On Construction of the (24, 12, 8) Golay Codes

Xiao-Hong Peng, Member, IEEE, and Paddy G. Farrell, Life Fellow, IEEE

Abstract—Two product array codes are used to construct the (24, 12, 8) binary Golay code through the direct sum operation. This construction provides a systematic way to find proper (8, 4, 4) linear block component codes for generating the Golay code, and it generates and extends previously existing methods that use a similar construction framework. The code constructed is simple to decode.

Index Terms—Array codes, block codes, code construction, direct sum, Golay codes.

I. INTRODUCTION

The (24, 12, 8) binary block code, denoted by \( C_{24} \), was originally constructed by extending the (23, 12, 7) Golay code [1], a unique 3-error correcting perfect code. Because of the optimality and attractive structure of \( C_{24} \), which is self dual and doubly even [2], it has received considerable attention, leading to a large number of construction methods. Using design theory, \( C_{24} \) can be formed through a 2-(11, 6, 3) design or the 5-(24, 8, 1) Steiner system [3]. All the codewords of \( C_{24} \) can also be generated by ordering a set of words of length 24 over the \( \{0, 1\} \) alphabet lexicographically [4]. Other approaches based on constructions in a larger field include the use of a Reed-Solomon code over \( \mathbb{F}_q \) [5], the hexacode over \( \mathbb{F}_4 \) [6] and the cubic residue code over \( \mathbb{F}_4 \) [7] or the Mathieu group \( M_{12} \) [8]. \( C_{24} \) can also be constructed using component codes with shorter length and smaller dimension. This method is based on the so-called Turyn \( [a + x|b + x|a + b + x] \) construction [9], where \( a, b \in C_x \), \( x \in C_v \), and \( C_x \) and \( C_v \) are two component codes with the same length. There are three examples utilizing this construction: i) \( C_x \) is the extended (7, 4, 3) cyclic Hamming code and \( C_v \) is formed by reversing the codewords of \( C_x \) except for the overall parity check added through the extension [9]; ii) \( C_x \) is the (8, 4, 4) first-order Reed-Muller code and \( C_v \) is formed by reversing the codewords of \( C_x \) except for the overall parity check [10]; and iii) \( C_x \) is also the (8, 4, 4) first-order Reed-Muller code and \( C_v \) is a column permutation of \( C_x \) [11].

In this paper, we present a construction of the (24, 12, 8) Golay code based on two array codes. In this construction, four component codes are involved: a (3, 2, 2) single-parity-check (SPC) code, a (3, 1, 3) repetition code and two (8, 4, 4) linear block codes. We have discovered that given an (8, 4, 4) code in systematic form, there exist eight other different (8, 4, 4) codes obtained either through proper row permutation on the parity submatrix 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, in all cases leads to the construction of the (24, 12, 8) Golay code. This construction systematizes and extends our previous [12] and other existing methods, including [2], [9]-[11], that apply the \( [a + x|b + x|a + b + x] \) framework and use two (8, 4, 4) codes. The code constructed can be, as in the case of related constructions [2], [11], decoded with low complexity.

II. CONSTRUCTION METHOD

A. The Generator matrices

The two array codes concerned are both two-dimensional product codes. A product code \( C \) is formed by a direct product [2] of two component codes \( C_i = (n_i, k_i, d_i) \) and \( C_j = (n_j, k_j, d_j) \). The generator matrix, \( G \), of \( C \) is represented in the form of a Kronecker product (denoted by \( \otimes \) ) of generator matrices of its component codes, \( G_i \) and \( G_j \), i.e.,

\[
G = G_i \otimes G_j = \left( g_{i,j}^{(1)} G_j \right) \quad \text{or} \quad G = G_2 \otimes G_1 = \left( g_{i,j}^{(2)} G_i \right)
\]

(1)

where \( G_i = \left( g_{i,j}^{(i)} \right) \) and \( G_j = \left( g_{i,j}^{(j)} \right) \). The resulting code is an \( (n_i n_j, k_i k_j, d_i d_j) \) product code, and \( G \) is of size \( (k_i k_j) \times (n_i n_j) \).
The first array code $C$ is the (24, 8, 8) product code constituted by $C = C_1 \times C_2$, where $C_1$ and $C_2$ denote an (8, 4, 4) linear systematic block code and a (3, 2, 2) single-parity-check code, respectively. The generator matrix of $C_2$ is

$$
G_2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}
$$

Therefore, according to (1), the generator matrix of $C$ is given by

$$
G = G_1 \otimes G_2 = \begin{bmatrix} G_1 & 0 & G_1 \\ 0 & G_1 & G_1 \end{bmatrix}
$$

(2)

where $G_1$ is the 4×8 generator matrix of $C_1$, and ‘0’ represents a 4×8 null matrix. It is noted that the (24, 8, 8) generator matrix of $C$ is always in position to the zero elements of the codewords of $C$, and vice versa. This means that $C_1$ and $C_2$ are guaranteed to be disjoint.

