SIAM J. DISCRETE MATH.
Vol. 16, No. 4, pp. 591–603

PROJECTIONS OF BINARY LINEAR CODES ONTO LARGER FIELDS*

JON-LARK KIM†, KEITH E. MELLINGER‡, AND VERA PLESS§

Abstract. We study certain projections of binary linear codes onto larger fields. These projections include the well-known projection of the extended Golay $[24, 12, 8]$ code onto the hexacode over GF(4) and the projection of the Reed–Muller code $R(2, 5)$ onto the unique self-dual $[8, 4, 4]$ code over GF(4). We give a characterization of these projections, and we construct several binary linear codes which have best known optimal parameters, for instance, $[20, 11, 5]$, $[40, 22, 8]$, $[48, 21, 12]$, and $[72, 31, 16]$. We also relate the automorphism group of a quaternary code to that of the corresponding binary code.

Key words. additive codes, projection onto larger fields

AMS subject classification. 94B35

DOI. 10.1137/S0895480102404367

1. Introduction.

The construction of good binary (linear) codes from shorter codes has been widely studied by coding theorists. One of the main reasons in this direction is to lower the decoding complexity of the original code. The $(u|u + v)$ construction [17], the projection of Z_4-linear codes onto nonlinear binary codes [14], and the projection of codes over $\mathrm{GF}(p^m)$ onto codes over $\mathrm{GF}(p)$ are such examples. Each of these constructions applies to a large class of binary codes.

We recall a projection construction that is quite different from those mentioned above. In the mid 1980s the third author [18] showed that the Golay code of length 24 (as well as the ternary Golay code of length 12) can be easily constructed from the Hexacode of length 6 over GF(4) (resp., the tetracode of length 4 over GF(3)). It was expected [18, p. 565] that one can construct, in a somewhat analogous fashion, good large binary codes whose decoding can be reduced, in part, to the decoding of a good quaternary code. However, only a few codes had the above type of projection construction.

Recently Gaborit, Kim, and Pless [12, 16] showed that the three singly even self-dual binary $[32, 16, 8]$ codes and three of the five doubly even self-dual $[32, 16, 8]$ codes have a similar projection. The construction of Amrani and Be'ery [1] of binary Reed–Muller codes is also an interesting generalization of a projection. These projections regard a binary linear code of length $4m$ as a set of $4 \times m$ arrays and then *project* these arrays onto a quaternary code of length m. A projection onto GF(16) was suggested by Esmaeili, Gulliver, and Khandani [10] to investigate whether the $[48, 24, 12]$ quadratic residue code has such a projection.

The purpose of our paper is to give a uniform characterization of these projections. We provide many examples of binary linear codes having these projections. In particular, we construct several binary linear codes that have best known optimal

*Received by the editors March 22, 2002; accepted for publication (in revised form) February 17, 2003; published electronically July 30, 2003.
http://www.siam.org/journals/sidma/16-4/40436.html

†Department of Mathematics and Statistics, University of Nebraska-Lincoln, Lincoln, NE 68588-0323 (jlkim@math.unl.edu).
‡Department of Mathematics, Mary Washington College, Fredericksburg, VA 22401 (kmelling@mwc.edu).
§Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago, Chicago, IL 60607-7045 (pless@math.uic.edu).

parameters, for instance, $[20, 11, 5], [40, 22, 8], [48, 21, 12]$, and $[72, 31, 16]$. We also relate the automorphism group of a quaternary code to that of the corresponding binary code. Sections 2 and 3 survey the basic facts about projections onto GF(4) and additive codes over GF(4). In section 4 we characterize which binary linear codes have a projection onto GF(4). In section 5 we apply results of section 4 to extremal binary self-dual codes, and section 6 discusses a projection onto GF(16). Finally, in section 7 we construct two codes having the best known parameters $[48, 21, 12]$ and $[72, 31, 16]$.

2. Projection. We begin with the projection of binary linear codes into quaternary codes (i.e., codes over GF(4)) as explained in [18]. Consider a $4 \times m$ array with zeros and ones in it. Label the four rows with the elements of GF(4): $0, 1, \omega, \overline{\omega}$. 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 obtain an element of GF(4). In this way we have a correspondence between binary vectors of length $4m$ and quaternary vectors of length m. 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 $\mathbf{w} = (1, 0, \overline{\omega}, 1, \omega, 1, \omega, \overline{\omega})$ of length 8. We denote this projection by $\text{Proj}(\mathbf{v}) = \mathbf{w}$. The columns of such an array associated with vector $\mathbf{v}$ will be referred to as the *columns of* $\mathbf{v}$ and the top row of the array will be referred to as the *top row of* $\mathbf{v}$. Note that Proj is a GF(2)-linear map from the set of binary vectors of length $4m$ to the set of quaternary vectors of length m.

Let the *parity of a column* be either even or odd, respectively, if an even or an odd number of ones exists 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 also has even parity. By a quaternary additive code $\mathcal{C}_4$ of length m we mean a set of vectors in $\text{GF}(4)^m$ that is closed under addition.

DEFINITION 2.1. *Let S be a set of binary vectors of length $4m$ and $\mathcal{C}_4$ a quaternary additive code of length m. Then S is said to have* projection O onto $\mathcal{C}_4$ *if the following conditions are satisfied:*

(P1) *For any vector $\mathbf{v} \in S$, Proj$(\mathbf{v}) \in \mathcal{C}_4$. Conversely, for any vector $\mathbf{w} \in \mathcal{C}_4$, all vectors $\mathbf{v}$ such that Proj$(\mathbf{v}) = \mathbf{w}$ are in S.*

(P2) *The columns of the array of any vector of S are either all even or all odd.*

(P3) *The parity of the top row of the array of any vector of S is the same as the column parity of the array.*

It is easy to see that the above set S is in fact a binary linear code of length $4m$. It is well known [18] that the extended Golay $[24, 12, 8]$ code has projection O onto the $[6, 3, 4]$ Hexacode. The main advantage of this projection is its ability to decode a binary code by decoding the projected code. Generally this lowers the decoding complexity. Hard decision decoding by hand using this projection was done in [18] and soft decision decoding was done by several authors [7, 21, 22, 23].

The Reed–Muller $[32, 16, 8]$ code $R(2, 5)$ has a similar projection [12]. We define such a projection, called projection E, as follows.

