Towards a group ring construction of codes using dihedral groups

Leo Creedon

School of Engineering and Design
Institute of Technology Sligo
Ireland

ALCOMA 15, March 17, 2015

- **Job Advertisement**
- Assistant Lecturer: Mathematics, Information Technology and Health Informatics in Institute of Technology Sligo, Ireland
- Deadline: Friday at noon.
- Email: creedon.leo@itsligo.ie
- http://itsligo.ie/vacancies/

An [n, k, d] code is a code with length n, rank k and minimum distance d.
In [Hurley and Hurley 2009] a new technique for constructing codes from group rings and circulant matrices is given.
This was applied in [Hurley and McLoughlin 2008] to construct the extended binary Golay code (the unique [24, 12, 8] linear block code).
Subsequently, in [McLoughlin 2012] a similar technique was used to construct the self-dual, doubly-even and extremal [48, 24, 12] binary linear block code.
Here these results are generalised (using the semi-simplicity of the underlying group algebra) to use unitary units to construct linear block codes of length $n = 3(2^n)$ for any positive whole number n.
Some of these results are based on joint work with Fergal Gallagher and Ian McLoughlin.

An [n, k, d] code is a code with length n, rank k and minimum distance d.
In [Hurley and Hurley 2009] a new technique for constructing codes from group rings and circulant matrices is given.
This was applied in [Hurley and McLoughlin 2008] to construct the extended binary Golay code (the unique [24, 12, 8] linear block code).
Subsequently, in [McLoughlin 2012] a similar technique was used to construct the self-dual, doubly-even and extremal [48, 24, 12] binary linear block code.
Here these results are generalised (using the semi-simplicity of the underlying group algebra) to use unitary units to construct linear block codes of length $n = 3(2^n)$ for any positive whole number n.
Some of these results are based on joint work with Fergal Gallagher and Ian McLoughlin.

An [n, k, d] code is a code with length n, rank k and minimum distance d.
In [Hurley and Hurley 2009] a new technique for constructing codes from group rings and circulant matrices is given.
This was applied in [Hurley and McLoughlin 2008] to construct the extended binary Golay code (the unique [24, 12, 8] linear block code).
Subsequently, in [McLoughlin 2012] a similar technique was used to construct the self-dual, doubly-even and extremal [48, 24, 12] binary linear block code.
Here these results are generalised (using the semi-simplicity of the underlying group algebra) to use unitary units to construct linear block codes of length $n = 3(2^n)$ for any positive whole number n.
Some of these results are based on joint work with Fergal Gallagher and Ian McLoughlin.

An [n, k, d] code is a code with length n, rank k and minimum distance d.
In [Hurley and Hurley 2009] a new technique for constructing codes from group rings and circulant matrices is given.
This was applied in [Hurley and McLoughlin 2008] to construct the extended binary Golay code (the unique [24, 12, 8] linear block code).
Subsequently, in [McLoughlin 2012] a similar technique was used to construct the self-dual, doubly-even and extremal [48, 24, 12] binary linear block code.
Here these results are generalised (using the semi-simplicity of the underlying group algebra) to use unitary units to construct linear block codes of length $n = 3(2^n)$ for any positive whole number n.
Some of these results are based on joint work with Fergal Gallagher and Ian McLoughlin.

An [n, k, d] code is a code with length n, rank k and minimum distance d.
In [Hurley and Hurley 2009] a new technique for constructing codes from group rings and circulant matrices is given.
This was applied in [Hurley and McLoughlin 2008] to construct the extended binary Golay code (the unique [24, 12, 8] linear block code).
Subsequently, in [McLoughlin 2012] a similar technique was used to construct the self-dual, doubly-even and extremal [48, 24, 12] binary linear block code.
Here these results are generalised (using the semi-simplicity of the underlying group algebra) to use unitary units to construct linear block codes of length $n = 3(2^n)$ for any positive whole number n.
Some of these results are based on joint work with Fergal Gallagher and Ian McLoughlin.

