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

Michael Kiermaier

Department of Mathematics
Universität Bayreuth

Eleventh International Workshop on Algebraic and Combinatorial Coding Theory ACCT2008

joint work with Alfred Wassermann, Bayreuth
Definition

- $R$ a finite commutative ring with 1.
- $\alpha \in R$.
- Let $v = (v_0, v_1, \ldots, v_{k-1}) \in R^k$.

$\alpha$-circulant matrix generated by $v$:

$$\text{circ}_\alpha(v) = \begin{pmatrix}
 v_0 & v_1 & v_2 & \ldots & v_{k-2} & v_{k-1} \\
 \alpha v_{k-1} & v_0 & v_1 & \ldots & v_{k-3} & v_{k-2} \\
 \alpha v_{k-2} & \alpha v_{k-1} & v_0 & \ldots & v_{k-4} & v_{k-3} \\
 \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
 \alpha v_{1} & \alpha v_{2} & \alpha v_{3} & \ldots & \alpha v_{k-1} & v_0 
\end{pmatrix}$$

- For $\alpha = 1$: circulant matrix
- For $\alpha = -1$: nega-circulant or skew-circulant matrix.
Double $\alpha$-circulant codes

Definition

Let $A \in R^{k \times k} = \text{circ}_\alpha(v)$ an $\alpha$-circulant matrix. A code $C \subseteq R^{2k}$ with generator matrix $(I_k | A)$ is called double $\alpha$-circulant code with generating word $v$.

$C$ self-dual

$\iff (I_k | A)(I_k | A)^t = 0$

$\iff AA^t = -I_k$. 

Michael Kiermaier

Double and bordered $\alpha$-circulant self-dual codes
The case $R = \mathbb{Z}_4$

**Definition**

- **$\mathbb{Z}_4$-linear code**: submodule of $\mathbb{Z}_4^n$
- **Lee weight $w_{\text{Lee}} : \mathbb{Z}_4 \rightarrow \mathbb{N}$**, \[
\begin{align*}
0 &\mapsto 0 \\
1, 3 &\mapsto 1 \\
2 &\mapsto 2
\end{align*}
\]
- Defined as usual: **Lee weight $w_{\text{Lee}}$ on $\mathbb{Z}_4^n$, Lee distance $d_{\text{Lee}}$ on $\mathbb{Z}_4^n \times \mathbb{Z}_4^n$, minimum Lee distance of a $\mathbb{Z}_4$-linear code.**
- **ring homomorphism "modulo 2":**
  \[
  \gamma : \mathbb{Z}_4 \rightarrow \mathbb{F}_2, \quad \begin{align*}
  0, 2 &\mapsto 0 \\
  1, 3 &\mapsto 1
  \end{align*}
  \]

**Goal**

We look for $\alpha$-circulant self-dual codes $C$ over $\mathbb{Z}_4$ with high minimum Lee distance!
Restrictions on the parameters

Restrictions on $\alpha$

- For $\alpha \in \{0, 2\}$: $d_{\text{Lee}}(C) \leq 4$.
- For $\alpha = 1$: $C$ cannot be self-dual.
- $\Rightarrow$ Only interesting case: $\alpha = -1$.

Restrictions on the length $n$

For each $c \in C$: $\sum_{i=0}^{n-1} c_i^2 = 0$

$\Rightarrow$ The number of units in $c$ is a multiple of 4.

$\Rightarrow$ $\gamma(C)$ is a binary self-dual doubly-even code.

$\Rightarrow$ $n$ is divisible by 8.

In the following: Let $k$ be a fixed dimension divisible by 4, $n = 2k$. 

Michael Kiermaier  
Double and bordered $\alpha$-circulant self-dual codes
**Definition**

- Let $V_4 \subseteq \mathbb{Z}_4^k$ be the set of all words generating self-dual double nega-circulant codes over $\mathbb{Z}_4$.
- Let $V_2 \subseteq \mathbb{F}_2^k$ be the set of all words generating self-dual doubly-even double circulant codes over $\mathbb{F}_2$.

It holds: $\gamma(V_4) \subseteq V_2$.

**Goal**

Find (the interesting part of) $V_4$. 

---

**Introduction**

- The construction algorithm
- Results

**Circulant matrices**

- The case $R = \mathbb{Z}_4$
Outline of the construction

Idea for the construction

- Construct $V_2$.
- **Lifting:**
  For each $v \in V_2$, find $\gamma^{-1}(v) \cap V_4$.
  Equivalently:
  Find all lift vectors $w \in \mathbb{F}_2^k$ such that $v + 2w \in V_4$.

Observation

The second step is time critical.
We need a fast algorithm!
The lifting step

- Given: $v \in V_2$.
  Let $\tilde{C}$ be the double circulant doubly-even self-dual binary code generated by $v$.
- Wanted: All lift vectors $w \in \mathbb{F}_2^k$ such that $v + 2w \in V_4$.
- Equivalently:
  \[
  \sum_{i=0}^{k-1} (v + 2w)^2_i = -1 \in \mathbb{Z}_4
  \]
  and
  \[
  \sum_{i=0}^{k-1-t} (v + 2w)_i (v + 2w)_{i+t} - \sum_{i=k-t}^{k-1} (v + 2w)_i (v + 2w)_{i+t} = 0 \in \mathbb{Z}_4
  \]
  for all $t \in \{1, \ldots, k/2\}$.
- Since $\tilde{C}$ is doubly-even $\Rightarrow$ First equation is always true.
Using $2^2 = 0_{\mathbb{Z}_4}$, the equations for $t \in \{1, \ldots, k/2\}$ are equivalent to:

$$\sum_{i=0}^{k-1-t} v_i v_{i+t} - \sum_{i=k-t}^{k-1} v_i v_{i+t} + 2 \sum_{i=0}^{k-1} (v_i w_{i+t} + v_{i+t} w_i) = 0_{\mathbb{Z}_4}$$

which is equivalent to $0 \pmod{2}$ since $\tilde{C}$ is self-dual.