Lemma 1: Code subspaces $C$ and $C'$ defined in (2) and (3) are disjoint.

Proof: We need to show that for any $\alpha$ and $\alpha'$ defined in (4), $\alpha + \alpha' = 0$ implies that $\alpha = 0$ and $\alpha' = 0$. Codeword $\alpha$ can be expressed as $(a, 0, a)$, $(0, b, b)$ or $(a, b, b)$, where $a, b \in C_1$, according to (2). Also, $\alpha'$ can be expressed as $(x, x, x)$, where $x \in C'$, according to (3). Suppose that $\alpha + \alpha' = 0$. Then we have

$$
\alpha + \alpha' = \begin{cases} 
(a + x, x, a + x) = 0 & \text{(i)} \\
(x, b + x, b + x) = 0 & \text{(ii)} \\
(a + x, b + x, a + b + x) = 0 & \text{(iii)}
\end{cases}
$$

From (iii), it implies that $a + x = 0, b + x = 0$ and $a + b + x = 0$. Thus it is easy to conclude that $\alpha = 0$, $b = 0$ and $x = 0$, leading to $\alpha = 0$ and $\alpha' = 0$. The same result can be attained for (i) and (ii).

Following Lemma 1, we now can regard code $\hat{C}$ as a result of the direct sum, denoted by $\oplus$, of $C$ and $C'$, i.e.,

$$
\hat{C} = C \oplus C'
$$

(5)

with the dimension: $\dim(\hat{C}) = \dim(C) + \dim(C') = 8 + 4 = 12$.

The generator matrix of $\hat{C}$ is therefore given by

$$
\hat{G} = \begin{bmatrix} G_1 & 0 & G_1 \\ 0 & G_1 & G_1 \end{bmatrix}
$$

(6)

We can see from (6) that $\hat{C}$ is an $(n, k) = (24, 12)$ linear code. We also notice that the codewords in $\hat{C}$ are of the form $[a + x][b + x][a + b + x]$, where $a, b \in C_1$ and $x \in C'$, which is also the case for the Turyn [9] or cubing [11] construction.

The minimum distance of $\hat{C}$ depends on the structures of $C_1$ and $C'$, or $G_1$ and $G_1'$. We present next a method of obtaining $G_1$ and $G_1'$ which guarantees that the minimum distance of $\hat{C}$ is 8.

Let $C_i$ be an (8, 4, 4) systematic code. The generator matrix of $C_i$ is expressed as

$$
G_i = \begin{bmatrix} I_4 & P \end{bmatrix}
$$

(7)
Here \( I_4 \) is the 4x4 identity matrix and \( P \) is a 4x4 parity submatrix of \( G_i \). 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 \( S = \{ (1110), (1011), (0111), (0111) \} \) 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 codewords of weight \( x \).

\( C_i' \) can be a systematic or non-systematic code. It will be shown later that for a given systematic \( G_i \) there exist eight different \( G_i', G_i''', \ldots, G_i'''' \), all leading to the construction of \( C_{24} \) when applying them to (6). Among them, \( G_i', \ldots, G_i'''' \) are systematic, while \( G_i''', G_i'''' \) are non-systematic, which will be discussed separately in sub-sections B and C.

**B. The Permutation Criteria for Constructing \( G_i', \ldots, G_i'''' \)**

When \( C_i' \) is a systematic code, its generator matrix is expressed by
\[
G_i' = (I_4, P') .
\]  
(8)

The parity submatrix of \( G_i', P' = (P_1', P_2', P_3', P_4')^T \), will be generated through certain row permutations, as described later in this section, of the parity submatrix \( P \) of \( G_i \). Note that the row permutation concerned here only takes place on the parity submatrix of \( G_i \), so it will change the structure of code subspace \( C_i \). Although this is equivalent to the column permutation of \( P \), the choice of using row permutation will make Theorem 1 given later in this session easier to prove. The parity submatrix \( P' \) as the permutation of \( P \) must satisfy the criteria stated below.

**Permutation Criteria:**

Cri(i) \( P_i' \neq P_j' \) for \( 1 \leq i \leq 4 \); and

Cri(ii) \( \{P_i', P_j'\} \neq \{P_i, P_j\} \) for \( 1 \leq i, j \leq 4 \) and \( i < j \). This means that any subset of two row vectors in \( P' \) is not identical to the corresponding subset in \( P \), where two subsets are said to be identical if they contain the same elements regardless of the order of the elements in the subset.

Before presenting the result of our construction given in Theorem 1, we prove a useful fact based on the above criteria in Lemma 2.

