Decoding Binary $R(2,5)$ by Hand

Philippe Gaborit
LACO, Université de Limoges, 87000 Limoges, France
e-mail: gaborit@unilim.fr

Jon-Lark Kim and Vera Pless
Department of Mathematics, Statistics, and Computer Science,
322 SEO(M/C 249),
University of Illinois–Chicago,
851 S. Morgan, Chicago, IL 60607-7045, USA
e-mail: jlkim@math.uic.edu, pless@math.uic.edu

Abstract

The main purpose of this paper is to decode the binary Reed-Muller $[32,16,8]$ code $R(2,5)$ by hand by two methods. One, the representation decoding method, is the analogue of the method used to decode the Golay code [8]. The other is the syndrome decoding method. We also describe how to decode other doubly-even self-dual $[32,16,8]$ codes C83(or $2g_{16}$) and C84(or $8f_4$).

Keywords Binary Reed-Muller code $R(2,5)$, Hamming code, Representation decoding method, Syndrome decoding method.

1 Introduction

It was shown [8] that the extended binary(ternary) Golay codes can be decoded by hand by projecting these codes onto quaternary(ternary) codes of smaller length. It has been open since then whether this idea can be applied to higher length binary codes. We will show that this is possible for the binary Reed-Muller $[32,16,8]$ code by using the linear Hamming $[8,4,4]$ code over $GF(4)$.

We briefly explain how the binary Reed-Muller $[32,16,8]$ can be constructed from the linear $[8,4,4]$ code over $GF(4)$ whose generator matrix comes from a binary Hamming extended $[8,4,4]$ code. From now on, we will call it the *linear Hamming* $[8,4,4]$ *code* $\mathcal{H}$ *over* $GF(4)$ although it is not one of the well-known extended Hamming codes over $GF(4)$. Its codewords will be called *Hamming codewords*. Recently it has been shown [4, 5, 6] that there are exactly 3 even self-dual additive codes of length 8 with minimum weight 4 over $GF(4)$. Among these three even codes, one is the linear Hamming $[8,4,4]$ code $\mathcal{H}$ over $GF(4)$. Furthermore it was shown [4, 5] that the binary Reed-Muller $[32,16,8]$ code can be obtained from $\mathcal{H}$ in the following way. Let $\widehat{\mathcal{H}}$ be the binary linear $[32,8]$ code obtained from $\mathcal{H}$ by replacing each $GF(4)$ component by a 4-tuple in $GF(2)^4$ as follows: $0 \to 0000$, $1 \to 0011$,

$\omega \to 0101$, $\overline{\omega} \to 0110$. Let d_4 be the $[4,1]$ binary linear code $\{0000, 1111\}$. Finally let $(d_4^8)_0$ be the $[32,7]$ binary linear code consisting of all codewords of weights divisible by 8 from the $[32,8]$ code d_4^8. Then $\rho(\mathcal{H}) = \widehat{\mathcal{H}} + (d_4^8)_0 + f_1$, where f_1 is the $[32,1]$ code generated by 1000 1000 $\cdots$ 1000, produces the binary Reed-Muller $[32,16,8]$ code.

The main purpose of this paper is to decode the binary Reed-Muller code $R(2,5)$ by hand by two methods. One, the representation decoding method, is the analogue of the method used to decode the Golay code [8]. The other is the syndrome decoding method. We remark that the syndrome decoding method can also be applied to decoding the Golay code. The advantage is that this method is purely algebraic and uses little knowledge of the structure of the Hexacode over $GF(4)$. At the end we also describe how to decode other doubly-even self-dual $[32,16,8]$ codes C83(or $2g_{16}$) and C84(or $8f_4$) in the notation of [2] by using the syndrome decoding method.

Since $R(2,5)$ is a $[32,16,8]$ code, its error-correcting capability is at most 3. It is also well known [1] that the covering radius of $R(2,5)$ is 6. Our decoding scheme can not only correct up to 3 errors, but can also detect 4,5, or 6 errors, and in addition give a coset representative of a coset of weight 4, 5, or 6.

The rest of this paper consists of three sections. In section 2, we show how to construct $R(2,5)$ from the linear Hamming $[8,4,4]$ code over $GF(4)$ using the idea of parity of columns. In section 3, we give the representation decoding and syndrome decoding algorithm and explain several examples in two ways. We also discuss the worst case of the syndrome decoding method and compare it with majority-logic decoding of $R(2,5)$. In section 4, we describe how to decode other doubly-even self-dual $[32,16,8]$ codes C83(or $2g_{16}$) and C84(or $8f_4$).

2 The Reed-Muller code and the Hamming code

The binary Reed-Muller code $R(2,5)$ is a doubly-even self-dual $[32,16,8]$ code. It is one of the five extremal doubly-even self-dual codes of length 32 [2]. The linear Hamming $[8,4,4]$ code $\mathcal{H}$ over $GF(4)$ is an even self-dual [8,4,4] code with respect to the ordinary inner product as well as the Hermitian inner product. For decoding we will use this ordinary inner product because of its easy calculation. We take

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \tag{1}$$

as a generator matrix of $\mathcal{H}$. We index each column of H from the left to the right by 1 to 8. This is how we refer to the columns of H, i.e. column 6 is $(1,1,0,1)^T$. Before we describe how to use H to decode $R(2,5)$, we recall the projection of binary codes into quaternary codes explained in [8]. Consider a 4×8 array with zeros and ones in it. Label the four rows with the elements of $GF(4)$; 0,1,ω, $\overline{\omega}$. Recall that $\overline{\omega} = \omega^2, \overline{\omega}^2 = \omega$, and $\overline{\omega} = 1+\omega$. If we take the inner product of a column of our array with the row labels, we get an element in $GF(4)$. In this way we have a correspondence between binary vectors of length 32 and quaternary vectors of length 8. For example, let $\mathbf{v} = (1,0,1,1,0,0,0,0,1,0,0,1,0,0,1,1,0,1,0,1,0,0,1,1,0,1,0,1,0,1,1,0)$ be the binary vector of length 32. Then

$$\mathbf{v} = \begin{array}{c|cccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ \omega & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ \overline{\omega} & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ \hline & 1 & 0 & \overline{\omega} & 1 & \omega & 1 & \omega & \overline{\omega} \end{array}$$

corresponds to(or projects onto) the quaternary vector $(1,0,\overline{\omega},1,\omega,1,\omega,\overline{\omega})$ of length 8. Note that this correspondence is linear, i.e., if b_i corresponds to q_i, $i = 1,2$, then $b_1 + b_2$ corresponds to $q_1 + q_2$.

Let the *parity of a column* be either even or odd if an even or an odd number of ones exist in the column. Define the *parity of the top row* in a similar fashion. Thus the first column of the 4×8 array of the above vector has odd parity, and the rest have even parity. The top row has even parity.

