + r_j \; or \; \overline{r_1 + r_j}$ and $y = r_1 + r_{j'} \; or \; \overline{r_1 + r_{j'}}$ for some $2 \le j, j', j'' \le 4$ such that $j \neq j' \neq j''$ **Rule (ii)** affirms that x' has two choices either $x' \in \{P_1 + P_{j''} \; , \; \overline{P_1 + P_{j''}}\}$ or $x' \in \{P_1 + P_{j'} \; , \; \overline{P_1 + P_{j'}}\}$.

Csae (i): When $x' \in \{P_1 + P_{j''} \; , \; \overline{P_1 + P_{j''}}\}$ then (9) implies that $y' \in \{P_1 + P_j \, , \, \overline{P_1 + P_j}\}$ and from **Rule (iii)**, $x'' \in \{ P_1 + P_{j'} \, , \overline{P_1 + P_{j'}} \}$ and $y'' \in \{ P_1 + P_{j''} \, , \overline{P_1 + P_{j''}} \}$.

Csae (ii): When $x' \in \{P_1 + P_{j'} \; , \; \overline{P_1 + P_{j'}}\}$ then (9) implies that $y' \in \{P_1 + P_{j''} \; or \; \overline{P_1 + P_{j''}}\}$ and from **Rule (iii)**, $x'' \in \{ P_1 + P_{j''} , \overline{P_1 + P_{j''}}\}$ and $y'' \in \{ P_1 + P_j \, , \overline{P_1 + P_j} \}$.

Thus, for these values of x, y, x', y', x'' and y'' together with

$g_h = (11110000) \; or \, (00001111) \; and \;\; g_{w=8} = (11111111)$

G_7' and G_8' in (8) become for case (i) and for case (ii) respectively:

$$G_7' = \begin{pmatrix} x & x' \\ y & y' \\ \multicolumn{2}{c}{g_h} \\ \multicolumn{2}{c}{g_{w=8}} \end{pmatrix} = \begin{pmatrix} r_1 + r_j \; or \; \overline{r_1 + r_j} & P_1 + P_{j''} \; or \; \overline{P_1 + P_{j''}} \\ r_1 + r_{j'} \; or \; \overline{r_1 + r_{j'}} & P_1 + P_j \; or \; \overline{P_1 + P_j} \\ \multicolumn{2}{c}{g_h} \\ \multicolumn{2}{c}{g_{w=8}} \end{pmatrix}$$

$$G_8' = \begin{pmatrix} x & x'' \\ y & y'' \\ \multicolumn{2}{c}{g_h} \\ \multicolumn{2}{c}{g_{w=8}} \end{pmatrix} = \begin{pmatrix} r_1 + r_j \; or \; \overline{r_1 + r_j} & P_1 + P_{j'} \; or \; \overline{P_1 + P_{j'}} \\ r_1 + r_{j'} \; or \; \overline{r_1 + r_{j'}} & P_1 + P_{j''} \; or \; \overline{P_1 + P_{j''}} \\ \multicolumn{2}{c}{g_h} \\ \multicolumn{2}{c}{g_{w=8}} \end{pmatrix} \quad (10)$$

$$G_7' = \begin{pmatrix} x & x' \\ y & y' \\ \multicolumn{2}{c}{g_h} \\ \multicolumn{2}{c}{g_{w=8}} \end{pmatrix} = \begin{pmatrix} r_1 + r_j \; or \; \overline{r_1 + r_j} & P_1 + P_{j''} \; or \; \overline{P_1 + P_{j''}} \\ r_1 + r_{j'} \; or \; \overline{r_1 + r_{j'}} & P_1 + P_j \; or \; \overline{P_1 + P_j} \\ \multicolumn{2}{c}{g_h} \\ \multicolumn{2}{c}{g_{w=8}} \end{pmatrix}$$

$$G_8' = \begin{pmatrix} x & x'' \\ y & y'' \\ \multicolumn{2}{c}{g_h} \\ \multicolumn{2}{c}{g_{w=8}} \end{pmatrix} = \begin{pmatrix} r_1 + r_j \; or \; \overline{r_1 + r_j} & P_1 + P_{j'} \; or \; \overline{P_1 + P_{j'}} \\ r_1 + r_{j'} \; or \; \overline{r_1 + r_{j'}} & P_1 + P_{j''} \; or \; \overline{P_1 + P_{j''}} \\ \multicolumn{2}{c}{g_h} \\ \multicolumn{2}{c}{g_{w=8}} \end{pmatrix} \quad (11)$$