**Lemma 2:** All weight-4 codewords of \( C_i \) and \( C_i' \) are distinct (here \( C_i' \) represents only \( C_i'(1), C_i'(2), \ldots, \) or \( C_i'(6) \)).

**Proof:** The weight-4 codewords of the \((8, 4, 4)\) code are generated by linear combinations of either 1, 2 or 3 row vectors of the generator matrix at a time. As both \( C_i \) and \( C_i' \) are systematic codes, we need only to prove in this case that any of such linear combinations of \( P \) is distinct from the corresponding one that involves the same subset of row vectors of \( P' \). In fact, combinations involving 1 and 2 row vectors are covered by Cri(i) and Cri(ii), respectively, while combinations involving 3 row vectors follows from Cri(i) as well since, given the total number of row vectors to be 4 for both \( P \) and \( P' \), Cri(ii) implies that \( \{P_i', P_j', P_l'\} \neq \{P_i, P_j, P_l\} \) for \( i, j, l = 1, 2, 3, 4 \) and \( i < j < l \).

**Theorem 1:** The code \( \hat{C} \) generated by (6), with \( G_i \) defined in (7) and \( G_i' \) defined in (8) and satisfying the Permutation Criteria is a \((24, 12, 8)\) linear code; i.e., \( C_{24} \).

**Proof:** The linearity of the code is obvious as \( \hat{C} \) is the direct sum of \( C \) and \( C' \) which both are linear. With Lemma 1, we need only to show that the minimum distance of \( \hat{C} \) is 8. The weights of the codewords of both \( C_i \) and \( C_i' \) are 0, 4 or 8.

From the structure of the codewords of \( \hat{C} \):
\[
\hat{c} = (a + x, b + x, a + b + x) \quad \text{where} \quad a, b \in C_i \quad \text{and} \quad x \in C_i',
\]
it follows, by applying Lemma 2, that \( wt(e + x) \geq 2 \) for any \( e \in C_i \) and \( x \in C_i' \), where \( e \) can be either \( a, b \) or \( a+b \), and \( wt(y) \) represents the weight of \( y \). It is obvious that \( wt(e + x) \geq 2 \) is a sufficient condition for \( wt(\hat{c}) \geq 8 \), except in the case where \( a, b, a+b \) and \( x \) all have weight 4 and \( a \neq b \).

This case has two sub-cases: if \( wt(a + x) = 2 \) and \( wt(b + x) = 2 \), then the condition \( wt(a+b) = 4 \) ensures that \( wt(a+x+b) = 6 \), because the support (positions of non-zero elements) of \( x \) must overlap with the supports of both \( a \) and \( b \) in two positions; if \( wt(c + x) = 2 \) and \( wt(d + x) = 4 \), or vice-versa, the supports overlap in only one position and \( wt(a+b+x) = 6 \). In either sub-case \( wt(\hat{c}) \geq 8 \).

It has been shown [14] that \( C_{24} \) is unique in terms of the code parameters such as the length, dimension, minimum distance and weight distribution, thus the construction presented here generates the \((24, 12, 8)\) Golay code.

Suppose that the parity submatrix of \( G_i \) is given as \( P = (P_1, P_2, P_3, P_4)^T \). We will show here that there exist six permutations of \( P, P' \), that all satisfy the criteria and can be used to construct \( G_i' \) and consequently \( C_{24} \). Form an index set \( L = \{1, 2, 3, 4\} \) representing the elements of \( P \). The six permutations satisfying the criteria can be found by checking each of the \( 4! = 24 \) permutations of \( L \) against the criteria, as follows:
Applying one-to-one mappings of these permutations onto \( P \) gives six corresponding permutations, \( P' = P'^{(r)} \) for \( 1 \leq r \leq 6 \), and consequently six different \( G'_{\ell} \); i.e., \( G'_{(1)}, \ldots, G'_{(6)} \), respectively. This will be the case for any choice of systematic \( G_{\ell} \), as the number of such permutations is always given by \( 3! = 6 \). This is because, in order to meet the criteria, the first row vector of the parity submatrix can be placed in any of 3 other positions (rows); then the vector thus displaced can be placed in any of 2 other positions (not its original position nor the original position of the first vector); in the same way, the third vector can only be placed in one designated position; and finally the fourth vector is placed in the only remaining position.

C. The Construction Rules for \( G'_{(7)} \) and \( G'_{(8)} \)

In addition to the six systematic \((8, 4, 4)\) code subspaces generated by \( G_{(1)}, \ldots, G_{(6)} \), there are two more \((8, 4, 4)\) code subspaces, which also satisfy the conditions for constructing \( C_{24} \) using (6) with the given \( C_{1} \). However, these two codes are not systematic since they have, unlike the other six codes, 8-tuples of weight 2 or 6, e.g., \((11110000) + (11010100) = (01111110)\). We call this type of weight-4 codewords 2-and-2 codewords.