DEFINITION 2.2. *Using the same notation as Definition* 2.1*, S is said to have* projection E onto $\mathcal{C}_4$ *if conditions* (P1) *and* (P2)*, as well as the following third condition* (P3′)*, are satisfied:*

(P3′) *The parity of the top row of the array of any vector of S is always even.*

3. Introduction to additive codes over GF(4). In this section we give some basic definitions and preliminaries related to additive codes, and we refer the reader to [4, 11] for more details. As before, an *additive code $\mathcal{C}_4$ over $GF(4)$ of length n* is an additive subgroup of $\mathrm{GF}(4)^n$. As $\mathcal{C}_4$ is a free GF(2)-module, it has size 2^k for some $0 \le k \le 2n$. We call $\mathcal{C}_4$ an $(n, 2^k)$ code. It has a basis, as a GF(2)-module, consisting of k basis vectors; a *generator matrix* of $\mathcal{C}_4$ will be a $k \times n$ matrix with entries in GF(4) whose rows form a basis of $\mathcal{C}_4$. Interest in additive codes over GF(4) has arisen because of their correspondence to quantum codes, as described in [4]. There is a natural inner product arising from the trace map. If we let $\mathrm{GF}(4) = \{0, 1, \omega, \overline{\omega}\}$, where $\overline{\omega} = \omega^2 = 1 + \omega$, the *trace* map $\mathrm{Tr} : \mathrm{GF}(4) \to \mathrm{GF}(2)$ is given by

$$\mathrm{Tr}(x) = x + x^2.$$

In particular $\mathrm{Tr}(0) = \mathrm{Tr}(1) = 0$ and $\mathrm{Tr}(\omega) = \mathrm{Tr}(\overline{\omega}) = 1$. The *conjugate* of $x \in \mathrm{GF}(4)$, denoted $\overline{x}$, is the image of x under the Frobenius automorphism; hence, $\overline{0} = 0$, $\overline{1} = 1$, and $\overline{\overline{\omega}} = \omega$. 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 $\mathrm{GF}(4)^n$ to be

$$\mathbf{x} \star \mathbf{y} = \sum_{i=1}^{n} \mathrm{Tr}(x_i \overline{y_i}).$$

Example 3.1. Let $\mathcal{G}_6$ be the $[6, 3, 4]$ *hexacode* whose generator matrix as a linear GF(4)-code is

$$\begin{bmatrix} 1 & 0 & 0 & 1 & \omega & \omega \\ 0 & 1 & 0 & \omega & 1 & \omega \\ 0 & 0 & 1 & \omega & \omega & 1 \end{bmatrix}.$$

This is also an additive $(6, 2^6, 4)$ code; thinking of $\mathcal{G}_6$ as an additive code, we see that it has generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 & \omega & \omega \\ \omega & 0 & 0 & \omega & \overline{\omega} & \overline{\omega} \\ 0 & 1 & 0 & \omega & 1 & \omega \\ 0 & \omega & 0 & \overline{\omega} & \omega & \overline{\omega} \\ 0 & 0 & 1 & \omega & \omega & 1 \\ 0 & 0 & \omega & \overline{\omega} & \overline{\omega} & \omega \end{bmatrix}.$$

If $\mathcal{C}_4$ is an additive code, its *dual*, denoted $\mathcal{C}_4^{\perp}$, is the additive code $\{\mathbf{x} \in \mathrm{GF}(4)^n \mid \mathbf{x} \star \mathbf{c} = 0 \text{ for all } \mathbf{c} \in \mathcal{C}_4\}$. If $\mathcal{C}_4$ is an $(n, 2^k)$ code, then $\mathcal{C}_4^{\perp}$ is an $(n, 2^{2n-k})$ code. As usual, $\mathcal{C}_4$ is *self-orthogonal* if $\mathcal{C}_4 \subseteq \mathcal{C}_4^{\perp}$ and *self-dual* if $\mathcal{C}_4 = \mathcal{C}_4^{\perp}$. In particular, if $\mathcal{C}_4$ is self-dual, $\mathcal{C}_4$ is an $(n, 2^n)$ code. The code $\mathcal{G}_6$ in Example 3.1 is self-dual as an additive code. (Any GF(4)-linear code that is self-orthogonal under the Hermitian inner product is a self-orthogonal additive code under the trace inner product.)

As usual, the *weight* $\mathrm{wt}(\mathbf{c})$ of $\mathbf{c} \in \mathcal{C}_4$ is the number of nonzero components of $\mathbf{c}$. The minimum weight d of $\mathcal{C}_4$ is the smallest weight of any nonzero codeword in $\mathcal{C}_4$. If $\mathcal{C}_4$ is an $(n, 2^k)$ additive code of minimum weight d, $\mathcal{C}_4$ is called an $(n, 2^k, d)$ code. We say $\mathcal{C}_4$ is *Type II* if $\mathcal{C}_4$ is self-dual and all codewords have even weight. It can be shown that Type II codes of length n exist if and only if n is even [11]. If $\mathcal{C}_4$ is self-dual but some codeword has odd weight (in which case the code cannot be GF(4) linear), we say the code is *Type I* (see [20, section 4.2]). There exists a bound on the minimum weight of an additive self-dual code [20, Theorem 33]. If d_I and d_{II} are the minimum distances of additive self-dual Type I and Type II codes, respectively, of length $n > 1$, then

$$d_I \leq \begin{cases} 2\left\lfloor \frac{n}{6} \right\rfloor + 1 & \text{if } n \equiv 0 \pmod 6, \\ 2\left\lfloor \frac{n}{6} \right\rfloor + 3 & \text{if } n \equiv 5 \pmod 6, \\ 2\left\lfloor \frac{n}{6} \right\rfloor + 2 & \text{otherwise,} \end{cases} \tag{3.1}$$

$$d_{II} \leq 2\left\lfloor \frac{n}{6} \right\rfloor + 2. \tag{3.2}$$

A code that meets the appropriate bound is called *extremal*. Note that (3.2) is the same as saying that $d = 2m + 2$ if $n = 6m + 2(i - 1)$, with $i = 1, 2$, or 3. Type II codes meeting the bound d_{II} have a unique weight enumerator. This property is not true for Type I extremal codes. A self-dual (with respect to the Hermitian inner product) linear code over GF(4) also satisfies bound (3.2), and an extremal code is a $[6m, 3m, 2m + 2]$ code.

We say that two additive codes $\mathcal{C}_4$ and $\mathcal{C}_4'$ are *equivalent* provided there is a map sending the codewords of $\mathcal{C}_4$ onto the codewords of $\mathcal{C}_4'$, where the map consists of a permutation of coordinates, followed by a scaling of coordinates by elements of GF(4), possibly followed by conjugation of some of the coordinates. Notice that permuting coordinates, scaling coordinates, and conjugating some coordinates of a self-orthogonal (or self-dual) code do not change self-orthogonality (or self-duality). The *automorphism group* of $\mathcal{C}_4$, denoted $\mathrm{Aut}(\mathcal{C}_4)$, consists of all bijections on codewords in $\mathcal{C}_4$ to codewords in $\mathcal{C}_4$, which permute coordinates, scale coordinates, and conjugate coordinates.

4. Projection of binary linear codes onto GF(4). In this section we characterize binary linear codes of length $4m$ having projection O or projection E onto GF(4). We let $\mathcal{C}$ (resp., $\mathcal{C}'$) be the set of binary vectors satisfying (P2) and (P3) (resp., (P2) and (P3′)). A standard counting argument shows that $\mathcal{C}$ (resp., $\mathcal{C}'$) is a linear $[4m, 3m]$ code. If we look at all the vectors in $\mathcal{C}$ that project to the zero vector, we obtain a subcode of $\mathcal{C}$, which we denote $\mathcal{D}$. The subcode $\mathcal{D}$ is generated by all even sums of weight 4 vectors, all of whose ones appear in the same column together with the one additional vector $f_1 = (1000\ 1000\ \cdots\ 1000\ 1000)$ if m is odd, or $f_2 = (1000\ 1000\ \cdots\ 1000\ 0111)$ if m is even. Similarly $\mathcal{C}'$ has such a subcode $\mathcal{D}$, which contains f_1 when m is even and contains f_2 when m is odd. A counting argument again shows that $\mathcal{D}$ has dimension m.