Lemma 1. *The set of all binary vectors of length 32 with the following properties is (up to equivalence) the binary Reed-Muller* $[32,16,8]$ *code:*

(i) *The parity of all the columns is the same(i.e., all even or all odd), and the parity of the top row is always even. All vectors of this form constitute a linear space.*

(ii) *The projection is in the linear Hamming* $[8,4,4]$ *code* $\mathcal{H}$ *over* $GF(4)$. *All vectors with this property form a linear space.*

Proof. It is easy to see that the set of all vectors satisfying property (i) or (ii) form a linear code. Thus their intersection, say $\mathcal{C}$, is also a linear code. We note that $\mathcal{H}$ has an information set consisting of some 4 columns of H. One such information set is the set of columns 2, 3, 4, and 5 of H in (1). So the other columns of H are determined by this information set. We want to count the number of vectors satisfying both properties (i) and (ii). First assume that all columns are even. Then there are 8 choices for each column in the information set. There are 2 choices for each column outside the information set except the last one which is automatically determined because of top row parity. Hence there are $8^4 \times 2^3 \times 1 = 2^{15}$ vectors when all columns are even. For the same reason we get $8^4 \times 2^3 \times 1 = 2^{15}$ vectors when all columns are odd. Therefore there are $2 \times 2^{15} = 2^{16}$ vectors, which implies that $\mathcal{C}$ is a [32,16] linear code. From the Introduction or [4, 5] we know that $\rho(\mathcal{H})$ gives $R(2,5)$. It is easy to see that this image satisfies both properties (i) and (ii). Since this image is a subcode of $\mathcal{C}$ with the same dimension 16, we can conclude that our image is exactly $\mathcal{C}$ as desired. □

3 Decoding the Reed-Muller code $R(2,5)$

We can represent all Hamming codewords in $\mathcal{H}$ by only 7 vectors with a special set of permutations. We call positions $(1,2),(3,4),(5,6)$, and $(7,8)$ blocks of $\mathcal{H}$ and note that in this representation $\mathcal{H}$ is invariant under all permutations of these

Table 1: Hamming Codewords

No.	Hamming Codewords								Number of This Type	Weight
1)	0	1	0	1	0	1	0	1	8×3	4
2)	1	1	0	0	1	1	0	0	6×3	4
3)	0	1	0	1	ω	$\overline{\omega}$	ω	$\overline{\omega}$	$8\times 6\times 3$	6
4)	0	0	1	1	ω	ω	$\overline{\omega}$	$\overline{\omega}$	24	6
5)	1	ω	1	ω	1	ω	1	ω	8×3	8
6)	1	1	ω	ω	1	1	ω	ω	6×3	8
7)	1	1	1	1	1	1	1	1	1×3	8

four blocks and under all even numbers of interchanges within the blocks. So by considering scalar multiplications, the 7 vectors in Table 1 and the zero vector describe all $4^4 = 256$ vectors of $\mathcal{H}$.

Table 2 shows all possible cases that we can have from the correspondence between binary vectors of length 32 and quaternary vectors of length 8. We give an explanation of Table 2 which is an analysis of the parities of the columns of a received vector. For example, let us consider Case II. Here the second column denotes the parity of columns. So $(7, \underline{1})$ means that seven columns have one parity and one column has the other parity. The third column shows all possible errors in each subcase. For example, $3 = 2 + \underline{1}$ means that there are 2 errors in one of the seven columns with one parity and 1 error in one column with the other parity. The fourth column shows correct columns. So (6) out of 7 means that 6 columns out of seven columns with one parity are correct even though which 6 columns are correct are not decided. In Case V, there are equal number of even parity and odd parity columns. To simplify the table, we omit symmetric cases such as $4 = 1+1+1+1, 6 = 1+1+1+3$, and $6 = \underline{2}+1+1+1+1$.

Remark 1. Even though it is possible to have a few other situations such as $5 = 1+1+1+1+1$ errors with a one in each of 5 columns or $6 = 1+1+1+1+1+1$ errors with a one in each of 6 columns, there are vectors in the same cosets as the last ones described in IV and III of Table 2 respectively. To see this for the 5 error case we note that 4 out of these 5 columns are independent so that there must be a weight 8 vector in $R(2, 5)$ with these 4 components. This implies that there is a coset representative of the type $5 = 2+\underline{1}+\underline{1}+\underline{1}$. Similarly the 6 error case reduces to $6 = 2+2+\underline{1}+\underline{1}$. Some situations cannot occcur such as 4 errors in one column and 2 in another(i.e. $6 = 4+2$). As the sum of any 2 columns consisting of all ones is in $R(2, 5)$, adding such a sum would give a cost leader of weight 2.

We will decode $R(2, 5)$ by hand in two ways. One method is representation decoding using the above representation in Table 1. The other is syndrome decoding using $\mathcal{H}$. In what follows we consider five cases. We compare these two methods in each case, where sometimes one seems easier than the other.

3.1 Representation Decoding Algorithm

We have H as before and the received vector $\mathbf{v}$ as a 4×8 binary matrix.

Step 1. Compute the parities of the columns of $\mathbf{v}$ and determine which case of Table 2 we are in.

Table 2: All Possible Cases

Case	Parity of Columns (One Parity, The Other)	Possible Errors	Correct Columns (): undecided col.
I	$(8, \underline{0})$	0 errors	8
		$2 = 2$	(7) out of 8
		$4 = 4$	(7) out of 8
		$4 = 2 + 2$	(6) out of 8
		$6 = 2 + 2 + 2$	(5) out of 8
II	$(7, \underline{1})$	$1 = \underline{1}$	7
		$3 = \underline{3}$	7
		$3 = 2 + \underline{1}$	(6) out of 7
		$5 = 2 + 2 + \underline{1}$	(5) out of 7
III	$(6, \underline{2})$	$2 = \underline{1} + \underline{1}$	6
		$4 = \underline{1} + \underline{3}$	6
		$4 = 2 + \underline{1} + \underline{1}$	(5) out of 6
		$6 = 2 + 2 + \underline{1} + \underline{1}$	(4) out of 6
IV	$(5, \underline{3})$	$3 = \underline{1} + \underline{1} + \underline{1}$	5
		$5 = \underline{1} + \underline{1} + \underline{3}$	5
		$5 = 2 + \underline{1} + \underline{1} + \underline{1}$	(4) out of 5
V	$(4, \underline{4})$	$4 = \underline{1} + \underline{1} + \underline{1} + \underline{1}$	4
		$6 = \underline{1} + \underline{1} + \underline{1} + \underline{3}$	4
		$6 = 2 + \underline{1} + \underline{1} + \underline{1} + \underline{1}$	(3) out of 4

Step 2. Compute the projection of $\mathbf{v}$, call it $\mathbf{y}$.

Step 3. From step 1 we know either (a) explicitly which columns are incorrect [lines 1 and 2 of cases II, III, IV, and V] or (b) we have partial information about the number or location of incorrect columns. We use this information and the simple description of $\mathcal{H}$ of Table 1 to find the closest vector(s) $\mathbf{y}'$ to $\mathbf{y}$ in $\mathcal{H}$.

Step 4. From step 3 we now know a correct projection $\mathbf{y}'$. We can adjust $\mathbf{v}$ to get its projection $\mathbf{y}'$ and to have the same column parities and top row parity even. Thus $\mathbf{v}$ is decoded as a codeword of $R(2,5)$. Then we stop.

