Decoding Some Doubly-Even Self-Dual $[32, 16, 8]$ Codes By Hand

Jon-Lark Kim and Vera Pless

Abstract. The purpose of this paper is to decode some binary doubly-even self-dual $[32, 16, 8]$ codes by hand. We will decode C84(or $8f_4$) in detail. Our method is the syndrome decoding method used in **[G3]** to decode the binary Reed-Muller code $R(2, 5)$. At the end we also describe how to decode another doubly-even self-dual $[32, 16, 8]$ code C83(or $2g_{16}$) and three singly-even self-dual $[32, 16, 8]$ codes by using the syndrome decoding method.

1991 Mathematics Subject Classification: primary 94B35; secondary 94B05.

1. Introduction

Our notation follows **[MS, P2]**. A *linear* $[n, k]$ *code* $\mathcal{C}$ over $GF(2)$ is a k-dimensional vector subspace of $GF(2)^n$, where $GF(2)$ is the Galois field with two elements. The *weight* $\mathrm{wt}(\mathbf{c})$ of a codeword $\mathbf{c} \in \mathcal{C}$ is the number of nonzero components of $\mathbf{c}$. The minimum nonzero weight d of all codewords in $\mathcal{C}$ is called the *minimum weight* of $\mathcal{C}$. An $[n, k, d]$ code is an $[n, k]$ code with minimum weight d. The *dual code* $\mathcal{C}^{\perp}$of $\mathcal{C}$ consists of vectors in $GF(2)$ orthogonal to all vectors in $\mathcal{C}$ with respect to the usual inner product. If $\mathcal{C} = \mathcal{C}^{\perp}$, then $\mathcal{C}$ is called a *self-dual* code. A self-dual binary code is called *doubly-even* if all codewords have weight $\equiv 0 \pmod 4$ and *singly-even* if some codeword has weight $\equiv 2 \pmod 4$. We note that self-dual binary codes exist only for even lengths. Moreover doubly-even self-dual codes exist only for lengths $n \equiv 0 \pmod 8$.

It was shown **[P1]** 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. It was shown **[G3]** that this is possible for the binary Reed-Muller $[32, 16, 8]$ code $R(2, 5)$ by using the linear Hamming $[8, 4, 4]$ code over $GF(4)$. We remind readers of the fact that $R(2, 5)$ is one of the 5 binary extremal doubly-even self-dual $[32, 16, 8]$ codes **[CP]**. Because of the *linear* structure of the Hamming $[8, 4, 4]$ code over $GF(4)$, $R(2, 5)$ was decoded

[**G3**] by two methods. One, the representation method, is the analogue of the method used to decode the Golay code [**P1**]. The other is the syndrome decoding method.

Even though there is an idea in [**G3**] about decoding other doubly-even self-dual $[32, 16, 8]$ codes C84 and C83 by hand, specific examples were not given. Actually decoding C84(or C83) is much more complicated than $R(2, 5)$ because the projected codes are non-linear and do not have binary generator matrices as the Hamming code over $GF(4)$ does.

The purpose of this paper is to decode some doubly-even self-dual $[32, 16, 8]$ binary codes by hand, i.e. C83 (or $2g_{16}$) and C84 (or $8f_4$) in the notation of [**CP**]. We will decode C84(or $8f_4$) in detail. Our method is the syndrome decoding method used in [**G3**] to decode the binary Reed-Muller code $R(2, 5)$. At the end we also describe how to decode another doubly-even self-dual $[32, 16, 8]$ code C83(or $2g_{16}$) and the three singly-even self-dual $[32, 16, 8]$ codes [**CS**] by using the syndrome decoding method.

Since C84(or C83) is a $[32, 16, 8]$ code, its error-correcting capability is at most 3. It is also well known [**AP**] that the covering radius of C84(or C83) 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 one or more coset representatives of cosets of weight 4, 5, or 6.

