On the Quaternary Projection of Binary Linear Block Codes

M. Esmaeili
Department of Mathematical Sciences
Isfahan University of Technology
Isfahan, Iran
emorteza@cc.iut.ac.ir

T.A. Gulliver
Dept. of Electrical and Computer Engineering
University of Victoria
P.O. Box 3055, STN CSC
Victoria, B.C., V8W 3P6 Canada
agullive@ece.uvic.ca

Abstract

The projection of binary linear block codes of length $4m$ on F_4^m is considered. Three types of projections, namely projections SE, E, and O are introduced. The BCH codes, Golay codes, Reed-Muller codes, and the quadratic residue code q_{32} are examined.

1 Introduction

A binary linear $[n, k]$ code C is a k-dimensional vector subspace of F_2^n, where F_2 is the finite field of two elements. The rate of a linear $[n, k]$ code C is defined as k/n. The elements of C are called codewords. The Hamming weight wt(x) of a codeword x is the number of non-zero coordinates. The minimum weight of C is the smallest weight among all non-zero codewords of C. An $[n, k, d]$ code is an $[n, k]$ code with minimum weight d.

The concept of projecting a binary linear code onto a larger field provides a foundation for the construction of larger codes from shorter ones, and the reduction of the decoding complexity by applying a two-level decoding algorithm [3, 8, 9, 10]. The projection of binary linear codes onto larger fields, in particular F_4, has been considered in [1, 4, 5, 6, 7, 8, 10]. Let

$F_4 = \{0, 1, \omega, \bar{\omega} = \omega^2\}$ be the finite field with four elements. The F_2-linear map Proj from F_2^4 to F_4 is defined by

$$\text{Proj}(x_1x_2x_3x_4) := < x_1, x_2, x_3, x_4 >< 0, 1, \omega, \bar{\omega} >= x_1 0 + x_2 1 + x_3\omega + x_4\bar{\omega}.$$

This mapping is a 4 to 1 projection, that is for each a $\in F_4$ there are four distinct length 4 binary strings that are mapped to a. Two of these strings have odd Hamming weight and are referred to as the odd interpretations of a, while the other two are called even interpretations.

Let v be a vector in F_2^{4m} where m is a positive integer. The vector v is represented by a $4 \times m$ array, denoted $A_{\mathbf{v}} = [a_{i,j}]$, where $a_{i,j}$ is the $\{4(j-1)+i\}$th component of v. The array $A_{\mathbf{v}}$ will be referred to as the array of v. Applying the mapping Proj to the columns of $A_{\mathbf{v}}$, the mapping is extended to F_2^{4m}, and F_2^{4m} is projected onto F_4^m.

The parity of a finite length binary string s is defined as the mod 2 addition of the components of s; that is the parity is 0 (resp. 1) if s has even (resp. odd) Hamming weight.

Let $\mathcal{C}_4$ be an additive code of length m over F_4 and let $\mathcal{C}_2$ be a set of binary vectors of length $4m$. Then according to [4, 7, 8, 10], it is said that $\mathcal{C}_2$ has projection O (resp. E) onto $\mathcal{C}_4$ if $\mathcal{C}_2$ is the largest set of binary vectors c of length $4m$ satisfying conditions T1, T2, and T3 (resp. T3′):

T1. $\text{Proj}(\mathbf{c}) \in \mathcal{C}_4$.

T2. The column parities of the array $A_{\mathbf{c}}$ are either all even or all odd.

T3. The parity of the first row of $A_{\mathbf{c}}$ is the same as the column parity of the array.

T3′. Regardless of the column parity, the parity of the first row of $A_{\mathbf{c}}$ is even.

For instance, the binary $[24, 12, 8]$ Golay code has projection O onto the $[6, 3, 4]$ quaternary code (hexacode) [8]. As another example, let M be the generator matrix of the extended $[32, 16, 8]$ BCH code obtained from the generator matrix of the cyclic $[31, 16, 7]$ BCH code by adding an overall parity check bit. Applying the permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 3 & 30 & 8 & 10 & 18 & 20 & 1 & 2 & 21 & 5 & 6 & 15 & 19 & 29 & 9 & 4 \\ \hline 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 & 32 \\ 17 & 23 & 11 & 24 & 13 & 22 & 28 & 7 & 27 & 16 & 31 & 25 & 12 & 32 & 14 & 26 \end{pmatrix}$$

on matrix M and using elementary row operations results in the matrix M' given below. The projection of this code under the mapping Proj is the quaternary $[8, 4, 4]$ code with generator matrix G_b. It is known that this is an E projection [1, 6]. The first eight rows of M' form the kernel of this

mapping.

