Experimental constructions of codes over rings and construction of an optimal unimodular lattice in dimension 43

P. Gaborit and A. Otmani
LACO, Université de Limoges,
87060 Limoges, France
e-mail: gaborit@unilim.fr, otmani@unilim.fr

Abstract

In this paper we consider two methods to construct codes over rings. The first method generalizes to rings the constructions of [GO], the second method uses the quadratic double circulant codes of [G]. As an application we extend the tables of best known self-dual codes over the ring $\mathbb{Z}_4 = \mathbb{Z}/(4)$ to length 42 for the Lee and Euclidean distances, we construct a self-dual code over the ring $\mathbb{Z}/(25)$ which gives the first unimodular lattice of dimension 43 and norm 4, and we construct codes over $\mathbb{Z}_4$ of rate $1/2$ which realize some of the best Lee and Hamming minimum distances for lengths 8 to 22.

Keywords : self-dual codes, lattices, codes over rings.

1 General construction

For general definitions and notation related to codes over rings and the different distances we refer to [RS]. In this paper we only consider the Euclidean scalar product.

Let R be a ring. Let C be a self-dual code over R of length n. Let G be a generator matrix of C. Now define $n \times n$ square matrices M_r satisfying for λ_r invertible in R: $M_r \cdot M_r^t = \lambda_r I_n$. For $\Pi_1, \ldots, \Pi_r$ permutations of the symmetric group S_n ($r \geq 1$), we consider the codes C_r with generator matrices G_r: $G_r = GM_1\Pi_1 \cdots M_r\Pi_r$. In fact this action keeps the self-duality of the code as we show it in the next proposition.

Proposition 1 *[GO] If the code C is self-dual then so is C_r.*

Since we are interested in simple constructions of codes, we take all matrices M_i to be equal to a simple matrix M, constructed from smaller square $b_i \times b_i$ matrices B_i ($i = 1, \ldots, p$) satisfying: $B_i \cdot B_i^T = \lambda I_{b_i}$, and from a β in R such that $\beta^2 = \lambda$. Then the block matrix M consists of k_i times the matrix B_i on the diagonal and k_β times β on the diagonal, with $k_\beta + \sum b_i k_i = n$.

Now, we identify the set $\{1, \ldots, n\}$ with the quotient ring $\mathbb{Z}_n$ and we take all the permutations equal to the same permutation π acting on $\mathbb{Z}_n$ as:

$$\forall z \in \mathbb{Z}_n, \quad \pi(z) = a \cdot (z + 1).$$

with a and n coprimes. We say that a code is obtained from construction $(a; r)$ when it is obtained after applying r times the matrice M and the permutation π to the matrix G.

2 Self-dual codes over $\mathbb{Z}_4$

We now consider the particular case of self-dual codes over the ring $\mathbb{Z}_4$. These codes have been classified up to length 15 and bounds for the Lee distance are given in [R], these bounds are tight up to length 24 [RS]. For higher lengths few is known except for lengths a multiple of 8, corresponding to Type II codes. In the following we extend tables of the best Lee and Euclidean distance for self-dual codes of lengths up to length 42.

We denote by O_8, K_4 and A_2 the following matrices corresponding to matrices of self-dual codes:

$$O_8 = \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 1 & 3 & 1 \\ 0 & 1 & 0 & 0 & 3 & 2 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 3 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 \end{pmatrix}, \ K_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{pmatrix} \text{ and } A_2 = (2).$$

We take for G the generator matrix obtained by the direct sum of n_3A_2, n_2K_4 and n_1O_8, with $n_1 = n$ div $8, n_2 = (n \bmod 8)$ div 4 and $n_3 = n \bmod 4$.

For the square $n \times n$ block matrix M, we consider the two matrices B_4 and B_6 defined respectively by:

$$B_4 = \begin{pmatrix} 2 & 1 & 3 & 1 \\ 3 & 2 & 1 & 1 \\ 1 & 3 & 1 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}, \ B_6 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

If n is a multiple of 4, then M is obtained by a sequence of matrices B_4 on the diagonal and else M is built by assuming that each B_i equals to the same matrix B_6 and that $\beta = 1$ with $k_\beta = n \bmod 6$ on the rest of the diagonal.

