Construction of Linear Codes using Cyclic and Dihedral Group Algebras (Part 2)

Fergal Gallagher

Institute of Technology Sligo
Ireland

Joint work with Leo Creedon and Ian McLoughlin

CIMPA Research School:
Algebraic Methods in Coding Theory
Ubatuba, Sao Paolo, Brazil
July 11, 2017

In this talk I will:

- Recall the use of a group ring matrix to generate a code.
- Recap on the motivation for finding $V_*(F_2C_{48})$.
- Give the structure of $V_*(F_2C_{48})$.
- Show how to reduce the search by ignoring equivalent codes.
- Show how to reduce the search further by ignoring elements of order dividing 8.
- Conclude. Discuss further work.

Let RG be a group ring with $|G| = n$.
Then for each element u of the group ring RG there is a unique $n \times n$ matrix U with coefficients from R according to a particular listing of the group elements $g_1, g_2, ..., g_n$.

The column headings are the group elements according to the group listing, and the row headings are the inverses of the group elements in the listing.

The entries of the matrix U consist of the product of the row and column headings.

Let RG be a group ring with $|G| = n$.
Then for each element u of the group ring RG there is a unique $n \times n$ matrix U with coefficients from R according to a particular listing of the group elements $g_1, g_2, ..., g_n$.

The column headings are the group elements according to the group listing, and the row headings are the inverses of the group elements in the listing.

The entries of the matrix U consist of the product of the row and column headings.

Let RG be a group ring with $|G| = n$.
Then for each element u of the group ring RG there is a unique $n \times n$ matrix U with coefficients from R according to a particular listing of the group elements $g_1, g_2, ..., g_n$.

The column headings are the group elements according to the group listing, and the row headings are the inverses of the group elements in the listing.

The entries of the matrix U consist of the product of the row and column headings.

Example

Let $u \in F_2 D_{96}$, where $D_{96} = \langle b, y | b^{48} = y^2 = 1, b^y = b^{-1} \rangle$.
Suppose $u = 1 + yv$ where $v \in F_2 C_{48}$.
Then $rank(U) = 48$.
Also $U = U^T$ because it is of the form

$$\begin{bmatrix} I & A \\ A & I \end{bmatrix}$$

where I is the identity matrix and $A^T = A$.

Now we want $U^2 = 0$, so that every row of U is orthogonal to every other row. Then the code generated by U will be a self dual code.

$U^2 = 0 \Leftrightarrow u^2 = 0 \Leftrightarrow (1 + yv)(1 + yv) = 0 \Leftrightarrow$
$1 + 2(yv) + yvyv = 0 \Leftrightarrow 1 + 0 + yyv^* v = 0 \Leftrightarrow v^* v = 1.$

Thus u generates a code which is self-dual if and only if $v \in V_*(F_2 C_{48})$.
That is a self-dual $[96, 48, d]$ code for some minimum distance d.

Now we want $U^2 = 0$, so that every row of U is orthogonal to every other row. Then the code generated by U will be a self dual code.

$$U^2 = 0 \Leftrightarrow u^2 = 0 \Leftrightarrow (1 + yv)(1 + yv) = 0 \Leftrightarrow$$
$$1 + 2(yv) + yvyv = 0 \Leftrightarrow 1 + 0 + yyv^* v = 0 \Leftrightarrow v^* v = 1.$$

Thus u generates a code which is self-dual if and only if $v \in V_*(F_2 C_{48})$.
That is a self-dual $[96, 48, d]$ code for some minimum distance d.

Now we want $U^2 = 0$, so that every row of U is orthogonal to every other row. Then the code generated by U will be a self dual code.

$$U^2 = 0 \Leftrightarrow u^2 = 0 \Leftrightarrow (1 + yv)(1 + yv) = 0 \Leftrightarrow$$
$$1 + 2(yv) + yvyv = 0 \Leftrightarrow 1 + 0 + yyv^*v = 0 \Leftrightarrow v^*v = 1.$$

Thus u generates a code which is self-dual if and only if $v \in V_*(F_2C_{48})$.
That is a self-dual $[96, 48, d]$ code for some minimum distance d.