Definition

A generator matrix of an (n, k) code C is a $k \times n$ matrix whose rowspace is the set of all codewords. If the entries of the matrix are over $\mathbb{F}_2$, then the code C is a subspace of dimension $\leq k$ in the larger vector space $\mathbb{F}_2^n$. Such a code is called a *linear block code*. The rank of the generator matrix must be equal to k. Thus we can put the generator matrix in *standard form* $[IP]$ with I being the $k \times k$ identity matrix on the left and P being a $k \times (n - k)$ *parity* matrix on the right.

Group Rings

Definition

Given a group G and a commutative ring R, define the group ring as the set of all formal finite linear combinations of elements of G, with coefficients in R. So $RG = \{\sum a_g g | a_g \in R, g \in G\}$. Define addition in the obvious way: $\sum a_g g + \sum b_g g = \sum (a_g + b_g) g$.
Define multiplication as
$(\sum_{g \in G} a_g g)(\sum_{h \in G} b_h h) = \sum_{g,h \in G} (a_g b_h)(gh)$
Usually R is a field, so RG is an algebra.

Definition

Given a group G and a commutative ring R, define the group ring as the set of all functions from G to R (with finite support).
Define addition pointwise $(f + g) : x \mapsto f(x) + f(y)$
and define multiplication using convolution of functions:
$(fg) : x \mapsto \sum_{uv=x} f(u)g(v) = \sum_{u \in G} f(u)g(u^{-1}x)$

Group Rings

Definition

Given a group G and a commutative ring R, define the group ring as the set of all formal finite linear combinations of elements of G, with coefficients in R. So $RG = \{\sum a_g g | a_g \in R, g \in G\}$. Define addition in the obvious way: $\sum a_g g + \sum b_g g = \sum (a_g + b_g) g$.
Define multiplication as
$(\sum_{g \in G} a_g g)(\sum_{h \in G} b_h h) = \sum_{g,h \in G} (a_g b_h)(gh)$
Usually R is a field, so RG is an algebra.

Definition

Given a group G and a commutative ring R, define the group ring as the set of all functions from G to R (with finite support).
Define addition pointwise $(f + g) : x \mapsto f(x) + f(y)$
and define multiplication using convolution of functions:
$(fg) : x \mapsto \sum_{uv=x} f(u)g(v) = \sum_{u \in G} f(u)g(u^{-1}x)$

- Let RG be a group ring with $|G| = n$. Then for each element of the group ring there is a unique $n \times n$ matrix with coefficients from R according to a particular listing of the group elements. A listing of the group elements is a permutation of the n group elements. For example, consider the group ring $\mathbb{F}_2 C_4$ with group listing $1, x, x^2, x^3$. We can form a group matrix as follows.

	1	x	x^2	x^3
1	1	x	x^2	x^3
x^3	x^3	1	x	x^2
x^2	x^2	x^3	1	x
x	x	x^2	x^3	1

- Let RG be a group ring with $|G| = n$. Then for each element of the group ring there is a unique $n \times n$ matrix with coefficients from R according to a particular listing of the group elements. A listing of the group elements is a permutation of the n group elements. For example, consider the group ring $\mathbb{F}_2 C_4$ with group listing $1, x, x^2, x^3$. We can form a group matrix as follows.
-

	1	x	x^2	x^3
1	1	x	x^2	x^3
x^3	x^3	1	x	x^2
x^2	x^2	x^3	1	x
x	x	x^2	x^3	1

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 consist of the product of the row and column headings. Thus we get the 4×4 group matrix

$$\begin{bmatrix} 1 & x & x^2 & x^3 \\ x^3 & 1 & x & x^2 \\ x^2 & x^3 & 1 & x \\ x & x^2 & x^3 & 1 \end{bmatrix}$$

With this group matrix, we can form a group ring matrix for each group ring element. For example consider the group ring element $x^2 + x^3$ in $\mathbb{F}_2 C_4$. Then the group ring matrix according to the group listing $1, x, x^2, x^3$ is the coefficients of the group elements x^2 and x^3 in the positions where these group elements appear in the group matrix.