Remark 2. This algorithm relies on the simple representation of $\mathcal{H}$. One cannot find such a simple representation structure for the other two even self-dual additive codes of length 8 with minimum weight 4 over $GF(4)$. This makes such a representation decoding algorithm non applicable for the other doubly-even self-dual $[32, 16, 8]$ codes $C83$ and $C84$, constructed from even self-dual addtive $GF(4)$ codes of length 8. We will discuss the syndrome decoding of these codes in section 4.

3.2 Syndrome Decoding Algorithm

We give the outline of the syndrome decoding algorithm of $R(2,5)$ using maximum-likelihood decoding. This means that we assume that the smallest number of errors have occurred. H is also taken as before and the received vector $\mathbf{v}$ as a 4×8 binary matrix.

Step 1. Compute the parities of the columns of $\mathbf{v}$ and determine which case of Table 2 we are in.

Step 2. Compute the projection of $\mathbf{v}$, call it $\mathbf{y}$.

Step 3. Compute the syndrome of $\mathbf{y}$ with respect to H.

Step 4. If the syndrome of $\mathbf{y}$ is zero and we are in case I of Table 2, we compute the parity of the top row of $\mathbf{v}$, else go to Step 5. If the parity is even, we say no errors have occurred and we stop. If odd, we are in case $4 = 4$ and we decode by complementing any column of $\mathbf{v}$ then stop.

Step 5. From step 1 we know either (a) explicitly which columns are incorrect [lines 1 and 2 of cases II, III, IV, and V] or (b) we have partial information about the number or location of incorrect columns. In case a) we write the syndrome as a combination of the incorrect columns using H. If successful, we go to step 6. If we find that other columns are wrong we go to case b). In case b) by trial and error we write the syndrome as a combination of known incorrect columns and possible unknown ones.

Step 6. From step 5 we get an error vector which we add to $\mathbf{y}$. We now know a correct projection $\mathbf{y}'$. We can adjust $\mathbf{v}$ to get its projection $\mathbf{y}'$ and to have the same column parities and top row parity even. Thus $\mathbf{v}$ is decoded as a codeword of $R(2,5)$. Then we stop.

To see this algorithm more clearly we give several examples.

3.3 Examples

The steps in these examples are the ones in section 3.2.

Example 1 (Case I). *All of the columns have the same parity.*

In this case we know that there are zero, two, four, or six errors by Table 2. Consider the following example.

$$\mathbf{v} = \begin{array}{c|cccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ \omega & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ \overline{\omega} & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ \hline \mathbf{y} & 0 & 1 & \omega & \omega & \overline{\omega} & \overline{\omega} & 1 & 1 \end{array}$$

Suppose all columns are correct. Clearly $\mathbf{v}$ is not a Reed-Muller codeword since the top row parity is odd. We note that $\mathbf{y}$ cannot be matched with any Hamming codeword of weight 8 since $\mathbf{y}$ has three distinct nonzero elements in $GF(4)$(see Table 1). We find a unique Hamming codeword closest to $\mathbf{y}$ of weight 6, i.e. $(0, \mathbf{0}, \omega, \omega, \overline{\omega}, \overline{\omega}, 1, 1)$. Hence we uniquely decode $\mathbf{v}$ as follows.

$$\begin{array}{c|cccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline 0 & 1 & \mathbf{0} & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & \mathbf{0} & 0 & 1 & 0 & 1 & 1 & 0 \\ \omega & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ \overline{\omega} & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ \hline & 0 & \mathbf{0} & \omega & \omega & \overline{\omega} & \overline{\omega} & 1 & 1 \end{array}$$

The syndrome decoding method gives a unique Hamming codeword matching $\mathbf{y}$ in a simple way. We compute the syndrome of $\mathbf{y}$ with H(Step 3).

$$H\mathbf{y}^T = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix},$$

which is column 2 of H. Since $H\mathbf{y}^T \neq 0$, go to Step 5. Then our error vector is $\mathbf{e} = (0,1,0,0,0,0,0,0)$ giving a Hamming codeword $\mathbf{x} = \mathbf{y} + \mathbf{e} = (0, \mathbf{0}, \omega, \omega, \varpi, \varpi, 1, 1)$, which we obtained before(Step 6). The rest is the same as before.

We consider another example.

$\mathbf{v} =$

	1	2	3	4	5	6	7	8
0	1	1	0	1	0	0	0	0
1	1	0	0	0	1	1	0	0
ω	1	1	1	0	1	0	1	0
ϖ	0	1	0	0	1	0	0	1
$\mathbf{y}$ =	ϖ	1	ω	0	0	1	ω	ϖ

Clearly errors have occurred since the top row parity is odd. So we suppose one column is not correct. Still we cannot find a Hamming codeword of weight 6. Suppose two columns are not correct. Then one can find Hamming codewords $(\varpi, \boldsymbol{\omega}, \mathbf{1}, 0, 0, 1, \omega, \varpi)$ and $(\varpi, 1, \omega, 0, 0, \boldsymbol{\omega}, \mathbf{1}, \varpi)$ by Table 1. So we decode $\mathbf{v}$ as follows.

	1	2	3	4	5	6	7	8
0	1	**0**	0	1	0	0	0	0
1	1	0	**1**	0	1	1	0	0
ω	1	1	**0**	0	1	0	1	0
ϖ	0	**0**	0	0	1	0	0	1
	ϖ	$\boldsymbol{\omega}$	**1**	0	0	1	ω	ϖ

,

	1	2	3	4	5	6	7	8
0	1	1	**1**	1	0	0	0	0
1	1	**1**	0	0	1	1	0	0
ω	1	**0**	1	0	1	0	1	0
ϖ	0	1	**1**	0	1	0	0	1
	ϖ	$\boldsymbol{\omega}$	**1**	0	0	1	ω	ϖ

,

	1	2	3	4	5	6	7	8
0	1	1	0	1	0	0	**1**	0
1	1	0	0	0	1	**0**	0	0
ω	1	1	1	0	1	**1**	1	0
ϖ	0	1	0	0	1	0	**1**	1
	ϖ	1	ω	0	0	$\boldsymbol{\omega}$	**1**	ϖ

,

	1	2	3	4	5	6	7	8
0	1	1	0	1	0	**1**	0	0
1	1	0	0	0	1	1	**1**	0
ω	1	1	1	0	1	0	**0**	0
ϖ	0	1	0	0	1	**1**	0	1
	ϖ	1	ω	0	0	$\boldsymbol{\omega}$	**1**	ϖ

Using the syndrome decoding method, we can get the above Hamming codewords. We have to solve the equation(Step 5 (b)):

$$H\mathbf{y}^T = \begin{bmatrix} 0 \\ 0 \\ \varpi \\ \varpi \end{bmatrix} = e_i S_i + e_j S_j, \quad (i \neq j),$$

where S_i means the column i of H in (1). If we take $i = 2$ and $j = 3$ and solve the above equation, then we get $e_2 = e_3 = \varpi$. This gives a Hamming codeword

$\mathbf{x} = \mathbf{y} + \mathbf{e} = (\overline{\omega}, \boldsymbol{\omega}, \mathbf{1}, 0, 0, 1, \omega, \overline{\omega})$. However if we take $i = 6$ and $j = 7$, then $e_6 = e_7 = \overline{\omega}$ giving another Hamming codeword $\mathbf{x} = \mathbf{y} + \mathbf{e} = (\overline{\omega}, 1, \omega, 0, 0, \boldsymbol{\omega}, \mathbf{1}, \overline{\omega})$. So we could decode $\mathbf{v}$ as above.