LEMMA 4.1. *Let $\mathcal{D}$ and $\mathcal{C}$ ($\mathcal{C}'$) be defined as above. Let $\mathbf{v}_1$ and $\mathbf{v}_2$ be two vectors in $\mathcal{C}$ (resp., $\mathcal{C}'$) such that $\mathbf{v}_1 \not\equiv \mathbf{v}_2 \pmod{\mathcal{D}}$. Then $Proj(\mathbf{v}_1) \neq Proj(\mathbf{v}_2)$.*

It easily follows that there is a one-to-one correspondence between the cosets of $\mathcal{D}$ in $\mathcal{C}$ ($\mathcal{C}'$) and $\mathrm{GF}(4)^m$ given by $\mathrm{Proj}(\mathbf{v} + \mathcal{D}) = \mathrm{Proj}(\mathbf{v})$.

LEMMA 4.2. *Let $\mathcal{C}_2$ be a binary linear subcode of $\mathcal{C}$ that also contains the subcode $\mathcal{D}$. Suppose that there are r linearly independent vectors $\mathbf{v}_{m+1}, \ldots, \mathbf{v}_{m+r}$ in $\mathcal{C}_2$ such that any nontrivial linear combination of them is not in $\mathcal{D}$. Then $Proj(\mathbf{v}_{m+1}), \ldots, Proj(\mathbf{v}_{m+r})$ are linearly independent over $GF(2)$.*

We can now give a characterization of a binary linear code $\mathcal{C}_2$ of length $4m$ that has either projection O or projection E onto an additive code over GF(4). The following results are easy to prove and will be used in future arguments.

PROPOSITION 4.3. *Let $\mathcal{C}_2$ be a binary linear $[4m, k, d]$ code with projection O (or projection E) onto an additive code $\mathcal{C}_4$ over $GF(4)$. Then*

1. *$d \leq d(\mathcal{D}) \leq 8$, where $d(\mathcal{D})$ is the minimum weight of $\mathcal{D}$, and $\mathcal{C}_4$ has dimension $r = k - m \geq 0$ over $GF(2)$;*
2. *there exist $(k-m)$ linearly independent vectors $\mathbf{v}_{m+1}, \ldots, \mathbf{v}_{m+(k-m)} = \mathbf{v}_k$ of $\mathcal{C}_2$ whose projection forms a basis for $\mathcal{C}_4$ as an additive code;*
3. *the vectors in part 2 above can be chosen so that $wt(\mathbf{v}_i) = 2wt(Proj(\mathbf{v}_i))$ for $i = m+1, \ldots, k$, and $wt(\mathbf{v}_i \cap \mathbf{v}_j) \equiv Proj(\mathbf{v}_i) \star Proj(\mathbf{v}_j) \pmod 2$ for $m+1 \leq i, j \leq k, i \neq j$.*

Proof. We prove only the projection O case. Clearly $d \leq d(\mathcal{D}) \leq 8$, as $\mathcal{D}$ is a subcode of $\mathcal{C}_2$. Since $\mathcal{C}_2$ has dimension k and $\mathcal{D}$ has dimension m, we know there exist $k - m$ linearly independent vectors $\mathbf{v}_{m+1}, \ldots, \mathbf{v}_{m+(k-m)} = \mathbf{v}_k$ in $\mathcal{C}_2$ such that any nontrivial linear combination of them is not in $\mathcal{D}$. Hence, by Lemma 4.2, $\mathrm{Proj}(\mathbf{v}_{m+1}), \ldots, \mathrm{Proj}(\mathbf{v}_k)$ are linearly independent over GF(2). Therefore $\mathcal{C}_4$ has dimension $k - m$ over GF(2) with basis $\{\mathrm{Proj}(\mathbf{v}_{m+1}), \ldots, \mathrm{Proj}(\mathbf{v}_k)\}$. This proves parts 1 and 2.

We can assume that the columns of the above $k - m$ linearly independent vectors $\mathbf{v}_{m+1}, \ldots, \mathbf{v}_k$ all have even parity by adding $f_1(m : \text{odd})$ or $f_2(m : \text{even})$ to those vectors of odd column parity. Furthermore, we may assume that the top row of each vector $\mathbf{v}_{m+1}, \ldots, \mathbf{v}_k$ consists of zeros of length m by adding proper codewords from $\mathcal{D}$. Hence, the columns of any vector from $\mathbf{v}_{m+1}, \ldots, \mathbf{v}_k$ have only one of the following four forms: $(0000), (0011), (0101), (0110)$. Thus for $m + 1 \leq i, j \leq k$, and $i \neq j$, $\mathrm{wt}(\mathbf{v}_i \cap \mathbf{v}_j) \equiv \mathrm{Proj}(\mathbf{v}_i) \star \mathrm{Proj}(\mathbf{v}_j) \pmod 2$ and $\mathrm{wt}(\mathbf{v}_i) = 2\mathrm{wt}(\mathrm{Proj}(\mathbf{v}_i))$, $i = m + 1, \ldots, k$. This proves part 3. ◻

We give an explicit construction of a binary linear code, which has projection O or projection E onto a given additive code $\mathcal{C}_4$. Suppose now that $\mathcal{C}_4$ is an additive $(m, 2^r)$ code, and let $\widehat{\mathcal{C}_4}$ be the binary linear $[4m, r]$ code obtained from $\mathcal{C}_4$ by replacing each $GF(4)$ component with a 4-tuple in $\mathrm{GF}(2)^4$ as follows : $0 \to 0000$, $1 \to 0011$, $\omega \to 0101$, $\overline{\omega} \to 0110$.

Construction O: $\rho_O(\mathcal{C}_4) = \widehat{\mathcal{C}_4} + \mathcal{D}$, where $\mathcal{D}$ contains f_1 when m is odd and f_2 when m is even.

Construction E: $\rho_E(\mathcal{C}_4) = \widehat{\mathcal{C}_4} + \mathcal{D}$, where $\mathcal{D}$ contains f_2 when m is odd and f_1 when m is even.

The above constructions were known [11] for additive self-dual codes. The next result follows from Proposition 4.3.

COROLLARY 4.4. *Let $\mathcal{C}_4$ be an additive $(m, 2^r)$ code with $0 \leq r \leq 2m$. Then,*

1. *$\rho_O(\mathcal{C}_4)$ and $\rho_E(\mathcal{C}_4)$ are binary linear $[4m, m + r]$ codes having projection O and projection E onto $\mathcal{C}_4$, respectively.*
2. *Any binary linear code having projection O or projection E onto $\mathcal{C}_4$ can be constructed in this way.*

Next we consider the natural question of whether two equivalent additive codes could be constructed from two inequivalent binary linear codes via projection O or projection E. We label the positions in a 4-tuple with the integers 1, 2, 3, and 4. With this notation, under the above mapping of each GF(4) component to a 4-tuple in $\mathrm{GF}(2)^4$, the multiplication of $x \in \mathrm{GF}(4)$ by ω corresponds to the cycle permutation (234) of each binary 4-tuple of x. Also the conjugation of $x \in \mathrm{GF}(4)$ corresponds to the transposition (34) of the binary 4-tuple of x. Trivially the permutation of coordinates of additive codes corresponds to the column permutation of their associated binary arrays. Hence we have shown the following.