Therefore, the structures of the generator matrices of these two codes, \( G'_{(7)} \) and \( G'_{(8)} \), will be characterized by the above features, and all weight-4 codewords generated by \( G'_{(7)} \) or \( G'_{(8)} \) must satisfy the statement given in Lemma 2; i.e., they are distinct from those generated by the given \( G_{1} \). Based on these conditions, the two generator matrices are designed in the forms

\[
G'_{(7)} = \begin{pmatrix} g'_{(7),1} \\ g'_{(7),2} \\ g'_{4} \\ g'_{5} \\ g'_{6} \end{pmatrix} \quad \text{and} \quad G'_{(8)} = \begin{pmatrix} g'_{(8),1} \\ g'_{(8),2} \\ g'_{4} \\ g'_{5} \\ g'_{6} \end{pmatrix}
\]

(10)

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

### Construction Rules:

**Rule(i)** Assign

\[
g'_{7,\ell,1} = g_{\ell,1} = x \quad \text{and} \quad g'_{7,\ell,2} = g_{\ell,2} = y,
\]

where \( x \) and \( y \) are any two different weight-2 4-tuple with \( \overline{x} \neq y \) (\( \overline{v} \) is the complement of \( v \)).

**Rule(ii)** \( g'_{8,\ell,m} \) \((\ell = 7, 8 \text{ and } m = 1, 2)\) must satisfy

\[
g'_{8,\ell,1} \neq g'_{8,\ell,1} \quad \text{and} \quad g'_{8,\ell,2} \neq g'_{8,\ell,2} \quad \text{for } m = 1, 2;
\]

\[
g'_{8,\ell,1} \neq g'_{8,\ell,2} \quad \text{and} \quad g'_{8,\ell,1} \neq g'_{8,\ell,2} \quad \text{for } \ell = 7, 8.
\]

**Rule(iii)** Assume that the nonzero elements of \( x \) are in its \( i \)-th and \( j \)-th positions, and that 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.

\[
g'_{8,\ell,1} \neq (P_{i} + P_{j}) \quad \text{and} \quad g'_{8,\ell,2} \neq (P_{i} + P_{j}) \quad \text{for } \ell = 7, 8;
\]

\[
g'_{8,\ell,1} \neq (P_{i} + P_{j}) \quad \text{and} \quad g'_{8,\ell,2} \neq (P_{i} + P_{j}) \quad \text{for } \ell = 7, 8.
\]

Here \( P_{m} \) \((1 \leq m \leq 4)\) are the row vectors of \( P \) in \( G_{1} \) given in (7).

### Theorem 2

Applying \( G'_{(7)} \) or \( G'_{(8)} \) given in (10) and satisfying the Construction Rules to the generator matrix given in (6), \( G'_{\ell} \), together with \( G_{1} \) defined in (7), generates \( C_{24} \).

The proof of Theorem 2 is provided in the APPENDIX.

### Example

Given \( G_{1} \) as the generator matrix of a systematic \((8, 4, 4)\) code, i.e.,

\[
G_{1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}
\]

and

\[
P = \begin{pmatrix} (1 & 1 & 0 & 1) \\ (0 & 1 & 1 & 1) \\ (1 & 1 & 0 & 0) \\ (1 & 0 & 1 & 1) \end{pmatrix} = (P_{1}, P_{2}, P_{3}, P_{4})^{T},
\]

and using the results given in (9), the six corresponding permutations of \( P, P'^{(r)} \) \((1 \leq r \leq 6)\), follow accordingly:

\[
P^{(r)} = \begin{pmatrix} (1 & 1 & 0) \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix},
\]

\[
P^{(r)} = \begin{pmatrix} (1 & 1 & 0) \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix},
\]

\[
P^{(r)} = \begin{pmatrix} (1 & 1 & 0) \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}.
\]
that all lead to the construction of $L \leq L^2$, or $L = L^3$ and by the Construction Rules and (10) for $L_i$. Rule(i) by choosing $g(R)$.

Different $G$ can then be constructed by using $g(R)$ and $g(L)$. We then follow Rule(ii) and Rule(iii) by assigning: $g(R) = (0110)$, $g(L) = (0101)$; and $g(L) = (0111)$. Finally, we have

$$G'_1 = \begin{pmatrix} g(R) \cr g(L) \end{pmatrix}, \quad G'_2 = \begin{pmatrix} g(R) \cr g(L) \end{pmatrix}, \quad G'_3 = \begin{pmatrix} g(R) \cr g(L) \end{pmatrix}$$

and $G'_4 = \begin{pmatrix} g(R) \cr g(L) \end{pmatrix}$. $G'_2$ can then be constructed by using $G_1$ and $G_1'$ in the framework of $G'$ given in (6), where $G'_1$ can be any one of the $G'_1, \ldots, G'_4$ formed above. The codes generated using different $G'_1$ will have the same weight distribution: $N(0) = 1, N(1) = 759, N(4) = 2576, N(8) = 759, N(24) = 1$.