It is obvious that all four rows of G_7' and G_8' in (10) and (11) are linearly independent. Now, we show an important result in following Lemma 1.

Lemma 1: The codes generated by these matrices are (8, 4, 4) code spaces.

Proof: This is equivalent to showing that both the codes have the weight distribution $\{N(0) = 1; N(4) = 14; N(8) = 1\}$ where $N(x)$ represents the number of the codeword's of weight x. From the structure of the matrices row 1, row 2 and row 3 are 4-weighted words. Also linear combination of any two, three and four rows results in 4-weighted words. Thus, the total number of such words is $3 + \binom{4}{2} + \binom{4}{3} + \binom{4}{4} = 14$. Other than these weight-4 words G_7' and G_8' have the all-one row $g_{w=8}$ which fulfill our requirement i.e. the matrices generate (8, 4, 4) code spaces. It is apparent that the matrices G_7' in (10) and (11) generate the same code for every choice of x' and y' with $2 \le j, j', j'' \le 4$ such that $j \neq j' \neq j''$. Same argument can be given for G_8' with x'' and y''.

The matrices G_7' and G_8' in (10) and (11) have an interesting property which is proved in the Theorem 2 given below.

Theorem 2: All 4-weighted codeword's of (8, 4, 4) codes generated by G_7' and G_8' are distinct from the 4-weighted codeword's of given (8, 4, 4) linear block code C_1 .

International Journal of Innovation in Science and Mathematics
Volume 3, Issue 2, ISSN (Online): 2347–9051

Proof: Let C_1 be a systematic (8, 4, 4) code space with generator matrix G_1 of the form $G_1 = (I_4 \mid P)$ where $I_4 = (r_1, r_2, r_3, r_4)^T$ and $P = (p_1, p_2, p_3, p_4)^T$. It doesn't generate the codeword's (00001111) and (11110000), but it will generate six 2-and-2 codeword's. From the structure of G_1, these six codeword's can be expressed as

$$\begin{aligned} cw1 &= (r_1 + r_2 \;\; P_1 + P_2),\; cw4 = (\overline{r_1 + r_2} \;\; \overline{p_1 + p_2}), \\ cw2 &= (r_1 + r_3 \;\; P_1 + P_3),\; cw5 = (\overline{r_1 + r_3} \;\; \overline{p_1 + p_3}), \\ cw3 &= (r_1 + r_4 \;\; P_1 + P_4),\; cw6 = (\overline{r_1 + r_4} \;\; \overline{p_1 + p_4}). \end{aligned} \tag{12}$$

Let us consider G_7' defined in (10), the 4-weighted codeword's formed by G_7' can be divided into three groups:

$(i)\; \xi_1, \xi_2, \xi_1 + \xi_2, \xi_1', \xi_2', (\xi_1 + \xi_1)'$;
$(ii)\; \overline{\xi}_1, \overline{\xi}_2, \overline{\xi_1 + \xi_2}, \overline{\xi'}_1, \overline{\xi_2'}, \overline{(\xi_1 + \xi_1)'}$;
(iii) (1111 0000), (0000 11111).

Where

$$\xi_1 = (r_1 + r_j \;\; P_1 + P_{j''} \;\; or \;\; \overline{P_1 + P_{j''}}),$$
$$\xi_2 = \left(r_1 + r_{j'} \;\; P_1 + P_j \;\; or \;\; \overline{P_1 + P_j}\right),$$

$u' = u + g_h$ where $u \in U = \{\xi_1, \xi_2, \xi_1 + \xi_2\}$; and
$\overline{v} = v + g_{w=8}$ where $v \in V = U \bigcup \{\xi_1', \xi_2',, (\xi_1 + \xi_2)'\}$.