Example 2 (Case II). *Seven of the columns have one parity, and one of the columns has the other parity.*

In this case we know that there are one, three, or five errors from Table 2. If there are at most three errors, then we can uniquely decode. Otherwise we can detect five errors and decode into some codeword.

		1	2	3	4	5	6	7	8
$\mathbf{v} =$	0	1	1	1	0	1	0	0	1
	1	1	1	0	1	1	1	1	0
	ω	1	0	0	0	1	0	1	1
	$\overline{\omega}$	0	1	0	0	1	0	1	1
	$\mathbf{y}$ =	$\overline{\omega}$	ω	0	1	0	1	0	1

Suppose seven odd columns are correct. So its projection is ($\overline{\omega}$,ω,0,1,–,1,0,1). Since there are three distinct nonzero elements in the projection, it cannot be matched with any Hamming codeword of weight 4. Since there are three 1's in it, it cannot be matched with any Hamming codeword of weight 6. Clearly it cannot be matched with any Hamming codeword of weight 8. So at least one odd column of the projection is not correct. Suppose there is a Hamming codeword of weight 4 matching the projection. Then the unknown fifth position of the projection should be 0. Then the first position or second position must also be 0. In either case we cannot find a Hamming codeword of weight 4 (see Table 1). If we try weight 6, then we will get the following Hamming codeword $(\overline{\omega}, \omega, 0, 1, \boldsymbol{\overline{\omega}}, \boldsymbol{\omega}, 0, 1)$ matching the projection. So we can uniquely decode the received vector $\mathbf{v}$.

	1	2	3	4	5	6	7	8
0	1	1	1	0	1	**1**	0	1
1	1	1	0	1	1	1	1	0
ω	1	0	0	0	1	0	1	1
$\overline{\omega}$	0	1	0	0	**0**	**1**	1	1
	$\overline{\omega}$	ω	0	1	$\boldsymbol{\overline{\omega}}$	$\boldsymbol{\omega}$	0	1

To use the syndrome decoding method, we need to solve the equation(Step 5 (b)):

$$H\mathbf{y}^T = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \overline{\omega} \end{bmatrix} = e_5 \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + e_i S_i,$$

where i should be 2, 4, 6, or 8. Simple computation tells us $i = 6$, in other words, $S_6 = (1, 1, 0, 1)^T$ giving $e_5 = e_6 = \overline{\omega}$. Thus we have the Hamming codeword $\mathbf{x} = \mathbf{y} + \mathbf{e} = (\overline{\omega}, \omega, 0, 1, \boldsymbol{\overline{\omega}}, \boldsymbol{\omega}, 0, 1)$, which was found before. The rest is the same as before.

Example 3 (Case III). *Six of the columns have one parity and two of the columns have the other parity.*

In this case we know that there are two, four, or six errors from Table 2. We try two errors first, and then keep going if we cannot correct 2 errors. Consider the following example.

$$
\mathbf{v} = \begin{array}{ccccccccc}
 & & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
\hline
0 & & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
\omega & & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
\overline{\omega} & & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\
\hline
\mathbf{y} & = & \overline{\omega} & 0 & 0 & \overline{\omega} & 1 & \omega & \overline{\omega} & 1
\end{array}
$$

Suppose that the six odd columns are correct. So its projection is ($\overline{\omega}$,0,0,$\overline{\omega}$,1,–,–,1). We find a Hamming codeword of weight 6 closest to this vector, i.e.,($\overline{\omega}$,0,0,$\overline{\omega}$,1,$\boldsymbol{\omega}$, $\boldsymbol{\omega}$,1) and uniquely decode $\mathbf{v}$ as follows.

$$
\begin{array}{c|cccccccc}
 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
\hline
0 & 1 & 1 & 0 & 0 & 1 & \mathbf{0} & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 & \mathbf{0} & 0 \\
\omega & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
\overline{\omega} & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\
\hline
 & \overline{\omega} & 0 & 0 & \overline{\omega} & 1 & \boldsymbol{\omega} & \boldsymbol{\omega} & 1
\end{array}
$$

If we use the syndrome decoding method, we consider the equation(Step 5 (a)):

$$
H\mathbf{y}^T = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} = e_6 \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} + e_7 \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}.
$$

Solving we get $e_6 = 0$ and $e_7 = 1$. So $\mathbf{x} = \mathbf{y} + \mathbf{e} = (\overline{\omega}, 0, 0, \overline{\omega}, 1, \boldsymbol{\omega}, \boldsymbol{\omega}, 1)$. The rest is the same as before.

We take another example.

$$
\mathbf{v} = \begin{array}{ccccccccc}
 & & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
\hline
0 & & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\
\omega & & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
\overline{\omega} & & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
\hline
\mathbf{y} & = & \overline{\omega} & 1 & 0 & \overline{\omega} & \omega & 1 & \overline{\omega} & 1
\end{array}
$$

Suppose that the six even columns are correct. Then their projection is ($\overline{\omega}$,1,–,–,ω,1,$\overline{\omega}$,1). This vector cannot be matched with any Hamming codeword of weight 4 since it has at least weight 6. Also this vector cannot be matched with any Hamming codeword of weight 6 since it has three 1's. Finally this vector cannot be matched with any Hamming codeword of weight 8 since it has three distinct nonzero elements. So we see that at least one even column should be corrected. We find two candidate Hamming codewords $(\overline{\omega}, 1, \boldsymbol{\overline{\omega}}, \mathbf{1}, \boldsymbol{\overline{\omega}}, 1, \overline{\omega}, 1)$ and $(\overline{\omega}, 1, \boldsymbol{\omega}, \mathbf{0}, \omega, \mathbf{0}, \overline{\omega}, 1)$. Hence we can decode $\mathbf{v}$ as follows:

	1	2	3	4	5	6	7	8
0	0	1	1	1	0	1	0	0
1	1	1	0	1	1	1	1	0
ω	1	0	0	**0**	**1**	0	1	1
ϖ	0	0	**1**	0	**0**	0	0	1
	ϖ	1	$\boldsymbol{\varpi}$	**1**	$\boldsymbol{\varpi}$	1	ϖ	1

,

	1	2	3	4	5	6	7	8
0	0	1	1	1	0	1	0	0
1	1	1	0	1	1	1	1	0
ω	1	0	**1**	1	0	**1**	1	1
ϖ	0	0	0	**1**	1	**1**	0	1
	ϖ	1	$\boldsymbol{\omega}$	**0**	ω	**0**	ϖ	1

If we use the syndrome decoding method, we need to solve the following equation(Step 5 (b)):

$$H\mathbf{y}^T = \begin{bmatrix} 0 \\ 1 \\ 1 \\ \omega \end{bmatrix} = e_3 \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} + e_4 \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} + e_i S_i,$$

where S_i should be one of columns 5, 6, 7, or 8 of H as otherwise the second equation $1 = e_3 0 + e_4 0$ will give a contradiction. We easily see that only S_5 and S_6 satisfy the above equation. When we consider S_5, we have $\mathbf{e} = (0,0,\varpi,\omega,1,0,0,0)$ giving $\mathbf{x} = \mathbf{y}+\mathbf{e} = (\varpi, 1, \boldsymbol{\varpi}, \mathbf{1}, \boldsymbol{\varpi}, 1, \varpi, 1)$. When we consider S_6, we have $\mathbf{e} = (0,0,\omega,\varpi,0,1,0,0)$ giving $\mathbf{x} = \mathbf{y} + \mathbf{e} = (\varpi, 1, \boldsymbol{\omega}, \mathbf{0}, \omega, \mathbf{0}, \varpi, 1)$. We obtained these Hamming codewords above. The rest is the same as before. In this example, the syndrome decoding method seems easier.

