Double and bordered $\alpha$-circulant self-dual codes over finite commutative chain rings

Michael Kiermaier and Alfred Wassermann

Abstract. In this paper we investigate codes over finite commutative rings $R$, whose generator matrices are built from $\alpha$-circulant matrices. For a non-trivial ideal $I \leq R$ we give a method to lift such codes over $R/I$ to codes over $R$, such that some isomorphic copies are avoided.

For the case where $I$ is the minimal ideal of a finite chain ring we refine this lifting method: We impose the additional restriction that lifting preserves self-duality. It will be shown that this can be achieved by solving a linear system of equations over a finite field.

Finally we apply this technique to $\mathbb{Z}_4$-linear double nega-circulant and bordered circulant self-dual codes. We determine the best minimum Lee distance of these codes up to length 64.

1. $\alpha$-circulant matrices

In this section, we give some basic facts on $\alpha$-circulant matrices, compare with [4, chapter 16], where some theory of circulant matrices is given, and with [1, page 84], where $\alpha$-circulant matrices are called $\{k\}$-circulant.

Definition 1.1. Let $R$ be a commutative ring, $k$ a natural number and $\alpha \in R$. A $(k \times k)$-matrix $A$ is called $\alpha$-circulant, if $A$ has the form

$$
\begin{pmatrix}
  a_0 & a_1 & a_2 & \ldots & a_{k-2} & a_{k-1} \\
  \alpha a_{k-1} & a_0 & a_1 & \ldots & a_{k-3} & a_{k-2} \\
  \alpha a_{k-2} & \alpha a_{k-1} & a_0 & \ldots & a_{k-4} & a_{k-3} \\
  \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
  \alpha a_1 & \alpha a_2 & \alpha a_3 & \ldots & \alpha a_{k-2} & a_0
\end{pmatrix}
$$

with $a_i \in R$ for $i \in \{0, \ldots, k-1\}$. For $\alpha = 1$, $A$ is called circulant, for $\alpha = -1$, $A$ is called nega-circulant or skew-circulant, and for $\alpha = 0$, $A$ is called semi-circulant.

An $\alpha$-circulant matrix $A$ is completely determined by its first row $v = (a_0, a_1, \ldots, a_{k-1}) \in R^k$. We denote $A$ by $\text{circ}_\alpha(v)$ and say that $A$ is the $\alpha$-circulant matrix generated by $v$.

In the following, $\alpha$ usually will be a unit or even $\alpha^2 = 1$.

We define $T_\alpha = \text{circ}_\alpha(0, 1, 0, \ldots, 0)$, that is

$$
T_\alpha = \begin{pmatrix}
  1 \\
  1 \\
  \ddots \\
  \alpha \\
  1
\end{pmatrix}
$$
Using $T_\alpha$, there is another characterization of an $\alpha$-circulant matrix: A matrix $A \in R^{k \times k}$ is $\alpha$-circulant iff $AT_\alpha = T_\alpha A$. This is seen directly by comparing the components of the two matrix products.

In the following it will be useful to identify the generating vectors $(a_0, a_1, \ldots, a_{k-1}) \in R^n$ with the polynomials $\sum_{i=0}^{k-1} a_i x^i \in R[x]$ of degree at most $k - 1$, which again can be seen as a set of representatives of the $R$-algebra $R[x]/(x^k - \alpha)$. Thus, we get an injective mapping $\text{circ}_\alpha : R[x]/(x^k - \alpha) \to R^{k \times k}$.