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 consist of the product of the row and column headings. Thus we get the 4×4 group matrix

$$\begin{bmatrix} 1 & x & x^2 & x^3 \\ x^3 & 1 & x & x^2 \\ x^2 & x^3 & 1 & x \\ x & x^2 & x^3 & 1 \end{bmatrix}$$

With this group matrix, we can form a group ring matrix for each group ring element. For example consider the group ring element $x^2 + x^3$ in $\mathbb{F}_2 C_4$. Then the group ring matrix according to the group listing $1, x, x^2, x^3$ is the coefficients of the group elements x^2 and x^3 in the positions where these group elements appear in the group matrix.

So the group ring matrix of $x^2 + x^3$ is

$$\begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

There is a ring isomorphism between the group ring and the ring of group ring matrices according to a group listing [Hurley and Hurley 2009].

Lemma (Hurley and Hurley 2009)

In a group algebra FG, a non-zero element u is a zero divisor if the corresponding group ring matrix does not have full rank, and is a unit otherwise.

Consider for example the group ring $\mathbb{F}_2 D_8$ with group listing $1, x, x^2, x^3, y, xy, x^2y, x^3y$. We can form a group matrix as follows

	1	x	x^2	x^3	y	xy	x^2y	x^3y
1	1	x	x^2	x^3	y	xy	x^2y	x^3y
x^3	x^3	1	x	x^2	xy	x^2y	x^3y	y
x^2	x^2	x^3	1	x	x^2y	x^3y	y	xy
x	x	x^2	x^3	1	x^3y	y	xy	x^2y
y	y	xy	x^2y	x^3y	1	x	x^2	x^3
xy	xy	x^2y	x^3y	y	x^3	1	x	x^2
x^2y	x^2y	x^3y	y	xy	x^2	x^3	1	x
x^3y	x^3y	y	xy	x^2y	x	x^2	x^3	1

Notice that the structure of the group matrix is $\begin{bmatrix} B & A \\ A & B \end{bmatrix}$ where B is a 4×4 circulant matrix and A is a 4×4 reverse circulant matrix. The group ring matrix will also have the same structure. Because A is reverse circulant, $A = A^T$.

Consider for example the group ring $\mathbb{F}_2 D_8$ with group listing $1, x, x^2, x^3, y, xy, x^2y, x^3y$. We can form a group matrix as follows

	1	x	x^2	x^3	y	xy	x^2y	x^3y
1	1	x	x^2	x^3	y	xy	x^2y	x^3y
x^3	x^3	1	x	x^2	xy	x^2y	x^3y	y
x^2	x^2	x^3	1	x	x^2y	x^3y	y	xy
x	x	x^2	x^3	1	x^3y	y	xy	x^2y
y	y	xy	x^2y	x^3y	1	x	x^2	x^3
xy	xy	x^2y	x^3y	y	x^3	1	x	x^2
x^2y	x^2y	x^3y	y	xy	x^2	x^3	1	x
x^3y	x^3y	y	xy	x^2y	x	x^2	x^3	1

Notice that the structure of the group matrix is $\begin{bmatrix} B & A \\ A & B \end{bmatrix}$ where B is a 4×4 circulant matrix and A is a 4×4 reverse circulant matrix. The group ring matrix will also have the same structure. Because A is reverse circulant, $A = A^T$.