Example 4 (Case IV). *Five of the columns have one parity, and three of the columns have the other parity.*

In this case we know that there are three or five errors from Table 2. We first try the three error case. If we cannot correct three errors, then we see that five errors occurred. Consider the following example.

		1	2	3	4	5	6	7	8
	0	0	1	1	0	0	1	0	1
$\mathbf{v} =$	1	0	1	1	1	1	1	1	1
	ω	0	0	1	1	0	0	0	1
	ϖ	1	0	0	1	1	1	0	1
	$\mathbf{y}\ =$	ϖ	1	ϖ	0	ω	ω	1	0

Suppose that the five odd columns are correct. Their projection is (ϖ,–,ϖ,0,–,ω,1,–). From Table 1 we see that $(\varpi, \mathbf{0}, \varpi, 0, \mathbf{1}, \omega, 1, \boldsymbol{\omega})$ is a Hamming codeword closest to this vector. Hence we uniquely decode $\mathbf{v}$ as follows.

	1	2	3	4	5	6	7	8
0	0	1	1	0	0	1	0	1
1	0	**0**	1	1	1	1	1	1
ω	0	0	1	1	0	0	0	**0**
ϖ	1	0	0	1	**0**	1	0	1
	ϖ	**0**	ϖ	0	**1**	ω	1	$\boldsymbol{\omega}$

For the syndrome decoding method, we need to solve the equation(Step 5 (a)):

$$H\mathbf{y}^T = \begin{bmatrix} 0 \\ 1 \\ \omega \\ \overline{\omega} \end{bmatrix} = e_2 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} + e_5 \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + e_8 \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}.$$

We have $e_2 = 1, e_5 = \overline{\omega}$, and $e_8 = \omega$ giving $\mathbf{x} = \mathbf{y} + \mathbf{e} = (\overline{\omega}, \mathbf{0}, \overline{\omega}, 0, \mathbf{1}, \omega, 1, \boldsymbol{\omega})$, which we got before. The rest is the same as before.

We consider another example.

$\mathbf{v} =$

		1	2	3	4	5	6	7	8
0		1	0	1	1	1	0	1	0
1		0	1	1	0	1	0	0	1
ω		1	1	0	0	1	0	1	0
$\overline{\omega}$		1	0	0	0	1	1	0	1
$\mathbf{y}$	$=$	1	$\overline{\omega}$	1	0	0	$\overline{\omega}$	ω	ω

Suppose that the five even columns are correct. Then their projection is (–,$\overline{\omega}$,1,–,0,–,ω,ω). It is easy to see that any Hamming codeword matching this vector has weight 6. Among Hamming codewords of weight 6 we get $(\boldsymbol{\overline{\omega}}, \overline{\omega}, 1, \mathbf{1}, 0, \mathbf{0}, \omega, \omega)$. Hence we can decode $\mathbf{v}$ as follows:

	1	2	3	4	5	6	7	8
0	1	0	1	1	1	**1**	1	0
1	0	1	1	**1**	1	**1**	0	1
ω	**0**	1	0	0	1	**1**	1	0
$\overline{\omega}$	1	0	0	0	1	1	0	1
	$\boldsymbol{\overline{\omega}}$	$\overline{\omega}$	1	**1**	0	**0**	ω	ω

,

	1	2	3	4	5	6	7	8
0	1	0	1	**0**	1	0	1	0
1	0	1	1	0	1	0	0	1
ω	**0**	1	0	**1**	1	0	1	0
$\overline{\omega}$	1	0	0	**1**	1	**0**	0	1
	$\boldsymbol{\overline{\omega}}$	$\overline{\omega}$	1	**1**	0	**0**	ω	ω

,

	1	2	3	4	5	6	7	8
0	**0**	0	1	1	1	0	1	0
1	**1**	1	1	**1**	1	0	0	1
ω	1	1	0	0	1	0	1	0
$\overline{\omega}$	**0**	0	0	0	1	**0**	0	1
	$\boldsymbol{\overline{\omega}}$	$\overline{\omega}$	1	**1**	0	**0**	ω	ω

We note that in this example there are five errors in order to satisfy the even top row parity. It is well known [1] that there are 6 coset leaders of weight 5 in $R(2,5)$. We have found three coset leaders of weight 5. If we look at Table 2 then there are two more possibilities to get coset leaders of weight 5. We will discuss this later.

We want to explain the syndrome decoding method in the above example. We again assume that the five even columns are correct. So errors happened in positions 1,4, and 6 of $\mathbf{y}$. As in Example 1 we need to solve the following equations (Step 5 (a)):

$$H\mathbf{y}^T = \begin{bmatrix} 0 \\ \overline{\omega} \\ 1 \\ \omega \end{bmatrix} = e_1 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + e_4 \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} + e_6 \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}.$$

It is easy to compute that $e_1 = \omega, e_4 = 1, e_6 = \overline{\omega}$. Hence the error vector is $\mathbf{e} = (\omega, 0, 0, 1, 0, \overline{\omega}, 0, 0)$. Thus the desired Hamming codeword is $\mathbf{x} = \mathbf{y} + \mathbf{e} = (\boldsymbol{\overline{\omega}}, \overline{\omega}, 1, \mathbf{1}, 0, \mathbf{0}, \omega, \omega)$. After this, the rest is the same as before.

Now we want to find three more coset leaders of weight 5 by the syndrome decoding method. We assume that three odd columns and one even column are not correct. We must solve the following equation (Step 5 (b)):

$$Hy^T = \begin{bmatrix} 0 \\ \overline{\omega} \\ 1 \\ \omega \end{bmatrix} = e_1 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + e_4 \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} + e_6 \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} + e_i S_i,$$

where $i = 2, 3, 5, 7, 8$. A straightforward computation tells us that there are three error vectors

$$(0,0,0,\overline{\omega},0,1,\omega,0), (\overline{\omega},0,0,0,0,\omega,1,0), \text{ and } (1,0,0,\omega,0,0,\overline{\omega},0).$$

Thus we get three corresponding Hamming codewords $\mathbf{x} = \mathbf{y} + \mathbf{e} =$

$$(\mathbf{1}, \overline{\omega}, 1, \boldsymbol{\overline{\omega}}, 0, \boldsymbol{\omega}, \mathbf{0}, \omega), (\boldsymbol{\omega}, \overline{\omega}, 1, \mathbf{0}, 0, \mathbf{1}, \boldsymbol{\overline{\omega}}, \omega), \text{ and } (\mathbf{0}, \overline{\omega}, 1, \boldsymbol{\omega}, 0, \boldsymbol{\overline{\omega}}, \mathbf{1}, \omega).$$

So we could decode $\mathbf{v}$ as follows and have found three more coset leaders.