Obviously $\text{circ}_\alpha(1) = I_k$, which denotes the $(k \times k)$-unit matrix, $\text{circ}_\alpha(\lambda f) = \lambda \text{circ}_\alpha(f)$ and $\text{circ}_\alpha(f + g) = \text{circ}_\alpha(f) + \text{circ}_\alpha(g)$ for all scalars $\lambda \in R$ and all $f$ and $g$ in $R[x]/(x^k - \alpha)$. Furthermore, it holds $\text{circ}_\alpha(e_i) = \text{circ}_\alpha(x^i) = T^\alpha_{i}$ for all $i \in \{0, \ldots, k - 1\}$ and $\text{circ}_\alpha(x^k) = \text{circ}_\alpha(\alpha) = \alpha I_k = T^\alpha_0$, where $e_i$ denotes the $i$th unit vector. So we have $\text{circ}_\alpha(x^i x^j) = \text{circ}_\alpha(x^i) \text{circ}_\alpha(x^j)$ for all $\{i, j\} \subset \mathbb{N}$. By linear extension it follows that $\text{circ}_\alpha$ is a monomorphism of $R$-algebras. Hence the image of $\text{circ}_\alpha$, which is the set of the $\alpha$-circulant $(k \times k)$-matrices over $R$, forms a commutative subalgebra of the $R$-algebra $R^{k \times k}$ and it is isomorphic to the $R$-algebra $R[x]/(x^k - \alpha)$. Especially, we get $\text{circ}_\alpha(a_0, \ldots, a_{k-1}) = \sum_{i=0}^{k-1} a_i T^\alpha_i$.

2. Double $\alpha$-circulant and bordered $\alpha$-circulant codes

DEFINITION 2.1. Let $R$ be a commutative ring and $\alpha \in R$. Let $A$ be an $\alpha$-circulant matrix. A code generated by a generator matrix

$$(I_k | A)$$

is called double $\alpha$-circulant code. A code generated by a generator matrix

$$
\begin{pmatrix}
\beta & \gamma & \cdots & \gamma \\
\delta & & & \\
I_k & & & A \\
\delta & & & \\
\end{pmatrix}
$$

with $\{\beta, \gamma, \delta\} \subset R$ is called bordered $\alpha$-circulant code. The number of rows of such a generator matrix is denoted by $k$, and the number of columns is denoted by $n = 2k$.

As usual, two codes $C_1$ and $C_2$ are called equivalent or isomorphic, if there is a monomial transformation that maps $C_1$ to $C_2$. 

DEFINITION 2.2. Let $R$ be a commutative ring and $k \in \mathbb{N}$. The symmetric group over the set $\{0, \ldots, k - 1\}$ is denoted by $S_k$. For a permutation $\sigma \in S_k$ the permutation matrix $S(\sigma)$ is defined as $S_{ij} = \delta_{i, \sigma(j)}$, where $\delta$ is the Kronecker delta. An invertible matrix $M \in \text{GL}(k, R)$ is called monomial, if $M = S(\sigma) D$ for a permutation $\sigma \in S_k$ and an invertible diagonal matrix $D$. The decomposition of a monomial matrix into the permutational and the diagonal matrix part is unique.

Let $\mathfrak{M} = \mathfrak{M}(k, R, \alpha)$ be the set of all pairs $(N, M)$ of monomial $(k \times k)$-matrices $M$ and $N$ over $R$, such that for each $\alpha$-circulant matrix $A \in R^{k \times k}$, the matrix $N^{-1}AM$ is again $\alpha$-circulant. An element $(N, M)$ of $\mathfrak{M}$ can be interpreted as a mapping $R^{k \times k} \to R^{k \times k}$, $A \mapsto N^{-1}AM$. The composition of mappings implies a group structure on $\mathfrak{M}$, and $\mathfrak{M}$ operates on the set of all $\alpha$-circulant matrices.

Now let $(N, M) \in \mathfrak{M}$. The codes generated by $(I | A)$ and by $(I | N^{-1}AM)$ are equivalent, since

$$
N^{-1}(I | A) \begin{pmatrix} N & 0 \\ 0 & M \end{pmatrix} = (I | N^{-1}AM)
$$

\footnote{Throughout this article, counting starts at 0. Accordingly, $\mathbb{N} = \{0, 1, 2, \ldots\}$}
and the matrix \( \begin{pmatrix} N & 0 \\ 0 & M \end{pmatrix} \) is monomial. Thus, \( \mathfrak{M} \) also operates on the set of all double \( \alpha \)-circulant generator matrices.

In general \( \mathfrak{M} \)-equivalence is weaker than the code equivalence: For example the vectors \( v = (1111101011011010) \in \mathbb{Z}_2^{16} \) and \( w = (1110010011100000) \in \mathbb{Z}_2^{16} \) generate two equivalent binary double circulant self-dual \([32, 16]\)-codes. But since the number of zeros in \( v \) and \( w \) is different, the two circulant matrices generated by \( v \) and \( w \) cannot be in the same \( \mathfrak{M} \)-orbit.