TABLE 4.1
Projection of binary linear codes onto GF(4).

(m, r)	Linear codes over GF(4) [3]	Parameters for binary codes via construction O or E	Highest minimum weight d_B [3]
$(7, 8)$	$[7, 4, 3]$	$[28, 15, 6]$	$d_B = 6$
$(8, 10)$	$[8, 5, 3]$	$[32, 18, 6]$	$d_B = 6 - 7$
$(9, 12)$	$[9, 6, 3]$	$[36, 21, 6]$	$d_B = 7 - 8$
$(10, 14)$	$[10, 7, 3]$	$[40, 24, 6]$	$d_B = 7 - 8$
$(7, 6)$	$[7, 3, 4]$	$[28, 13, 7]$	$d_B = 8$
$(8, 8)$	$[8, 4, 4]$	$[32, 16, 8]$	$d_B = 8$
$(9, 10)$	$[9, 5, 4]$	$[36, 19, 8]$	$d_B = 8$
$(10, 12)$	$[10, 6, 4]$	$[40, 22, 8]$	$d_B = 8$
$(11, 14)$	$[11, 7, 4]$	$[44, 25, 8]$	$d_B = 8 - 9$
$(12, 16)$	$[12, 8, 4]$	$[48, 28, 8]$	$d_B = 8 - 10$
$(13, 18)$	$[13, 9, 4]$	$[52, 31, 8]$	$d_B = 8 - 10$
$(14, 20)$	$[14, 10, 4]$	$[56, 34, 8]$	$d_B = 8 - 10$
$(15, 22)$	$[15, 11, 4]$	$[60, 37, 8]$	$d_B = 8 - 10$
$(16, 24)$	$[16, 12, 4]$	$[64, 40, 8]$	$d_B = 9 - 11$
$(17, 26)$	$[17, 13, 4]$	$[68, 43, 8]$	$d_B = 9 - 12$

LEMMA 4.5. *Let $\mathcal{C}_4$ and $\mathcal{C}'_4$ be additive codes that are equivalent via maps defined in section 3. Then $\rho_O(\mathcal{C}_4)$ and $\rho_O(\mathcal{C}'_4)$ are equivalent by some coordinate permutation. Similarly $\rho_E(\mathcal{C}_4)$ and $\rho_E(\mathcal{C}'_4)$ are equivalent.*

COROLLARY 4.6. *Let $\mathcal{C}_4$ be an additive code. The automorphism group of $\mathcal{C}_4$ is isomorphic to a subgroup of the automorphism group of $\rho_O(\mathcal{C}_4)$ (resp., $\rho_E(\mathcal{C}_4)$).*

4.1. Examples.

Example 4.7. Let P_5 be the Pentacode [21], an additive self-dual $(5, 2^5, 3)$ code over GF(4). Ran and Snyders [21, Lemma 4] showed that a binary linear $[20, 10, 5]$ code P_{20}^b has projection O onto P_5. If we define $P_{20}^c = \rho_E(P_5)$, then P_{20}^c is also a binary linear $[20, 10, 5]$ code. The software package Magma [5] was used to show that P_{20}^b and P_{20}^c have the same weight distribution and isomorphic automorphism groups of order 1920 and that they are not equivalent. We remark that P_{20}^b and P_{20}^c have minimum weight, which is one less than the optimal [3] binary $[20, 10, 6]$ codes.

Example 4.8. Consider the case when $m = 5$. There exists a linear $[5, 3, 3]$ code $\mathcal{C}_4$ over GF(4) [3]. It has parameters $(5, 2^6, 3)$ as an additive code. By Corollary 4.4, $\rho_O(\mathcal{C}_4)$ and $\rho_E(\mathcal{C}_4)$ are both binary linear $[20, 11]$ codes. It is not difficult to prove that the minimum weights of these binary codes is 5. It is known [3] that binary $[20, 11, 5]$ codes are optimal. Hence we have shown that some such codes have projection O or projection E.

Example 4.9. Let $\mathcal{C}_4$ be any additive $(m, 2^r, 3)$ code, where $m \geq 6$. Then $\rho_O(\mathcal{C}_4)$ and $\rho_E(\mathcal{C}_4)$ have minimum weight 6. In this way we obtain optimal binary $[28, 15, 6]$ codes having projection O or projection E onto a linear $[7, 4, 3]$ code over GF(4). See Table 4.1 for more codes, where the fourth column denotes the highest minimum weight of the corresponding binary $[n, k]$ code together with the theoretical upper bound.

Example 4.10. Consider the case when $m = 10$. There exists a linear $[10, 6, 4]$ code $\mathcal{C}_4$ over GF(4) [3]. It has parameters $(10, 2^{12}, 4)$ as an additive code. By Corollary 4.4, both $\rho_O(\mathcal{C}_4)$ and $\rho_E(\mathcal{C}_4)$ are binary linear $[40, 22]$ codes. We want to show that the minimum weight of these binary codes is 8 in order to obtain optimal [3] binary $[40, 22, 8]$ codes. Without loss of generality, let $\mathbf{w}$ be a codeword in $\mathcal{C}_4$ whose first four coordinates are nonzero. Such a vector $\mathbf{w}$ necessarily exists, as the minimum weight of $\mathcal{C}_4$ is 4. Then in the case of even parity columns, the columns corresponding to the nonzero coordinates each contain two 1's. In the case of odd parity columns, there is at least one 1 in *every* column. Hence the minimum weight of $\rho_O(\mathcal{C}_4)$ and $\rho_E(\mathcal{C}_4)$ is 8. We have shown that there exist binary optimal $[40, 22, 8]$ codes that have projection O or projection E.

Generalizing this example, let $\mathcal{C}_4$ be any additive $(m, 2^r, 4)$ code, where $m \geq 7$. Then (i) if $m = 7$, the minimum weight of $\rho_O(\mathcal{C}_4)$ and $\rho_O(\mathcal{C}_4)$ is 7 and (ii) if $m \geq 8$, the minimum weight of $\rho_O(\mathcal{C}_4)$ and $\rho_O(\mathcal{C}_4)$ is 8. We get several optimal binary codes having projection O or projection E on $\mathcal{C}_4$. See Table 4.1 for more examples.

5. Projections of binary self-dual codes onto GF(4). In this section, we characterize binary self-dual codes of length $8k$ that have either projection O or projection E. The following proposition will be useful when we determine which binary self-dual codes have projection O or projection E.

