Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080107

A New Construction for the Extended Binary Golay Code

Suat Karadeniz and Bahattin Yildiz[*]

Department of mathematics, Fatih University, 34500, Istanbul, Turkey

Received: 24 May. 2013, Revised: 7 Sep. 2013, Accepted: 8 Sep. 2013
Published online: 1 Jan. 2014

Abstract: We give a new construction of the extended binary Golay code. The construction is carried out by taking the Gray image of a self-dual linear code over the ring $R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ of length 6 and size 2^{12}. Writing a typical generating matrix of the form $[I_3|A]$, with A being a 3×3 matrix over R, and finding some dependencies among the entries of A, we are able to set a general form for the generating matrices of self-dual codes of length 6. Using some special properties of elements of R, we end up with a family of generating matrices all of which give us the extended binary Golay code. We also prove the minimum distance property analytically.

Keywords: extremal codes, extended binary Golay code, Gray map, Lee weight, self-dual codes, codes over rings

1 Introduction

The binary Golay code is a perfect code with parameters $[23,12,7]$, and was first introduced by Golay in [5]. By adding a parity check to the Golay code, the extended binary Golay code is obtained. The extended binary Golay code is a self-dual Type II optimal code with parameters $[24,12,8]$ and is unique up to equivalence. The extended binary Golay code has received a considerable attention by researchers and many different constructions have been introduced. For some of these constructions we refer to [6], [7], [2].

In this work, we give a different construction than the ones mentioned above. We consider a larger alphabet, i.e., the ring $R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ which is a non-chain Frobenius ring. Self-dual codes over rings have been studied quite extensively, viz. [1], [4]. Self-dual codes over the ring R were studied in [9]. In that work, the extended Golay was obtained from R by a brute search. But, here we use a more systematic approach and the rich algebraic structure of the ring R to find a large family of generating matrices all of which lead to the extended binary Golay code. We also find the parameters analytically from the generating matrices over R.

In section 2, we give some of the general properties of the ring R, and self-dual codes over R from [8] and [9].

In section 3, we describe the construction. The construction reduces to finding a 3×3 matrix over R with some dependencies and restrictions and using this, we are able to find a family of generating matrices all of which result in the extended binary Golay code.

We then give an analytical proof for the minimum distance of the class of codes that we consider in section 4.

We finish with some remarks and possible directions for future work.

2 Self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$

Most of what follows can be found in [8] and [9]. The ring $R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ is defined as a characteristic 2 ring subject to the restrictions $u^2 = v^2 = 0$ and $uv = vu$. Note that R is not a chain ring, but its ideals can easily be described as

$$\{0\} \subseteq I_{uv} = uv(R) = \{0, uv\} \subseteq I_u, I_v, I_{u+v} \subseteq I_{u,v} \subseteq I_1 = R \tag{2.1}$$

where

$$\begin{aligned} I_u &= u(R) = \{0, u, uv, u+uv\}, \\ I_v &= v(R) = \{0, v, uv, v+uv\}, \\ I_{u+v} &= (u+v)(R) = \{0, u+v, uv, u+v+uv\}, \\ I_{u,v} &= \{0, u, v, u+v, uv, u+uv, v+uv, u+v+uv\}. \end{aligned}$$

Note that $I_{u,v}$ is the maximal ideal of R that contains all the zero divisors with everything outside $I_{u,v}$ being a unit. Also we have

$$\text{for any } a \in R \quad a^2 = \begin{cases} 1 \text{ if } a \text{ is a unit} \\ 0 \text{ otherwise} \end{cases} \tag{2.2}$$

[*] Corresponding author e-mail: byildiz@fatih.edu.tr

Moreover, the ring entails the following properties which will later be used in our constructions:

$$(non-unit)*(non-unit) = 0 \text{ or } uv, \tag{2.3}$$

$$(non-unit)*(non-unit)*(non-unit) = 0 \tag{2.4}$$

and

$$(unit)*(xy) = xy, \text{ if } x,y \text{ are non-units.} \tag{2.5}$$

Linear codes over R of length n are defined as always to be R-submodules of R^n.