3. Monomial transformations of \( \alpha \)-circulant matrices

Let \( R \) be a commutative ring, \( k \in \mathbb{N} \) and \( \alpha \in R \) a unit. In this section we give some elements \((N, M)\) of the group \( \mathfrak{M} = \mathfrak{M}(R, k, \alpha) \) defined in the last section. In part they can be deduced from [4, chapter 16, §6, problem 7].

Quite obvious elements of \( \mathfrak{M} \) are \((I_k, T_\alpha)\), \((T_\alpha, I_k)\), \((I_k, D)\) and \((D, I_k)\), where \( D \) denotes an invertible scalar matrix.

For certain \( \alpha \) further elements of \( \mathfrak{M} \) are given by the following lemma, which is checked by a calculation:

**Lemma 3.1.** Let \( \alpha \in R \) with \( \alpha^2 = 1 \) and \( s \in \{0, \ldots, k - 1\} \) with \( \gcd(s, k) = 1 \). Let \( \sigma = (i \mapsto si \mod k) \in S_k \). We define \( D \) as the diagonal matrix which has \( \alpha^{((s+1)i+[s/k])} \) as \( i \)-th diagonal entry, and we define the monomial matrix \( M = S(\sigma)D \). Then \((M, M) \in \mathfrak{M}\)

More specifically: Let \( f \in R[x]/(x^k - \alpha) \). It holds:

\[
M^{-1} \text{circ}_\alpha(f)M = \text{circ}_\alpha(f((\alpha x)^s))
\]

Finally, there is an invertible transformation \( A \mapsto M^{-1}AM \) that converts an \( \alpha \)-circulant matrix into a \( \beta \)-circulant matrix for certain pairs \((\alpha, \beta)\):

**Lemma 3.2.** Let \( R \) be a commutative ring, \( \alpha \in R \) a unit and \( \{i, j\} \subset \mathbb{N} \). Let \( A \) be an \( \alpha^i \)-circulant \((k \times k)\)-matrix over \( R \) and \( M \) the diagonal matrix with the diagonal vector \((1, \alpha^j, \alpha^{2j}, \ldots, \alpha^{(k-1)j})\). Then \( M^{-1}AM \) is an \( \alpha^{i-j} \)-circulant matrix. For \( \alpha^2 = 1 \) the matrix \( M \) is orthogonal.

4. The lift of an \( \alpha \)-circulant matrix

If we want to construct all equivalence classes of double \( \alpha \)-circulant codes over a commutative ring \( R \), it is enough to consider orbit representatives of the group action of \( \mathfrak{M} \) on the set of all double \( \alpha \)-circulant generator matrices, or equivalently, on the set of all \( \alpha \)-circulant matrices.

Furthermore, we can benefit from non-trivial ideals of \( R \): Let \( I \) be an ideal of \( R \) with \( \{0\} \neq I \neq R \), and \( \overline{\cdot} : R \rightarrow R/I \) the canonical projection of \( R \) onto \( R/I \). We set \( \mathfrak{M} = \mathfrak{M}(k, R, \alpha) \) and \( \mathfrak{M} = \{(N, M) : (N, M) \in \mathfrak{M}\} \). It holds \( \mathfrak{M} \subseteq \mathfrak{M}(k, R/I, \overline{\alpha}) \). Let \( e : R/I \rightarrow R \) be a mapping that maps each element \( r + I \) of \( R/I \) to a representative element \( r \in R \).

**Definition 4.1.** Let \( A = \text{circ}_\alpha(v) \) be an \( \overline{\alpha} \)-circulant matrix with generating vector \( v \in R/I \). An \( \alpha \)-circulant matrix \( B \) over \( R \) is called lift of \( A \), if \( B = A \). In this case we also say that the code generated by \((I_k | B)\) is a lift of the code generated by \((I_k | A)\). The lifts of \( A \) are exactly the matrices of the form \( \text{circ}_\alpha(e(v)) + \text{circ}_\alpha(w) \) with \( w \in I^k \). The vector \( w \) is called lift vector.