$$M' = \begin{matrix}
11111111000000000000000000000000 \\
00001111111100000000000000000000 \\
00000000111111110000000000000000 \\
00000000000011111111000000000000 \\
00000000000000001111111100000000 \\
00000000000000000000111111110000 \\
00000000000000000000000011111111 \\
10001000100010001000100010001000 \\
01010000011010101100000000000000 \\
00110000010100110110000000000000 \\
00000101111110011010110000000000 \\
00000011000010101100011000000000 \\
00000000011000001100011011000000 \\
00000000001100001010001110100000 \\
00000000000000101110000000011010 \\
00000000000000011011000010011100
\end{matrix} \qquad G_b = \begin{bmatrix} 1 & 0 & 0 & 0 & \bar{\omega} & \omega & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & \bar{\omega} & 1 & \omega \\ 0 & 0 & 1 & 0 & \omega & 1 & \omega & 0 \\ 0 & 0 & 0 & 1 & \bar{\omega} & 0 & \bar{\omega} & 1 \end{bmatrix}. \tag{1}$$

Consider now the matrices M and $M4$ given below.

$$M = \begin{bmatrix} 1111 & 1111 & 0000 & 0000 \\ 0000 & 0000 & 1111 & 1111 \\ 0101 & 0011 & 1001 & 1010 \\ 1000 & 0111 & 1011 & 1101 \end{bmatrix} \qquad M4 = \begin{bmatrix} \omega & 1 & \bar{\omega} & \omega \\ 0 & 0 & 1 & \omega \end{bmatrix}$$

Any row of matrix M, and hence any linear combination of them, satisfies conditions T1, T2 and T3, and the binary code $\mathcal{C}$ with generator matrix M is projected onto the additive quaternary code $\mathcal{C}_4$ introduced by matrix $M4$. This code, however, is not the largest one with these properties, and hence based on the given definition it does not have projection O onto $\mathcal{C}_4$.

The only implication of considering the largest set $\mathcal{C}$ satisfying conditions T1, T2, and T3 (resp. T3′), is that such a set $\mathcal{C}$ contains $E_m \otimes R_4$, where E_m is the $[m, m-1, 2]$ even weight code, R_4 is the $[4, 1, 4]$ repetition code and $\otimes$ denotes Kronecker product. This property allows one to consider an inverse function Proj^{-1} from F_4 to F_2^4 such that the strings $\mathrm{Proj}^{-1}(x)$, $x \in F_4$, have even parity and their first components are the same. Though this uniformity of Proj^{-1} has a very limited impact on the reduction of decoding complexity, it imposes a strict bound on the size of the class of projectable codes and their minimum distances. Since these codes contain $E_m \otimes R_4$, their minimum distances do not exceed 8 and hence asymptotically they are poor. Therefore, it seems there does not exist convincing reasons behind putting strong restrictions such as *being the largest set* on the definition of projections E and O. From both the theoretical and application perspectives, it is natural to relax the definition slightly so that it can be applied to a much larger set of codes.

In this paper we generalise the definition of projection by removing the *largeness* constraint considered previously, in particular in [7], and distinguish three types of projections, namely projections SE, E and O. The codes considered in this paper can have an arbitrarily large minimum distance.

In Section 2, we introduce the three types of projections and characterise the corresponding classes of codes. The given criteria are quite different

from those given in [7], and enable one to easily recognise a code belonging to any of these three classes. In Section 3, we consider Reed-Muller codes and the $[32, 16, 8]$ quadratic residue code. We show that only the second-order RM codes and their subcodes have projection E. It is shown that although the $[32, 16, 8]$ quadratic residue code has none of the three projections, it contains a 14-dimensional subcode having projection E.

2 Projections SE, E and O

In this section, we introduce three types of projections and completely determine the codes that have these projections. Several examples illustrating the projections are provided. The examples also explain how such codes can be constructed.

Definition 1 A vector $\mathbf{v} \in F_2^{4m}$ is said to be column-uniform if the columns of $A_{\mathbf{v}}$ are either all odd or all even. In addition, $\mathbf{v}$ is even (resp. odd) if the first row and the columns of $A_{\mathbf{v}}$ have even (resp. odd) parity. If $A_{\mathbf{v}}$ is column-uniform with odd column parity, but the first row of $A_{\mathbf{v}}$ has even parity, then $\mathbf{v}$ is called a weakly-odd vector. A linear binary code $\mathcal{C}$ is called column-uniform if any codeword $\mathbf{c} \in \mathcal{C}$ is column-uniform.