III. REMARKS

The example given above shows that for the given generator matrix of a systematic (8, 4, 4) code, $G_i = (I_4, P)$, there exist eight different $G'_1, G'_2 = (I_4, P^m)$ $(1 \leq m \leq 6)$ plus $G'_7$ and $G'_8$, that all lead to the construction of $C_{24}$. These eight different $G'_1$ and the original $G_1$ represent different (8, 4, 4) code subspaces, although they have the same code parameters $(n, k, d)$ and weight distribution $N(0) = 1, N(4) = 14, N(8) = 1$. We have observed some interesting properties among this group of subspaces. Denoted by $S^{(i)}_{8,4}$ $(0 \leq i \leq 8)$ the set of weight-4 codewords generated by an (8, 4, 4) linear code over $GF(2)$, and $S^{(i)}_{8,4}$ is generated by $C_i$ and $S^{(i)}_{8,4}, \ldots, S^{(i)}_{8,4}$ by $C'_1, \ldots, C'_4$, respectively. Thus the following properties exist:

Pro(i) $|S^{(i)}_{8,4}| = 14$ for $0 \leq i \leq 8$.

Pro(ii) $S^{(i)}_{8,4} \cap S^{(j)}_{8,4} = \{ \}$ for $1 \leq i \leq 8$.

Pro(iii) $|S^{(i)}_{8,4} \cap S^{(j)}_{8,4}| = 2, \ i, j \in \{1, \ldots, 8\}$ and $i \neq j$.

Pro(i) is obvious as the weight-4 codewords are the results of the linear combinations of either 1, 2 or 3 row vectors of the generator matrix of the (8, 4, 4) code, i.e.,

$$|S^{(i)}_{8,4}| = \sum_{j=1}^{3} \binom{4}{j} = 14.$$ Pro(ii) is guaranteed by Lemma 2 for $G'_1, \ldots, G'_4$, and by the Construction Rules and (10) for $G'_7$ and $G'_8$. Pro(iii) is also true based on the Permutation Criteria and the Construction Rules. If one wishes to generate some weight-4 codewords that belong to more than two codes of $\{ C'_1, \ldots, C'_4 \}$, then one or more permutation pattern(s) $L^m$ $(1 \leq m \leq 6)$ of (9) need(s) to be replaced, which will cause the Permutation Criteria to be unsatisfied. The same consequence applies to the Construction Rules if similar changes are required for $g'_1, g'_2, \ldots, g'_m$ ($m = 1, 2$).

According to Pro(iii), the number of the distinct weight-4 codewords contributed by the eight codes $C'_1, \ldots, C'_4$ is given by

$$\left| \bigcup_{i=1}^{8} S^{(i)}_{8,4} \right| = 14 + (14 - 2) + (14 - 4) + \ldots + (14 - 12) = \sum_{j=1}^{6} (14 - 2j) = 56$$

Furthermore, the total number of the distinct weight-4 codewords from the nine codes, $C_i$ and $C'_1, \ldots, C'_8$ is

$$\left| \bigcup_{i=1}^{8} S^{(i)}_{8,4} \right| = |S^{(i)}_{8,4}| + 56 = 14 + 56 = 70$$

This figure means that the nine (8, 4, 4) code subspaces used in our scheme for the purpose of constructing $C_{24}$ have contained all the possible weight-4 8-tuples, since $\binom{8}{4} = 70$.

This property is demonstrated in TABLE I, where all the possible weight-4 codewords generated by $G_i$ and
The weight-4 codewords of the (8, 4, 4) codes (results from Example)

| Code  | Weight-4 codewords (in decimal) |
|-------|---------------------------------|
| C<sub>1</sub> | 29  39  58  78  83  105  116  139  150  172  177  197  216  226 |
| C<sub>1</sub>' | 23  43  60  77  90  102  113  142  153  165  178  195  212  232 |
| C<sub>2</sub> | 27  46  53  77  86  99  120  135  156  169  178  202  209  228 |
| C<sub>3</sub> | 30  45  51  75  85  102  120  135  153  170  180  204  210  225 |
| C<sub>4</sub> | 23  46  57  75  92  101  114  141  154  163  180  198  209  232 |
| C<sub>5</sub> | 30  43  53  71  89  108  114  141  147  166  184  202  212  225 |
| C<sub>6</sub> | 27  45  54  71  92  106  113  142  149  163  184  201  210  228 |
| C<sub>7</sub> | 15  51  60  86  89  101  106  149  154  166  169  195  204  240 |
| C<sub>8</sub> | 15  54  57  85  90  99  108  147  156  165  170  198  201  240 |

The relationships between the ordinal numbers of the columns of $Q$ and the 56 weight-4 codewords belonging to $S^{(1)}_{\text{ex}}$, ..., $S^{(8)}_{\text{ex}}$ can be easily worked out from Table I.