---

2To avoid confusion, we point out that \( I^k \) denotes the \( k \)-fold Cartesian product \( I \times \ldots \times I \) here.
To find all double $\alpha$-circulant codes over $R$, we can run over all lifts of all double $\bar{\alpha}$-circulant codes over $R/I$. The crucial point now is that for finding at least one representative all equivalence classes of double $\alpha$-circulant codes over $R$, it is enough to run over the lifts of a set of representatives of the group action of $\mathfrak{M}$ on the set of all $\bar{\alpha}$-circulant codes over $R/I$:

**Lemma 4.1.** Let $A$ and $B$ be two $\bar{\alpha}$-circulant matrices over $R/I$ which are in the same $\mathfrak{M}$-orbit. Then for each lift of $A$ there is a lift of $B$ which is in the same $\mathfrak{M}$-orbit.

**Proof.** Because $A$ and $B$ are in the same $\mathfrak{M}$-orbit, there is a pair of monomial matrices $(N, M) \in \mathfrak{M}$ such that $N^{-1}AM = B$. Let $a \in (R/I)^k$ be the generating vector of $A$ and $b \in (R/I)^k$ the generating vector of $B$. Since $\text{circ}_\alpha(e(a)) = A$ and $\text{circ}_\alpha(e(b)) = B$ it holds $N^{-1}\text{circ}_\alpha(e(a))M = \text{circ}_\alpha(e(b)) + K$, where $K \in I^{k \times k}$. $\text{circ}_\alpha(e(b))$ is of course $\alpha$-circulant, and $N^{-1}\text{circ}_\alpha(e(a))M$ is $\alpha$-circulant because of $(N, M) \in \mathfrak{M}$. Thus, also $K$ is $\alpha$-circulant and therefore there is a $z \in I^k$ with $\text{circ}_\alpha(z) = K$.

Now, let $w \in I^k$ be some lift vector. $N^{-1}\text{circ}_\alpha(w)M \in I^{k \times k}$ is $\alpha$-circulant and generated by a lift vector $w' \in I^k$. Then $N^{-1}(\text{circ}_\alpha(e(a)) + \text{circ}_\alpha(w))M = \text{circ}_\alpha(e(b)) + \text{circ}_\alpha(z + w')$, and $z + w' \in I^k$. Therefore, the lift of $A$ by the lift vector $w$ and the lift of $B$ by the lift vector $z + w'$ are in the same $\mathfrak{M}$-orbit. \qed

It is not hard to adapt this approach to bordered $\alpha$-circulant codes. One difference is an additional restriction on the appearing monomial matrices: Its diagonal part must be a scalar matrix. The reason for this is that otherwise the monomial transformations would destroy the border vectors $(\gamma \ldots \gamma)$ and $(\delta \ldots \delta)^t$.

Circulant matrices are often used to construct self-dual codes. Thus we are interested in a fast way to generate the lifts that lead to self-dual codes. The next section gives such an algorithm for the case that $R$ is a finite chain ring and $I$ is its minimal ideal.

### 5. Self-dual double $\alpha$-circulant codes over finite commutative chain rings

We want to investigate self-dual double $\alpha$-circulant codes. Here we need $\alpha^2 = 1$. This is seen by denoting the rows of a generator matrix $G$ of such a code by $w_0 \ldots w_{k-1}$, and by comparing the scalar products $\langle w_0, w_i \rangle$ and $\langle w_1, w_2 \rangle$, which must be both zero. Furthermore, given $\alpha^2 = 1$, we see that $\langle w_0, w_i \rangle = \langle w_j, w_{i+j} \rangle$, where $i + j$ is taken modulo $k$. Thus $G$ generates a self-dual code if $\langle w_0, w_0 \rangle = 1$ and for all $j \in \{1, \ldots, [k/2]\}$ the scalar products $\langle w_0, w_j \rangle$ are equal to 0.

**Definition 5.1.** A ring $R$ is called *chain ring*, if its left ideals are linearly ordered by inclusion.

For the theory of finite chain rings and linear codes over finite chain rings see [2].

