Construction of Linear Codes using Cyclic and Dihedral Group Algebras

Leo Creedon

Institute of Technology Sligo
Ireland

Joint work with Fergal Gallagher and Ian McLoughlin

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

Conference Announcement:
Irish Mathematical Society Annual General Meeting,
IT Sligo, Ireland, August 31 and September 1, 2017

The talk:

"It is, as is natural in the doings of young mathematicians, very full of symbols."
Augustus De Morgan in a letter to John Herschel, 1845.

- Non-abelian codes in the modular group algebra $F_2 D_{2k}$.
- The connection between unitary units of group algebras and self-dual codes
- Some results on searching for extremal Type II codes of length 96 using unitary units of $F_2 C_{2^n 3}$

The talk:

"It is, as is natural in the doings of young mathematicians, very full of symbols."

Augustus De Morgan in a letter to John Herschel, 1845.

- Non-abelian codes in the modular group algebra $F_2 D_{2k}$.
- The connection between unitary units of group algebras and self-dual codes
- Some results on searching for extremal Type II codes of length 96 using unitary units of $F_2 C_{2^n 3}$

The talk:

"It is, as is natural in the doings of young mathematicians, very full of symbols."
Augustus De Morgan in a letter to John Herschel, 1845.

- Non-abelian codes in the modular group algebra $F_2 D_{2k}$.
- The connection between unitary units of group algebras and self-dual codes
- Some results on searching for extremal Type II codes of length 96 using unitary units of $F_2 C_{2^n 3}$

The talk:

"It is, as is natural in the doings of young mathematicians, very full of symbols."
Augustus De Morgan in a letter to John Herschel, 1845.

- Non-abelian codes in the modular group algebra $F_2 D_{2k}$.
- The connection between unitary units of group algebras and self-dual codes
- Some results on searching for extremal Type II codes of length 96 using unitary units of $F_2 C_{2^n 3}$

A linear code is a subspace of a vector space. We consider only the binary field F_2.

A **Type II code** is a subspace C of F_2^{2k} such that
1. All elements of C have Hamming weight congruent to 0 modulo 4.
2. The subset $C^{\perp} = \{x | x \in F_2^{2k}, x.c = 0 \; \forall c \in C\}$ of all vectors perpendicular to all elements of C is C itself (with respect to the usual dot product). So C is **self-dual**.

Type II codes are known to have minimum distance $d \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + 4$.

The code is called extremal if equality holds.

A linear code is a subspace of a vector space. We consider only the binary field F_2.

A **Type II code** is a subspace C of F_2^{2k} such that
1. All elements of C have Hamming weight congruent to 0 modulo 4.
2. The subset $C^\perp = \{x | x \in F_2^{2k}, x.c = 0 \; \forall c \in C\}$ of all vectors perpendicular to all elements of C is C itself (with respect to the usual dot product). So C is **self-dual**.

Type II codes are known to have minimum distance $d \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + 4$.

The code is called extremal if equality holds.

A linear code is a subspace of a vector space. We consider only the binary field F_2.

A **Type II code** is a subspace C of F_2^{2k} such that
1. All elements of C have Hamming weight congruent to 0 modulo 4.
2. The subset $C^{\perp} = \{x | x \in F_2^{2k}, x.c = 0 \; \forall c \in C\}$ of all vectors perpendicular to all elements of C is C itself (with respect to the usual dot product). So C is **self-dual**.

Type II codes are known to have minimum distance $d \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + 4$.

The code is called extremal if equality holds.

A linear code is a subspace of a vector space. We consider only the binary field F_2.

A **Type II code** is a subspace C of F_2^{2k} such that
1. All elements of C have Hamming weight congruent to 0 modulo 4.
2. The subset $C^\perp = \{x | x \in F_2^{2k}, x.c = 0 \; \forall c \in C\}$ of all vectors perpendicular to all elements of C is C itself (with respect to the usual dot product). So C is **self-dual**.

Type II codes are known to have minimum distance $d \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + 4$.

The code is called extremal if equality holds.

Group ring matrices are defined in Hurley and Hurley's 2009 paper. They begin by defining the group matrix of a listing of a group.

Let $L = \{g_0, g_1, \ldots, g_{n-1}\}$ be a listing of a group G where n is the order of G. The group matrix is the matrix with entries $g_j^{-1} g_i$ in row i and column j for $0 \leq i, j \leq n$.

Thus the group matrix is the multiplication table of G with the rows permuted so that they are labelled by the inverses of the labels of the columns in order.

The diagonal entries are all equal to the identity of the group.

When G is the underlying group in a group ring, a group ring matrix is then defined for each group ring element u. It is obtained by replacing each entry in the group matrix by its coefficient in u.

The map obtained by this process is a ring isomorphism between the group ring and the group ring matrices according to the listing L.

Group ring matrices are defined in Hurley and Hurley's 2009 paper. They begin by defining the group matrix of a listing of a group.

Let $L = \{g_0, g_1, \ldots, g_{n-1}\}$ be a listing of a group G where n is the order of G. The group matrix is the matrix with entries $g_j^{-1} g_i$ in row i and column j for $0 \leq i, j \leq n$.

Thus the group matrix is the multiplication table of G with the rows permuted so that they are labelled by the inverses of the labels of the columns in order.

The diagonal entries are all equal to the identity of the group.

When G is the underlying group in a group ring, a group ring matrix is then defined for each group ring element u. It is obtained by replacing each entry in the group matrix by its coefficient in u.

The map obtained by this process is a ring isomorphism between the group ring and the group ring matrices according to the listing L.

Group ring matrices are defined in Hurley and Hurley's 2009 paper. They begin by defining the group matrix of a listing of a group.

Let $L = \{g_0, g_1, \ldots, g_{n-1}\}$ be a listing of a group G where n is the order of G. The group matrix is the matrix with entries $g_j^{-1}g_i$ in row i and column j for $0 \leq i, j \leq n$.

Thus the group matrix is the multiplication table of G with the rows permuted so that they are labelled by the inverses of the labels of the columns in order.

The diagonal entries are all equal to the identity of the group.

When G is the underlying group in a group ring, a group ring matrix is then defined for each group ring element u. It is obtained by replacing each entry in the group matrix by its coefficient in u.

The map obtained by this process is a ring isomorphism between the group ring and the group ring matrices according to the listing L.

Group ring matrices are defined in Hurley and Hurley's 2009 paper. They begin by defining the group matrix of a listing of a group.