Defining $(b_1, \ldots, b_{k-1}) \in \mathbb{F}_2^{k-1}$ by

$$2b_t = \sum_{i=0}^{k-1-t} v_i v_{i+t} - \sum_{i=k-t}^{k-1} v_i v_{i+t}$$

this gives

$$2 \sum_{i=0}^{k-1} (v_i w_{i+t} + v_{i+t} w_i) = 2b_t \quad \text{for all } t \in \{1, \ldots, k/2\}$$
That leads to

\[ \sum_{i=0}^{k-1} (v_i w_{i+t} + v_{i+t} w_i) = b_t \]

which is a linear system of equations for the \( w_i \) over the finite field \( \mathbb{F}_2 \).

**Conclusion**

- For a given vector \( v \in V_2 \), the possible lift vectors \( w \in \mathbb{F}_2^k \) can be computed by solving a linear system of equations over \( \mathbb{F}_2 \).
- The dimension of the solution space is \( k/2 \).
Lemma (compare MacWilliams/Sloane 1977)

Let \( \sigma : \mathbb{Z}_4^k \rightarrow \mathbb{Z}_4^k \) a mapping of one of the following types:

- \( \sigma(v) = -v \).
- \( \sigma(v) \) is a cyclic shift of \( v \).
- There is an \( s \in \{1, \ldots, k-1\} \) with \( \gcd(s, k) = 1 \) such that for all \( i \): \( \sigma(v)_i = v_{si} \).

Then the nega-circulant codes generated by the vectors \( v \) and \( \sigma(v) \) are equivalent.

Definition

Let \( G \) be the group generated by these mappings \( \sigma \).
Updated algorithm

**Observation**
- $G$ operates on $V_4$. One representative of each orbit is enough!
- $\gamma(G)$ operates on $V_2$.

**Updated construction algorithm**
- Construct exactly one representative of each orbit under the action of $\gamma(G)$ on $V_2$.
- **Lifting:** For each such $\gamma(G)$-representative $v$, find a representative of all $G$-orbits on the lift vectors $w \in \mathbb{F}_2^k$ with $v + 2w \in V_4$. 

Michael Kiermaier
Double and bordered $\alpha$-circulant self-dual codes
Lifting and the minimum distance

Lemma

Let $C$ be a $\mathbb{Z}_4$-linear code. It holds:

$$d_{\text{Ham}}(\gamma(C)) \leq d_{\text{Lee}}(C) \leq 2d_{\text{Ham}}(\gamma(C))$$

Updated lifting step

- During the algorithm:
  The variable $\delta$ stores the best minimum Lee distance found so far.

- **Lifting:** Run through the $\gamma(G)$-representatives $v$ of $V_2$, ordered by decreasing minimum Hamming weight $d_2(v)$ of the binary code generated by $v$. As soon as $d_2(v) \leq \delta$, we are finished.
Best possible Lee distances among all self-dual $\mathbb{Z}_4$-linear self-dual codes of the respective type:

<table>
<thead>
<tr>
<th>$n$</th>
<th>8</th>
<th>16</th>
<th>24</th>
<th>32</th>
<th>40</th>
<th>48</th>
<th>56</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>double nega-circulant</td>
<td>6</td>
<td>8</td>
<td>12</td>
<td>14</td>
<td>14</td>
<td>18</td>
<td>16</td>
<td>20</td>
</tr>
<tr>
<td>bordered circulant</td>
<td>6</td>
<td>8</td>
<td>12</td>
<td>14</td>
<td>14</td>
<td>18</td>
<td>18</td>
<td>20</td>
</tr>
</tbody>
</table>

Bordered circulant: Generated by

$$
\begin{pmatrix}
\alpha & \beta \cdots \beta \\
\gamma \\
\vdots \\
\gamma \\
\end{pmatrix}
$$

where $A$ is $(k - 1) \times (k - 1)$ circulant, and $\alpha, \beta, \gamma$ suitable.
Most computation time goes into the computation of the minimum Lee distances. A fast algorithm was crucial. For $n = 64$: About 10 times faster than the algorithm in Magma.

This algorithm allowed us to compute some previously unknown minimum Lee distances of $\mathbb{Z}_4$-linear QR-codes.
Generalizations of the construction method

- Instead of only \( \mathbb{Z}_4 \): Can be done for all finite commutative chain rings.
  Example \( \mathbb{Z}_8 \): Two nested lifting steps \( \mathbb{F}_2 \rightarrow \mathbb{Z}_4 \rightarrow \mathbb{Z}_8 \).
- Direct adaption to bordered circulant \( \alpha \)-circulant self-dual codes.
Thanks for your attention!