PROPOSITION 5.1. *Let $\mathcal{C}_2$ be a binary self-dual $[4m, 2m, d]$ code with projection O (or projection E) onto a quaternary additive code $\mathcal{C}_4$. Then*

1. *m is even.*
2. *$\mathcal{C}_4$ has dimension m over $GF(2)$.*
3. *$\mathcal{C}_4$ is a self-dual code under the trace inner product. Furthermore when $\mathcal{C}_2$ is doubly even, $\mathcal{C}_4$ is even.*

Proof. We prove the claim only for projection O. By definition, $\mathcal{D}$ is a subcode of $\mathcal{C}_2$. We take f_1 or f_2 in $\mathcal{D}$, depending on (P3). Since $\mathcal{C}_2$ is self-dual, $\mathrm{wt}(f_1)$ and $\mathrm{wt}(f_2)$ are even. As $\mathrm{wt}(f_1) = m$ and $\mathrm{wt}(f_2) = m + 2$, it follows that m is even. This proves part 1. Part 2 follows from part 1 of Proposition 4.3. Part 3 follows from part 3 of Proposition 4.3. ∎

We can say a little more about the relationship between the automorphism group of an even additive code $\mathcal{C}_4$ and its associated binary linear code in the case when the binary linear code is self-orthogonal.

PROPOSITION 5.2. *Let $\mathcal{C}_4$ be an even additive $(m, 2^r)$ code that lifts to a self-orthogonal binary linear code $\mathcal{C}_2$ of length $4m$ via construction O or E given above. Then $Aut(\mathcal{C}_2)$ contains a subgroup of order 2^r, which is not induced by a subgroup of $Aut(\mathcal{C}_4)$.*

Proof. We consider only construction E, as the proof for construction O is similar. Let $\mathbf{v}$ be a vector of $\widehat{\mathcal{C}_4}$ whose columns have even parity. We associate a unique coordinate permutation $p_{\mathbf{v}}$ with the vector $\mathbf{v}$ in the following way. If a column of $\mathbf{v}$ contains all 1's or all 0's, then every position in that column is fixed under $p_{\mathbf{v}}$. If a column of $\mathbf{v}$ contains exactly two 1's, then the permutation $p_{\mathbf{v}}$ interchanges the coordinate positions in that column which contain 1's and also interchanges the coordinate positions which contain 0's. For instance, the permutation associated with the vector

$$\mathbf{v} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

is given by the coordinate permutation $(1, 2)(3, 4)(9, 12)(10, 11)(13, 14)(15, 16)(17, 19)$ $(18, 20)$. We claim that such a coordinate permutation leaves the code invariant and

TABLE 5.1
Automorphism group orders of some self-dual codes.

$\mathcal{C}$	$\lvert\mathrm{Aut}(\mathcal{C})\rvert$	$\lvert\mathrm{Aut}(\rho_E(\mathcal{C}))\rvert$	$\lvert\mathrm{Aut}(\rho_O(\mathcal{C}))\rvert$
$\mathcal{G}_6$	$2^4 \cdot 3^3 \cdot 5$	$2^{10} \cdot 3^3 \cdot 5$	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
$\mathcal{C}_1$	$2^7 \cdot 3^2$	$2^{15} \cdot 3^2 \cdot 5 \cdot 7$	$2^{15} \cdot 3^2$
$\mathcal{C}_2$	$2^4 \cdot 3 \cdot 7$	$2^{12} \cdot 3 \cdot 7$	$2^{12} \cdot 3 \cdot 7$
$\mathcal{C}_3$	$2^7 \cdot 3^2 \cdot 7$	$2^{15} \cdot 3^2 \cdot 5 \cdot 7 \cdot 31$	$2^{15} \cdot 3^2 \cdot 7$

hence is part of the full automorphism group of the binary linear code $\rho_E(\mathcal{C}_4)$. Hence, we need to show that the image of any codeword under such a permutation is still in the code.

Let $\mathbf{w}$ be any binary codeword in $\rho_E(\mathcal{C}_4)$ with even column parity and let $p_\mathbf{v}$ be a permutation associated with vector $\mathbf{v}$ as above. If $\mathbf{w}$ is fixed under $p_\mathbf{v}$, then we are done. Otherwise, we consider the columns of $\mathbf{w}$ whose coordinates are not fixed under $p_\mathbf{v}$. Let c_i be any such column of $\mathbf{w}$. Then c_i contains exactly two 1's and, since this column of $\mathbf{w}$ is not fixed under $p_\mathbf{v}$, we know that c_i meets the corresponding column of $\mathbf{v}$ in exactly one position. Because of the self-orthogonality condition, there must be another column of $\mathbf{w}$, say c_j, with the same property. Letting $d_{i,j}$ be the element of the subcode $\mathcal{D}$ with all 1's in the ith and jth columns and 0's everywhere else, we see that the action of $p_\mathbf{v}$ on the ith and jth columns of $\mathbf{w}$ is the same as adding $d_{i,j}$ to $\mathbf{w}$. We conclude that the image of the codeword $\mathbf{w}$ under the coordinate permutation $p_\mathbf{v}$ is equal to $\mathbf{w} + \mathbf{d}$, where $\mathbf{d}$ is some element of $\mathcal{D}$.

Now let $\mathbf{u}$ be any binary codeword in $\rho_E(\mathcal{C}_4)$ with odd column parity. Any such vector can be written as $f_1 + \mathbf{w}$ for some vector $\mathbf{w}$ with even column parity. Hence, it is sufficient to check that the image of f_1 under $p_\mathbf{v}$ is still in the code $\mathcal{C}_2$. Since $\mathcal{C}_4$ is an even code, the action of $p_\mathbf{v}$ on f_1 will only permute the positions in an even number of columns of f_1. Let $\mathbf{d_v}$ be the element of $\mathcal{D}$ that has all 1's in the columns where $\mathbf{v}$ has weight 2. Then, one can easily check that the image of f_1 under the permutation $p_\mathbf{v}$ is equal to $f_1 + \mathbf{v} + \mathbf{d_v}$.

Hence, we have shown that the permutation $p_\mathbf{v}$ leaves the code $\rho_E(\mathcal{C}_4)$ invariant. Note that any nontrivial permutation as described above does not permute columns, but does permute the top position of any column on which it does not act trivially. This shows that every such permutation cannot be induced from an element of $Aut(\mathcal{C}_4)$. Since the number of codewords of $\widehat{\mathcal{C}_4}$ is exactly 2^r, this completes the proof. ◻

Note that the action of a permutation $p_\mathbf{v}$ on a particular column can be viewed as an element of the Klein 4 group, that is, a cycle permutation corresponding to (1,2)(3,4), (1,3)(2,4), or (1,4)(2,3). This observation can be used to show that for any two permutations $p_{\mathbf{v_1}}$ and $p_{\mathbf{v_2}}$, the composition gives the permutation $p_{\mathbf{v_1}+\mathbf{v_2}}$.