Let $L = \{g_0, g_1, \ldots, g_{n-1}\}$ be a listing of a group G where n is the order of G. The group matrix is the matrix with entries $g_j^{-1} g_i$ in row i and column j for $0 \leq i, j \leq n$.

Thus the group matrix is the multiplication table of G with the rows permuted so that they are labelled by the inverses of the labels of the columns in order.

The diagonal entries are all equal to the identity of the group.

When G is the underlying group in a group ring, a group ring matrix is then defined for each group ring element u. It is obtained by replacing each entry in the group matrix by its coefficient in u.

The map obtained by this process is a ring isomorphism between the group ring and the group ring matrices according to the listing L.

Group ring matrices are defined in Hurley and Hurley's 2009 paper. They begin by defining the group matrix of a listing of a group.

Let $L = \{g_0, g_1, \ldots, g_{n-1}\}$ be a listing of a group G where n is the order of G. The group matrix is the matrix with entries $g_j^{-1}g_i$ in row i and column j for $0 \leq i, j \leq n$.

Thus the group matrix is the multiplication table of G with the rows permuted so that they are labelled by the inverses of the labels of the columns in order.

The diagonal entries are all equal to the identity of the group.

When G is the underlying group in a group ring, a group ring matrix is then defined for each group ring element u. It is obtained by replacing each entry in the group matrix by its coefficient in u.

The map obtained by this process is a ring isomorphism between the group ring and the group ring matrices according to the listing L.

Group ring matrices are defined in Hurley and Hurley's 2009 paper. They begin by defining the group matrix of a listing of a group.

Let $L = \{g_0, g_1, \dots, g_{n-1}\}$ be a listing of a group G where n is the order of G. The group matrix is the matrix with entries $g_j^{-1} g_i$ in row i and column j for $0 \leq i, j \leq n$.

Thus the group matrix is the multiplication table of G with the rows permuted so that they are labelled by the inverses of the labels of the columns in order.

The diagonal entries are all equal to the identity of the group.

When G is the underlying group in a group ring, a group ring matrix is then defined for each group ring element u. It is obtained by replacing each entry in the group matrix by its coefficient in u.

The map obtained by this process is a ring isomorphism between the group ring and the group ring matrices according to the listing L.

Consider the dihedral group with $2k$ elements given by the presentation $D_{2k} = \langle y, b | y^2 = 1, b^k = 1, yby = b^{-1} \rangle$.

We map the element $\alpha = \sum_{i=0}^{k-1} \alpha_i b^i + \beta_i y b^i$ to the binary $2k$-tuple $[\alpha_0, \alpha_1, \ldots, \alpha_{k-1}, \beta_0, \beta_1, \ldots, \beta_{k-1}]$.
This effectively creates a listing of D_{2k}.

If the left half of the $2k$-tuple is cycled, it gives a $k \times k$ circulant matrix and if the right half of the $2k$-tuple is reverse cycled, it gives a $k \times k$ reverse circulant matrix which we call A.

Consider the dihedral group with $2k$ elements given by the presentation $D_{2k} = \langle y, b | y^2 = 1, b^k = 1, yby = b^{-1} \rangle$.

We map the element $\alpha = \sum_{i=0}^{k-1} \alpha_i b^i + \beta_i y b^i$ to the binary $2k$-tuple $[\alpha_0, \alpha_1, \ldots, \alpha_{k-1}, \beta_0, \beta_1, \ldots, \beta_{k-1}]$.
This effectively creates a listing of D_{2k}.

If the left half of the $2k$-tuple is cycled, it gives a $k \times k$ circulant matrix and if the right half of the $2k$-tuple is reverse cycled, it gives a $k \times k$ reverse circulant matrix which we call A.

Consider the dihedral group with $2k$ elements given by the presentation $D_{2k} = \langle y, b | y^2 = 1, b^k = 1, yby = b^{-1} \rangle$.

We map the element $\alpha = \sum_{i=0}^{k-1} \alpha_i b^i + \beta_i y b^i$ to the binary $2k$-tuple $[\alpha_0, \alpha_1, \ldots, \alpha_{k-1}, \beta_0, \beta_1, \ldots, \beta_{k-1}]$.
This effectively creates a listing of D_{2k}.

If the left half of the $2k$-tuple is cycled, it gives a $k \times k$ circulant matrix and if the right half of the $2k$-tuple is reverse cycled, it gives a $k \times k$ reverse circulant matrix which we call A.

Then following the work of Hurley and Hurley [7], defining

$$U = \begin{bmatrix} B & A \\ A & B \end{bmatrix},$$

there is a ring isomorphism between the group ring $F_2 D_{2k}$ and a ring of matrices given by $\alpha = \sum_{i=0}^{k-1} \alpha_i b^i + \beta_i y b^i \to U$.

If $u = 1 + \sum_{i=0}^{k-1} \beta_i y b^i$ then $B = I$, so

$$U = \begin{bmatrix} I & A \\ A & I \end{bmatrix},$$

and the rowspace of U defines a code. U can be row reduced to $G = [I\ A]$ which is the generator matrix of the same code.

Then following the work of Hurley and Hurley [7], defining

$$U = \begin{bmatrix} B & A \\ A & B \end{bmatrix},$$

there is a ring isomorphism between the group ring $F_2 D_{2k}$ and a ring of matrices given by $\alpha = \sum_{i=0}^{k-1} \alpha_i b^i + \beta_i y b^i \to U$.

If $u = 1 + \sum_{i=0}^{k-1} \beta_i y b^i$ then $B = I$, so

$$U = \begin{bmatrix} I & A \\ A & I \end{bmatrix},$$

and the rowspace of U defines a code. U can be row reduced to $G = [I\ A]$ which is the generator matrix of the same code.

Lemma (C., Gallagher, McLoughlin)

The code generated by $u = 1 + yv$ as described above is the principal left ideal of u in $F_2 D_{2k}$.

Proof.

Let C be the code generated by $u = 1 + yv$, corresponding to the generator matrix of $[I\ A]$. Row i of $G = [I\ A]$ is the $2k$-tuple of coefficients of $b^i u$ in order according to the listing of the group. So $\{b^i u | 0 \leq i < k\} \subseteq C$ and is therefore a basis of C.

Note that $yb^i u = yb^i(1 + yv) = yb^i + b^{-i}yyv = yb^i + b^{-i}v = b^{-i}v + yb^i$. So row i of $[A\ I]$ is the $2k$-tuple of coefficients of $yb^i u$ in order according to the listing of the group.