Definition 2 Let $\mathcal{C}$ be a linear binary code of length $4m$ and let $\mathcal{C}_4$ be a quaternary additive code of length m. The code $\mathcal{C}$ is said to have a strong E projection (SE projection) onto $\mathcal{C}_4$ if it satisfies conditions P1 and P2:
P1 $\mathrm{Proj}(\mathcal{C}) := \{\mathrm{Proj}(\mathbf{c}) |\ \mathbf{c} \in \mathcal{C}\} = \mathcal{C}_4$.
P2 All codewords in $\mathcal{C}$ are even.

We say $\mathcal{C}$ has projection E onto $\mathcal{C}_4$ if it satisfies conditions P1 and P2′:
P2′ Any codeword $\mathbf{c} \in \mathcal{C}$ is either even or weakly-odd.

We say that $\mathcal{C}$ has projection O onto $\mathcal{C}_4$ if it satisfies conditions P1, P2″ and P3:
P2″ Any codeword $\mathbf{c} \in \mathcal{C}$ is either even or odd.
P3 $\mathcal{C}$ contains at least one odd codeword.

It follows from the above definition that a code with projection SE also has projection E, but the converse is not true. According to the definition, if $\mathcal{C}$ has any of the three projections SE, E and O onto $\mathrm{Proj}(\mathcal{C})$ then it is column-uniform, and that under conditions P2″ and P3, precisely half of the codewords in $\mathcal{C}$ are odd.

Lemma 1 A linear binary code $\mathcal{C}$ is column-uniform if and only if the dual code $\mathcal{C}^{\perp}$ contains the code $[m, m-1, 2] \otimes [4, 1, 4]$, denoted $E_m \otimes R_4$.

Proof Suppose $\mathcal{C}$ is column-uniform and $\mathbf{c} \in \mathcal{C}$. Consider a word $\mathbf{w} \in E_m \otimes R_4$. Each column of $A_{\mathbf{w}}$ has weight either 0 or 4, and the number of

weight-4 columns in $A_{\mathbf{w}}$ is even. If $\mathbf{c}$ is even then obviously the F_2-inner product of each column of $A_{\mathbf{c}}$ with its corresponding column in $A_{\mathbf{w}}$ is zero and hence $\mathbf{w} \cdot \mathbf{c} = 0$. If $\mathbf{c}$ is odd then the inner product of each weight-4 column of $A_{\mathbf{w}}$ with its corresponding column in $A_{\mathbf{c}}$ is 1, and hence, as the number of nonzero columns in $A_{\mathbf{w}}$ is even, we have $\mathbf{w} \cdot \mathbf{c} = 0$. Therefore, $E_m \otimes R_4 \subseteq \mathcal{C}^{\perp}$.

Conversely, suppose $E_m \otimes R_4 \subseteq \mathcal{C}^{\perp}$ and consider a codeword $\mathbf{c} \in \mathcal{C}$. We show that $\mathbf{c}$ is either odd or even. Without loss of generality, assume the first two columns in $A_{\mathbf{c}}$ have different parities. Then the inner product of $\mathbf{w} = 1111\ 1111\ 0000 \cdots 0000$, a word in $E_m \otimes R_4$, with $\mathbf{c}$ is 1, which is a contradiction. ■

Corollary 1 A linear binary code $\mathcal{C}$ having any of the three projections SE, E and O satisfies $E_m \otimes R_4 \subseteq \mathcal{C}^{\perp}$.

Lemma 2 All codewords in $\mathcal{C} \subseteq F_2^{4m}$ are column-uniform with even column parity if and only if $I_m \otimes R_4 \subseteq \mathcal{C}^{\perp}$, where I_m is the universal code of length m.

Proof Consider a codeword $\mathbf{c} \in \mathcal{C}$ with array $A_{\mathbf{c}}$. Suppose all columns in $A_{\mathbf{c}}$ have even parity. Then the vector 1111 is orthogonal to each column of $A_{\mathbf{c}}$, and hence any word in $I_m \otimes R_4$ is orthogonal to $\mathbf{c}$. This proves the forward implication.