2. Preliminaries

Let $GF(4) = \{0, 1, \omega, \overline{\omega}\}$ be the Galois field of four elements. An *additive code* $\mathcal{C}$ *over* $GF(4)$ *of length* n is an additive subgroup of $GF(4)^n$. As $\mathcal{C}$ is a free $GF(2)$-module, it has size 2^k for some $0 \le k \le 2n$. We call $\mathcal{C}$ an $(n, 2^k)$ code. It has a basis, as a $GF(2)$-module, consisting of k basis vectors; a *generator matrix* of $\mathcal{C}$ will be a $k \times n$ matrix with entries in $GF(4)$ whose rows are a basis of $\mathcal{C}$.

When we consider additive codes over $GF(4)$, we define the symmetric bilinear dot product, $\cdot\ :\ GF(4) \times GF(4) \to GF(2)$ by $1 \cdot \omega = \omega \cdot 1 = 1, 1 \cdot \overline{\omega} = \overline{\omega} \cdot 1 = 1, \omega \cdot \overline{\omega} = \overline{\omega} \cdot \omega = 1$ and $x \cdot x = 0 \cdot x = 0$ for all $x \in GF(4)$. 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 nonzero distinct elements in $GF(4)$.

If $\mathcal{C}$ is an additive code, its *dual*, denoted $\mathcal{C}^\perp$, is the additive code $\{\mathbf{x} \in GF(4)^n \mid \mathbf{x} \star \mathbf{c} = 0 \text{ for all } \mathbf{c} \in \mathcal{C}\}$. If $\mathcal{C}$ is an $(n, 2^k)$ code, then $\mathcal{C}^\perp$ is an

Table 1: Generator matrices for even additive self-dual codes over GF(4)

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

$(n, 2^{2n-k})$ code. As usual, $\mathcal{C}$ is *self-orthogonal* if $\mathcal{C} \subseteq \mathcal{C}^{\perp}$ and *self-dual* if $\mathcal{C} = \mathcal{C}^{\perp}$. In particular, if $\mathcal{C}$ is self-dual, $\mathcal{C}$ is an $(n, 2^n)$ code.

The *weight* $\mathrm{wt}(\mathbf{c})$ of $\mathbf{c} \in \mathcal{C}$ is the number of nonzero components of $\mathbf{c}$. The minimum weight d of $\mathcal{C}$ is the smallest weight of any nonzero codeword in $\mathcal{C}$. If $\mathcal{C}$ is an $(n, 2^k)$ additive code of minimum weight d, $\mathcal{C}$ is called an $(n, 2^k, d)$ code. $\mathcal{C}$ is *Type II* if $\mathcal{C}$ is self-dual and all codewords have even weight; it is a fact that Type II codes of length n exist only if n is even [**G1,G2,H**]. If $\mathcal{C}$ is self-dual but some codeword has odd weight (in which case the code cannot be $GF(4)$-linear), the code is *Type I* (see section 4.2 in [**RS**]).

Recently it has been shown [**G1,G2,H**] that there are exactly 3 even self-dual additive $(8, 2^8, 4)$ codes of length 8 over $GF(4)$. Among these three even codes, one is the linear Hamming $[8, 4, 4]$ code $\mathcal{H}$ over $GF(4)$ and the others are $\mathcal{C}_i (i = 1, 2)$ over $GF(4)$ with generator matrices G_i respectively *QC_8d*, and *QC_8c* in Table 1 [**G1,G2**]. Furthermore it was shown [**G1,G2**] that the binary Reed-Muller $[32, 16, 8]$ code $R(2, 5)$, C84, and C83 can be obtained in the following way. Let $\mathcal{C}_0 = \mathcal{H}$ over $GF(4)$. Let $\mathcal{C}_i (i = 1, 2)$ be defined as above. Let $\widehat{\mathcal{C}}_i (i = 0, 1, 2)$ be the binary linear $[32, 8]$ code obtained from $\mathcal{C}_i (i = 0, 1, 2)$ 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 $\{0000, 1111\}$. 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. Finally let f_1 be the $[32, 1]$ code generated by $1000\ 1000\ \cdots\ 1000$.

Lemma 2.1 ([G1,G2]). *$\rho(\mathcal{C}_i) = \widehat{\mathcal{C}}_i + (d_4^8)_0 + f_1$ for $i = 0, 1, 2$ produces the binary Reed-Muller $[32, 16, 8]$ code $R(2, 5)$, C84, and C83, respecctively.*

3. Two doubly-even self-dual $[32, 16, 8]$ codes

We describe how to decode the doubly-even self-dual $[32, 16, 8]$ codes C83(or $2g_{16}$) and C84(or $8f_4$) in the notation of [**CP**] by using the syndrome decoding method.