In this section $R$ will be a finite commutative chain ring, which is not a finite field, and $\alpha$ an element of $R$ with $\alpha^2 = 1$. There is a ring element $\theta \in R$ which generates the maximal ideal $R\theta$ of $R$. The number $q$ is defined by $R/R\theta \cong \mathbb{F}_q$, and $m$ is defined by $|R| = q^m$. Because $R$ is not a field, we have $m \geq 2$. The minimal ideal of $R$ is $R\theta^{m-1}$. $\mathfrak{M}$ is defined as in section [2] with with the difference that all monomial matrices $M$ should be orthogonal, that is $MM^t = I_k$.

Thus each $\mathfrak{M}$-image of a generator matrix of a self-dual code again generates a self-dual code. Now let $I = R\theta^{m-1}$ be the minimal ideal of $R$. As in section [4] let $e : R/I \rightarrow R$ be a mapping that assigns each element of $R/I$ to a representative in $R$, now with the additional condition $e(\bar{\alpha}) = \alpha$. 


We mention that if \((I_k | B)\) generates a double \(\alpha\)-circulant self-dual code over \(R\), then \((I_k | \bar{B})\) generates a double \(\tilde{\alpha}\)-circulant self-dual code over \(R/I\). So \(B\) is among the lifts of all \(\tilde{\alpha}\)-circulant matrices \(A\) over \(R/I\) such that \((I_k | A)\) generates a self-dual double \(\tilde{\alpha}\)-circulant code. Let \(A = \text{circ}_\alpha(a)\) be an \(\tilde{\alpha}\)-circulant matrix over \(R/I\) such that \((I_k | A)\) generates a self-dual code. So \(AA^t = -I_k\), and therefore

\[
c_0 := 1 + \sum_{i=0}^{k-1} e(a_i)^2 \quad \text{and}
\]

\[
c_j := \sum_{i=0}^{j-1} \alpha e(a_i) e(a_{k-j+i}) + \sum_{i=j}^{k-1} e(a_i) e(a_{i-j}) \quad \text{for all } j \in \{1, \ldots, \lfloor k/2 \rfloor \}
\]

We want to find all lifts \(B = \text{circ}_\alpha(e(a)) + \text{circ}_\alpha(w)\) of \(A\) with \(w \in I^k\) such that \(BB^t = -I_k\). As we have seen, this is equivalent to

\[
0 = 1 + \sum_{i=0}^{k-1} (e(a_i) + w_i)^2 \quad \text{and}
\]

\[
0 = \sum_{i=0}^{j-1} (e(a_i) + w_i)(\alpha e(a_{k-j+i}) + w_{k-j+i}) + \sum_{i=j}^{k-1} (e(a_i) + w_i)(e(a_{i-j}) + w_{i-j})
\]

where the second equation holds for all \(j \in \{1, \ldots, \lfloor k/2 \rfloor \}\). Using \(I \cdot I = 0\), we get

\[
0 = c_0 + 2 \sum_{i=0}^{k-1} e(a_i)w_i \quad \text{and}
\]

\[
0 = c_j + \sum_{i=0}^{j-1} (e(a_i)w_{k-j+i} + \alpha e(a_{k-j+i})w_i) + \sum_{i=j}^{k-1} (e(a_i)w_{i-j} + e(a_{i-j})w_i)
\]

This is a \(R\)-linear system of equations for the components \(w_i \in I\) of the lift vector. Using the fact that the \(R\)-modules \(R/(R\theta)\) and \(I\) are isomorphic, and \(R/(R\theta) \cong F_q\), this can be reformulated as a linear system of equations over the finite field \(F_q\), which can be solved efficiently. Since \(R/I\) is again a commutative chain ring, the lifting step can be applied repeatedly. Thus, starting with the codes over \(F_q\), the codes over \(R\) can be constructed by \(m-1\) nested lifting steps.

Again, this method can be adapted to bordered \(\alpha\)-circulant matrices over commutative finite chain rings.

6. Application: Self-dual codes over \(\mathbb{Z}_4\)

For a fixed length \(n\) we want to find the highest minimum Lee distance \(d_{\text{Lee}}\) of double nega-circulant and bordered circulant self-dual codes over \(\mathbb{Z}_4\). In \([5]\) codes of the bordered circulant type of length up to 32 were investigated.