Conversely, suppose $I_m \otimes R_4 \subseteq \mathcal{C}^{\perp}$ and let $\mathbf{c}$ be a codeword in $\mathcal{C}$ with array $A_{\mathbf{c}}$. For each i, $1 \leq i \leq m$, there is a unique word $\mathbf{w}_i$ in $I_m \otimes R_4$ whose array $A_{\mathbf{w}_i}$ has four nonzero entries in its ith column and is zero elsewhere. Thus $\mathbf{w}_i \cdot \mathbf{c} = 0$, implying that the ith column of $A_{\mathbf{c}}$ has even parity. ■

Lemma 3 Given a linear binary code $\mathcal{C}$ of length $4m$, the parity of the first row of all $A_{\mathbf{c}}$, $\mathbf{c} \in \mathcal{C}$, is even if and only if the vector $\mathbf{f}_e := 1000\ 1000 \cdots 1000$, the nonzero vector of $[m, 1, m] \otimes [1000]$, is in $\mathcal{C}^{\perp}$.

Proof The first row of $A_{\mathbf{f}_e}$ is the nonzero codeword of the repetition code $R_m = [m, 1, m]$, and so $\mathbf{f}_e \cdot \mathbf{c} = 0$ if and only if the all-one vector of length m is orthogonal to the first row of $A_{\mathbf{c}}$, that is if and only if the parity of the first row of $A_{\mathbf{c}}$ is even. ■

Proposition 1 A linear binary code $\mathcal{C} \subseteq F_2^{4m}$ has projection SE onto $\mathrm{Proj}(\mathcal{C})$ if and only if $I_m \otimes R_4 + R_m \otimes [1000] \subseteq \mathcal{C}^{\perp}$.

Proof By definition, $\mathcal{C}$ has projection SE onto $\mathrm{Proj}(\mathcal{C})$ if and only if all codewords in $\mathcal{C}$ are even, that is the first row and the columns of any array $A_{\mathbf{c}}$, $\mathbf{c} \in \mathcal{C}$, have even parity. Thus the result follows from Lemma 2 and Lemma 3. ■

Proposition 2 A linear binary code $\mathcal{C} \subseteq F_2^{4m}$ has projection E onto Proj($\mathcal{C}$) if and only if $E_m \otimes R_4 + R_m \otimes [1000] \subseteq \mathcal{C}^\perp$; in particular a self-dual code $\mathcal{C}$ has projection E onto Proj($\mathcal{C}$) if and only if $E_m \otimes R_4 + R_m \otimes [1000] \subseteq \mathcal{C}$.

Proof By definition, $\mathcal{C}$ has projection E onto Proj($\mathcal{C}$) if and only if any codeword $\mathbf{c} \in \mathcal{C}$ is either even or weakly-odd, that is $\mathcal{C}$ is column-uniform and the first row of any $\mathbf{c} \in \mathcal{C}$ is always even. Therefore, the result follows from Lemma 1 and Lemma 3.■

Example 1 (BCH codes) The extended $[32, 16, 8]$ BCH code with generator matrix (1) is self-dual and contains $E_8 \otimes R_4 + R_8 \otimes [1000]$ (the first eight rows of M'), implying that it has projection E. The extended $[32, 11, 12]$ BCH code, with generator matrix $M_{32.11.12}$ given below, is the intersection of the $[32, 16, 8]$ BCH and $[32, 16, 8]$ QR codes. Therefore, it has projection E as its dual, a $[32, 21, 6]$ code, contains the $[32, 16, 8]$ BCH code and hence includes $E_8 \otimes R_4 + R_8 \otimes [1000]$.

$$M_{32.11.12} = \begin{bmatrix}
1111 & 0000 & 1111 & 1111 & 1111 & 0000 & 0000 & 0000 \\
0000 & 1111 & 0000 & 1111 & 1111 & 1111 & 0000 & 0000 \\
0000 & 0000 & 1111 & 0000 & 1111 & 1111 & 1111 & 0000 \\
0000 & 0000 & 0000 & 1111 & 1111 & 0000 & 1111 & 1111 \\
0110 & 1111 & 1100 & 0110 & 0101 & 0000 & 0000 & 0000 \\
0011 & 1100 & 0101 & 1001 & 0101 & 0110 & 0000 & 0000 \\
0000 & 0110 & 1001 & 1100 & 1010 & 0011 & 1100 & 0000 \\
0000 & 0011 & 1100 & 1001 & 0000 & 1010 & 0011 & 1100 \\
0000 & 0000 & 0101 & 1111 & 1001 & 0101 & 0110 & 0000 \\
0000 & 0000 & 0000 & 0101 & 0011 & 1111 & 0011 & 1010 \\
0001 & 1101 & 1000 & 1000 & 0010 & 0111 & 0010 & 1000
\end{bmatrix}$$

Consider the vector $\mathbf{f}_o := 1000\ 1000 \cdots 0111$ of length $4m$ and weight $m+2$. It can be shown that a linear binary code $\mathcal{C} \subseteq F_2^{4m}$ has projection O onto Proj($\mathcal{C}$) if and only if $E_m \otimes R_4 + \mathbf{f}_o \subseteq \mathcal{C}^\perp$ and $\mathbf{f}_e \notin \mathcal{C}^\perp$. From the code construction perspective, however, this criteria is not very useful and hence we prefer the following characterisation for the class of odd codes.