It is known [**G3**] 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 1. The advantage of K is that it has only two nonzero elements 1 and ω, which simplify the computation of syndromes. Thus we will decode C84(or $8f_4$) by using K in detail.

We index each column of K from left to right by 1 to 8. This is how we refer to the columns of K, i.e. column 6 is $(\omega,\omega,\omega,0,0,1,0,0)^T$.

Before we describe how to use K to decode C84(or $8f_4$), we recall the projection of binary codes onto quaternary codes explained in [**P1**]. 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 (Euclidean) 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.

Let $\mathcal{C}_i (i=1,2)$ be the additive codes over $GF(4)$ with generator matrices G_i respectively K and QC_8c. When we prove the analogue of Lemma 1 in [**G3**] 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 lemma.

Lemma 3.1. *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 the set satisfying (i) and (ii) is easy. 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) by Lemma 2.1, we conclude that $\rho(\mathcal{C}_1)(\rho(\mathcal{C}_2))$ is C84(C83). This completes the proof. $\square$

As an example, we compute the syndrome $K\mathbf{e}^T$ of $\mathbf{e} = (1,0,0,0,0,0,0,0)$ with respect to the trace inner product. We get

$$K\mathbf{e}^T = (0,0,0,1,1,1,0,0)^T.$$

Likewise if we let $\mathbf{e}' = (\omega,0,0,0,0,0,0,0)$ then

$$K\mathbf{e}'^T = (1,0,0,0,0,0,0,0)^T.$$

Also if we let $\mathbf{e}'' = (\varpi,0,0,0,0,0,0,0)$ then

$$K\mathbf{e}''^T = K(\mathbf{e}+\mathbf{e}')^T = K\mathbf{e}^T + K\mathbf{e}'^T = (1,0,0,1,1,1,0,0)^T,$$

since the trace inner product is bilinear.

Now we briefly describe the idea of decoding the code C84 by using $\mathcal{K}$ to understand the decoding algorithm(section 4.1. Let 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 we will see in the next section, we will have some idea of which columns are in error. After we know this, our aim is to find the correct projection in $\mathcal{K}$. In order to do this we compute the syndrome of $\mathbf{y}$ with respect to K. This is always a binary vector. We want to express this as a linear combination of the vectors in Table 2. These vectors are obtained by taking the trace inner product of all possible weight one vectors $\mathbf{e}$ with the columns of K. Let the non-zero component of $\mathbf{e}$ be e_i. If $e_i = 1$, $\mathbf{e}$ is binary. If $e_i = \omega$(or ϖ), the weight one vector $\mathbf{e}$ has one ω(or ϖ) component. We use $e_{i,1}, e_{i,\omega}$, and $e_{i,\varpi}$

Table 2: Syndromes $K\mathbf{e}^T$ of $\mathbf{e}^T$ with wt($\mathbf{e}$)=1 and $e_i \neq 0$

i	1	2	3	4	5	6	7	8
	0	0	0	1	1	1	0	0
	0	0	0	0	1	1	1	0
$K\mathbf{e}^T$	0	0	0	0	0	1	1	1
with	1	0	0	0	0	0	1	1
$e_i = 1$	1	1	0	0	0	0	0	1
	1	1	1	0	0	0	0	0
	0	1	1	1	0	0	0	0
	0	0	1	1	1	0	0	0

i	1	2	3	4	5	6	7	8
	1	0	0	0	0	0	0	0
	0	1	0	0	0	0	0	0
$K\mathbf{e}^T$	0	0	1	0	0	0	0	0
with	0	0	0	1	0	0	0	0
$e_i = \omega$	0	0	0	0	1	0	0	0
	0	0	0	0	0	1	0	0
	0	0	0	0	0	0	1	0
	0	0	0	0	0	0	0	1

i	1	2	3	4	5	6	7	8
	1	0	0	1	1	1	0	0
	0	1	0	0	1	1	1	0
$K\mathbf{e}^T$	0	0	1	0	0	1	1	1
with	1	0	0	1	0	0	1	1
$e_i = \overline{\omega}$	1	1	0	0	1	0	0	1
	1	1	1	0	0	1	0	0
	0	1	1	1	0	0	1	0
	0	0	1	1	1	0	0	1

for $i = 1, \cdots, 8$ to denote the binary coefficients of the syndrome $K\mathbf{e}^T$ of $\mathbf{e}^T$ with wt($\mathbf{e}$)=1 and $e_i = 1, \omega$, and $\overline{\omega}$ respectively.