By extending the notion of the Lee weight and the Gray map from [4], we define

Definition 2.1. $\phi : R^n \to \mathbb{F}_2^{4n}$, which is given by

$$\phi(\overline{a}+u\overline{b}+v\overline{c}+uv\overline{d}) = (\overline{a}+\overline{b}+\overline{c}+\overline{d}, \overline{c}+\overline{d}, \overline{b}+\overline{d}, \overline{d}),$$

is defined to be the Gray map from R^n to $\mathbb{F}_2^{4n}$, where $\overline{a}, \overline{b}, \overline{c}, \overline{d} \in \mathbb{F}_2^n$.

and

Definition 2.2. For any element $a+ub+vc+uvd \in R$, we define $w_L(a+ub+vc+uvd) = w_H(a+b+c+d, c+d, b+d, d)$, where w_H denotes the ordinary Hamming weight for binary vectors, to be the Lee weight of $a+ub+vc+uvd$.

Note that the units $1, 1+u, 1+v$ and $1+u+v+uv$ each have Lee weights 1 while the other units, $1+uv$, $1+u+uv$, $1+v+uv$, $1+u+v$ have weights 3. We will call the units that have weight 1 to be *basic* units and the others will be labeled as *non-basic* units. One can quickly observe that (basic)·(basic) = basic, (non-basic)·(non-basic) = basic and that (non-basic)·(basic) = non-basic.

The non-zero non-units all have Lee weight 2 except uv, which has Lee weight 4.

From the definitions it can be deduced that ϕ is a linear distance-preserving map; thus we obtain the following lemma, which will later be useful:

Lemma 2.3. If C is a linear code over R of length n, size 2^k and minimum Lee distance d, then $\phi(C)$ is a binary $[4n, k, d]$-linear code.

The inner product and duality can be defined next. For $(x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \in R^n$, we define

$$<(x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n)> = x_1y_1 + x_2y_2 + \cdots + x_ny_n \tag{2.6}$$

where the operations are performed in the ring R.

Definition 2.4. Let C be a linear code over R of length n, then we define the *dual* of C as

$$C^{\perp} := \{\overline{y} \in (R)^n | <\overline{y}, \overline{x}> = 0, \quad \forall \overline{x} \in C\}.$$

C is said to be self-orthogonal if $C \subseteq C^{\perp}$, and it is self-dual if $C = C^{\perp}$. A self-dual code over R is said to be of Type II if the Lee weights of all codewords are divisible by 4, otherwise it is said to be of Type I.

The following theorem is very useful in connecting self-dual codes over R to binary self-dual codes:

Theorem 2.5.([9]) Suppose C is a self-dual linear code over R of length n. Then $\phi(C)$ is a self-dual binary linear code of length $4n$.

Because the Gray map is distance preserving, we get the following corollary:

Corollary 2.6. If C is a Type I (respectively Type II) code over R with parameters $(n, 2^k, d)$, then $\phi(C)$ is a binary Type I (respectively, Type II) code of parameters $[4n, k, d]$.

3 The Construction

We construct the extended Golay code as the Gray image of a linear code over R of length 6.

We start with three free generators over R, i.e. we take a generating matrix of the form $G = [I_3|A]$, where A is a 3×3 matrix over R. Let C be the code generated by such a matrix. Since the generators are free and linearly independent, we know that $|C| = (16)^3 = 2^{12}$, and hence $\phi(C)$ is a binary linear code with parameters $[24, 12]$. In order to ensure that C is self-dual it is enough to show that C is self-orthogonal. For self-orthogonality, first, the rows of G must contain an even number of units by [9]; and the rows must be orthogonal to each other. So, each row of A must contain either one or three units. But it is easy to see that in the latter case, the rows cease to be orthogonal. So we take the matrix A to be in the following form:

$$A = \begin{bmatrix} x_1 & y_1 & y_2 \\ y_3 & x_2 & y_4 \\ y_5 & y_6 & x_3 \end{bmatrix}, \tag{3.1}$$

where x_i's are units and y_j's are non-units. y_3, y_5 and y_6 can be determined uniquely over R in terms of the other entries by using orthogonality equations. This gives us a general form for self-dual codes of length 6. The equations for y_3, y_5 and y_6 are given in the following:

$$y_3 = x_1(y_1x_2 + y_2y_4) = x_1x_2y_1 + y_2y_4 \tag{3.2}$$

by (2.3), (2.4) and (2.5). Similarly

$$y_5 = x_1x_3y_2 + y_1y_4 \tag{3.3}$$

$$y_6 = x_2x_3y_4 + y_1y_2. \tag{3.4}$$

Now, we give some further necessary conditions on A to guarantee that C is extremal:

Lemma 3.1. For the minimum weight of C to be at least 8, the non-units in the same row of A cannot be from the same ideal I_u, I_v, I_{u+v}. Consequently, rows of A cannot contain 0 or uv since they are common to all ideals.