Using Bovdi and Scazaks method,
$V_*(F_2 C_{48}) \simeq C_2^7 \times C_4^3 \times C_8 \times C_{16}^2 \times C_3$.

There are $2^{24} * 3 = 50,331,648$ elements in this group.
For each $v \in V_*(F_2 C_{48})$, the element $u = 1 + yv$ generates a self-dual code.

However, some of these codes are equivalent, so we can reduce the search.

Using Bovdi and Scazaks method,
$V_*(F_2C_{48}) \simeq C_2^7 \times C_4^3 \times C_8 \times C_{16}^2 \times C_3$.

There are $2^{24} * 3 = 50,331,648$ elements in this group.
For each $v \in V_*(F_2C_{48})$, the element $u = 1 + yv$ generates a self-dual code.

However, some of these codes are equivalent, so we can reduce the search.

Using Bovdi and Scazaks method,
$V_*(F_2C_{48}) \simeq C_2^7 \times C_4^3 \times C_8 \times C_{16}^2 \times C_3$.

There are $2^{24} * 3 = 50,331,648$ elements in this group.
For each $v \in V_*(F_2C_{48})$, the element $u = 1 + yv$ generates a self-dual code.

However, some of these codes are equivalent, so we can reduce the search.

Recall that two binary codes C_1 and C_2 are **equivalent** if there exists a permutation matrix P such that $C_1 P = C_2$.

Let b be the generator of the group C_{48}.
$b^i(b^i)^* = b^i(b^{-1}) = 1$.
So $\langle b \rangle \simeq C_{48} \simeq (C_{16} \times C_3) < V_*(F_2 C_{48})$.

Recall that two binary codes C_1 and C_2 are **equivalent** if there exists a permutation matrix P such that $C_1 P = C_2$.

Let b be the generator of the group C_{48}.
$b^i (b^i)^* = b^i (b^{-1}) = 1$.
So $\langle b \rangle \simeq C_{48} \simeq (C_{16} \times C_3) < V_*(F_2 C_{48})$.

Let $u \in F_2 D_{96}$, where $D_{96} = \langle b, y | b^{48} = y^2 = 1, b^y = b^{-1} \rangle$.
Suppose $u = 1 + yv$ where $v \in F_2 C_{48}$.

Lemma (Creedon, G., McLoughlin)

The code generated by $u = 1 + yv$ is equivalent to the code generated by $u_i = 1 + yb^i v$ for $i \in \{1, \ldots, 47\}$.

Proof.

Let $u_i = 1 + yb^i v$ for $i \in \{1, \ldots, 47\}$.

The group ring matrix U_i is of the form $\begin{bmatrix} I & A_i \\ A_i & I \end{bmatrix}$.

A_i is the matrix resulting from cycling the columns of A, i times. Hence the row space of U_i is generated by $\begin{bmatrix} I & A_i \end{bmatrix}$ that is a column permutation of $\begin{bmatrix} I & A \end{bmatrix}$ and so is equivalent to the code generated by u. $\square$

Let $u \in F_2 D_{96}$, where $D_{96} = \langle b, y | b^{48} = y^2 = 1, b^y = b^{-1} \rangle$.
Suppose $u = 1 + yv$ where $v \in F_2 C_{48}$.

Lemma (Creedon, G., McLoughlin)

The code generated by $u = 1 + yv$ is equivalent to the code generated by $u_i = 1 + yb^i v$ for $i \in \{1, \ldots, 47\}$.

Proof.

Let $u_i = 1 + yb^i v$ for $i \in \{1, \ldots, 47\}$.

The group ring matrix U_i is of the form $\begin{bmatrix} I & A_i \\ A_i & I \end{bmatrix}$.

A_i is the matrix resulting from cycling the columns of A, i times.
Hence the row space of U_i is generated by $\begin{bmatrix} I & A_i \end{bmatrix}$ that is a column permutation of $\begin{bmatrix} I & A \end{bmatrix}$ and so is equivalent to the code generated by u. $\square$

Recall that we have
$V_*(F_2C_{48}) \simeq C_2^7 \times C_4^3 \times C_8 \times C_{16}^2 \times C_3$.