For example, let $\mathbf{y} = (\overline{\omega}, \omega, 0, \omega, 0, 0, \omega, 0)$ 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 syndrome equation:

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

where the coefficients on the right side are binary. 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 $\mathbf{e} = (\omega, \overline{\omega}, 0, 0, 0, 0, 0, 0)$, 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. Then we decode our received 4×8 array according to Table 3 as we will see in the next section.

4. Decoding the doubly-even self-dual code C84

Now we decode the doubly-even self-dual code C84 by hand in detail by using the syndrome decoding method. We recall from Section 3 that when we decode C84, we use the even self-dual additive code $\mathcal{K}$ with generator matrix K in Table 1. We give an explanation of Table 3 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

Table 3: 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
		$6 = 1 + 1 + 1 + 1 + 1 + 1$	$\underline{2}$
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
		$5 = 1 + 1 + 1 + 1 + 1$	$\underline{3}$
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

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 $6 = \underline{2} + 1 + 1 + 1 + 1$[both of which may need to be considered].

4.1. Decoding Algorithm We give the outline of a maximum-likelihood syndrome decoding algorithm of C84. Maximum-likelihood means that we assume that the smallest number of errors have occurred. We have K 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 3 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 K.

Step 4. If the syndrome of $\mathbf{y}$ is zero and we are in case I of Table 3, 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 Table 2. 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 C84. Then we stop.

To see this algorithm more clearly we give some specific examples.

4.2. Examples

Example 4.1 (Case I). All the columns have the same parity.

In this case we know that there are zero, two, four, or six errors by Table 3. Consider the following example.

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

Suppose the parity of all columns is correct(step 1). The projection of the received vector $\mathbf{v}$ is $\mathbf{y} = (\overline{\omega}, \omega, 0, \omega, \overline{\omega}, \omega, 1, \omega)$(step 2). Even though the top row is even, we are not sure if this $\mathbf{v}$ is a codeword of C84 before we compute the syndrome of $\mathbf{y}$ with respect to K(step 3).

$$K\mathbf{y}^T = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

If $\mathbf{v}$ were a codeword of C84, then $K\mathbf{y}^T$ would be a zero vector of length 8 by Lemma 3.1 (ii)(step 4). Thus $\mathbf{v}$ is not a codeword. To decode $\mathbf{v}$ we need to find a vector in $\mathcal{K}$ closest to $\mathbf{y}$(step 5 b)). We first note that the trace inner product of the 7th column of K and $(0, 0, 0, 0, 0, 0, 1, 0)$ i.e. the syndrome $K\mathbf{e}^T$ with wt($\mathbf{e}$)=1 and $e_7 = 1$(see Table 2) is $(0,1,1,1,0,0,0,0)$. Therefore we found an error in the 7th position of $\mathbf{y}$. Hence our error vector is $\mathbf{e} = (0,0,0,0,0,0,1,0)$ giving a vector $\mathbf{x} = \mathbf{y} + \mathbf{e} = (\overline{\omega}, \omega, 0, \omega, \overline{\omega}, \omega, \mathbf{0}, \omega)$ in $\mathcal{K}$. For checking, we can actually write $\mathbf{x}$ as a linear combination of rows of K. That is, $\mathbf{x}$ = 1st + 5th rows of K. We observe that only the 1st and 5th coordinates of $\mathbf{x}$ have 1 or $\overline{\omega}$. This is true in general. Whenever we want to write $\mathbf{x}$ as a linear combination of rows of K, we just consider coordinates of $\mathbf{x}$ having 1 or $\overline{\omega}$, whose corresponding rows are a linear combination of $\mathbf{x}$.