Proposition 3 A linear binary code $\mathcal{C} \subseteq F_2^{4m}$ has projection O onto Proj($\mathcal{C}$) if and only if $\mathcal{C} = \mathcal{C}' + \mathbf{w}$ for some odd vector $\mathbf{w}$ and a linear code $\mathcal{C}'$ that has projection SE.

Proof The sum of two even (odd) words is even while the sum of an odd word with an even word is odd. This together with the fact that a linear code $\mathcal{C}$ having projection O contains at least one odd codeword completes the proof. ■

Corollary 2 It follows from Proposition 1 that the minimum distance of a self-dual code $\mathcal{C}$ with projection SE satisfies $\mathrm{d}(\mathcal{C}) \leq \{m, 4\}$. Proposition 2 implies that a self-dual code $\mathcal{C}$ with projection E satisfies $\mathrm{d}(\mathcal{C}) \leq \{m, 8\}$. Based on the results in the paragraph preceding Proposition 3, for a self-dual code $\mathcal{C}$ with projection O, we have $\mathrm{d}(\mathcal{C}) \leq \{8, m+2\}$.

The last two statements of this corollary were already known (the first part of Proposition 4.3 in [7]). Note however that based on our approach, these bounds hold only for self-dual projectable codes, while they apply to all codes considered in [7]. Our approach allows one to construct codes with arbitrarily large d (which would necessarily differ from the codes in [7] if $d > 8$).

The $[32, 11, 12]$ BCH code considered in Example 1 is an instance of a code that has projection E and minimum distance larger than 8. In fact, the approach presented in this paper allows one to construct projectable codes with arbitrary large minimum distance.

Example 2 (Binary Golay codes) Consider the $[24, 12, 8]$ Golay code g_{24} with generator matrix

$$\begin{bmatrix}
1111 & 1111 & 0000 & 0000 & 0000 & 0000 \\
0000 & 1111 & 1111 & 0000 & 0000 & 0000 \\
0000 & 0000 & 1111 & 1111 & 0000 & 0000 \\
0000 & 0000 & 0000 & 1111 & 1111 & 0000 \\
0000 & 0000 & 0000 & 0000 & 1111 & 1111 \\
1100 & 0000 & 0000 & 1100 & 1010 & 1010 \\
0000 & 1100 & 0000 & 1010 & 1100 & 1010 \\
0000 & 0000 & 1100 & 1010 & 1010 & 1100 \\
1010 & 0000 & 0000 & 1010 & 1001 & 1001 \\
0000 & 1010 & 0000 & 1001 & 1010 & 1001 \\
0000 & 0000 & 1010 & 1001 & 1001 & 1010 \\
0111 & 1000 & 1000 & 1000 & 1000 & 1000
\end{bmatrix}$$

As mentioned previously, this code has projection O onto the $[6, 3, 4]$ hexacode. This can be easily verified by examining the rows of the matrix. Removing the last row of the matrix (the only odd row), we obtain a generator for the $[24, 11, 8]$ half-Golay code h_{24}. All codewords of h_{24} are even and hence h_{24} has projection SE onto the hexacode. If the last row of the above matrix is replaced by the weakly-odd word 100010001000100010001000, we obtain the $[24, 12, 6]$ Type I code, known as the odd Golay code h_{24}^+. This is a self-dual code containing $E_6 \otimes R_4 + R_6 \otimes [1000]$, implying that h_{24}^+ has projection E onto the hexacode.

According to Proposition 1, if a code $\mathcal{B}$ includes $I_m \otimes R_4 + R_m \otimes [1000]$ then the dual code $\mathcal{B}^\perp$ has projection SE, and any code with projection SE can be constructed in this way. Thus the largest and smallest codes that have projection SE are $\{I_m \otimes R_4 + R_m \otimes [1000]\}^\perp$ and the trivial code $\mathbf{0}$, respectively.

Note that $I_m \otimes R_4 + R_m \otimes [1000]$ is of length $4m$ and dimension $m+1$, and hence an immediate consequence of this result is that the number of even words in F_2^{4m} is 2^{3m-1}, which is the number of codewords in $\{I_m \otimes R_4 + R_m \otimes [1000]\}^\perp$.