Since codeword's of group (iii) are not present in C_1 together with the fact $\alpha \neq \delta \Rightarrow \overline{\alpha} \neq \overline{\delta}$ we need only to show that the codeword's of group (i) are distinct from the codeword's in (12). From the structure of G_7' defined in (10) the codeword's of group (i) can be expressed as:

$$\left.\begin{aligned} \xi_1 &= (r_1 + r_j \;\; P_1 + P_{j''} \;\; or \;\; \overline{P_1 + P_{j''}}), \\ \xi_2 &= (r_1 + r_{j'} \;\; P_1 + P_j \;\; or \;\; \overline{P_1 + P_j}), \\ \xi_1 + \xi_2 &= (\overline{r_1 + r_{j''}} \;\; \overline{P_1 + P_{j'}} \; or \; P_1 + P_{j'}), \\ \xi_1' &= (r_1 + r_j \;\; \overline{P_1 + P_{j''}} \;\; or \;\; P_1 + P_{j''}), \\ \xi_2 &= (r_1 + r_{j'} \;\; \overline{P_1 + P_j} \;\; or \;\; P_1 + P_j), \\ (\xi_1 + \xi_2)' &= (\overline{r_1 + r_{j''}} \;\; P_1 + P_{j'} \;\; or \;\; \overline{P_1 + P_{j'}}) \end{aligned}\right\}. \tag{13}$$

Evidently, from (12) and (13) it is proved that the codeword's of group (i) are distinct from the codeword's in (12). Now it can be concluded that all the 4-weighted codeword's of C_7' are distinct from those of C_1. In a similar manner the above result can be proved for C_8'.

Now, we'll show by a theorem that the code generated by (2) is the extended Golay code. The methodology of the proof of this theorem adopted here is very standard originally given by Turyn [3] then used by Peng and Farrell [6].

Theorem 3: Let G_1, G_7' and G_8' are the generator matrices (defined in (1), (10) and (11) respectively) of C_1, C_7' and C_8'. Then the code obtained by (2) is the (24, 12, 8) Golay code.

Proof: With reference of Lemma 1, it is required to prove that the minimum distance of the code generated by (2) is 8 which is equivalent to showing that the minimum weight of the words generated by G_{24} is 8. Let ξ be any nonzero word generated by G_{24} defined in (2) then ξ is of the form $\xi = (a + x \mid b + x \mid a + b + x)$ where $a, b \in C_1$ and $x \in C_7'$. Each of a, b, x has weight 0, 4 and 8 and

$$w(\xi) = w(a + x) + w(b + x) + w(a + b + x). \tag{14}$$

Theorem 2 ensures that

$$w(\zeta + x) \geq 2 \text{ where } \zeta \in C_1 \text{ and } x \in C_i';\ (i = 7, 8). \tag{15}$$

Now, we have the following cases for the weights of a, b and x: (i) If exactly one of the a, b and x is of weight 4, $w(\xi) \geq 8$. (ii) If exactly two of a, b and x are of weight 4, (15) ensures that $w(\xi) \geq 8$. (iii) If all a, b and x are of weight 4 then we have the following two subcases: (1) If $a = b$, $a + b = 0$ (the all zero 8-tuple) together with (14) and (15) imply $w(\xi) \geq 8$. (2) $a \neq b$ and $a + b = 4$, this subcase can further be divided in two subcases: (2.1) When $w(a + x) = 2$ and $w(b + x) = 4$ or vice-versa then $w(a + b + x) \geq 2$. (2.2) When $w(a + x) = 2$ and $w(b + x) = 2$ then

$$\begin{aligned} w(a + b + x) = {} & w(a + x) + w(b + x) \\ & - \text{number of positions where } x \text{ is 1} \\ & \quad \text{and either } a \text{ is 0 or } b \text{ is 0 (not both)} \\ & + \text{number of positions where } a, b \text{ and } x \text{ all are1.} \end{aligned}$$

Both the subcases (2.1) and (2.2) together with (14) and (15) leads to $w(\xi) \geq 8$. Apart from the cases stated above if atleast one of the a, b and x is of weight 8 then obviously the minimum weight of ξ is 8. Hence in all the cases $w(\xi) \geq 8$.