COROLLARY 5.3. *Let $\mathcal{C}_4$ be an even additive $(m, 2^r)$ code that lifts to a self-orthogonal binary linear code $\mathcal{C}_2$ of length $4m$ via construction O or E given above. Then $2^r \cdot |Aut(\mathcal{C}_4)|$ divides $|Aut(\mathcal{C}_2)|$.*

We note that this result about automorphism groups partially explains the size of the automorphism groups of the binary codes given in Table 5.1, which originally appeared in [11, section 5, p. 149].[1] Here, $\mathcal{G}_6$ is the $(6, 2^6, 4)$ hexacode, and $\mathcal{C}_1, \mathcal{C}_2$, and $\mathcal{C}_3$ are the three $(8, 2^8, 4)$ Type II codes. Note that the orders of the binary linear codes all satisfy the relationship given in the corollary above. In fact, the entire automorphism group is completely determined for those cases in which the binary

[1]Table reprinted with permission of the American Mathematical Society, Providence, RI.

code is singly even. This is the case for only one of the doubly even codes, namely $\rho_E(\mathcal{C}_2)$.

5.1. Examples. In the following we consider an extremal Type II self-dual $[8k, 4k, 4\lfloor\frac{n}{24}\rfloor+4]$ code.

Example 5.4. When $k=1$ we get the unique Hamming $[8,4,4]$ code $\mathcal{H}_3$. Let i_2 be the self-dual linear $[2,1,2]$ code over GF(4) with generator matrix $[1\;\;1]$. Then the set of vectors satisfying conditions (P1), (P2), and (P3) with $\mathcal{C}_4 = i_2$ in Definition 2.1 gives $\mathcal{H}_3$. In other words, $\mathcal{H}_3$ has projection O onto i_2.

Example 5.5. When $k=2$, there are exactly two Type II $[16,8,4]$ binary codes $A_8 \oplus A_8$ and E_{16} in the notation of [19]. By using exactly two Type II additive quaternary $(4,2^4,2)$ codes from [15, Table 1] or [13], we see that $A_8 \oplus A_8$ and E_{16} have projection E onto $(4,2^4,2)$ codes. The Type I $[16,8,4]$ binary code F_{16} has projection E onto the Type I $(4,2^4,2)$ code from [15, Table 2] or [13].

Example 5.6. When $k=3$, it is well known [18] that the extended Golay code has projection O onto the hexacode. If we consider projection E onto the hexacode, we get the Type I $[24,12,6]$ code [12].

Example 5.7. When $k=4$, we consider the five Type II $[32,16,8]$ codes given in [6]. Several authors [1, 11, 12, 24] are interested in a projection construction for some of these codes. It is known [11, Example 5.4] that applying construction E to the three Type II additive $(8,2^8,4)$ codes produces three of these five, i.e., $2g_{16}, 8f_4$, and r_{32} in the notation of [6].

It is claimed in [24] that the extended quadratic residue code q_{32} has projection O onto a quaternary linear $[8,4,4]$ code B given by Yuan, Chen, and Ma [24, p. 410]. In an example, they construct a singly even [32,16,8] code, which they claim is the quadratic residue code. However, the latter code is doubly even. Their example contains a weight 14 vector, which was claimed to be in q_{32}. We note that the code B in [24, p. 410] is equivalent to the unique linear self-dual $[8,4,4]$ code over GF(4) with generator matrix of the binary Hamming $[8,4,4]$ code. So the set of vectors in [24, Definition 1] is actually r_{32}, one of the three Type I $[32,16,8]$ codes given in [8].

Furthermore we prove here that q_{32} does not have projection E onto an additive code over GF(4). It is easy to see that Type II $[32,16,8]$ codes do not have projection O.

PROPOSITION 5.8. *Exactly three Type II* $[32,16,8]$ *codes out of the five Type II codes, namely* $2g_{16}, 8f_4$*, and* r_{32}*, have projection E onto the three Type II additive* $(8,2^8,4)$ *codes.*

Proof. Let $\mathcal{C}_2$ be one of the five Type II $[32,16,8]$ codes which have projection E onto one of the three Type II additive $(8,2^8,4)$ codes. Then by part 1 and part 2 of Corollary 4.4, we note that at most three Type II $[32,16,8]$ codes are constructed. From the discussion in Example 5.7, these three codes are in fact $2g_{16}, 8f_4$, and r_{32}. This completes the proof. ◻

There is an alternative way to prove Proposition 5.8. Suppose that $\mathcal{C}_2$ is one of the five Type II $[32,16,8]$ codes which have projection E onto one of the three Type II additive $(8,2^8,4)$ codes. By Proposition 4.3, $\mathcal{C}_2$ contains the set $\mathcal{D}_0$ of all even sums of weight 4 vectors with all four 1's in a column. The set $\mathcal{D}_0$ gives rise to an *octet*, that is, a weight 4 coset of $\mathcal{C}_2$ containing exactly eight weight 4 vectors (see [8, p. 1328]). As codes q_{32} and $16f_2$ have no octets while codes $2g_{16}, 8f_4$, and r_{32} have one or more [8], the above proposition follows.

Example 5.9. For $k=5$, there are at most 19 Type II $[40,20,8]$ codes having projection E onto additive $(10,2^{10},4)$ codes, as there are exactly 19 Type II $(10,2^{10},4)$

codes given in [2, 11].

6. Projections of binary codes onto GF(16). So far we have investigated projections of binary linear codes onto GF(4) using arrays with four rows. It is natural to consider a generalization to arrays with more rows. In this case we need other field extensions of GF(2) apart from GF(4). Esmaeili, Gulliver, and Khandani [10] first studied a projection of binary linear codes onto GF(16) as follows.

Let GF(16) be generated by α such that $\alpha^4 + \alpha + 1 = 0$, where α is a primitive element of GF(16). We write a binary vector of length $6m$ as a $6 \times m$ array whose rows are indexed by $0, 1, \alpha, \alpha^2, \alpha^3, \beta$, where $\beta = \alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3$. As before, we take the inner product of a column of our array with the row labels, producing an element of GF(16). It is easy to see that for any element x in GF(16), there are exactly two columns of odd parity and two columns of even parity which project to x. For example, let $x = \alpha^4$. Then $(111000)^t$, and its complement are two odd columns projecting to α^4. Similarly $(011000)^t$, and its complement are two even columns projecting to α^4.

Now we can define projection O and projection E onto GF(16) as we defined them onto GF(4) in section 2. It is clear that the binary $[48, 24, 12]$ quadratic residue code q_{48} does not have projection O or projection E onto any additive code over GF(4) since the minimum weight of q_{48} is greater than 8. It is also shown [10, Theorem 2] by computer search that q_{48} does not have projection O onto any linear code over GF(16). We show this without a computer search. Suppose that q_{48} has projection O or projection E onto an additive code of length 8 over GF(16). Then q_{48} would have a subcode generated by all even sums of weight 6 vectors, all of whose ones appear in the same column. This subcode gives rise to a weight 6 coset of q_{48} containing exactly eight weight 6 vectors. However, it is known [9, Table I] that there is no such coset of q_{48}. Therefore q_{48} cannot have projection O or projection E onto any additive code of length 8.