As the sum of two odd or two even words is even, and the sum of an odd word with an even word is odd, it follows that the number of odd words in

F_2^{4m} is also 2^{3m-1}. Similarly, it follows from Proposition 2 that the dual of any code $\mathcal{B}$ containing $E_m \otimes R_4 + R_m \otimes [1000]$ has projection E, and any code having projection E can be obtained in this way. Therefore, the largest and smallest codes that have projection E are $\{E_m \otimes R_4 + R_m \otimes [1000]\}^{\perp}$ and the trivial code **0**, respectively. The code $E_m \otimes R_4 + R_m \otimes [1000]$ has length $4m$ and dimension m, and hence the dual code $\{E_m \otimes R_4 + R_m \otimes [1000]\}^{\perp}$ consists of 2^{3m} codewords. This implies that the number of weakly-odd words in F_2^{4m} is $2^{3m} - 2^{3m-1} = 2^{3m-1}$. Therefore we have the following corollary.

Corollary 3 The number of odd, even, and weakly-even vectors in the vector space F_2^{4m} are the same and equal to 2^{3m-1}.

3 Reed-Muller Codes and the [32, 16, 8] Quadrati Residue Code

3.1 Reed-Muller codes

Let $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ be two n-tuples. The Boolean product of $\mathbf{a}$ and $\mathbf{b}$ is defined as $\mathbf{ab} := (a_1 b_1, \ldots, a_n b_n)$. The product of i n-tuples is referred to as a Boolean product of degree i. Given a positive integer m, consider the 2^m – tuples $\mathbf{v}_0$, $\mathbf{v}_1$, ..., and $\mathbf{v}_m$ such that $\mathbf{v}_0$ has Hamming weight 2^m, and $\mathbf{v}_i$, $1 \leq i \leq m$, is the concatenation of 2^{m-i} identical blocks of length 2^i, each of which is divided into 2 sub-blocks of length 2^{i-1} such that the first sub-block is the string of all ones, and the second sub-block is the string of all zeros.

Let $0 \leq r \leq m$, and S be the set consisting of $\mathbf{v}_0$ and all the Boolean products of the elements of $D = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$ up to degree r. The subspace of $F_2^{2^m}$, generated by S is defined as the r^{th} order Reed-Muller (RM) code of length 2^m, and is denoted by $\mathcal{R}(r, m)$. The set S is a linearly independent set of vectors. Therefore, $\mathcal{R}(r, m)$ is a $[2^m, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r}]$ code with a generator matrix G_m^r whose rows are precisely the elements of S. For example, $\mathcal{R}(2, 4)$, has the following generator matrix

$$G_4^2 = \left[\begin{array}{c} \mathbf{v}_0 \\ \mathbf{v}_4 \\ \mathbf{v}_3 \\ \mathbf{v}_2 \\ \mathbf{v}_1 \\ \hline \mathbf{v}_4\mathbf{v}_3 \\ \mathbf{v}_4\mathbf{v}_2 \\ \mathbf{v}_4\mathbf{v}_1 \\ \mathbf{v}_3\mathbf{v}_2 \\ \mathbf{v}_3\mathbf{v}_1 \\ \mathbf{v}_2\mathbf{v}_1 \end{array}\right] = \left[\begin{array}{cccc} 1111 & 1111 & 1111 & 1111 \\ 1111 & 1111 & 0000 & 0000 \\ 1111 & 0000 & 1111 & 0000 \\ 1100 & 1100 & 1100 & 1100 \\ 1010 & 1010 & 1010 & 1010 \\ \hline 1111 & 0000 & 0000 & 0000 \\ 1100 & 1100 & 0000 & 0000 \\ 1010 & 1010 & 0000 & 0000 \\ 1100 & 0000 & 1100 & 0000 \\ 1010 & 0000 & 1010 & 0000 \\ 1000 & 1000 & 1000 & 1000 \end{array}\right].$$

The first five rows of this matrix represent the first-order RM code $\mathcal{R}(1, 4)$.

Thus $\mathcal{R}(1,4)$ has projection SE onto the additive code $\begin{bmatrix} 1 & 1 & 1 & 1 \\ \omega & \omega & \omega & \omega \end{bmatrix}$. In fact, the first-order RM code $\mathcal{R}(1,m)$ has projection SE onto the additive code $R_m \otimes \begin{bmatrix} 1 \\ \omega \end{bmatrix}$ [1].

The generator matrix G_4^2 shows that $\mathcal{R}(2,4)$ has projection E onto $\mathcal{R}(1,2) + \omega\mathcal{R}(1,2)$. Examining the generator matrix of $\mathcal{R}(2,m)$, it is clear that for any m this code has projection E onto $\mathcal{R}(1,m-2) + \omega\mathcal{R}(1,m-2)$.