If would be nice if could write $V_*(F_2C_{48})$ as $\langle b \rangle \times K$.
Then we could list only the elements of K and check the codes resulting from these.

This would reduce the search to $\frac{2^{24}(3)}{48} = 2^{20}$ different codes.

Recall that we have
$V_*(F_2C_{48}) \simeq C_2^7 \times C_4^3 \times C_8 \times C_{16}^2 \times C_3$.

If would be nice if could write $V_*(F_2C_{48})$ as $\langle b \rangle \times K$.
Then we could list only the elements of K and check the codes resulting from these.

This would reduce the search to $\frac{2^{24}(3)}{48} = 2^{20}$ different codes.

Recall that we have
$V_*(F_2C_{48}) \simeq C_2^7 \times C_4^3 \times C_8 \times C_{16}^2 \times C_3$.

If would be nice if could write $V_*(F_2C_{48})$ as $\langle b \rangle \times K$.
Then we could list only the elements of K and check the codes resulting from these.

This would reduce the search to $\frac{2^{24}(3)}{48} = 2^{20}$ different codes.

Bovdi and Scazaks method for constructing the generators of $V_*(F_2C_{48})$ does just that.
Here C_{48} = $\langle b\rangle$ = $(\langle b^3\rangle \times \langle b^{16}\rangle)$
Let $\langle a\rangle \times \langle h\rangle$ where $a = b^3$ and let $h = b^{16}$.
Thus C_{48} =$\langle a\rangle \times \langle h\rangle$

The full list of generators of $V_*(F_2C_{48})$ is on the next slide.

Bovdi and Scazaks method for constructing the generators of $V_*(F_2C_{48})$ does just that.
Here C_{48} = $\langle b\rangle$ = $(\langle b^3\rangle \times \langle b^{16}\rangle)$
Let $\langle a\rangle \times \langle h\rangle$ where $a = b^3$ and let $h = b^{16}$.
Thus C_{48} =$\langle a\rangle \times \langle h\rangle$

The full list of generators of $V_*(F_2C_{48})$ is on the next slide.

$$
\begin{aligned}
&V_*(F_2C_{48}) \simeq \\
&\langle 1+\hat{a}\rangle \times \langle 1+a+a^7+a^9+a^{15}\rangle\times \\
&\langle 1+a+a^3+a^5+a^7+a^9+a^{11}+a^{13}+a^{15}\rangle\times \\
&\langle 1+h(1+a+a^8+a^9)+h^{-1}(1+a^7+a^8+a^{15})\rangle\times \\
&\langle 1+h(1+a+a^2+a^3+a^8+a^9+a^{10}+a^{11})+h^{-1}(1+a^5+ \\
&a^6+a^7+a^8+a^{13}+a^{14}+a^{15})\rangle\times \\
&\langle 1+h(1+a+a^4+a^5+a^8+a^9+a^{12}+a^{13})+h^{-1}(1+a^3+ \\
&a^4+a^7+a^8+a^{11}+a^{12}+a^{15})\rangle\times \\
&\langle 1+h\hat{a}+h^{-1}\hat{a}\rangle\times\langle a+a^2+a^3+a^4+a^8+a^{10}+a^{12}+a^{13}+a^{15}\rangle\times \\
&\langle 1+a^3+a^5+a^{11}+a^{13}+\hat{a}+h(1+a+a^4+a^5+\hat{a})+h^{-1}(a^2+ \\
&a^8+a^{10}+a^{11}+a^{12}+a^{15})\rangle\times \\
&\langle 1+a\hat{a^2}+h(1+a+a^2+a^3+a^4+a^5+a^6+a^7)+h^{-1}(a^2+ \\
&a^4+a^6+a^8+a^9+a^{11}+a^{13}+a^{15})\rangle\times \\
&\langle 1+a+a^2+a^4+a^5+a^6+a^7+a^{10}+a^{11}+a^{12}+a^{14}+h(a+ \\
&a^2+a^3+a^4+a^5+a^6+a^8+a^{12}+a^{13}+a^{14})+h^{-1}(1+a^3+ \\
&a^7+a^8+a^{10}+a^{11}+a^{12}+a^{13})\rangle\times \\
&\langle a\rangle\times\langle a^{14}+h(a^{14}+a^{15})+h^{-1}(a^{14}+a^{15})\rangle\times\langle h\rangle.
\end{aligned}
$$

Using Bovdi and Szacaks method we can write $V_*(F_2 C_{48})$ as $\langle b \rangle \times K$.