Hence we uniquely decode $\mathbf{v}$ as follows(step 6).

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

Example 4.2 (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 3. If there are at most three errors, then we can uniquely decode. Otherwise we can detect five errors and decode into some codeword. We explain this case in the next example.

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

Suppose the parity of the seven odd columns is correct(step 1). So the sixth column of this array has at least one error. No syndrome equation involving two syndromes works. Note that we have to include at least one syndrome $K\mathbf{e}^T$ with $e_6 = 1, \omega$ or $\overline{\omega}$ since there is an error in the sixth column. By trial and error we consider the following equation(these syndromes can be found in Table 2)(step 5 b)).

$$K\mathbf{y}^T = \begin{bmatrix} 0\\1\\1\\0\\1\\1\\1\\1 \end{bmatrix} = e_{4,1} \begin{bmatrix} 1\\0\\0\\0\\0\\0\\1\\1 \end{bmatrix} + e_{5,\omega} \begin{bmatrix} 0\\0\\0\\0\\1\\0\\0\\0 \end{bmatrix} + e_{6,\overline{\omega}} \begin{bmatrix} 1\\1\\1\\0\\0\\1\\0\\0 \end{bmatrix}.$$

Solving we get $e_{4,1} = 1, e_{5,\omega} = 1$, and $e_{6,\overline{\omega}} = 1$(recall that these coefficients are binary). Thus we get an error vector $\mathbf{e} = (0,0,0,\mathbf{1},\boldsymbol{\omega},\boldsymbol{\overline{\omega}},0,0)$, giving $\mathbf{x} = \mathbf{y} + \mathbf{e} = (\overline{\omega},0,1,\mathbf{0},\boldsymbol{\omega},\mathbf{1},\overline{\omega},\omega)$ in $\mathcal{K}$. Actually $\mathbf{x}$ = 1st + 3rd + 6th + 7th rows of K as observed in Example 4.1. Hence we decode $\mathbf{v}$ as follows(step 6).

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

Example 4.3 (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 3. Consider the following example.

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

Suppose that the parity of the six odd columns is correct(step 1). Noting that

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

we know that more than two erros have occurred since the sixth and seventh columns already have errors. From the above syndrom equation we get an error vector $\mathbf{e} = (\boldsymbol{\omega},0,0,0,0,0,0,0)$ giving $\mathbf{x} = \mathbf{y} + \mathbf{e} = (\mathbf{1},0,0,\overline{\omega},1,\boldsymbol{\omega},\boldsymbol{\overline{\omega}},1)$ in $\mathcal{K}$(step 5 b)). Actually $\mathbf{x}$ = 1st + 4th + 5th + 7th rows of K. Hence we decode $\mathbf{v}$ as follows(step 6).

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

Example 4.4 (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 3. We first try the three error case. If we cannot correct three errors, then we see that five errors occurred. Consider the following example.

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

Suppose that the parity of the five odd columns is correct(step 1). We consider the equation(step 5 b)):

$$
K\mathbf{y}^T = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = e_{5,\varpi} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}.
$$

Thus we get an error vector $\mathbf{e} = (0, 0, 0, 0, \boldsymbol{\varpi}, 0, 0, 0)$ giving $\mathbf{x} = \mathbf{y} + \mathbf{e} = (\varpi, \mathbf{1}, \varpi, 0, \mathbf{1}, \omega, 1, \mathbf{0})$ in $\mathcal{K}$. Actually $\mathbf{x}$ = 1st + 2nd + 3rd + 5th + 7th rows of K. Hence we decode $\mathbf{v}$ as follows(step 6).

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

Example 4.5 (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 3. We first try 4 errors. If we cannot detect any 4 errors, then we say that 6 errors occurred. We consider an example.