Thus the code C equals the matrix image of the set $F_2 D_{2k} u$. This is because $(\sum_{i=1}^{k-1} \alpha_i b^i + \sum_{i=1}^{k-1} \beta_i yb^i)u = (\sum_{i=1}^{k-1} \alpha_i b^i)u + (\sum_{i=1}^{k-1} \beta_i yb^i)u$ is sent by the matrix map to a linear combination of the rows of $[I\ A]$ plus a linear combination of the rows of $[A\ I]$, so it is in C. □

Lemma (C., Gallagher, McLoughlin)

The code generated by $u = 1 + yv$ as described above is the principal left ideal of u in F_2D_{2k}.

Proof.

Let C be the code generated by $u = 1 + yv$, corresponding to the generator matrix of $[I\ A]$. Row i of $G = [I\ A]$ is the $2k$-tuple of coefficients of $b^i u$ in order according to the listing of the group. So $\{b^i u | 0 \leq i < k\} \subseteq C$ and is therefore a basis of C.

Note that

$yb^i u = yb^i(1 + yv) = yb^i + b^{-i}yyv = yb^i + b^{-i}v = b^{-i}v + yb^i$. So row i of $[A\ I]$ is the $2k$-tuple of coefficients of $yb^i u$ in order according to the listing of the group.

Thus the code C equals the matrix image of the set $F_2D_{2k}u$. This is because $(\sum_{i=1}^{k-1} \alpha_i b^i + \sum_{i=1}^{k-1} \beta_i yb^i)u = (\sum_{i=1}^{k-1} \alpha_i b^i)u + (\sum_{i=1}^{k-1} \beta_i yb^i)u$ is sent by the matrix map to a linear combination of the rows of $[I\ A]$ plus a linear combination of the rows of $[A\ I]$, so it is in C. $\square$

- Hurley and McLoughlin (2008) have used this technique to construct the well known extended binary Golay code. This [24,12,8] code is an extremal Type II code.
- Then Mclaughlin (2010) used the same technique to construct a [48,24,12] code which is again an extremal Type II code.
- These are the only known examples of extremal [24m,12m,4m+4] codes (i.e. only $m = 1$ and $m = 2$ are known to exist).
- This motivates the use of this dihedral technique to search for other extremal [24m,12m,4m+4] codes.
- These codes are important because:

  1. By a result of Rains an extremal self-dual code of length a multiple of 24 must be a Type II code

  2. Malevich in his PhD thesis states that "extremal codes of length a multiple of 24 are of particular interest mainly because these codes hold 5-designs."

- Hurley and McLoughlin (2008) have used this technique to construct the well known extended binary Golay code. This [24,12,8] code is an extremal Type II code.
- Then Mclaughlin (2010) used the same technique to construct a [48,24,12] code which is again an extremal Type II code.
- These are the only known examples of extremal [24m,12m,4m+4] codes (i.e. only $m = 1$ and $m = 2$ are known to exist).
- This motivates the use of this dihedral technique to search for other extremal [24m,12m,4m+4] codes.
- These codes are important because:

  1. By a result of Rains an extremal self-dual code of length a multiple of 24 must be a Type II code

  2. Malevich in his PhD thesis states that "extremal codes of length a multiple of 24 are of particular interest mainly because these codes hold 5-designs."

- Hurley and McLoughlin (2008) have used this technique to construct the well known extended binary Golay code. This [24,12,8] code is an extremal Type II code.
- Then Mclaughlin (2010) used the same technique to construct a [48,24,12] code which is again an extremal Type II code.
- These are the only known examples of extremal [24m,12m,4m+4] codes (i.e. only $m = 1$ and $m = 2$ are known to exist).
- This motivates the use of this dihedral technique to search for other extremal [24m,12m,4m+4] codes.
- These codes are important because:

  1. By a result of Rains an extremal self-dual code of length a multiple of 24 must be a Type II code

  2. Malevich in his PhD thesis states that "extremal codes of length a multiple of 24 are of particular interest mainly because these codes hold 5-designs."

- Hurley and McLoughlin (2008) have used this technique to construct the well known extended binary Golay code. This [24,12,8] code is an extremal Type II code.
- Then Mclaughlin (2010) used the same technique to construct a [48,24,12] code which is again an extremal Type II code.
- These are the only known examples of extremal [24m,12m,4m+4] codes (i.e. only $m = 1$ and $m = 2$ are known to exist).
- This motivates the use of this dihedral technique to search for other extremal [24m,12m,4m+4] codes.
- These codes are important because:

  1. By a result of Rains an extremal self-dual code of length a multiple of 24 must be a Type II code

  2. Malevich in his PhD thesis states that "extremal codes of length a multiple of 24 are of particular interest mainly because these codes hold 5-designs."

- Hurley and McLoughlin (2008) have used this technique to construct the well known extended binary Golay code. This [24,12,8] code is an extremal Type II code.
- Then Mclaughlin (2010) used the same technique to construct a [48,24,12] code which is again an extremal Type II code.
- These are the only known examples of extremal [24m,12m,4m+4] codes (i.e. only $m = 1$ and $m = 2$ are known to exist).
- This motivates the use of this dihedral technique to search for other extremal [24m,12m,4m+4] codes.
- These codes are important because:

  1. By a result of Rains an extremal self-dual code of length a multiple of 24 must be a Type II code

  2. Malevich in his PhD thesis states that "extremal codes of length a multiple of 24 are of particular interest mainly because these codes hold 5-designs."

Denote by C a code generated by the element $1 + yv$ using this dihedral technique.
Note that if C is a binary self-dual code then each codeword has even weight. If every codeword has weight divisible by 4, then we have a *doubly even* code or a Type II code.
If v has weight equal to $-1(mod 4)$, then $u = 1 + yv$ is a Type II code (otherwise it is a Type I code) (Pless and Huffman page 10).

So the dihedral codes given in this paper are either Type I or Type II codes. It can be quickly determined which is the case, since the code given by $u = 1 + yv$ will be Type II if and only if its first row has weight divisible by 4.
It has been shown that the extremal [24,12,8] code and the extremal [48,24,12] codes can be constructed as dihedral codes using this technique.

Here it is proven that this technique does not construct the putative [96,48,20] extremal code.

However, this technique does construct [96,48,16] codes, which are the best known Type II codes of length 96.

Denote by C a code generated by the element $1 + yv$ using this dihedral technique.
Note that if C is a binary self-dual code then each codeword has even weight. If every codeword has weight divisible by 4, then we have a *doubly even* code or a Type II code.
If v has weight equal to $-1(mod 4)$, then $u = 1 + yv$ is a Type II code (otherwise it is a Type I code) (Pless and Huffman page 10).