Based on the above results, our construction method presented here can be considered to have extended the existing schemes that apply the $\lfloor a + x|b+x|a+b+x\rfloor$ framework and use two (8, 4, 4) codes. For instance, the original Turyn construction employs two (8, 4, 4) codes: the extended (7, 4, 3) cyclic Hamming code and its specified version [9, p.588] generated by

$$G_{(7,4,3)} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and

$$G_{(7,4,3)}' = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

respectively. This construction is just one of the 8 possible cases given in the above example, i.e., $G_1$ and $G_1' = G_1^{(r)} = (I_8 \cdot P^{(r)})$ obtained in Example are the results of applying elementary row operations over $G_{(7,4,3)}$ and $G_{(7,4,3)}'$, respectively. In the same way, it can be shown that the Forney’s construction [11] employing the (8, 4, 4) first-order Reed-Muller code and its permutation is also covered by our scheme, as the choices of
and one of the corresponding 8 possible \( G'_i \),

\[
G'_i = \begin{pmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0
\end{pmatrix}, \quad \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 0 & 1 & 1
\end{pmatrix}, \quad \begin{pmatrix}
0 & 0 & 0 & 1 & 1 & 0 & 1 & 1
\end{pmatrix}
\]

represent exactly the same code subspaces as the two generator matrices \( G_{(s,2)} \) and \( G_{(s,4)} \) given in [11, p.1174] do, respectively.

IV. CONCLUSION

In summary, we have shown that the (24, 12, 8) binary Golay code can be constructed as the direct sum of two array codes involving four component codes, two of which are simple linear block codes (a repetition code and an SP code). The other two component codes are two different (8, 4, 4) codes; one of them is a systematic code and the other is its modified version. There exist eight different such modified codes which meet the construction criteria or rules presented. It is not difficult to show that the eight corresponding (24, 12, 8) codes formed using our construction represent eight different, though partly overlapped, code subspaces, but they are all equivalent or isomorphic to the (24, 12, 8) Golay code.

We have also demonstrated that the generator matrix \( G_i \) and eight corresponding generator matrices \( G'_{(s,1)}, \ldots, G'_{(s,8)} \) involved in our construction can generate all possible codewords (including weight-4 and weight-8) that any (8, 4, 4) code can do. In this sense, the method presented here may be viewed as the generalization of all existing approaches to constructing the (24, 12, 8) Golay code using the \( a + x(b + x) \) construction and two (8, 4, 4) codes. It is worth pointing out that in our method the generator matrices \( G'_{(s,1)}, \ldots, G'_{(s,8)} \) can also be described as the result of column permutations of \( G_i \), though a lengthier proof may be required.

There are various ways to decode the (24, 12, 8) Golay code, such as the decoders based on the hexacode constructions for hard-decision [16-18] and soft-decision [19, 20] decoding. For the construction based on (6), a regular trellis can be built using different techniques [11, 21]. This trellis has three sections of length 8 and 64 states at each section boundary. Essentially, it consists of eight structurally identical sub-trellises, thus enabling simple and fast maximum likelihood decoding as these sub-trellises can be processed in parallel. Trellises with such a structure are desirable because this can considerably reduce interconnections within the IC, and the chip-size, which are major concerns in implementing trellis decoding using DSP and VLSI technologies [22, 23]. The decoding complexity can be further reduced by simplifying the sub-trellises through initial-decoding on the component code \( C_i \) [24].

APPENDIX

PROOF OF THEOREM 2

Theorem 2: Applying \( G'_{(s,1)} \) or \( G'_{(s,2)} \) given in (10) and satisfying the Construction Rules to the generator matrix given in (6), as \( G'_i \), together with \( G_i \) defined in (7), generates \( C_{(s,3)} \).