	1	2	3	4	5	6	7	8
0	**0**	0	1	1	1	0	1	0
1	0	1	1	0	1	**1**	**1**	1
ω	1	1	0	0	1	0	1	0
$\overline{\omega}$	1	0	0	**1**	1	1	**1**	1
	1	$\overline{\omega}$	1	$\boldsymbol{\overline{\omega}}$	0	$\boldsymbol{\omega}$	**0**	ω

,

	1	2	3	4	5	6	7	8
0	1	0	1	**0**	1	0	1	0
1	0	1	1	0	1	0	0	1
ω	1	1	0	0	1	**1**	**0**	0
$\overline{\omega}$	**0**	0	0	0	1	1	**1**	1
	$\boldsymbol{\omega}$	$\overline{\omega}$	1	**0**	0	**1**	$\boldsymbol{\overline{\omega}}$	ω

,

	1	2	3	4	5	6	7	8
0	1	0	1	1	1	**1**	1	0
1	**1**	1	1	0	1	0	**1**	1
ω	1	1	0	**1**	1	0	1	0
$\overline{\omega}$	1	0	0	0	1	1	**1**	1
	0	$\overline{\omega}$	1	$\boldsymbol{\omega}$	0	$\boldsymbol{\overline{\omega}}$	**1**	ω

Example 5 (Case V). *Four of the columns have even parity, and four of the columns have odd parity.*

In this case we know that there are 4 or 6 errors from Table 2. Since we are using maximum likelihood decoding, we first try 4 errors. If we cannot detect any 4 errors, then we say that 6 errors occurred. We consider an example.

$\mathbf{v} =$

		1	2	3	4	5	6	7	8
0		1	1	0	1	1	0	1	1
1		1	0	0	1	0	1	0	0
ω		1	1	1	0	0	1	1	0
$\overline{\omega}$		1	1	1	1	0	0	0	0
$\mathbf{y}$	=	0	1	1	ω	0	$\overline{\omega}$	ω	0

We first describe the representation decoding method. Suppose that the even columns are correct. So the correct projection is $(0,-,1,-,-,\overline{\omega},\omega,-)$. From Table 1 the vector $(0,-,1,-,-,\overline{\omega},\omega,-)$ cannot be matched with any Hamming codeword of weight 4. Clearly this vector cannot be matched with any Hamming codeword of weight 8 since it has at least one zero. We can quickly find a matching Hamming codeword $(0,\mathbf{0},1,\mathbf{1},\boldsymbol{\overline{\omega}},\overline{\omega},\omega,\boldsymbol{\omega})$ of weight 6 from Table 1. Hence the following is a Reed-Muller codeword.

	1	2	3	4	5	6	7	8
0	1	1	0	1	1	0	1	1
1	1	**1**	0	1	0	1	0	0
ω	1	1	1	0	0	1	1	**1**
$\overline{\omega}$	1	1	1	**0**	**1**	0	0	0
	0	**0**	1	**1**	$\boldsymbol{\overline{\omega}}$	$\overline{\omega}$	ω	$\boldsymbol{\omega}$

This is enough to decode. We also show how this method can find other error vectors. To do this we observe that it is possible that the odd columns of $\mathbf{v}$ are correct. So suppose that the odd columns are correct. So the correct projection is $(-,1,-,\omega,0,-,-,0)$. This projection vector can be matched with a Hamming codeword $(\boldsymbol{\omega},1,\mathbf{1},\boldsymbol{\omega},0,\boldsymbol{\overline{\omega}},\boldsymbol{\overline{\omega}},0)$ of weight 6. Hence the following is another Reed-Muller codeword.

	1	2	3	4	5	6	7	8
0	1	1	**1**	1	1	**1**	1	1
1	1	0	0	1	0	1	**1**	0
ω	**0**	1	1	0	0	1	1	0
$\overline{\omega}$	1	1	1	1	0	0	0	0
	$\boldsymbol{\omega}$	1	**1**	ω	0	$\boldsymbol{\overline{\omega}}$	$\boldsymbol{\overline{\omega}}$	0

Next we describe the syndrome decoding method. Recall that our projection vector $\mathbf{y}=(0,1,1,\omega,0,\overline{\omega},\omega,0)$. When we suppose that even columns are correct, we see that errors happened among the positions 2, 4, 5, or 8 of $\mathbf{y}$. Hence it suffices to solve the following equation (Step 5 (a)):

$$H\mathbf{y}^T=\begin{bmatrix}\overline{\omega}\\1\\1\\0\end{bmatrix}=e_2\begin{bmatrix}1\\0\\0\\1\end{bmatrix}+e_4\begin{bmatrix}1\\0\\1\\1\end{bmatrix}+e_5\begin{bmatrix}1\\1\\0\\0\end{bmatrix}+e_8\begin{bmatrix}1\\1\\1\\1\end{bmatrix},$$

where the columns on the right side correspond to columns of H defined in (1). Solving we get $e_2=1, e_4=\overline{\omega}, e_5=\overline{\omega}$, and $e_8=\omega$. Hence the error vector is $\mathbf{e}=(0,1,0,\overline{\omega},\overline{\omega},0,0,\omega)$. Thus the desired Hamming codeword is $\mathbf{x}=\mathbf{y}+\mathbf{e}=(0,\mathbf{0},1,\mathbf{1},\boldsymbol{\overline{\omega}},\overline{\omega},\omega,\boldsymbol{\omega})$. After this, the rest is the same as before.

When we suppose that the odd columns are correct, we see that errors happened among the positions 1, 3, 6, or 7 of $\mathbf{y}$. Hence it suffices to solve the following equation (Step 5 (a)):

$$H\mathbf{y}^T=\begin{bmatrix}\overline{\omega}\\1\\1\\0\end{bmatrix}=e_1\begin{bmatrix}1\\0\\0\\0\end{bmatrix}+e_3\begin{bmatrix}1\\0\\1\\0\end{bmatrix}+e_6\begin{bmatrix}1\\1\\0\\1\end{bmatrix}+e_7\begin{bmatrix}1\\1\\1\\0\end{bmatrix},$$

where the columns on the right side correspond to columns of H defined in (1). Solving we get $e_1 = \omega, e_3 = 0, e_6 = 0$, and $e_7 = 1$. Hence the error vector is $\mathbf{e} = (\omega, 0, 0, 0, 0, 0, 0, 1, 0)$. Thus the desired Hamming codeword is $\mathbf{x} = \mathbf{y} + \mathbf{e} = (\boldsymbol{\omega}, 1, \mathbf{1}, \omega, 0, \overline{\boldsymbol{\omega}}, \overline{\boldsymbol{\omega}}, 0)$. After this, the rest is the same as before. We note that in this example we have a unique solution for either case(odd or even columns are error positions). However we remark the following. Suppose that the errors were in a different set of 4 linearly dependent columns of H (e.g. the first four positions of a projected vector are errors). Then we will have, if one exists, 4 distinct solutions for the syndrome equations since the matrix consisting of the 4 linearly dependent columns of H has nullity 1.