So the dihedral codes given in this paper are either Type I or Type II codes. It can be quickly determined which is the case, since the code given by $u = 1 + yv$ will be Type II if and only if its first row has weight divisible by 4.
It has been shown that the extremal [24,12,8] code and the extremal [48,24,12] codes can be constructed as dihedral codes using this technique.

Here it is proven that this technique does not construct the putative [96,48,20] extremal code.

However, this technique does construct [96,48,16] codes, which are the best known Type II codes of length 96.

Denote by C a code generated by the element $1 + yv$ using this dihedral technique.
Note that if C is a binary self-dual code then each codeword has even weight. If every codeword has weight divisible by 4, then we have a *doubly even* code or a Type II code.
If v has weight equal to $-1(mod 4)$, then $u = 1 + yv$ is a Type II code (otherwise it is a Type I code) (Pless and Huffman page 10).

So the dihedral codes given in this paper are either Type I or Type II codes. It can be quickly determined which is the case, since the code given by $u = 1 + yv$ will be Type II if and only if its first row has weight divisible by 4.
It has been shown that the extremal [24,12,8] code and the extremal [48,24,12] codes can be constructed as dihedral codes using this technique.

Here it is proven that this technique does not construct the putative [96,48,20] extremal code.

However, this technique does construct [96,48,16] codes, which are the best known Type II codes of length 96.

Denote by C a code generated by the element $1 + yv$ using this dihedral technique.
Note that if C is a binary self-dual code then each codeword has even weight. If every codeword has weight divisible by 4, then we have a *doubly even* code or a Type II code.
If v has weight equal to $-1(mod4)$, then $u = 1 + yv$ is a Type II code (otherwise it is a Type I code) (Pless and Huffman page 10).

So the dihedral codes given in this paper are either Type I or Type II codes. It can be quickly determined which is the case, since the code given by $u = 1 + yv$ will be Type II if and only if its first row has weight divisible by 4.
It has been shown that the extremal [24,12,8] code and the extremal [48,24,12] codes can be constructed as dihedral codes using this technique.

Here it is proven that this technique does not construct the putative [96,48,20] extremal code.

However, this technique does construct [96,48,16] codes, which are the best known Type II codes of length 96.

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

If P is a permutation matrix with $C_1 P = C_1$ then P is a **code automorphism** of the binary code C_1.

Due to a result of Dontcheva (2002), it is known that for the extremal [96,48,20] code, (if it exists) only 2, 3, and 5 can occur as prime divisors of the order of the automorphism group.

Since the code in this paper is the left ideal $F_2 D_{96} u = F_2 D_{96}(1 + yv)$, D_{96} is a group of automorphisms of the code (by an earlier lemma). Since $|D_{96}| = 2^5 3$, this possibility is not excluded by the prime divisors of the automorphism group.

Further restrictions are imposed on the automorphism group of a [96,48,20] code and these are also satisfied by D_{96}.

In what follows, we show that the codes generated as such ideals $F_2 D_{96}(1 + yv)$ are (unfortunately) not extremal, using a different technique.

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

If P is a permutation matrix with $C_1 P = C_1$ then P is a **code automorphism** of the binary code C_1.

Due to a result of Dontcheva (2002), it is known that for the extremal [96,48,20] code, (if it exists) only 2, 3, and 5 can occur as prime divisors of the order of the automorphism group.

Since the code in this paper is the left ideal $F_2 D_{96} u = F_2 D_{96}(1 + yv)$, D_{96} is a group of automorphisms of the code (by an earlier lemma). Since $|D_{96}| = 2^5 3$, this possibility is not excluded by the prime divisors of the automorphism group.

Further restrictions are imposed on the automorphism group of a [96,48,20] code and these are also satisfied by D_{96}.

In what follows, we show that the codes generated as such ideals $F_2 D_{96}(1 + yv)$ are (unfortunately) not extremal, using a different technique.

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

If P is a permutation matrix with $C_1 P = C_1$ then P is a **code automorphism** of the binary code C_1.

Due to a result of Dontcheva (2002), it is known that for the extremal [96,48,20] code, (if it exists) only 2, 3, and 5 can occur as prime divisors of the order of the automorphism group.

Since the code in this paper is the left ideal $F_2 D_{96} u = F_2 D_{96}(1 + yv)$, D_{96} is a group of automorphisms of the code (by an earlier lemma). Since $|D_{96}| = 2^5 3$, this possibility is not excluded by the prime divisors of the automorphism group.

Further restrictions are imposed on the automorphism group of a [96,48,20] code and these are also satisfied by D_{96}.

In what follows, we show that the codes generated as such ideals $F_2 D_{96}(1 + yv)$ are (unfortunately) not extremal, using a different technique.

Two binary codes C_1 and C_2 are **equivalent** if there exists a permutation matrix P such that $C_1P = C_2$.

If P is a permutation matrix with $C_1P = C_1$ then P is a **code automorphism** of the binary code C_1.

Due to a result of Dontcheva (2002), it is known that for the extremal [96,48,20] code, (if it exists) only 2, 3, and 5 can occur as prime divisors of the order of the automorphism group.

Since the code in this paper is the left ideal $F_2D_{96}u = F_2D_{96}(1 + yv)$, D_{96} is a group of automorphisms of the code (by an earlier lemma). Since $|D_{96}| = 2^5 3$, this possibility is not excluded by the prime divisors of the automorphism group.

Further restrictions are imposed on the automorphism group of a [96,48,20] code and these are also satisfied by D_{96}.

In what follows, we show that the codes generated as such ideals $F_2D_{96}(1 + yv)$ are (unfortunately) not extremal, using a different technique.

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

If P is a permutation matrix with $C_1 P = C_1$ then P is a **code automorphism** of the binary code C_1.

Due to a result of Dontcheva (2002), it is known that for the extremal [96,48,20] code, (if it exists) only 2, 3, and 5 can occur as prime divisors of the order of the automorphism group.

Since the code in this paper is the left ideal $F_2 D_{96} u = F_2 D_{96}(1 + yv)$, D_{96} is a group of automorphisms of the code (by an earlier lemma). Since $|D_{96}| = 2^5 3$, this possibility is not excluded by the prime divisors of the automorphism group.

Further restrictions are imposed on the automorphism group of a [96,48,20] code and these are also satisfied by D_{96}.