Consider for example the group ring $\mathbb{F}_2 D_8$ with group listing $1, x, x^2, x^3, y, xy, x^2y, x^3y$. We can form a group matrix as follows

	1	x	x^2	x^3	y	xy	x^2y	x^3y
1	1	x	x^2	x^3	y	xy	x^2y	x^3y
x^3	x^3	1	x	x^2	xy	x^2y	x^3y	y
x^2	x^2	x^3	1	x	x^2y	x^3y	y	xy
x	x	x^2	x^3	1	x^3y	y	xy	x^2y
y	y	xy	x^2y	x^3y	1	x	x^2	x^3
xy	xy	x^2y	x^3y	y	x^3	1	x	x^2
x^2y	x^2y	x^3y	y	xy	x^2	x^3	1	x
x^3y	x^3y	y	xy	x^2y	x	x^2	x^3	1

Notice that the structure of the group matrix is $\begin{bmatrix} B & A \\ A & B \end{bmatrix}$ where B is a 4×4 circulant matrix and A is a 4×4 reverse circulant matrix. The group ring matrix will also have the same structure. Because A is reverse circulant, $A = A^T$.

Self-Dual Unitary Unit Codes

Let $U(RG)$ denote the units of RG.
Let $V(RG)$ denote the normalised units of RG.
Let $\alpha = \sum a_i g_i \in RG$ where $a_i \in R$ and $g_i \in G$. Then consider the map

$$* : \sum a_i g_i \to \sum a_i g_i^{-1}$$

This map is an involution.
That is to say, $*$ is an antiautomorphism of order 2.
That is to say, $(\alpha\beta)^* = \beta^*\alpha^*$ and $(\alpha^*)^* = \alpha$ for all $\alpha, \beta \in RG$.
An element $\alpha \in RG$ is called unitary if $\alpha\alpha^* = 1 = \alpha^*\alpha$ (i.e. $\alpha^* = \alpha^{-1}$).
$*$ is known as the classical involution of the group ring (there are also non-classical involutions)
Let H be a subset of an arbitrary group ring RG.
Then H_* denotes the unitary units of H.

Self-Dual Unitary Unit Codes

Let $U(RG)$ denote the units of RG.
Let $V(RG)$ denote the normalised units of RG.
Let $\alpha = \sum a_i g_i \in RG$ where $a_i \in R$ and $g_i \in G$. Then consider the map

$$* : \sum a_i g_i \to \sum a_i g_i^{-1}$$

This map is an involution.
That is to say, $*$ is an antiautomorphism of order 2.
That is to say, $(\alpha\beta)^* = \beta^*\alpha^*$ and $(\alpha^*)^* = \alpha$ for all $\alpha, \beta \in RG$.
An element $\alpha \in RG$ is called unitary if $\alpha\alpha^* = 1 = \alpha^*\alpha$ (i.e. $\alpha^* = \alpha^{-1}$).
$*$ is known as the classical involution of the group ring (there are also non-classical involutions)
Let H be a subset of an arbitrary group ring RG.
Then H_* denotes the unitary units of H.

Self-Dual Unitary Unit Codes

Let $U(RG)$ denote the units of RG.
Let $V(RG)$ denote the normalised units of RG.
Let $\alpha = \sum a_i g_i \in RG$ where $a_i \in R$ and $g_i \in G$. Then consider the map

$$* : \sum a_i g_i \to \sum a_i g_i^{-1}$$

This map is an involution.
That is to say, $*$ is an antiautomorphism of order 2.
That is to say, $(\alpha\beta)^* = \beta^*\alpha^*$ and $(\alpha^*)^* = \alpha$ for all $\alpha, \beta \in RG$.
An element $\alpha \in RG$ is called unitary if $\alpha\alpha^* = 1 = \alpha^*\alpha$ (i.e. $\alpha^* = \alpha^{-1}$).
$*$ is known as the classical involution of the group ring (there are also non-classical involutions)
Let H be a subset of an arbitrary group ring RG.
Then H_* denotes the unitary units of H.