We give in Table 1 the best Lee distance (d_L) known for self-dual codes of lengths 25 to 42 and we also give their Euclidean distance (d_E). A reference $(a; r)$ in the table precises the construction used to find the code.

n	d_L	d_E	reference
25	8	8	(1;5)
26	8	8	(1;5)
27	8	8	(1;5)
28	10	12	(15;11)
29	10	12	(2;180)
30	10	12	(11;5)
31	12	12	[RS]
32	14	16	[RS]
33	10	12	(1;10)

n	d_L	d_E	reference
34	10	12	(1;10)
35	10	12	(1;10)
36	12	12	(19;44)
37	12	12	(2;1059)
38	12	12	(3;22)
39	14	16	[GH]
40	14	16	(21;223),[RS]
41	12	12	(1;23)
42	12	16	(1;58)

Table 1: Best known Lee and Euclidean distances for self-dual codes over $\mathbb{Z}_4$

3 Self-dual codes over $\mathbb{Z}_{25}$

Self-dual codes over the ring $\mathbb{Z}_{25}$ have not really been studied, in that case no efficient Gray map is known but it is still possible to apply Construction A of [CS] to build unimodular lattices. One obtains for $x = (x_1, \cdots, x_n)$:

$$A_{25}(C) := \frac{1}{5}\{x \in \mathbb{Z}^n | (x_1 \bmod 25, \cdots, x_n \bmod 25) \in C\},$$

and the minimum norm of $A_{25}(C)$ is $min(5, \frac{d_E(C)}{25})$.

We take for generator matrix G of length n the direct sum of $[2,1,2]$ codes with generator matrix $(12,9)$ to which we add the code generated by (5) at the beginning of the diagonal if n is odd. We let:

$$B_3 = \begin{pmatrix} 8 & 9 & 9 \\ 9 & 8 & 9 \\ 9 & 9 & 8 \end{pmatrix}.$$

Then applying different permutations as in the previous section we obtained a code with minimum Euclidean weight 100 with generator matrix $(A_1 A_2)$, where A_1 is a 22×21 matrix composed from the identity matrix of size 21 and a last line of zeros and :

$$A_2 = \begin{pmatrix}
2, 24, 1, 7, 15, 2, 10, 12, 4, 2, 21, 21, 8, 23, 15, 6, 13, 22, 11, 19, 22, 11 \\
0, 16, 0, 18, 21, 2, 8, 19, 23, 4, 4, 5, 21, 3, 7, 7, 8, 2, 18, 8, 0, 22 \\
3, 7, 18, 21, 21, 16, 20, 22, 14, 1, 15, 13, 17, 8, 7, 17, 9, 14, 11, 5, 4, 18 \\
2, 24, 16, 6, 20, 7, 19, 11, 22, 19, 10, 7, 22, 20, 18, 21, 23, 0, 18, 7, 10, 1 \\
1, 4, 20, 17, 4, 20, 16, 11, 19, 7, 11, 3, 2, 7, 14, 12, 4, 4, 21, 13, 18, 24 \\
1, 21, 12, 13, 17, 2, 17, 12, 23, 21, 12, 0, 24, 2, 10, 12, 14, 1, 18, 16, 22, 12 \\
1, 15, 21, 9, 20, 11, 3, 15, 13, 13, 23, 2, 23, 5, 0, 7, 24, 23, 8, 1, 21, 6 \\
4, 6, 4, 22, 24, 16, 8, 0, 21, 4, 18, 11, 19, 7, 7, 16, 15, 9, 7, 12, 1, 3 \\
1, 20, 23, 0, 10, 9, 8, 12, 4, 7, 8, 7, 16, 19, 18, 8, 1, 24, 16, 17, 8, 19 \\
4, 16, 18, 17, 17, 5, 21, 0, 14, 9, 22, 14, 12, 19, 12, 18, 4, 0, 11, 0, 24, 4 \\
0, 12, 14, 6, 11, 14, 20, 20, 24, 20, 6, 9, 8, 24, 15, 0, 3, 21, 8, 8, 21, 23 \\
4, 2, 2, 20, 3, 1, 0, 22, 16, 9, 23, 2, 19, 7, 0, 19, 10, 8, 1, 0, 12, 16 \\
4, 14, 6, 15, 7, 13, 21, 16, 16, 2, 15, 4, 20, 15, 2, 5, 1, 19, 18, 20, 24, 13 \\
1, 19, 5, 22, 23, 5, 15, 16, 21, 0, 12, 23, 23, 10, 0, 10, 24, 11, 17, 20, 5, 17 \\
3, 23, 3, 9, 21, 15, 17, 7, 22, 0, 14, 24, 4, 11, 4, 15, 21, 15, 18, 21, 16, 14 \\
1, 12, 11, 19, 12, 19, 11, 18, 20, 9, 0, 14, 23, 18, 3, 11, 3, 8, 8, 3, 15, 21 \\
2, 5, 8, 20, 14, 8, 14, 10, 2, 19, 2, 0, 21, 7, 0, 20, 1, 15, 4, 7, 5, 0 \\
3, 24, 12, 6, 13, 21, 12, 6, 4, 19, 22, 1, 6, 0, 2, 2, 20, 4, 3, 7, 17, 20 \\
2, 6, 23, 20, 17, 23, 11, 15, 2, 20, 3, 13, 24, 6, 14, 14, 16, 13, 4, 4, 2, 12 \\
0, 17, 9, 17, 14, 17, 5, 20, 15, 7, 14, 23, 2, 15, 9, 6, 16, 23, 11, 4, 2, 22 \\
0, 0, 14, 20, 15, 0, 17, 14, 6, 1, 3, 22, 1, 7, 0, 17, 11, 6, 0, 21, 1, 15 \\
5, 10, 15, 0, 15, 15, 0, 15, 10, 10, 10, 5, 15, 15, 15, 20, 20, 5, 20, 20, 15, 15
\end{pmatrix}.$$

By construction A this code leads to the first extremal unimodular lattice of dimension 43. The only remaining open cases for potential optimal unimodular lattices of norm 4 are dimensions 37 and 41 [NS].