In what follows, we show that the codes generated as such ideals $F_2 D_{96}(1 + yv)$ are (unfortunately) not extremal, using a different technique.

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

If P is a permutation matrix with $C_1 P = C_1$ then P is a **code automorphism** of the binary code C_1.

Due to a result of Dontcheva (2002), it is known that for the extremal [96,48,20] code, (if it exists) only 2, 3, and 5 can occur as prime divisors of the order of the automorphism group.

Since the code in this paper is the left ideal $F_2 D_{96} u = F_2 D_{96}(1 + yv)$, D_{96} is a group of automorphisms of the code (by an earlier lemma). Since $|D_{96}| = 2^5 3$, this possibility is not excluded by the prime divisors of the automorphism group.

Further restrictions are imposed on the automorphism group of a [96,48,20] code and these are also satisfied by D_{96}.

In what follows, we show that the codes generated as such ideals $F_2 D_{96}(1 + yv)$ are (unfortunately) not extremal, using a different technique.

Notation and terminology

If R is a commutative ring and G is a group, then let RG denote the group ring. The unit group of RG is the group of invertible elements of RG and is written as $U(RG)$.

If $\alpha = \sum a_g g \in RG$ then $aug(\alpha) = \sum a_g \in R$ is called the augmentation of α. $V(RG)$ denotes the group of invertible elements of RG of augmentation 1 and is called the group of normalised units of RG.

Definition

Let $\alpha = \sum x_i g_i \in RG$ where $x_i \in R$, $x_i \neq 0$ and $g_i \in G$. Then consider the map $* : \sum x_i g_i \to \sum x_i g_i^{-1}$.
This map is known as the classical involution of the group ring.

An element $\alpha \in RG$ is called *unitary* (or a *unitary unit*) if $\alpha\alpha^* = 1 = \alpha^*\alpha$ (i.e. $\alpha^* = \alpha^{-1}$).

The unitary units form a subgroup of $U(RG)$, written as $U_*(RG)$. $V_*(RG)$ denotes the group of unitary normalised units of RG.
An element $\alpha \in RG$ is called *symmetric* if $\alpha = \alpha^*$.

Notation and terminology

If R is a commutative ring and G is a group, then let RG denote the group ring. The unit group of RG is the group of invertible elements of RG and is written as $U(RG)$.

If $\alpha = \sum a_g g \in RG$ then $aug(\alpha) = \sum a_g \in R$ is called the augmentation of α. $V(RG)$ denotes the group of invertible elements of RG of augmentation 1 and is called the group of normalised units of RG.

Definition

Let $\alpha = \sum x_i g_i \in RG$ where $x_i \in R$, $x_i \neq 0$ and $g_i \in G$. Then consider the map $* : \sum x_i g_i \to \sum x_i g_i^{-1}$.
This map is known as the classical involution of the group ring.

An element $\alpha \in RG$ is called *unitary* (or a *unitary unit*) if $\alpha\alpha^* = 1 = \alpha^*\alpha$ (i.e. $\alpha^* = \alpha^{-1}$).

The unitary units form a subgroup of $U(RG)$, written as $U_*(RG)$.
$V_*(RG)$ denotes the group of unitary normalised units of RG.
An element $\alpha \in RG$ is called *symmetric* if $\alpha = \alpha^*$.

Notation and terminology

If R is a commutative ring and G is a group, then let RG denote the group ring. The unit group of RG is the group of invertible elements of RG and is written as $U(RG)$.

If $\alpha = \sum a_g g \in RG$ then $aug(\alpha) = \sum a_g \in R$ is called the augmentation of α. $V(RG)$ denotes the group of invertible elements of RG of augmentation 1 and is called the group of normalised units of RG.

Definition

Let $\alpha = \sum x_i g_i \in RG$ where $x_i \in R$, $x_i \neq 0$ and $g_i \in G$. Then consider the map $* : \sum x_i g_i \to \sum x_i g_i^{-1}$.
This map is known as the classical involution of the group ring.

An element $\alpha \in RG$ is called *unitary* (or a *unitary unit*) if $\alpha\alpha^* = 1 = \alpha^*\alpha$ (i.e. $\alpha^* = \alpha^{-1}$).

The unitary units form a subgroup of $U(RG)$, written as $U_*(RG)$. $V_*(RG)$ denotes the group of unitary normalised units of RG. An element $\alpha \in RG$ is called *symmetric* if $\alpha = \alpha^*$.

Notation and terminology

If R is a commutative ring and G is a group, then let RG denote the group ring. The unit group of RG is the group of invertible elements of RG and is written as $U(RG)$.

If $\alpha = \sum a_g g \in RG$ then $aug(\alpha) = \sum a_g \in R$ is called the augmentation of α. $V(RG)$ denotes the group of invertible elements of RG of augmentation 1 and is called the group of normalised units of RG.

Definition

Let $\alpha = \sum x_i g_i \in RG$ where $x_i \in R$, $x_i \neq 0$ and $g_i \in G$. Then consider the map $* : \sum x_i g_i \to \sum x_i g_i^{-1}$.
This map is known as the classical involution of the group ring.

An element $\alpha \in RG$ is called *unitary* (or a *unitary unit*) if $\alpha\alpha^* = 1 = \alpha^*\alpha$ (i.e. $\alpha^* = \alpha^{-1}$).

The unitary units form a subgroup of $U(RG)$, written as $U_*(RG)$.
$V_*(RG)$ denotes the group of unitary normalised units of RG.
An element $\alpha \in RG$ is called *symmetric* if $\alpha = \alpha^*$.

Notation and terminology

If R is a commutative ring and G is a group, then let RG denote the group ring. The unit group of RG is the group of invertible elements of RG and is written as $U(RG)$.

If $\alpha = \sum a_g g \in RG$ then $aug(\alpha) = \sum a_g \in R$ is called the augmentation of α. $V(RG)$ denotes the group of invertible elements of RG of augmentation 1 and is called the group of normalised units of RG.

Definition

Let $\alpha = \sum x_i g_i \in RG$ where $x_i \in R$, $x_i \neq 0$ and $g_i \in G$. Then consider the map $* : \sum x_i g_i \to \sum x_i g_i^{-1}$.
This map is known as the classical involution of the group ring.

An element $\alpha \in RG$ is called *unitary* (or a *unitary unit*) if $\alpha\alpha^* = 1 = \alpha^*\alpha$ (i.e. $\alpha^* = \alpha^{-1}$).