Thus we need only check the elements of K and so we can reduce the search to $\frac{2^{24}(3)}{48} = 2^{20}$ different codes.

Using Bovdi and Szacaks method we can write $V_*(F_2C_{48})$ as $\langle b \rangle \times K$.

Thus we need only check the elements of K and so we can reduce the search to $\frac{2^{24}(3)}{48} = 2^{20}$ different codes.

Recall that unitary units of the form $b^i v$ create equivalent codes to v.
To see that two unitary units are cycles of each other, we look at an element's "cycle type".

Example

Let $\alpha = 1 + b^3 + b^{24} + b^{29} + b^{43}$.
Then α has cycle type $(3, 21, 5, 14, 5)$.
Consider $b^{23}\alpha = b^4 + b^{18} + b^{23} + b^{26} + b^{47}$.
Then $b^{23}\alpha$ has cycle type $(14, 5, 3, 21, 5)$ which is the same as the cycle type of α (except it has been cycled).

Recall that unitary units of the form $b^i v$ create equivalent codes to v.
To see that two unitary units are cycles of each other, we look at an element's "cycle type".

Example

Let $\alpha = 1 + b^3 + b^{24} + b^{29} + b^{43}$.
Then α has cycle type $(3, 21, 5, 14, 5)$.
Consider $b^{23}\alpha = b^4 + b^{18} + b^{23} + b^{26} + b^{47}$.
Then $b^{23}\alpha$ has cycle type $(14, 5, 3, 21, 5)$ which is the same as the cycle type of α (except it has been cycled).

Lemma (Creedon, G., McLoughlin)

Let $C_{48} = \langle b \rangle$. Assume $V_*(F_2C_{48}) \simeq \langle b \rangle \times K$. Then every element of K has a different cycle type. Further, all of the different cycle types of $V_*(F_2C_{48})$ occur in K.

Proof.

We can partition $V_*(F_2C_{48})$ into $b^0K \cup b^1K \cup ... \cup b^{47}K$.
i) Suppose α_1, α_2 are two distinct elements in K with the same cycle type. Then $b^i\alpha_1 = \alpha_2 \ \exists\ i \neq 0$.
Then $b^i\alpha_1 \in K$ and so $b^i \in K$. This contradiction implies that all elements of K have different cycle types.
ii) The coset b^0K (=K) contains a set of cycle types. The coset b^iK will contain the exact same set of cycle types (cycled i times). Thus every coset has the same set of cycle types as K. Thus any cycle type occurring in $V_*(F_2C_{48})$ occurs in K. $\square$

Lemma (Creedon, G., McLoughlin)

Let $C_{48} = \langle b \rangle$. Assume $V_*(F_2C_{48}) \simeq \langle b \rangle \times K$. Then every element of K has a different cycle type. Further, all of the different cycle types of $V_*(F_2C_{48})$ occur in K.

Proof.

We can partition $V_*(F_2C_{48})$ into $b^0K \cup b^1K \cup \ldots \cup b^{47}K$.
i) Suppose α_1, α_2 are two distinct elements in K with the same cycle type. Then $b^i\alpha_1 = \alpha_2 \; \exists \; i \neq 0$.
Then $b^i\alpha_1 \in K$ and so $b^i \in K$. This contradiction implies that all elements of K have different cycle types.
ii) The coset b^0K (=K) contains a set of cycle types. The coset b^iK will contain the exact same set of cycle types (cycled i times). Thus every coset has the same set of cycle types as K. Thus any cycle type occurring in $V_*(F_2C_{48})$ occurs in K. $\square$

Theorem (Creedon, G., McLoughlin)

The elements of $V_*(F_2C_{48})$ of order 2 form the set
$\{1 + a_0(1 + b^{24}) + \sum_{i=1}^{11} a_i(b^i + b^{24+i} + b^{48-i} + b^{24-i}) + a_{12}(b^{12} + b^{36}) | a_i \in F_2\}$
and do not generate extremal codes.