4 Construction of optimal $\mathbb{Z}_4$ codes of rate $1/2$

In [G], quadratic double circulant (QDC) codes were introduced over fields. Although these codes can be generalized over any ring we only consider in this section the case of the ring $\mathbb{Z}_4$. Over $\mathbb{Z}_4$, self-dual QDC codes for lengths a multiple of $2p+2$ with $p = 8k+3$ a prime were considered in [CalS] but it is also possible to consider these codes for other primes, in that case one loses self-duality but one still obtains codes with good parameters, often better or equal than those of self-dual codes for lengths inferior to 23.

For q a power of an odd prime and a, b and c in $\mathbb{Z}_4$ we consider the $q \times q$ quadratic matrix $Q_q(a,b,c)$ and the $(q+1) \times (q+1)$ matrix $S_q(a,b,c)$ (with $\alpha = a, \beta = \gamma = 1$) defined in [G]. We recall that the QDC codes are the codes with generator matrices $P_q(a,b,c) = (I|Q_q(a,b,c))$ and $B_q = (I|S_q(a,b,c))$.

We give in Table 2 the best known Lee distances (d_L), and Hamming distances (d_H) for lengths 8 to 24 of $\mathbb{Z}_4$ codes of rate 1/2. The notation $S(C)$ corresponds to the code obtained after shortening the code C in the first column and adding the all 2 word to the shortened code. The code C_{17} is constructed by taking the extension of the quadratic residue code over $\mathbb{Z}_4$ of length 17 (XQ_{17}) in a cyclic form. The code can then be written in the form (IA) and C_{17} is obtained by multiplying the first row by 2 and then deleting the first column. For length 22 two different codes are given.

n	d_L	d_H	Code
8	6	4	[RS]
9	4	3	$P_5(3,2,1)$
10	5	4	$P_5(0,3,1)$
11	6	3	$S(B_5(0,3,1))$
12	6	4	$B_5(0,3,1)$
13	6	3	$S(P_7(2,3,2))$
14	8	4	$P_7(2,1,3)$
15	6	4	[RS]
16	8	4	[RS]
17	8	5	C_{17}
18	8	6	XQ_{17}
19	6	3	[RS]
20	8	4	[RS]
21	8	5	[RS]
22	10	6	$P_{11}(0,1,2)$
	9	7	$P_{11}(3,2,1)$
23	10	7	[RS]
24	12	8	[RS]

Table 2: Best known codes of rate 1/2 over $\mathbb{Z}_4$ of length 8 to 24

The support of words of fixed Hamming weight of these codes contain in general 1-designs. As in the $GF(2)$ case the supports of words of XQ_{17} with a given Hamming weight hold 2-designs and 3-designs if one considers the reunion with the words of the dual. Also the code of length 10 holds a 3-$(10,5,3)$ design in its words of Hamming weight 5. Although there is a unique linear binary $[28,14,8]$ code, the binary image of the code of length 14 gives a new non-linear $(28,2^{14},8)$ code. It is also worth noticing that the Lee weight distribution of the code of length 11 corresponds to the weight distribution of the unique $[22,11,6]$ self-dual binary code.

REFERENCES

[CalS] A. R. Calderbank and N.J.A. Sloane, "Double circulant codes over $\mathbb{Z}_4$ and unimodular lattices", *J. Alg. Comb.*, **6**, p. 119-131,(1997).

[CS] J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, Springer (1993).

[G] P. Gaborit, "Quadratic Double Circulant Codes over Fields" *J. Combin. Theory Ser. A*, **97**, p. 85-107, (2002).

[GH] A. Gulliver and M. Harada, "An optimal unimodular lattice in dimension 39", *J. Combin. Theory Ser. A*, **88**, p. 158-161, (1999).

[GO] P. Gaborit and A. Otmani, "Experimental constructions of self-dual codes", *submitted to Finite Fields and Th. Appl.*

[NS] G. Nebe and N.J.A. Sloane, "The Catalogue of Lattices", *http://akpublic.research.att.com/ njas/lattices*

[R] E. M. Rains, "Bounds for self-dual codes over $\mathbb{Z}_4$", *Finite Fields and Th. Appl.*, **6**, p. 146-163, (2000).

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