The unitary units form a subgroup of $U(RG)$, written as $U_*(RG)$.
$V_*(RG)$ denotes the group of unitary normalised units of RG.
An element $\alpha \in RG$ is called *symmetric* if $\alpha = \alpha^*$.

Lemma (C., Gallagher, McLoughlin)

The code C generated by $u = 1 + yv$ is self-dual if and only if v is a unitary unit of F_2C_k if and only if A is an orthogonal $k \times k$ matrix with entries in F_2.

Proof.

The code C is the span of the rows of the group ring matrix U of $1 + yv$. Assume the code is self-dual. So $UU^T = 0$. The sub-matrix A is reverse circulant, so U is symmetric. Thus $U^2 = 0$. Due to the ring homomorphism between the group ring matrices and the group ring F_2D_{2k}, this implies that

$u^2 = (1 + yd)^2 = 1 + (yd)^2 = 1 + y^2d^*d = 1 + d^*d = 0$. Thus $d^*d = 1$, so d is a unitary unit in F_2C_k.

Conversely, assume that d is a unitary unit in F_2C_k. Then $UU^T = 0$, so $C \subseteq C^\perp$. But the $k \times k$ identity matrix is a sub-matrix of U so the null-space of U is at most of dimension k. Thus $C = C^\perp$. □

The problem now is to classify the unitary units of F_2C_k.

Lemma (C., Gallagher, McLoughlin)

The code C generated by $u = 1 + yv$ is self-dual if and only if v is a unitary unit of F_2C_k if and only if A is an orthogonal $k \times k$ matrix with entries in F_2.

Proof.

The code C is the span of the rows of the group ring matrix U of $1 + yv$. Assume the code is self-dual. So $UU^T = 0$. The sub-matrix A is reverse circulant, so U is symmetric. Thus $U^2 = 0$. Due to the ring homomorphism between the group ring matrices and the group ring F_2D_{2k}, this implies that

$u^2 = (1 + yd)^2 = 1 + (yd)^2 = 1 + y^2d^*d = 1 + d^*d = 0$. Thus $d^*d = 1$, so d is a unitary unit in F_2C_k.

Conversely, assume that d is a unitary unit in F_2C_k. Then $UU^T = 0$, so $C \subseteq C^\perp$. But the $k \times k$ identity matrix is a sub-matrix of U so the null-space of U is at most of dimension k. Thus $C = C^\perp$. □

The problem now is to classify the unitary units of F_2C_k.

Lemma (C., Gallagher, McLoughlin)

The code C generated by $u = 1 + yv$ is self-dual if and only if v is a unitary unit of F_2C_k if and only if A is an orthogonal $k \times k$ matrix with entries in F_2.

Proof.

The code C is the span of the rows of the group ring matrix U of $1 + yv$. Assume the code is self-dual. So $UU^T = 0$. The sub-matrix A is reverse circulant, so U is symmetric. Thus $U^2 = 0$. Due to the ring homomorphism between the group ring matrices and the group ring F_2D_{2k}, this implies that
$u^2 = (1 + yd)^2 = 1 + (yd)^2 = 1 + y^2d^*d = 1 + d^*d = 0$. Thus
$d^*d = 1$, so d is a unitary unit in F_2C_k.
Conversely, assume that d is a unitary unit in F_2C_k. Then $UU^T = 0$, so $C \subseteq C^\perp$. But the $k \times k$ identity matrix is a sub-matrix of U so the null-space of U is at most of dimension k. Thus $C = C^\perp$. □

The problem now is to classify the unitary units of F_2C_k.

Classification of $V_*(F_2C_k)$

- A.Bovdi and Szakacs (1989) described the structure of the unitary units of the normalised unit group $V_*(FG)$ when G is a finite abelian p-group and F is a finite field of characteristic p where p is an odd prime.
- For arbitrary primes p, A.Bovdi and Szakacs (1995) give a technique for finding the generators for the Sylow-p subgroup of the unitary units of F_pG where G is an abelian group.
- This technique will be used here to find a generating set of the unitary units of F_2C_{24} and F_2C_{48}. These units are then used to generate codes of length 48 and 96 respectively.

Classification of $V_*(F_2C_k)$

- A.Bovdi and Szakacs (1989) described the structure of the unitary units of the normalised unit group $V_*(FG)$ when G is a finite abelian p-group and F is a finite field of characteristic p where p is an odd prime.
- For arbitrary primes p, A.Bovdi and Szakacs (1995) give a technique for finding the generators for the Sylow-p subgroup of the unitary units of F_pG where G is an abelian group.
- This technique will be used here to find a generating set of the unitary units of F_2C_{24} and F_2C_{48}. These units are then used to generate codes of length 48 and 96 respectively.

- A.Bovdi and Szakacs (1989) described the structure of the unitary units of the normalised unit group $V_*(FG)$ when G is a finite abelian p-group and F is a finite field of characteristic p where p is an odd prime.
- For arbitrary primes p, A.Bovdi and Szakacs (1995) give a technique for finding the generators for the Sylow-p subgroup of the unitary units of F_pG where G is an abelian group.
- This technique will be used here to find a generating set of the unitary units of F_2C_{24} and F_2C_{48}. These units are then used to generate codes of length 48 and 96 respectively.

Lemma (C., Gallagher, McLoughlin)

$U(F_2C_{3(2^n)})$ is isomorphic to the direct product of a 2-group and a copy of the cyclic group of order 3. It has exponent $3(2^n)$.

Proof.

$U(F_2C_{3(2^n)}) \simeq U(F_2(C_3 \times C_{2^n})) \simeq U((F_2C_3)C_{2^n}) \simeq U((F_2 \oplus F_4)C_{2^n}) \simeq U(F_2C_{2^n} \oplus F_4C_{2^n}) \simeq U(F_2C_{2^n}) \times U(F_4C_{2^n}) \simeq U(F_2C_{2^n}) \times V(F_4C_{2^n}) \times U(F_4)$. Every element of $U(F_2C_{2^n})$ has order dividing 2^n since if $\alpha = \sum a_i g_i \in U(F_2C_{2^n})$ then $\alpha^{2^n} = \sum a_i^{2^n} g_i^{2^n} = \sum a_i^{2^n} = \sum a_i \in F_2$, so $\alpha^{2^n} = 1$.
Similarly every element of $V(F_4C_{2^n})$ has order dividing 2^n since if $\alpha = \sum a_i g_i \in V(F_4C_{2^n})$ then $\alpha^{2^n} \in F_4$, but α^{2^n} has augmentation 1, so $\alpha^{2^n} = 1$. Clearly $U(F_4) \simeq C_3$, so $U(F_2C_{3(2^n)})$ is the direct product of a 2-group and a copy of C_3. □

Corollary (C., Gallagher, McLoughlin)

$V_*(F_2C_{3(2^n)})$ is isomorphic to the direct product of its Sylow-2 subgroup and a copy of the cyclic group of order 3.
$V_*(F_2C_{3(2^n)})$ has exponent $3(2^n)$.