Proof.

(First part omitted).
If $v \in V_*(F_2C_{48})$ has order 2 then $\widehat{b^{24}}v = \widehat{b^{24}} + 0 + 0 + 0 = \widehat{b^{24}}$.
Letting $u = 1 + yv$, then $u + b^{24}u = \widehat{b^{24}}(1 + yv) =$
$\widehat{b^{24}} + \widehat{b^{24}}yv = \widehat{b^{24}} + y\widehat{b^{24}}v = \widehat{b^{24}} + y\widehat{b^{24}} = 1 + b^{24} + y + yb^{24}$
which has weight 4, so unitary units of order 2 do not generate extremal codes. □

Theorem (Creedon, G., McLoughlin)

The elements of $V_*(F_2C_{48})$ of order 2 form the set
$\{1 + a_0(1 + b^{24}) + \sum_{i=1}^{11} a_i(b^i + b^{24+i} + b^{48-i} + b^{24-i}) + a_{12}(b^{12} + b^{36}) | a_i \in F_2\}$
and do not generate extremal codes.

Proof.

(First part omitted).
If $v \in V_*(F_2C_{48})$ has order 2 then $\widehat{b^{24}}v = \widehat{b^{24}} + 0 + 0 + 0 = \widehat{b^{24}}$.
Letting $u = 1 + yv$, then $u + b^{24}u = \widehat{b^{24}}(1 + yv) =$
$\widehat{b^{24}} + \widehat{b^{24}}yv = \widehat{b^{24}} + y\widehat{b^{24}}v = \widehat{b^{24}} + y\widehat{b^{24}} = 1 + b^{24} + y + yb^{24}$
which has weight 4, so unitary units of order 2 do not generate extremal codes. □

Theorem (Creedon, G., McLoughlin)

The elements of $V_*(F_2C_{48})$ of order 4 are contained in the set $\left\{a_0b^0 + a_{12}b^{12} + a_{24}b^{24} + a_{36}b^{36} + \sum_{k=1}^{3}\sum_{i=1\, k\neq 12,24,36}^{47} a_{i_k}(b^i + b^{12k+i}) \text{where} \sum a_i = 1\right\}$ *and do not generate extremal codes.*

Proof.

(First part omitted).
If $v \in V_*(F_2C_{48})$ has order 4 then, letting $u = 1 + yv$,

$$(\widehat{b^{12}})u = (\widehat{b^{12}}) + y\left[(a_0 + a_{12} + a_{24} + a_{36})(\widehat{b^{12}}) + 0\right]$$

$= (1 + b^{12} + b^{24} + b^{36}) + y(1 + b^{12} + b^{24} + b^{36})$.
This codeword has weight 8, so unitary units of order 4 do not generate extremal codes. $\square$

Theorem (Creedon, G., McLoughlin)

The elements of $V_*(F_2C_{48})$ of order 4 are contained in the set $\left\{a_0b^0 + a_{12}b^{12} + a_{24}b^{24} + a_{36}b^{36} + \sum_{k=1}^{3}\sum_{i=1\, k\neq 12,24,36}^{47} a_{i_k}(b^i + b^{12k+i}) \textit{where} \sum a_i = 1\right\}$ *and do not generate extremal codes.*

Proof.

(First part omitted).

If $v \in V_*(F_2C_{48})$ has order 4 then, letting $u = 1 + yv$,

$$(\widehat{b^{12}})u = (\widehat{b^{12}}) + y\left[(a_0 + a_{12} + a_{24} + a_{36})(\widehat{b^{12}}) + 0\right]$$

$= (1 + b^{12} + b^{24} + b^{36}) + y(1 + b^{12} + b^{24} + b^{36})$.