First we notice that the length \(n\) must be a multiple of 8: Let \(C\) be a bordered circulant or a double nega-circulant code of length \(n\) and \(c\) a codeword of \(C\). We have \(0 = \langle c, c \rangle = \sum_{i=0}^{n-1} c_i^2 \in \mathbb{Z}_4\). The last expression equals the number of units in \(c\) modulo 4, so the number of units of each codeword is a multiple of 4. It follows that the image \(C\) of \(C\) over \(\mathbb{Z}_2\) is a doubly-even self-dual code of length \(n\), which can only exist for lengths \(n\) divisible by 8.

Furthermore, it holds

\[
d_{\text{Lee}}(C) \leq 2d_{\text{Ham}}(\bar{C})
\]

(1)
As a result, we only need to consider the lifts of codes $\tilde{C}$ which have a sufficiently high minimum Hamming distance.

We explain the algorithm for the case of the nega-circulant codes: In a first step, for a given length $n$ we generate all doubly-even double circulant self-dual codes over $\mathbb{Z}_2$. This is done by enumerating Lyndon words of length $n$ which serve as generating vectors for the circulant matrix. Next, we filter out all duplicates with respect to the group action of $\mathcal{M}$, where $\mathcal{M}$ is the group generated by the elements given in section 3 which consist of pairs of orthogonal monomial matrices.

A variable $d$ will keep the best minimum Lee distance we already found. We initialize $d$ with 0. Now we loop over all binary codes $C_{\mathbb{Z}_2}$ in our list, from the higher to the lower minimum Hamming distance of $C_{\mathbb{Z}_2}$: If $2d_{\text{Ham}}(C_{\mathbb{Z}_2}) \leq d$ we are finished because of (1). Otherwise, as explained in section 5, we solve a system of linear equations over $\mathbb{Z}_2$ and get all self-dual lifts of $C_{\mathbb{Z}_2}$. For these lifts we compute the minimum Lee distance and update $d$ accordingly.

Most of the computation time is spent on the computation of the minimum Lee distances. Thus it was a crucial point to write a specialized algorithm for this purpose. It is described in [3].

The results of our search are displayed in the following table. For given length $n$, it lists the highest minimum Lee distance of a self-dual code of the respective type:

| $n$ | 8   | 16  | 24  | 32  | 40  | 48  | 56  | 64  |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|
|     | 6   | 8   | 12  | 14  | 14  | 18  | 16  | 20  |
|     | 6   | 8   | 12  | 14  | 14  | 18  | 18  | 20  |

We see that the results are identical for the two classes of codes, except for length 56. Using (1) there is a simple reason that for this length no double circulant self-dual code over $\mathbb{Z}_4$ with minimum Lee distance greater than 16 exists: The best doubly-even double circulant self-dual binary code has only minimum Hamming distance 8.

Acknowledgment

This research was supported in part by Deutsche Forschungsgemeinschaft WA 1666/4-1.

References

[1] Philip J. Davis. *Circulant Matrices*. Chelsea publishing, New York, second edition, 1994.
[2] Thomas Honold and Ivan Landjev. Linear codes over finite chain rings. *Electr. J. Comb.*, 7, 2000.
[3] Michael Kiermaier and Alfred Wassermann. On the Minimum Lee Distance of Quadratic Residue Codes over $\mathbb{Z}_4$. In *Proceedings of the International Symposium on Information Theory (ISIT)*, 2008. to appear.
[4] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977.
[5] Masaaki Harada T. Aaron Gulliver. Extremal double circulant Type II codes over $\mathbb{Z}_4$ and construction of 5-(24, 10, 36) designs. *Discrete Mathematics*, 194:129–137, 1999.

Michael Kiermaier, Mathematical Department, University of Bayreuth, D-95440 Bayreuth, Germany

E-mail address: michael.kiermaier@uni-bayreuth.de

URL: http://www.mathe2.uni-bayreuth.de/michaelk/

Alfred Wassermann, Mathematical Department, University of Bayreuth, D-95440 Bayreuth, Germany

E-mail address: alfred.wassermann@uni-bayreuth.de

URL: http://did.mat.uni-bayreuth.de/~alfred/home/index.html