The code $\mathcal{R}(r,m)$ has projection E if and only if the dual code $\mathcal{R}(r,m)^{\perp} = \mathcal{R}(m-r-1,m)$ contains $E_m \otimes R_4 + R_m \otimes [1000]$. Obviously, for any $t \geq 2$, the code $\mathcal{R}(t,m)$ includes $R_m \otimes [1000] = \mathbf{v}_1\mathbf{v}_2$. On the other hand, it follows from $\sum_{i=0}^{m-3} \binom{m-2}{i} = 2^{m-2} - 1$ that the smallest integer t for which $\mathcal{R}(t,m)$ contains $E_m \otimes R_4$ is $m-3$. Setting $m-3 = m-r-1$, we conclude that only the second-order RM codes and their subcodes have projection E.

3.2 The $[32,16,8]$ quadratic residue code

It is known that out of five Type II $[32,16,8]$ codes, exactly three codes $2g_{16}$, $8f_4$, and r_{32} have projection E, and hence the quadratic residue (QR) code q_{32} does not have this property [7]. In this section we show that q_{32} contains a 14-dimensional subcode having projection E and therefore it may be referred to as a code with
semi-E projection.

Proposition 4 The $[32,16,8]$ QR code contains a 14-dimensional subcode with projection E.

Proof A generator matrix for the uniformly efficient permutation of the $[32,16,8]$ QR code in [2] is given by

$$M = \begin{matrix}
11111111000000000000000000000000 \\
11100010111100000000000000000000 \\
10111000110011000000000000000000 \\
10100110010010110000000000000000 \\
00000000000000000000000011111111 \\
00000000000000000000111101010101 \\
00000000000000000011001101110010 \\
00000000000000001101011100000110 \\
00011110111000100101000001000001 \\
01100110010000000000010001000010 \\
00100010011000100001000001000100 \\
10001000100010000001010001001000 \\
00111100010000100000000001010000 \\
11100010011010100100010001100000 \\
01100000011000000101010100000000 \\
00110000100010000101011000000000
\end{matrix}$$

Applying the following permutation π and a few elementary row operations to this matrix, we obtain the matrix $M_{q_{32}}$ given below.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 2 & 3 & 4 & 8 & 6 & 7 & 1 & 5 & 9 & 11 & 10 & 12 & 13 & 15 & 14 & 16 \\ \hline 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 & 32 \\ 18 & 20 & 17 & 19 & 21 & 23 & 22 & 24 & 30 & 26 & 31 & 28 & 32 & 25 & 29 & 27 \end{pmatrix},$$

$$M_{q_{32}} = \begin{bmatrix} M_5 \\ M_9 \\ M_2 \end{bmatrix} = \left[\begin{array}{cccccccc} 1111 & 1111 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\ 0000 & 1111 & 1111 & 0000 & 0000 & 0000 & 0000 & 0000 \\ 0000 & 0000 & 1111 & 1111 & 1111 & 1111 & 0000 & 0000 \\ 0000 & 0000 & 0000 & 0000 & 0000 & 1111 & 1111 & 0000 \\ 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 1111 & 1111 \\ \hline 0111 & 0111 & 0111 & 0111 & 0111 & 0111 & 0111 & 0111 \\ 1010 & 1010 & 1010 & 1010 & 0000 & 0000 & 0000 & 0000 \\ 0000 & 0000 & 0000 & 0000 & 1010 & 1010 & 1010 & 1010 \\ 0110 & 1001 & 0000 & 1111 & 0011 & 0110 & 0000 & 0000 \\ 0000 & 0110 & 0101 & 0110 & 0101 & 1100 & 1100 & 0000 \\ 0000 & 0011 & 1010 & 1100 & 0101 & 0000 & 0000 & 0000 \\ 0000 & 0000 & 1001 & 1001 & 0101 & 0101 & 0000 & 0000 \\ 0000 & 0000 & 0011 & 0011 & 1001 & 1100 & 0110 & 0011 \\ 0000 & 0000 & 0000 & 0101 & 1001 & 1010 & 0110 & 0000 \\ \hline 0000 & 0000 & 0011 & 1101 & 0100 & 1010 & 0000 & 0000 \\ 0000 & 0000 & 0000 & 0000 & 0111 & 0111 & 0111 & 0111 \end{array}\right].$$