Proof: We first show that the two codes generated using \( G'_{(s,1)} \) and \( G'_{(s,2)} \), respectively, which are constructed base on (10) and the Construction Rules, are (8, 4, 4) codes. This is equivalent to showing that both codes can generate 14 weight-4 codewords, given the weight distribution of the (8, 4, 4) code: \{\( N(0) = 1, N(4) = 14, N(8) = 1 \)\}. It is apparent that the 4 rows of either \( G'_{(s,1)} \) or \( G'_{(s,2)} \) are linearly independent. Since \( g'_{(s,1)} \), \( g'_{(s,2)} \) and \( g'_{(s,1)} + g'_{(s,2)} \) (\( l = 7, 8 \)) are all weight-4 8-tuples or 2-and-2 codewords according to Rule(i) & Rule(ii), linear combinations of any 2, 3 and 4 row vectors of \( G'_{(s,1)} \) or \( G'_{(s,2)} \) all result in weight-4 codewords. The total number of the weight-4 codewords that \( G'_{(s,1)} \) or \( G'_{(s,2)} \) can generate is

\[ 3 + \sum_{j=2}^{8} \binom{4}{j} = 14 \] ; here ‘3’ represents the number of the rows with 4 nonzero elements of \( G'_{(s,1)} \) or \( G'_{(s,2)} \), except the all-one row \( g'_{(s,1)} \). Of the 14 weight-4 codewords, in addition to codewords \( (0001111) \) and \( (11110000) \), there are 12 2-and-2 codewords, owing to the special structures of \( G'_{(s,1)} \) and \( G'_{(s,2)} \) in (10) that contain \( g'_{(s,1)} \) and \( g'_{(s,2)} \).

We then show that all weight-4 codewords of \( C_{(s,1)} \) and \( C_{(s,2)} \), or \( C_{(s,3)} \), are distinct. As \( C_{(s,1)} \) is a systematic (8, 4, 4) code and \( C_{(s,2)} \) contains a 4×4 identity matrix, it does not have the codewords \( (00011111) \) and \( (11110000) \), but has 6 codewords 2-and-2 codewords because there are in total \( \binom{4}{2} = 6 \) linear combinations involving 2 row vectors of \( G_i \). Based on (7), these 6 codewords can be expressed as

\[
\text{cw}1=(1100 \ P_{1,i}), \text{cw}2=(1010 \ P_{1,i}), \text{cw}3=(1001 \ P_{1,i}), \\
\text{cw}4=(0011 \ P_{1,i}), \text{cw}5=(0101 \ P_{1,i}), \text{cw}6=(0110 \ P_{1,i})
\]

Here \( P_{1,i} = P_i + P_j \) for \( 1 \leq i, j \leq 4 \) and \( P_i, P_j \in P \) given in (7). Obviously, the left halves of the 6 codewords are unique weight-2 4-tuples, so are the right halves otherwise some combinations of such codewords could result in the codewords of weight < 4. It is easy to show that \( P_{3,4} = \overline{P_{1,2}}, P_{2,4} = \overline{P_{1,3}} \) and \( P_{2,3} = \overline{P_{1,4}} \) since \( G_i \) has the all-one codeword \( g'_{(s,1)} \). This means
that these 6 codewords form 3 complementary pairs, i.e., cw4 = cw1, cw5 = cw2 and cw6 = cw3. The 12 2-and-2 codewords of C(7) or C(n) can be divided into three groups:

(i) \( a, a', \overline{a}, \overline{a'} \);

(ii) \( b, b', \overline{b}, \overline{b'} \);

(iii) \( a + b, (a + b)', \overline{a + b}, (a + b)' \).

Here \( a \) and \( b \) represent \( g_{0,1} \) and \( g_{0,2} \) for \( l = 7, 8 \), respectively, and \( u' = u + (00001111) \) where \( u \in U = \{ a, b, (a+b) \} \) and \( \overline{v} = v + (11111111) \) where \( v \in V = U \cup \{ a', b', (a+b)' \} \). Without loss of generality, we assign \( a^{(i)} \) (or \( g_{0,1}^{(i)} \)) = (1100) (the left half of cw1) and \( b^{(i)} \) (or \( g_{0,2}^{(i)} \)) = (1010) (the left half of cw2) for \( l = 7, 8 \), according to Rule(i). Rule(iii) ensures that \( a^{(k)} \neq P_{1,2}, a'^{(k)} \neq P_{1,2}, b^{(k)} \neq P_{1,3} \) and \( b'^{(k)} \neq P_{1,3} \).

Now it can be concluded that \( a, a', b, b' \) are distinct from all the codewords of \( C_1 \) (cw1, \ldots, cw6) as any corresponding pair of them differ in either left or right half of the 8-tuple. The same conclusion applies to \( \overline{a}, \overline{a'}, \overline{b} \) and \( \overline{b'} \), since \( s \neq t \) implies \( \overline{s} \neq \overline{t} \). For the last group of the 12 codewords, due to the fact that \( (a+b)^{(i)} = a^{(i)} + b^{(i)} \), \( (1100)+ (1010) = (0110) \) (the left half of cw6) and \( P_{1,2} + P_{1,3} = P_{2,3} \), it can also be concluded that the 4 codewords \( a + b, (a + b)', \overline{a + b} \) and \( (a+b)' \) are distinct from cw1, \ldots, cw6 by applying the method and properties described above.