Furthermore we can prove that any $[48, 24, 12]$ binary code $\mathcal{C}_2$ does not have projection O or projection E onto an additive code of length 8 over GF(16). If it did, then $\mathcal{C}_2$ would be projected onto an additive $(8, 2^{16}, d \geq 6)$ code $\mathcal{C}_{16}$ over GF(16). It is well known [3, p. 299] that any q-ary (n, M, d) code has at most q^{n-d+1} vectors in it. Applying this to $\mathcal{C}_{16}$ we get $2^{16} \leq 16^{8-d+1}$, so $d \leq 5$. This is a contradiction.

Proposition 6.1. *No binary* $[48, 24, 12]$ *code has projection O or projection E onto GF*(16).

7. Projections of codes with large minimum weight. We note that projection O and projection E are very useful when the minimum weight of the binary code is at most 8. In what follows, we generalize projection E so that we can construct a binary $[48, 21, 12]$ code and a $[72, 31, 16]$ code which both have a projection onto an additive GF(4) code. Interestingly, these codes are optimal [3].

Apart from the projection of a binary 4-tuple to an element of GF(4) from section 2, we recall two other maps **TOP** and **PAR** defined in [1, p. 2562]. **TOP** is the mapping of a binary 4-tuple (v_1, v_2, v_3, v_4) to v_1. **PAR** is the mapping of a binary 4-tuple (v_1, v_2, v_3, v_4) to $v_1 + v_2 + v_3 + v_4$. Both of these maps are linear. We extend these maps onto a $4 \times m$ binary array, operating on every column of the array.

Under this notation, we define a projection as follows.

Definition 7.1. *Let* S *be a set of binary vectors of length* $4m$ *written as* $4 \times m$ *arrays as before. Let* $\mathcal{P}$ *and* $\mathcal{T}$ *be binary codes of length* m *and let* $\mathcal{C}_4$ *be a quaternary additive code of length* m*. Then* S *is said to have* projection G onto $\mathcal{C}_4$ *if the following conditions are satisfied:*

(G1) *For any vector* $\mathbf{v} \in S$, $Proj(\mathbf{v}) \in \mathcal{C}_4$. *Conversely, for any vector* $\mathbf{w} \in \mathcal{C}_4$, *all vectors* $\mathbf{v}$ *such that* $Proj(\mathbf{v}) = \mathbf{w}$ *are in* S.
(G2) **PAR** *of any vector of* S *is in* $\mathcal{P}$.
(G3) **TOP** *of any vector of* S *is in* $\mathcal{T}$.

We call codes $\mathcal{P}$ *and* $\mathcal{T}$ *a* parity code *and a* top code*, respectively.*

Taking the parity code as the repetition $[m, 1, m]$ code and the top code as the even $[m, m-1, 2]$ code, projection G is the same as projection E. Now we give properties of projection G. Since its proof is similar to that of Proposition 4.3, we omit the details.

PROPOSITION 7.2. *Let* $\mathcal{C}_2$ *be a binary linear* $[4m, k, d]$ *code with projection G onto an additive code* $\mathcal{C}_4$ *over* $GF(4)$. *Let* $\mathcal{P}$ *be a parity code with dimension* k_1 *and* $\mathcal{T}$ *a top code with dimension* k_2. *Then*

1. $\mathcal{C}_4$ *has dimension* $r = k - (k_1 + k_2) \geq 0$ *over* $GF(2)$.
2. *There exist* r *linearly independent vectors* $\mathbf{v}_{k_1+k_2+1}, \ldots, \mathbf{v}_{k_1+k_2+r} = \mathbf{v}_k$ *of* $\mathcal{C}_2$ *whose projection forms a basis for* $\mathcal{C}_4$ *as an additive code.*

We remark that part 3 of Proposition 4.3 does not hold in general.

7.1. Examples.

Example 7.3. It was shown in Theorem 1 and Corollary 2 of [1] that the binary Reed–Muller $R(r, m)$ code, where $r \geq 1$ and $m > r + 1$, has a projection onto $R(r-1, m-2)$ over GF(4). This fact can be described in terms of projection G by taking $\mathcal{C}_2 = R(r, m)$, $\mathcal{C}_4 = R(r-1, m-2)$, $\mathcal{P} = R(r-2, m-2)$, and $\mathcal{T} = R(r, m-2)$. In the case of the first-order Reed–Muller $R(1, m)$ code for $m > 2$, we understand $\mathcal{P}$ as the zero code of length 2^{m-2}.

Example 7.4. We will construct a binary $[48, 21, 12]$ code having projection G onto the unique self-dual additive $(12, 2^{12}, 6)$ code over GF(4) called the dodecacode [4, 11]. For the top code, we consider a binary optimal $[12, 8, 3]$ code, which is easy to construct. We also take the repetition $[12, 1, 12]$ code as the parity code. Then by Proposition 7.2 we construct a binary $[48, 21, 12]$ code having projection G onto the dodecacode. See Table 7.1 for the generator matrix of the binary $[48, 21, 12]$ code and Table 7.2 for its weight distribution. This code has an automorphism group of order 2 generated by the following transposition found by Magma:

$$(1,29)(2,31)(3,30)(4,32)(5,33)(6,36)(7,35)(8,34)(9,25)(10,26)(11,28)$$
$$(12,27)(13,21)(14,24)(15,22)(16,23)(37,45)(38,48)(39,46)(40,47)$$

Example 7.5. We can similarly construct a binary $[72, 31, 16]$ code having projection G onto the quaternary linear $[18, 9, 8]$ code S_{18} [20]. We take as the top code a binary $[18, 12, 4]$ code and as the parity code the repetition code of length 18. Then by Proposition 7.2 we get a binary $[72, 31, 16]$ code having projection G onto S_{18}.

7.2. Decoding. We sketch a hard decision decoding algorithm for binary linear codes having projection G. The decoding idea is analogous to the syndrome decoding algorithm [12] and, generally, the decoding algorithm given in [16].

Let $\mathcal{C}_2$ have projection G onto $\mathcal{C}_4$ with the parity code $\mathcal{P}$ and the top code $\mathcal{T}$. In order to make the situation simple we assume that $\mathcal{P}$ is the repetition code of proper length. Suppose $\mathbf{v}$ is a received vector. First we compute the parities of the columns of $\mathbf{v}$ and take the majority parity among them. We regard the columns of $\mathbf{v}$ with this parity as correct columns. Then we project $\mathbf{v}$ onto a vector $\mathbf{w}$ over GF(4). We find a closest codeword $\mathbf{x}$ in $\mathcal{C}_4$ to $\mathbf{w}$ by solving a syndrome equation with respect to H_4, the parity check matrix of $\mathcal{C}_4$. See [16] for more details. We then lift $\mathbf{x}$ to a