Proof. Assume the non-units of one of the rows are in the same ideal, say, I_u. By multiplying the corresponding row of G by u, a codeword of weight 4 is obtained. □

The equations (3.2), (3.3) and (3.4) force that the pairs $\{y_1,y_3\}$, $\{y_2,y_5\}$ and $\{y_4,y_6\}$ be in the same one of the ideals I_u,I_v,I_{u+v}. Moreover y_2 and y_4 should not be in the same ideal I_u,I_v,I_{u+v}, because if they were, this would mean that y_5 and y_6 would be in the same ideal which is impossible by Lemma 3.1.

Lemma 3.2. For the minimum Lee weight of C to be at least 8, the units x_i must all be chosen from non-basic units.

Proof. Recall that the Lee weight of basic units is 1. So if x_1, say, were a basic unit, for the weight of the first row to be ≥ 8, at least one of the non-units in the first row must be uv,($w_L(uv)=4$) which is impossible by Lemma 3.1. □

To sum up, in order to get a code with minimum weight at least 8, x_i's must all be non-basic units, and without loss of generality, we can take $y_1 \in I'_u = I_u \setminus \{0,uv\}$; $y_2 \in I'_v = I_v \setminus \{0,uv\}$ and $y_4 \in I'_{u+v} = I_{u+v} \setminus \{0,uv\}$.

We can summarize the construction in the following form:

$$A = \begin{bmatrix} \text{non-basic unit} & I'_u & I'_v \\ * & \text{non-basic unit} & I'_{u+v} \\ * & * & \text{non-basic unit} \end{bmatrix}, \tag{3.5}$$

where the entries marked with $*$ are the dependent entries given by the equations (3.2)-(3.4).

As an example we can give the following matrix for A:

$$\begin{bmatrix} 1+uv & u & v \\ u+uv & 1+uv & u+v \\ v+uv & u+v+uv & 1+uv \end{bmatrix}.$$

Remark 3.3. Considering the general form of A obtained in the construction, we have a total of $4\cdot4\cdot4\cdot6\cdot4\cdot2=3072$ different generating matrices in the standard form for the extended binary Golay code over R.

Remark 3.4. If we take the x_i's in the construction described above to be basic units, then we obtain the unique extremal Type I code of parameters $[24,12,6]$.

4 The Minimum Weight

We give an analytical proof that the code generated by $G=[I_3|A]$ with A described as above has minimum Lee weight 8. Consider the rows of G, say r_1,r_2,r_3. First of all, $w_L(r_i)=8$ for $i=1,2,3$. To look at the multiples of the rows, take without loss of generality the first row $r_1=[1,0,0,x_1,y_1,y_2]$ where x_1 is a non-basic unit and $y_1 \in I'_u$ and $y_2 \in I'_v$. If a is a basic unit, then ax_1 is a non-basic unit and ay_1 and ay_2 stay in the same ideals as before so $w_L(ar_1)=8$. Similarly, if a is a non-basic unit we get $w_L(ar_1)=8$. If $a \in I'_u$, then $ay_1=0$ but $ay_2=uv$ and hence $w_L(ar_1)=8$. Similarly, multiplying by all non-units yield weight 8 or 12. This is true for the other rows as well. Now, C is self-dual and all the multiples of generators have weights divisible by 4, which means C must be of Type II. So in order to prove that C has minimum weight 8 all we have to do is to show that we cannot have a weight 4 codeword in C.

Any codeword in C is of the form $\alpha_1r_1+\alpha_2r_2+\alpha_3r_3$, where $\alpha_i \in R$. We have already considered the case where exactly one of the α_i is non-zero.