Remark 3. We comment on the worst cases of the syndrome decoding algorithm. It is easy to see that the computation of step 1 through step 3 in section 3.2 is the same for all possible cases in Table 2. In step 4 we either go to step 5, stop, or decode by complementing any column of $\mathbf{v}$. If we are in step 5 a), then since we already know which columns are incorrect, we just solve the syndrome equation which will involve at most 4 columns of H(see Example 5). However if we are in step 5 b), the situation is more complicated. The worst case is Case I i.e. $(8, \underline{0})$, in particular, the subcase $6 = 2 + 2 + 2$. Since we do not know which three columns out of 8 columns of $\mathbf{v}$ are incorrect, we could try $\begin{pmatrix} 8 \\ 3 \end{pmatrix} = 56$ sets of 3 columns until we get one solvable syndrome equation. Note that there are 32 vectors of weight 6 in a coset of weight 6 of $R(2,5)$ [1]. Given a set of 3 columns giving the correct syndrome equation, there are 4 vectors of weight 6 in this coset of weight 6 since complementing any two of the 3 columns gives the same projection and preserves parities of columns and the top row. Thus 8 sets of 3 columns will hold all of sets of 3 columns giving the correct syndrome. Thus the probability that we find a desired syndrome equation is $8/56 = 1/7$. However in the worst case we have to try $56 - 7 = 49$ sets of 3 columns.

Remark 4. We emphasize that the syndrome decoding method, one of our hand decoding of $R(2,5)$, does not require much memory while the well-known decoding method of $R(2,5)$, majority-logic decoding [7, Ch. 13 Sec. 6] is useful in *machine* decoding. Since majority-logic decoding stores 80 equations in 4 variables and another 80 equations in 2 variables, it cannot be used for decoding by hand. The syndrome decoding method can be easily implemented on a computer.

4 Decoding the other $[32, 16, 8]$ codes

We describe how to decode the other doubly-even self-dual $[32, 16, 8]$ codes C83(or $2g_{16}$) and C84(or $8f_4$) in the notation of [2] by using the syndrome decoding method. We remark that our representation decoding method is not easy to apply to the other two codes. When we decode the binary Reed-Muller $[32, 16, 8]$ code, the structure of the *linear* Hamming code over $GF(4)$ was crucial. However the other two $[32, 16, 8]$ codes C84 and C83 were obtained in [4, 5] from even additive self-dual codes $\mathcal{C}_i (i = 1, 2)$ over $GF(4)$ with minimum weight 4 with generator matrices G_i respectively QC_8d, and QC_8c in Table 3. In fact, if we follow the notation in the Introduction, then $\rho(\mathcal{C}_i) = \widehat{\mathcal{C}_i} + (d_4^8)_0 + f_1$ for $i = 1, 2$ produces C84 and C83, respectively.

Table 3: Generator matrices for even additive self-dual codes over GF(4)

$$
QC\_8c = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & \omega & \omega & 0 \\ 0 & 1 & 0 & 0 & 1 & \overline{\omega} & \overline{\omega} & 0 \\ 0 & 0 & 1 & 0 & \overline{\omega} & 1 & 0 & \omega \\ \omega & \omega & 0 & 0 & \omega & \omega & \omega & \omega \\ \omega & 0 & \omega & 0 & 1 & 1 & \omega & \omega \\ \omega & 0 & 0 & \omega & \overline{\omega} & \overline{\omega} & 1 & 1 \end{bmatrix}, \quad
QC\_8d = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & \omega & \omega & 0 \\ 0 & 1 & 0 & 0 & 1 & \omega & 0 & \omega \\ 0 & 0 & 1 & 0 & \overline{\omega} & 1 & 0 & \omega \\ \omega & \omega & 0 & 0 & \omega & 1 & \overline{\omega} & 1 \\ \omega & 0 & \omega & 0 & 1 & 0 & 1 & 0 \\ \omega & 0 & 0 & \omega & \overline{\omega} & \omega & \omega & \overline{\omega} \end{bmatrix}, \quad
K = \begin{bmatrix} 1 & 0 & 0 & \omega & \omega & \omega & 0 & 0 \\ 0 & 1 & 0 & 0 & \omega & \omega & \omega & 0 \\ 0 & 0 & 1 & 0 & 0 & \omega & \omega & \omega \\ \omega & 0 & 0 & 1 & 0 & 0 & \omega & \omega \\ \omega & \omega & 0 & 0 & 1 & 0 & 0 & \omega \\ \omega & \omega & \omega & 0 & 0 & 1 & 0 & 0 \\ 0 & \omega & \omega & \omega & 0 & 0 & 1 & 0 \\ 0 & 0 & \omega & \omega & \omega & 0 & 0 & 1 \end{bmatrix}
$$

We showed that the code with generator matrix QC_8d is equivalent to a cyclic even additive self-dual code $\mathcal{K}$ over $GF(4)$. This cyclic code has the generator matrix K in Table 3. The advantage of K is that it has only two nonzero elements 1 and ω, which simplify the computation of syndromes.

Let $\mathcal{C}_i (i = 1, 2)$ be additive codes over $GF(4)$ with generator matrices G_i respectively K and QC_8c. When we prove the analogue of Lemma 1 for C84(C83) we need to modify its proof since $\mathcal{C}_1(\mathcal{C}_2)$ is not linear. In this case we recall that $\mathcal{C}_1(\mathcal{C}_2)$ has 2^8 codewords. Keeping the above notation, we have the following analogue of Lemma 1.

Lemma 2. *The set of all binary vectors of length 32 with the following properties is (up to equivalence) C84(C83):*

(i) *The parity of all the columns is the same(i.e., all even or all odd), and the parity of the top row is always even. All vectors of this form constitute a linear space.*

(ii) *The projection is in $\mathcal{C}_1(\mathcal{C}_2)$. All vectors with this property form a linear space.*

Proof. The linearity of this set was explained in Lemma 1. The nontrivial thing is to determine its dimension. From now on, we identify a binary vector of length 32 with a 4×8 array. First suppose that all columns of our 4×8 arrays are even and the first row is even. Then for each codeword $\mathbf{y}$ in $\mathcal{C}_1(\mathcal{C}_2)$ there are 2^7 arrays whose projection is $\mathbf{y}$ as there are 2 choices for each column and one for the last column because of top row parity. Since there are 2^8 codewords in $\mathcal{C}_1(\mathcal{C}_2)$ we see that there are $2^7 \times 2^8 = 2^{15}$ arrays whose projection is in $\mathcal{C}_1(\mathcal{C}_2)$ when all columns are even. For the same reason we get $2^7 \times 2^8 = 2^{15}$ when all columns are odd. Therefore the dimension of the set of vectors of length 32 satisfying (i) and (ii) is 16, as desired. Since $\rho(\mathcal{C}_1)(\rho(\mathcal{C}_2))$ satisfies (i) and (ii) and produces C84(C83), we conclude that $\rho(\mathcal{C}_1)(\rho(\mathcal{C}_2))$ is C84(C83). This completes the proof. $\square$

We note that in fact Lemma 1 can be proved by using the argument in the proof of Lemma 2.