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

Suppose that the even columns are correct(step 1). Thus we have errors in positions 2,4,5, and 8. So we consider the equation:

$$
K\mathbf{y}^T = \begin{bmatrix}1\\1\\1\\1\\1\\1\\1\\1\end{bmatrix} = e_{2,1}\begin{bmatrix}0\\0\\0\\0\\1\\1\\1\\0\end{bmatrix} + e_{2,\omega}\begin{bmatrix}0\\1\\0\\0\\0\\0\\0\\0\end{bmatrix} + e_{4,1}\begin{bmatrix}1\\0\\0\\0\\0\\0\\1\\1\end{bmatrix} + e_{4,\omega}\begin{bmatrix}0\\0\\0\\1\\0\\0\\0\\0\end{bmatrix} +
$$
$$
e_{5,1}\begin{bmatrix}1\\1\\0\\0\\0\\0\\0\\1\end{bmatrix} + e_{5,\omega}\begin{bmatrix}0\\0\\0\\0\\1\\0\\0\\0\end{bmatrix} + e_{8,1}\begin{bmatrix}0\\0\\1\\1\\1\\0\\0\\0\end{bmatrix} + e_{8,\omega}\begin{bmatrix}0\\0\\0\\0\\0\\0\\0\\1\end{bmatrix}.
$$

Solving this equation, we have a unique solution as follows : $e_{2,1} = 1, e_{2,\omega} = 0, e_{4,1} = 0, e_{4,\omega} = 0, e_{5,1} = 1, e_{5,\omega} = 1, e_{8,1} = 1, e_{8,\omega} = 0$. Thus we get an error vector $\mathbf{e} = (0, \mathbf{1}, 0, 0, \boldsymbol{\overline{\omega}}, 0, 0, \mathbf{1})$ giving $\mathbf{x} = \mathbf{y} + \mathbf{e} = (0, \mathbf{0}, 1, \boldsymbol{\omega}, \boldsymbol{\overline{\omega}}, \overline{\omega}, \omega, \mathbf{1})$ in $\mathcal{K}$. Actually $\mathbf{x}$ = 3rd + 5th + 6th + 8th rows of K. Hence we decode $\mathbf{v}$ as follows(step 6).

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

Since we decoded, we need not go further, i.e. we do not consider the other possibility that the odd columns of $\mathbf{v}$ are correct.

Remark 4.6. 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 4.7. It is well known [**CS**] that there are three singly-even self-dual $[32, 16, 8]$ codes. It was shown [**G1,G2**] that the three singly-even self-dual $[32, 16, 8]$ codes are constructed from the extended Hamming $[8, 4, 4]$ code H over $GF(4)$, QC_8c, and QC_8d. 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. If we follow the notation in the preliminaries, 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 [**G1,G2**]. So we can decode the three singly-even self-dual $[32, 16, 8]$ codes by the syndrome decoding method with the difference 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.

Remark 4.8. We comment on the worst cases of the decoding algorithm. It is easy to see that the computation of step 1 through step 3 in section 4.1 is the same for all possible cases in Table 3. In step 4 we 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 8 columns in Table 2(see Example 4.5). 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 C84(also C83) [**AP**]. 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 them. 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.

References

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

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

[CS] J. H. Conway and N. J. A. Sloane, "A new upper bound on the minimal distance of self-dual code," *IEEE Trans. Inform. Theory,* vol. 36, pp 1319-1333, Nov. 1990.

[G1] 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 Sep. 1999, 535-544.

[G2] ——, "On additive $GF(4)$ codes," to appear in *Proceedings of the DIMACS Workshop on Codes and Association Schemes*, ed. A. Barg and S. Litsyn, AMS, Nov. 1999.

[G3] P. Gaborit, J.-L. Kim, and V. Pless, "Decoding binary $R(2,5)$ by hand," preprint, 2000.

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

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

[P1] V. Pless, "Decoding the Golay codes," *IEEE Trans. Inform. Theory* **IT-32**(1986), 561–567.

[P2] V. Pless, *Introduction to the Theory of Error-Correcting Codes,* 3rd ed. New York : John Wiley and Sons(1998)

[RS] E. M. Rains and N. J. A. Sloane, "Self-dual codes," in *Handbook of Coding Theory*, ed. V. S. Pless and W. C. Huffman. Amsterdam: Elsevier, 1998, pp. 177–294.

University of Illinois–Chicago,
Mathematics, Statistics, and Computer Science(M/C 249), 322 SEO, 851 S. Morgan, Chicago, IL 60607-7045, USA
jlkim@math.uic.edu ; pless@math.uic.edu