Lemma (C., Gallagher, McLoughlin)

$U(F_2 C_{3(2^n)})$ is isomorphic to the direct product of a 2-group and a copy of the cyclic group of order 3. It has exponent $3(2^n)$.

Proof.

$U(F_2 C_{3(2^n)}) \simeq U(F_2(C_3 \times C_{2^n})) \simeq U((F_2 C_3)C_{2^n}) \simeq U((F_2 \oplus F_4)C_{2^n}) \simeq U(F_2 C_{2^n} \oplus F_4 C_{2^n}) \simeq U(F_2 C_{2^n}) \times U(F_4 C_{2^n}) \simeq U(F_2 C_{2^n}) \times V(F_4 C_{2^n}) \times U(F_4)$. Every element of $U(F_2 C_{2^n})$ has order dividing 2^n since if $\alpha = \sum a_i g_i \in U(F_2 C_{2^n})$ then $\alpha^{2^n} = \sum a_i^{2^n} g_i^{2^n} = \sum a_i^{2^n} = \sum a_i \in F_2$, so $\alpha^{2^n} = 1$.
Similarly every element of $V(F_4 C_{2^n})$ has order dividing 2^n since if $\alpha = \sum a_i g_i \in V(F_4 C_{2^n})$ then $\alpha^{2^n} \in F_4$, but α^{2^n} has augmentation 1, so $\alpha^{2^n} = 1$. Clearly $U(F_4) \simeq C_3$, so $U(F_2 C_{3(2^n)})$ is the direct product of a 2-group and a copy of C_3. $\square$

Corollary (C., Gallagher, McLoughlin)

$V_*(F_2 C_{3(2^n)})$ is isomorphic to the direct product of its Sylow-2 subgroup and a copy of the cyclic group of order 3.
$V_*(F_2 C_{3(2^n)})$ has exponent $3(2^n)$.

Lemma (C., Gallagher, McLoughlin)

$U(F_2C_{3(2^n)})$ is isomorphic to the direct product of a 2-group and a copy of the cyclic group of order 3. It has exponent $3(2^n)$.

Proof.

$U(F_2C_{3(2^n)}) \simeq U(F_2(C_3 \times C_{2^n})) \simeq U((F_2C_3)C_{2^n}) \simeq U((F_2 \oplus F_4)C_{2^n}) \simeq U(F_2C_{2^n} \oplus F_4C_{2^n}) \simeq U(F_2C_{2^n}) \times U(F_4C_{2^n}) \simeq U(F_2C_{2^n}) \times V(F_4C_{2^n}) \times U(F_4)$. Every element of $U(F_2C_{2^n})$ has order dividing 2^n since if $\alpha = \sum a_i g_i \in U(F_2C_{2^n})$ then $\alpha^{2^n} = \sum a_i^{2^n} g_i^{2^n} = \sum a_i^{2^n} = \sum a_i \in F_2$, so $\alpha^{2^n} = 1$.
Similarly every element of $V(F_4C_{2^n})$ has order dividing 2^n since if $\alpha = \sum a_i g_i \in V(F_4C_{2^n})$ then $\alpha^{2^n} \in F_4$, but α^{2^n} has augmentation 1, so $\alpha^{2^n} = 1$. Clearly $U(F_4) \simeq C_3$, so $U(F_2C_{3(2^n)})$ is the direct product of a 2-group and a copy of C_3. □

Corollary (C., Gallagher, McLoughlin)

$V_*(F_2C_{3(2^n)})$ is isomorphic to the direct product of its Sylow-2 subgroup and a copy of the cyclic group of order 3.
$V_*(F_2C_{3(2^n)})$ has exponent $3(2^n)$.

Definition

Let the group $C_{3(2^n)}$ have presentation $\langle b | b^{3(2^n)} = 1 \rangle$. Define $a = b^3$ and define $C = \langle a \rangle$, a cyclic group of order 2^n. Let $h = b^{2^n}$ and define $H = \langle h \rangle$, a cyclic group of order 3. So $C \times H \simeq C_{3(2^n)}$.

Theorem (C., Gallagher, McLoughlin)

For $n > 1$ the group $V_*(F_2 C_{3(2^n)})$ has basis

$$\{(1 + (a+1)^{\alpha})^*(1 + (a+1)^{\alpha})^{-1} | \alpha = 5, 9, 13, \dots, 2^n - 3\} \cup$$

$$\{(1 + h(a+1)^{\alpha})^*(1 + h(a+1)^{\alpha})^{-1} | \alpha = 1, 3, 5, \dots, 2^n - 1\} \cup$$

$$\{a\} \cup \{1 + (a+1)^{2^n - 1}\} \cup \{h\}$$

Proof.

The proof relies on the Corollary above and on a result of A.Bovdi and Szakacs (1995). □

Definition

Let the group $C_{3(2^n)}$ have presentation $\langle b | b^{3(2^n)} = 1\rangle$. Define $a = b^3$ and define $C = \langle a\rangle$, a cyclic group of order 2^n. Let $h = b^{2^n}$ and define $H = \langle h\rangle$, a cyclic group of order 3. So $C \times H \simeq C_{3(2^n)}$.

Theorem (C., Gallagher, McLoughlin)

For $n > 1$ the group $V_*(F_2 C_{3(2^n)})$ has basis

$$\{(1+(a+1)^\alpha)^*(1+(a+1)^\alpha)^{-1} | \alpha = 5, 9, 13, \ldots, 2^n - 3\} \cup$$

$$\{(1+h(a+1)^\alpha)^*(1+h(a+1)^\alpha)^{-1} | \alpha = 1, 3, 5, \ldots, 2^n - 1\} \cup$$

$$\{a\} \cup \{1+(a+1)^{2^n-1}\} \cup \{h\}$$

Proof.

The proof relies on the Corollary above and on a result of A.Bovdi and Szakacs (1995). □

Definition

Let the group $C_{3(2^n)}$ have presentation $\langle b | b^{3(2^n)} = 1 \rangle$. Define $a = b^3$ and define $C = \langle a \rangle$, a cyclic group of order 2^n. Let $h = b^{2^n}$ and define $H = \langle h \rangle$, a cyclic group of order 3. So $C \times H \simeq C_{3(2^n)}$.