Next we consider the case where all α_i's are non-zero. We have the following subcases:

Case 1: All α_i's are units. Then all the coordinates of $\overline{c}=\alpha_1r_1+\alpha_2r_2+\alpha_3r_3$ are units and consequently has weight >4.

Case 2: If two of the α_i's are units, then the weight of the first three coordinates ≥ 4 and at least one of the next three coordinates is a unit and hence $w_L(\overline{c})>4$.

Case 3: In the remaining cases the first three coordinates have weight >4.

The last case to consider is when exactly two of the α_i's are non-zero. Without loss of generality, we might assume $\alpha_1,\alpha_2 \neq 0$. If both α_1 and α_2 are units, then $\overline{c}$ has four unit entries and one non-zero entry, so has weight >4. If one of them is a unit and the other a non-unit, the first four coordinates have weight at least 3, and the last coordinate cannot be zero since y_2 and y_4 cannot be in the same ideal. The last coordinate will be a non-zero non-unit and hence will have weight at least 2, forcing the codeword to have weight at least 5. If both α_1 and α_2 are non-units, then the first three coordinates of $\overline{c}$ have weight at least 4 and the last three coordinates cannot be zero at the same time by the constraints given in Lemma 3.1. This completes the proof.

5 Conclusion

The construction of the extended binary Golay code over the ring R described in this work is quite simple since the length of the code to consider is reduced to 6 and the number of generators to consider is reduced to 3 with just one 3×3 matrix determining the code. The special properties of the elements of the ring R help us understand many of the properties of the code quite easily. Thus we were able to obtain a class of generating matrices all of which lead to the extended binary Golay code. We were also able to prove that the minimum weight of the codes obtained from the construction is 8.

Note that, in [9], we gave a linear code over R whose binary image is equivalent to the extended binary Golay code. However, we had obtained that code by just a brute search, and we just gave that as an example without mentioning any of the algebraic structure that we used in this paper. We should also mention that the construction that we give here seems promising in obtaining other codes with good parameters.

A possible future direction for research on this topic could be finding a decoding and encoding algorithm for this construction by using the properties of the ring R. This might prove to be quite useful for engineering purposes.

Acknowledgement

The authors are grateful to the anonymous referees for a careful checking of the details and for helpful comments that improved the presentation of this paper.

References

[1] A. Bonnecaze, P. Solé, C. Bachoc and B. Mourrain, *Type II codes over* $\mathbb{Z}_4$, IEEE Tran. Inform. Theory, **43**, 969–976 (1997).

[2] R. Chapman, *Construction of the Golay codes: A survey*, (1997), [Online]. Available: http://www.secamlocal.ex.ac.uk/people/staff/rjchapma/rjc.html.

[3] C. H. Conway and N. J. A. Sloane, *A new upper bound on the minimal distance of self-dual codes*, IEEE Tran. Inform. Theory, **36**, 1319–1333 (1991).

[4] S.T. Dougherty, P. Gaborit, M. Harada and P. Solé, *Type II codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Infrom. Theory, **45**, 32–45 (1999).

[5] M. J. E. Golay, *Notes on digital coding*, Proc.IRE, **37**, 657 (1949).

[6] I. McLoughlin and T. Hurley, *A Group ring construction of the extended binary Golay code*, IEEE Trans. Infrom. Theory, **54**, 4381–4383 (2008).

[7] X. H. Peng and P. Farrell, *On construction of the* $(24,12,8)$ *Golay codes*, IEEE Trans. Infrom. Theory, **52**, 3669–3675 (2006).

[8] B. Yildiz and S. Karadeniz, *Linear codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des. Codes Cryptogr., **54**, 61–81 (2010).

[9] B. Yildiz and S. Karadeniz, *Self-dual codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, J. Franklin Inst., **347**, 1888–1894 (2010).

Suat Karadeniz is an Assistant Professor of mathematics at Fatih University of Istanbul, Turkey. He received the PhD degree in Mathematics From Fatih University, Istanbul, Turkey. His research interests are in the areas of algebraic coding theory, in particular, codes over rings and self-dual codes.

Bahattin Yildiz is Associate Professor of Mathematics at Fatih University, Istanbul Turkey. He received his PhD degree from California Institute of Technology(CALTECH), CA, USA in 2006. His research interests are in the areas of coding theory and combinatorics.