Thus the code constructed by (2) is (24, 12, 8) code which is unique in terms of its parameters [2]. Hence the construction leads to the extended binary Golay code.

IV Conclusion

A particular case is proposed where the construction rules given in [6] fail to form such non systematic (8, 4, 4) codespaces which can be used to generate the extended binary Golay code through $|a+x|b+x|a+b+x|$ construction. We have redefined the construction rules for the generator matrices of non systematic (8, 4, 4) codespaces and it is proved that these codes together with the given systematic (8, 4, 4) linear block code form (24,12,8) Golay code.

REFERENCES.

[1] F. J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1978.
[2] V. Pless, "On the uniqueness of the Golay code," *J. Comb. Theory*, vol.5, pp. 215–228, Nov. 1968.
[3] E. F. Assmus, Jr., H. F. Mattson, and R. J. Turyn, Research to Develop the Algebraic Theory of Codes Air Force Cambridge Res. Lab, Bedford, 1967, Mass., Sci. Rep. AFCRL-67-0365.
[4] N. J. A. Sloane, S. M. Reddy, and C. L. Chen, "New binary codes," *IEEE Trans. Inf. Theory*, vol. 18, pp. 503–510, July 1972.
[5] G. D. Forney, "Coset codes—Part II: Binary lattices and related codes," *IEEE Trans. Inf. Theory*, vol. 34, pp. 1152–1187, Sep. 1988.
[6] X.-H. Peng and P. Farrell, "On construction of the (24; 12; 8) Golay codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 8, pp. 3669–3675, Aug. 2006.
[7] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.
[8] R. E. Blahut, *Algebraic Codes for Data Transmission*. Cambridge,U.K.: Cambridge Univ. Press, 2004.
[9] H. Anton, *Elementary Linear Algebra*. New York: Wiley, 2003.
[10] G. D. Forney, "Coset codes-part I: Introduction and geometrical classification," *IEEE Trans. Inf. Theory*, vol. 34, no. 5, pp. 1123–1151, Sep. 1988.
[11] Vikas Dhaka and O.P. Vinocha , "Augmented product construction of Barnes-Wall lattices". Applied mathematical sciences, Vol. 5, no. 61-64, 3107-3119, 2011, ISSN 1312- 885X.
[12] Vikas Dhaka and O.P. Vinocha, "On construction of Barnes-Wall lattices". Journal of Mathematical and Computational science, (3) 2013, No. 5, 1271-1285, ISSN 1927-5307.

AUTHOR'S PROFILE

Nidhi Nijhawan
is currently pursuing her Ph.D as a senior research scholar from the Department of Operational Research, University of Delhi, Delhi. She has obtained her M.Phil and M.Sc degrees in Operational Research from the University of Delhi, Delhi in 2008 and 2005 respectively. Her present research interests are software reliability growth modeling, coding theory and soft computing.
email: nijhawan.nidhi82@gmail.com

Vikas Dhaka
obtained his Ph.D and M.Sc degrees in Mathematics from the Maharaja Ganga Singh University, Bikaner, Rajasthan in 2013 and 2005, respectively. Currently, he is an Assistant Professor in Miranda House, University of Delhi, Delhi. He has published several papers in the area of Coding Theory. His research interests include Information Theory, Error-Correcting codes and their encoding and decoding.
email: vdhaka84@gmail.com

Jatin Anand
He is presently working as assistant professor in Miranda House, University of Delhi. He obtained Masters Degree in Mathematics from University of Delhi. His areas of interest include Operator Theory, Hardy Spaces, Coding Theory and ancient Indian Mathematics.
email: jatin.msf@gmail.com