This codeword has weight 8, so unitary units of order 4 do not generate extremal codes. $\square$

Theorem (Creedon, G., McLoughlin)

The elements of $V_*(F_2C_{48})$ of order 8 do not generate extremal codes.

Proof.

The proof is similar to the previous two. Here is a summary.
Let $v \in V_*(F_2C_{48})$ such that v has order 8.
Then let $u = 1 + yv$ and consider the matrix U.
Take the 8-row combination of rows 1, 1+6, 1+12, ..., 1+42 and the result is a codeword of weight 16.
Thus the elements of $V_*(F_2C_{48})$ of order 8 do not generate extremal codes. $\square$

Theorem (Creedon, G., McLoughlin)

The elements of $V_*(F_2C_{48})$ of order 8 do not generate extremal codes.

Proof.

The proof is similar to the previous two. Here is a summary.
Let $v \in V_*(F_2C_{48})$ such that v has order 8.
Then let $u = 1 + yv$ and consider the matrix U.
Take the 8-row combination of rows 1, 1+6, 1+12, ..., 1+42 and the result is a codeword of weight 16.
Thus the elements of $V_*(F_2C_{48})$ of order 8 do not generate extremal codes. □

Corollary

If there exist extremal codes of the form $u = 1 + yv$ where $u \in F_2D_{96}$ and $v \in V_*(F_2C_{48})$, then they exist for some v with order exactly 16.

So instead of searching the 2^{20} different codes to find their minimum distances, we need only search those of order 16. This reduces the search to 2^{19} different codes.

Corollary

If there exist extremal codes of the form $u = 1 + yv$ *where* $u \in F_2 D_{96}$ *and* $v \in V_*(F_2 C_{48})$*, then they exist for some* v *with order exactly 16.*

So instead of searching the 2^{20} different codes to find their minimum distances, we need only search those of order 16. This reduces the search to 2^{19} different codes.

Further Work

- Adapt the technique to use other group algebras FG where G has order 96 and search again for extremal self-dual $[96, 48, 20]$ codes
- Apply the same technique to groups of order 72 and 120 to search for extremal self-dual codes of those lengths.
- Apply this technique for FG where $|G| = 2^n(m)$ for $m \neq 3$.
- Approach these problems using a decomposition of the (non-semisimple) group algebra $F_2 C_{2^n 3}$.

Thank You!

A. A. Bovdi and A. Szakacs, Unitary subgroup of the group of units of a modular group algebra of a finite abelian p-group, *Mat. Zametki 45(6) (1989), 23–29.*

A. A. Bovdi and A. Szakacs, A basis for the unitary subgroup of the group of units in a finite commutative group algebra, *Publ. Math., 46:1-2 (1995), 97–120.*

O. Broche and A. del Rio, Wedderburn decomposition of finite group algebras, *Finite fields and Their Applications (2007), 71-79.*

Dean Crnkovic, Sanja Rukavina and Loredana Simcic, Binary doubly-even self-dual codes of length 72 with large automorphism groups, *Mathematical Communications Vol. 18 No. 2 (2013), 297-308*

R. Dontcheva, On the doubly-even self-dual codes of length 96. *IEEE Trans. Inform. Theory, 48(2):557–561, 2002*

D.S. Dummit and R.M.Foote, Abstract Algebra, *John Wiley and Sons, Inc, 3rd Edition (2004).*

P. Hurley and T. Hurley, Codes from Zero Divisors and Units in Group Rings, *International Journal of Information and Coding Theory, Vol. 1, No. 1, (2009), 57-87.*

Ian McLoughlin and Ted Hurley A Group Ring Construction of the extended binary Golay code, *IEEE Transactions on Information Theory* 54.9 (2008): 4381-4381

Ian McLoughlin

G. Nebe, E. M. Rains, N. J. A. Sloane, Self-dual codes and invariant theory, *Algorithms and Computation in Mathematics, Vol. 17, Springer, Berlin, 2006*

V. Pless and W.C.Huffman, Handbook of Coding Theory Vol. 1, *Elsevier, (1998)*

C. Polcino Milies and S. K. Sehgal, An Introduction to Group Rings, *Kluwer Academic Publishers (2002).*