Theorem (C., Gallagher, McLoughlin)

For $n > 1$ the group $V_*(F_2 C_{3(2^n)})$ has basis

$$\{(1 + (a+1)^\alpha)^*(1 + (a+1)^\alpha)^{-1} | \alpha = 5, 9, 13, \ldots, 2^n - 3\} \cup$$

$$\{(1 + h(a+1)^\alpha)^*(1 + h(a+1)^\alpha)^{-1} | \alpha = 1, 3, 5, \ldots, 2^n - 1\} \cup$$

$$\{a\} \cup \{1 + (a+1)^{2^n - 1}\} \cup \{h\}$$

Proof.

The proof relies on the Corollary above and on a result of A.Bovdi and Szakacs (1995). □

Lemma (Lucas' Theorem)

Let n and i be positive integers with $n \geq i$, let p be a prime, write n in its base p decomposition as $n = \sum_{j=0}^{d} n_j p^j$ and write i in its base p decomposition as $i = \sum_{j=0}^{d} i_j p^j$ where $0 \leq n_j \leq p-1$ and $0 \leq i_j \leq p-1$ for all $0 \leq j \leq d$.
Then $\binom{n}{i} = \prod_{j=0}^{d} \binom{n_j}{i_j} \pmod{p}$.

Lemma (C., Gallagher, McLoughlin)

In $V_*(F_2 C_{3(2^n)})$, $1 + (a+1)^{2^n - 1} = 1 + \hat{a}$ and hence has multiplicative order 2.

Proof.

Apply Lucas' Theorem with $p = 2$. Since $2^n - 1 = 1 + 1(2^1) + 1(2^2) + \cdots + 1(2^{n-1}) = \sum_{j=0}^{2^{n-1}} 1(2^j)$ then for any $i = \sum_{j=0}^{2^{n-1}} i_j 2^j \leq 2^n - 1$ we have $\binom{2^n - 1}{i} = \prod_{j=0}^{2^{n-1}} \binom{1}{i_j} = \prod_{j=0}^{2^{n-1}} 1 = 1$.
Hence

$$(1+a)^{2^n - 1} = \sum_{i=0}^{2^n - 1} \binom{2^n - 1}{i} a^i = \sum_{i=0}^{2^n - 1} 1 a^i = \hat{a}$$

Lemma (Lucas' Theorem)

Let n and i be positive integers with $n \geq i$, let p be a prime, write n in its base p decomposition as $n = \sum_{j=0}^{d} n_j p^j$ and write i in its base p decomposition as $i = \sum_{j=0}^{d} i_j p^j$ where $0 \leq n_j \leq p-1$ and $0 \leq i_j \leq p-1$ for all $0 \leq j \leq d$.
Then $\binom{n}{i} = \prod_{j=0}^{d} \binom{n_j}{i_j}$ (mod p).

Lemma (C., Gallagher, McLoughlin)

In $V_*(F_2 C_{3(2^n)})$, $1 + (a+1)^{2^n - 1} = 1 + \hat{a}$ and hence has multiplicative order 2.

Proof.

Apply Lucas' Theorem with $p = 2$. Since $2^n - 1 = 1 + 1(2^1) + 1(2^2) + \cdots + 1(2^{n-1}) = \sum_{j=0}^{2^{n-1}} 1(2^j)$ then for any $i = \sum_{j=0}^{2^{n-1}} i_j 2^j \leq 2^n - 1$ we have $\binom{2^n - 1}{i} = \prod_{j=0}^{2^{n-1}} \binom{1}{i_j} = \prod_{j=0}^{2^{n-1}} 1 = 1$.
Hence

$$(1+a)^{2^n - 1} = \sum_{i=0}^{2^n - 1} \binom{2^n - 1}{i} a^i = \sum_{i=0}^{2^n - 1} 1 a^i = \hat{a}$$

Lemma (Lucas' Theorem)

Let n and i be positive integers with $n \geq i$, let p be a prime, write n in its base p decomposition as $n = \sum_{j=0}^{d} n_j p^j$ and write i in its base p decomposition as $i = \sum_{j=0}^{d} i_j p^j$ where $0 \leq n_j \leq p-1$ and $0 \leq i_j \leq p-1$ for all $0 \leq j \leq d$.
Then $\binom{n}{i} = \prod_{j=0}^{d} \binom{n_j}{i_j}$ (mod p).

Lemma (C., Gallagher, McLoughlin)

In $V_*(F_2 C_{3(2^n)})$, $1 + (a+1)^{2^n - 1} = 1 + \hat{a}$ and hence has multiplicative order 2.

Proof.

Apply Lucas' Theorem with $p = 2$. Since $2^n - 1 = 1 + 1(2^1) + 1(2^2) + \cdots + 1(2^{n-1}) = \sum_{j=0}^{2^{n-1}} 1(2^j)$ then for any $i = \sum_{j=0}^{2^{n-1}} i_j 2^j \leq 2^n - 1$ we have $\binom{2^n - 1}{i} = \prod_{j=0}^{2^{n-1}} \binom{1}{i_j} = \prod_{j=0}^{2^{n-1}} 1 = 1$.
Hence

$$(1+a)^{2^n - 1} = \sum_{i=0}^{2^n - 1} \binom{2^n - 1}{i} a^i = \sum_{i=0}^{2^n - 1} 1 a^i = \hat{a}$$

Lemma (C., Gallagher, McLoughlin)

$(1+(a+1)^{4i+1})^*(1+(a+1)^{4i+1})^{-1}$ *has order dividing* 2^{n-2}.

Similar results give the defining relations of the group

$$V_*(F_2C_{2^{n-1}3})$$

In particular,

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

Lemma (C., Gallagher, McLoughlin)

$(1+(a+1)^{4i+1})^*(1+(a+1)^{4i+1})^{-1}$ *has order dividing* 2^{n-2}.

Similar results give the defining relations of the group

$$V_*(F_2C_{2^{n-1}3})$$

In particular,

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

Lemma (C., Gallagher, McLoughlin)

$(1+(a+1)^{4i+1})^*(1+(a+1)^{4i+1})^{-1}$ *has order dividing* 2^{n-2}.

Similar results give the defining relations of the group

$$V_*(F_2C_{2^{n-1}3})$$

In particular,

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

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 A Group Ring Construction of the Extended Binary Golay Code, *Des. Codes Cryptogr.* (2012) 63:29–41

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).*