By now we have shown that the structures of \( G_{(7)} \) and \( G_{(5)} \) given in (10) and the Construction Rules guarantee the same conclusion presented in Lemma 2; i.e., all weight-4 codewords of \( C_1 \) and \( C_{(7)} \) or \( C_{(5)} \) are distinct. The rest of the proof is analogous to that for Theorem 1.

\[\square\]

ACKNOWLEDGMENT

The authors wish to thank the anonymous reviewers and the Associate Editor, Robert McEliece, for their detailed and helpful comments and suggestions.

REFERENCES

[1] M. J. E. Golay, “Notes on digital coding,” in Proc. IEEE, 37, pp.637, 1949.
[2] F. J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes. North-Holland, 1998.
[3] P. J. Cameron and J. H. van Lint, Design, Graphs, Codes and their Links. Cambridge University Press, 1991.
[4] J. H. Conway and N. J. A. Sloane, “Lexicographic codes: error-correcting codes from game theory,” IEEE Trans. Inf. Theory, vol. 32, pp.337-438, 1986.
[5] G. Pasquier, “The Golay code obtained from an extended cyclic code over \( \mathbb{F}_3 \),” Eur. J. Combinatorics, vol.1, pp.369-370, 1980.
[6] J. H. Conway and N. J. A. Sloane, Sphere Packing, Lattices and Groups. Springer-Verlag, 1988.
[7] R. Chapman, “Higher power residue codes,” Finite Field and Their App., vol. 3, pp.353-369, 1997.
[8] R. T. Curtis, “Geometric interpretations of the ‘natural’ generators of the Mathieu groups,” Math. Proc. Cambridge Philos. Soc., vol. 107, pp.19-26, 1990.
[9] 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, Mass., Sci. Rep. AFCLR-67-0365, 1967.
[10] 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.
[11] G. D. Forney, “Coset codes – Part II: Binary lattices and related codes,” IEEE Trans. Inf. Theory, vol.34, pp.1152-1187, Sept. 1988.
[12] X.-H. Peng and P. G. Farrell, “Optimal augmentation of product codes,” Elec. Letters, vol.40, no.12, pp.750-752, 10th June 2004.
[13] B. Honary and G. Markarian, “New simple encoder and trellis decoder for Golay Codes,” IEE Elec. Letters, vol.29, no. 25, pp.2170-2171, Dec. 1993.
[14] P. V. Pless, “On the uniqueness of the Golay code,” J. Comb. Theory, vol. 5, pp.215-228, Nov. 1968.
[15] M. Hall, Combinatorial Theory. Blaisdell Publishing, 1967.
[16] V. Pless, “Decoding the Golay codes,” IEEE Trans. Inf. Theory, vol.32, pp.561-567, July 1986.
[17] O. Amrani, Y. Be’ery, A. Vardy, F.-W. Sun, and H. C. A. van Tilborg, “The Leech lattice and the Golay code: bounded-distance decoding and multilevel construction,” IEEE Trans. Inf. Theory, vol.41, pp.1495-1499, Sept. 1995.
[18] A. Vardy, “Even more efficient bounded-distance decoding of the hexacode, the Golay code and Leech lattice,” IEEE Trans. Inf. Theory, vol.32, pp.561-567, July 1986.
[19] H. T. Moorthy, S. Lin and G. T. Uehara, “Good trellises for IC and lattices, including the Golay code and the Leech lattice,” IEEE Trans. Inf. Theory, vol. 32, pp.41-50, 1986.
[20] A. Vardy and Y. Be’ery, “Maximum-likelihood soft decision decoding of BCH codes,” IEEE Trans. Inf. Theory, vol.40, pp.546-554, March 1994.
[21] A. Lafourcade and A. Vardy, “Optimal sectionalization of a trellis,” IEEE Trans. Inf. Theory, vol.42, pp.689-703, May 1996.
[22] H. T. Moorathy, S. Lin and G. T. Uehara, “Good trellises for IC implementation of Viterbi decoders for linear block codes,” IEEE Trans. Comms. vol. 45, pp.52-63, Jan. 1997.
[23] P. J. Black and T. H. Meng, “A 140-Mb/s, 32-state, Radix-4 Viterbi decoder,” IEEE J. Solid-State Circuits, vol. 27, Dec. 1992.
[24] X.-H. Peng, A. G. Burr, P. G. Farrell and J. M. Gil-Garcia, “Fast soft-decision decoding for block codes using a trellis,” in Proc. IEEE Int. Symp. Information Theory, MIT, MA, USA, Aug. 1998, pp.180.