TABLE 7.1
Generator matrix of the binary $[48, 21, 12]$ *code.*

$$\begin{bmatrix}
1111 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 1111 & 1111 & 0000 & 0000 \\
0000 & 1111 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 1111 & 0000 & 1111 & 0000 \\
0000 & 0000 & 1111 & 0000 & 0000 & 0000 & 0000 & 0000 & 1111 & 0000 & 0000 & 1111 \\
0000 & 0000 & 0000 & 1111 & 0000 & 0000 & 0000 & 0000 & 0000 & 1111 & 1111 & 0000 \\
0000 & 0000 & 0000 & 0000 & 1111 & 0000 & 0000 & 0000 & 0000 & 1111 & 0000 & 1111 \\
0000 & 0000 & 0000 & 0000 & 0000 & 1111 & 0000 & 0000 & 0000 & 0000 & 1111 & 1111 \\
0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 1111 & 0000 & 1111 & 1111 & 1111 & 0000 \\
0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 1111 & 1111 & 0000 & 1111 & 1111 \\
1000 & 0111 & 0111 & 0111 & 0111 & 0111 & 0111 & 0111 & 1000 & 1000 & 0111 & 0111 \\
0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 \\
0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 \\
0011 & 0011 & 0011 & 0011 & 0011 & 0011 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\
0101 & 0101 & 0101 & 0101 & 0101 & 0101 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\
0000 & 0000 & 0000 & 0011 & 0101 & 0110 & 0000 & 0000 & 0000 & 0011 & 0101 & 0110 \\
0000 & 0000 & 0000 & 0101 & 0110 & 0011 & 0000 & 0000 & 0000 & 0101 & 0110 & 0011 \\
0011 & 0110 & 0101 & 0000 & 0000 & 0000 & 0011 & 0110 & 0101 & 0000 & 0000 & 0000 \\
0101 & 0011 & 0110 & 0000 & 0000 & 0000 & 0101 & 0011 & 0110 & 0000 & 0000 & 0000 \\
0000 & 0000 & 0000 & 0011 & 0110 & 0101 & 0101 & 0110 & 0011 & 0000 & 0000 & 0000 \\
0000 & 0000 & 0000 & 0101 & 0011 & 0110 & 0011 & 0101 & 0110 & 0000 & 0000 & 0000 \\
0011 & 0101 & 0110 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0110 & 0101 & 0011 \\
0110 & 0011 & 0101 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0011 & 0110 & 0101
\end{bmatrix}.$$

TABLE 7.2
Weight distribution of the binary $[48, 21, 12]$ *code.*

Weights	No.	Weights	No.	Weights	No.	Weights	No.
0	1	18	56832	26	203264	34	3072
12	2065	20	374012	28	373142	36	1884
14	2944	22	201984	30	56192	40	4
16	49254	24	722548	32	49953	44	1

binary vector $\mathbf{v}'$. There are often several choices for $\mathbf{v}'$. When the syndrome of $\mathbf{v}'$ with respect to H, the parity check matrix of $\mathcal{T}$, is zero, we take $\mathbf{v}'$ as a codeword of $\mathcal{C}_2$. Otherwise we go back to the previous step, finding a closest codeword in $\mathcal{C}_4$ to $\mathbf{w}$ by solving another syndrome equation. We repeat this step until we get a binary vector $\mathbf{v}'$ whose syndrome with respect to H is zero.

We can apply this algorithm to the second-order Reed–Muller code $R(2, m)$, as it has projection G with the repetition code as the parity code. We remark that a soft decision decoding for the first-order Reed–Muller code $R(1, m)$ was explained in [1]. It appears that a soft decision decoding for binary linear codes having projection G is possible in a similar fashion; see [1, 7, 10, 21, 22, 23, 24]. It would be interesting to find a fast hard or fast soft decision decoding algorithm for projection G.

Acknowledgments. We would like to thank T. A. Gulliver for providing his preprint [10] and Y. Be'ery for providing [24]. The first author would also like to thank O. Amrani for his helpful discussion.

REFERENCES

[1] O. AMRANI AND Y. BE'ERY, *Reed-Muller codes: Projections on* $GF(4)$ *and multilevel construction*, IEEE Trans. Inform. Theory, 47 (2001), pp. 2560–2565.

[2] C. BACHOC AND P. GABORIT, *On extremal additive* $GF(4)$*-codes of lengths* 10 *to* 18, J. Théorie Nombres Bordeaux, 12 (2000), pp. 225–271.

[3] A. E. BROUWER, *Bounds on the size of linear codes*, in Handbook of Coding Theory, V. S. Pless and W. C. Huffman, eds., Elsevier, Amsterdam, 1998, pp. 295–461.

[4] A. R. CALDERBANK, E. M. RAINS, P. W. SHOR, AND N. J. A. SLOANE, *Quantum error correction via codes over* $GF(4)$, IEEE Trans. Inform. Theory, 44 (1998), pp. 1369–1387.

[5] J. CANNON AND C. PLAYOUST, *An Introduction to Magma*, University of Sydney, Sydney, Australia, 1994.

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

[7] J. H. Conway and N. J. A. Sloane, *Decoding techniques for codes and lattices, including the Golay code and the Leech lattice*, IEEE Trans. Inform. Theory, 32 (1986), pp. 41–50.

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

[9] P. Delsarte, *Four fundamental parameters of a code and their combinatorial significance*, Inform. and Control, 23 (1973), pp. 407–438.

[10] 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, 49 (2003), pp. 1527–1535.

[11] P. Gaborit, W. C. Huffman, J.-L. Kim, and V. Pless, *On additive* $GF(4)$ *codes*, in Proceedings of the DIMACS Workshop on Codes and Association Schemes, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. 56, AMS, Providence, RI, 2001, pp. 135–149.

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

[13] T. A. Gulliver and J.-L. Kim, *Circulant based extremal additive self-dual codes over* $GF(4)$, IEEE Trans. Inform. Theory, submitted.

[14] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The* Z_4*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory, 40 (1994), pp. 301–319.

[15] G. Höhn, *Self-Dual Codes over the Kleinian Four Group*, preprint, 1996. Updated version available online at http://xxx.lanl.gov/ps/math.CO/0005266.

[16] J.-L. Kim and V. Pless, *Decoding some doubly-even self-dual* $[32, 16, 8]$ *codes by hand*, in Proceedings of a Conference Honoring Professor Dijen Ray-Chaudhuri on the Occasion of His 65th Birthday, Ohio State Univ. Math. Res. Inst. Publ. 10, Ohio State University, Columbus, OH, 2002, pp. 165–178.

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

[18] V. Pless, *Decoding the Golay codes*, IEEE Trans. Inform. Theory, 32 (1986), pp. 561–567.

[19] V. Pless, *A classification of self-orthogonal codes over* $GF(2)$, Discrete Math., 3 (1972), pp. 209–246.

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

[21] M. Ran and J. Snyders, *Constrained designs for maximum likelihood soft decoding of* $RM(2, m)$ *and the extended Golay codes*, IEEE Trans. Comm., 43 (1989), pp. 812–820.

[22] J. Snyders and Y. Be'ery, *Maximum likelihood soft decoding of binary block codes and decoders for the Golay codes*, IEEE Trans. Inform. Theory, 35 (1989), pp. 963–975.

[23] A. Vardy and Y. Be'ery, *More efficient soft decoding of the Golay codes*, IEEE Trans. Inform. Theory, 37 (1991), pp. 667–672.

[24] J. Yuan, C. S. Chen, and S. Ma, *Two-level decoding of* $(32, 16, 8)$ *quadratic residue code*, Proc. IEEE, 140 (1993), pp. 409–414.