Recall that when we consider additive codes over $GF(4)$, we use the *trace* map, i.e. for x in $GF(4)$, $\mathrm{Tr}(x) = x + x^2 \in GF(2)$. Define the symmetric bilinear dot prodcut $\cdot\ :\ GF(4) \times GF(4) \to GF(2)$ by $x \cdot y = \mathrm{Tr}(x\overline{y})$ so that $1 \cdot \omega = \omega \cdot 1 = 1, 1 \cdot \overline{\omega} = \overline{\omega} \cdot 1 = 1, \omega \cdot \overline{\omega} = \overline{\omega} \cdot \omega = 1$ and zero otherwise. We now define the *trace* *inner product* of two vectors $\mathbf{x} = (x_1 x_2 \cdots x_n)$ and $\mathbf{y} = (y_1 y_2 \cdots y_n)$ in $GF(4)^n$ to be

$$\mathbf{x} \star \mathbf{y} = \sum_{i=1}^{n} x_i \cdot y_i \in GF(2).$$

Note that $x_i \cdot y_i = 1$ if and only if x_i and y_i are distinct nonzero elements in $GF(4)$. As an example, we compute the syndrome of $u_1 = (1,0,0,0,0,0,0,0)$ with respect to $\mathcal{K}$, in other words, we want to compute $K \star {u_1}^T$. Then by the trace inner product we get

$$K \star {u_1}^T = (0,0,0,1,1,1,0,0)^T.$$

Likewise if we let $u_2 = (\omega,0,0,0,0,0,0,0)$ then

$$K \star {u_2}^T = (1,0,0,0,0,0,0,0)^T.$$

Also if we let $u_3 = (\varpi,0,0,0,0,0,0,0)$ then

$$K \star {u_3}^T = K \star (u_1 + u_2)^T = K \star {u_1}^T + K \star {u_2}^T = (1,0,0,1,1,1,0,0)^T$$

since the computation is closed under addition.

Now we briefly describe the idea of decoding the code C84 by using $\mathcal{K}$. Let $\mathbf{v}$ be a received vector of length 32. As before, we write it as a 4×8 array with rows indexed by $0, 1, \omega$, and ϖ. Then we compute the projection onto a quaternary vector $\mathbf{y}$ of length 8. The problem is how to find a codeword of $\mathcal{K}$ closest to $\mathbf{y}$ as in the case of the linear Hamming codeword. For example, let $\mathbf{y} = (\varpi,\omega,0,\omega,0,0,\omega,0)$ be our quaternary vector of length 8 obtained by projecting a binary vector of length 32. To make the explanation simple, suppose that we know that only the first two positions of $\mathbf{y}$ are error positions. Then we compute the following equation:

$$K \star \mathbf{y}^T = \begin{bmatrix} 1\\1\\0\\0\\1\\1\\1\\0 \end{bmatrix} = e_{1,1} \begin{bmatrix} 0\\0\\0\\1\\1\\1\\0\\0 \end{bmatrix} + e_{1,\omega} \begin{bmatrix} 1\\0\\0\\0\\0\\0\\0\\0 \end{bmatrix} + e_{2,1} \begin{bmatrix} 0\\0\\0\\0\\1\\1\\1\\0 \end{bmatrix} + e_{2,\omega} \begin{bmatrix} 0\\1\\0\\0\\0\\0\\0\\0 \end{bmatrix},$$

where the coefficients in the right side are taken to be 0 or 1. We solve this equation to get $e_{1,\omega} = 1, e_{2,\omega} = 1, e_{1,1} = 0$, and $e_{2,1} = 1$. Thus the error vector is $\mathbf{e} = (\omega,\varpi,0,0,0,0,0,0)$, implying that the codeword $\mathbf{x}$ of $\mathcal{K}$ is

$$\mathbf{x} = \mathbf{y} + \mathbf{e} = (\mathbf{1},\mathbf{1},0,\omega,0,0,\omega,0),$$

which is, in fact, the sum of the first two rows of K. And then we decode our received 4×8 array according to Table 2 as we did in the decoding of the $R(2,5)$.

For decoding the code C83 using QC_8c, we follow the same steps as above. However the syndrome equation will be more complicated since the generator matrix of QC_8c has as entries three nonzero elements in $GF(4)$.

Remark 5. When we decode these two codes C84 and C83 by Table 2, we would have to add two more cases which were removed for $R(2,5)$ in Remark 1, i.e. $6 = 1+1+1+1+1+1$ and $5 = 1+1+1+1+1$. This is because we cannot apply to our additive codes the idea of an information set which was possible for the linear Hamming $[8,4,8]$ code.

Remark 6. It is well known [3] that there are three singly-even self-dual $[32, 16, 8]$ codes. It was shown [4, 5] that the three singly-even self-dual $[32, 16, 8]$ codes are constructed from H in Section 2, QC_8c, and QC_8d. In fact, if we follow the notation in the Introduction and let $\mathcal{C}_i (i = 1, 2, 3)$ denote even additive self-dual codes with generator matrices G_i respectively H, QC_8c, and QC_8d, then $\rho(\mathcal{C}_i) = \widehat{\mathcal{C}_i} + (d_4^8)_0 + f_3$ for $i = 1, 2, 3$, where f_3 is the $[32, 1]$ code generated by $1000\ 1000\ \cdots\ 1000\ 0111$, produces the three singly-even self-dual $[32, 16, 8]$ codes. So we can decode the three singly-even self-dual $[32, 16, 8]$ codes by the syndrome decoding method since the only difference is that the top row parity is equal to the parity of all columns when we write a binary vector $\mathbf{v}$ of length 32 as a 4×8 array as before.

References

[1] E. F. Assmus and V. Pless, On the covering radius of extremal self-dual codes, IEEE Trans. Inform. Theory 29 (1983), 359-363.

[2] J. H. Conway and V. Pless, On the enumeration of self-dual codes, J. Comb. Theory 28A (1980), 26-53.

[3] J. H. Conway and N. J. A. Sloane, A new upper bound on the minimal distance of self-dual code, IEEE Trans. Inform. Theory 36 (1990), 1319-1333.

[4] P. Gaborit, W. C. Huffman, J.-L. Kim, and V. Pless, On the classification of extremal additive codes over $GF(4)$, Proceedings of the 37th Allerton Conference on Communication, Control, and Computing, UIUC (1999), 535-544.

[5] ——, On additive $GF(4)$ codes, DIMACS Workshop on Codes and Association Schemes, ed. A. Barg and S. Litsyn, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., Amer. Math. Soc., Providence, RI, Vol. 56 (2001), 135-149.

[6] G. Höhn, Self-dual codes over the Kleinian four group, preprint, 1996. An updated version in http://xxx.lanl.gov/(math.CO/0005266).

[7] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, (North-Holland, New York, 1977).

[8] V. Pless, Decoding the Golay codes, IEEE Trans. Inform. Theory 32 (1986), 561-567.