By inspection one can easily verify that among the first 14 rows of $M_{q_{32}}$, the sixth row is weakly-odd and the rest are even, and hence q_{32} contains a 14-dimensional subcode with projection E onto the $(8, 2^8, 4)$ quaternary additive code $\mathcal{C}_4(q_{32})$ with generator matrix

$$M_4 = \begin{bmatrix} \omega & \omega & \omega & \omega & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega & \omega & \omega & \omega \\ \bar{\omega} & \bar{\omega} & 0 & 0 & \bar{\omega} & \bar{\omega} & 0 & 0 \\ 0 & \bar{\omega} & \omega & \bar{\omega} & \omega & 1 & 1 & 0 \\ 0 & 1 & \omega & 1 & \omega & 0 & 0 & 0 \\ 0 & 0 & \bar{\omega} & \bar{\omega} & \omega & \omega & 0 & 0 \\ 0 & 0 & 1 & 1 & \bar{\omega} & 1 & \bar{\omega} & 1 \\ 0 & 0 & 0 & \omega & \bar{\omega} & \omega & \bar{\omega} & 0 \end{bmatrix}. \tag{2}$$

Note that under the mapping Proj, the last row in $M_{q_{32}}$ is projected onto $\mathbf{0} \in F_4^8$, and hence a 15-dimensional subcode of q_{32} is projected onto $\mathcal{C}_4(q_{32})$. This projection, however, is not one of the three projections SE, E and O, as the last row of $M_{q_{32}}$ is not column-uniform. ■

Consider $\mathbf{r}_{14} + \mathbf{r}_{15}$, the sum of the 14th and 15th rows of $M_{q_{32}}$. The quaternary vector $\mathrm{Proj}(\mathbf{r}_{14} + \mathbf{r}_{15})$ has Hamming weight 3. Therefore, by the mapping Proj, this presentation of q_{32} is projected onto an additive $(8, 2^9, 3)$ quaternary code and the mapping has a 7-dimensional kernel with basis consisting of the first six plus the last rows of matrix $M_{q_{32}}$. Note that this is just one dimension less than the kernel of the three Type II $[32, 16, 8]$ codes, including the BCH code introduced by (1), that have projection E [7]. From perspective of the size of the kernel of Proj, to the best of our knowledge, this presentation of q_{32} is better than any given in the literature. We conjecture that, under the mapping Proj, the kernel of any representation of q_{32} has dimension at most 7.

References

[1] O. Amrani and Y. Be'ery, "Reed-Muller codes: Projections on GF(4) and multilevel construction," *IEEE Trans. Inform. Theory*, vol. 47, no. 6, pp. 2560–2565, Sept. 2001.

[2] H. Chen and J.T. Coffey,"Trellis structure and higher weights of extremal self-dual codes," *Designs, Codes and Crypt.*, vol. 24, no. 1, pp. 15–36, 2001.

[3] J.H. Conway and N.J.A. Sloane, "Soft Decoding techniques for codes and lattices, including the Golay code and the Leech lattice," *IEEE Trans. Inform. Theory*, vol. 32, no. 1, pp. 41–50, Jan. 1986.

[4] M. Esmaeili, T.A. Gulliver and A.K. Khandani, "On the Pless-construction and ML Decoding of the (48,24,12) quadratic residue code," *IEEE Trans. Inform. Theory*, vol. 49, no. 6, pp. 1527–1535, June 2003.

[5] M. Esmaeili and A.K. Khandani, "Acyclic Tanner graphs and maximum-likelihood decoding of linear block codes," *IEE Proc. Commun.*, vol. 147, no. 6, pp. 322–332, Dec. 2000.

[6] P. Gaborit, J.-L. Kim and V. Pless , "Decoding binary R(2,5) by hand," *Discrete Math.* vol. 264, pp. 55–73, Mar. 2003.

[7] J.-L. Kim, K.E. Mellinger and V. Pless, "Projections of binary linear block codes onto larger fields," *SIAM J. Discrete Math.*, vol. 16, no. 4, pp. 591–603, 2003.

[8] V. Pless,"Decoding the Golay codes," *IEEE Trans. Inform. Theory*, vol. 32, no. 4, pp. 561–567, July 1986.

[9] M. Ran and J. Snyders, "Constrained designs for maximum likelihood soft decoding of RM(2,m) and the extended Golay codes," *IEEE Trans. Commun.*, vol. 43, no. 2/3/4, pp. 812–820, Feb./Mar./Apr. 1995.

[10] A. Vardy and Y. Be'ery, "More efficient soft decoding of the Golay codes," *IEEE Trans. Inform. Theory*, vol. 37, no. 3, pp. 667–672, May 1991.