Self-Dual Unitary Unit Codes

Let $U(RG)$ denote the units of RG.
Let $V(RG)$ denote the normalised units of RG.
Let $\alpha = \sum a_i g_i \in RG$ where $a_i \in R$ and $g_i \in G$. Then consider the map

$$* : \sum a_i g_i \to \sum a_i g_i^{-1}$$

This map is an involution.
That is to say, $*$ is an antiautomorphism of order 2.
That is to say, $(\alpha\beta)^* = \beta^*\alpha^*$ and $(\alpha^*)^* = \alpha$ for all $\alpha, \beta \in RG$.
An element $\alpha \in RG$ is called unitary if $\alpha\alpha^* = 1 = \alpha^*\alpha$ (i.e. $\alpha^* = \alpha^{-1}$).
$*$ is known as the classical involution of the group ring (there are also non-classical involutions)
Let H be a subset of an arbitrary group ring RG.
Then H_* denotes the unitary units of H.

Self-Dual Unitary Unit Codes

Let $U(RG)$ denote the units of RG.
Let $V(RG)$ denote the normalised units of RG.
Let $\alpha = \sum a_i g_i \in RG$ where $a_i \in R$ and $g_i \in G$. Then consider the map

$$* : \sum a_i g_i \to \sum a_i g_i^{-1}$$

This map is an involution.
That is to say, $*$ is an antiautomorphism of order 2.
That is to say, $(\alpha\beta)^* = \beta^*\alpha^*$ and $(\alpha^*)^* = \alpha$ for all $\alpha, \beta \in RG$.
An element $\alpha \in RG$ is called unitary if $\alpha\alpha^* = 1 = \alpha^*\alpha$ (i.e. $\alpha^* = \alpha^{-1}$).
$*$ is known as the classical involution of the group ring (there are also non-classical involutions)
Let H be a subset of an arbitrary group ring RG.
Then H_* denotes the unitary units of H.

Self-Dual Unitary Unit Codes

Let $u \in \mathbb{F}_2 D_{2n}$ and let $u = 1 + yd$ where d is a sum of some of the powers of x

(i.e. $d \in \mathbb{F}_2 C_n$ with $C_n = \langle x \rangle$ and $D_{2n} = \langle x, y | x^n = y^2 = 1, x^y = x^{-1} \rangle$).

Then the group ring matrix of u according to the listing $1, x, .., x^n, y, xy, .., x^n y$ is of the form $\begin{bmatrix} I & A \\ A & I \end{bmatrix}$.

Now $u^2 = 0 \Leftrightarrow (1 + yd)^2 = 0 \Leftrightarrow 1^2 + 2(yd) + ydyd = 0 \Leftrightarrow 1 + d^* d = 0 \Leftrightarrow d^* d = 1$.

Thus if $d^* d = 1$ (i.e. d is a unitary unit of $\mathbb{F}_2 C_n$), then u generates a code which is self dual and the code C generated by the group ring element u is self-dual.

Note that if C is a binary self-orthogonal code then each codeword has even weight. Such a code is called an *even* code or a Type I code. If every codeword has weight divisible by 4, then we have a doubly even code or a Type II code.

If d has weight equal to $-1 (mod 4)$, then it is a Type II code.

Self-Dual Unitary Unit Codes

Let $u \in \mathbb{F}_2 D_{2n}$ and let $u = 1 + yd$ where d is a sum of some of the powers of x
(i.e. $d \in \mathbb{F}_2 C_n$ with $C_n = \langle x \rangle$ and
$D_{2n} = \langle x, y | x^n = y^2 = 1, x^y = x^{-1} \rangle$).
Then the group ring matrix of u according to the listing $1, x, .., x^n, y, xy, .., x^n y$ is of the form $\begin{bmatrix} I & A \\ A & I \end{bmatrix}$.
Now $u^2 = 0 \Leftrightarrow (1 + yd)^2 = 0 \Leftrightarrow 1^2 + 2(yd) + ydyd = 0 \Leftrightarrow$
$1 + d^* d = 0 \Leftrightarrow d^* d = 1$.
Thus if $d^* d = 1$ (i.e. d is a unitary unit of $\mathbb{F}_2 C_n$), then u generates a code which is self dual and the code C generated by the group ring element u is self-dual.
Note that if C is a binary self-orthogonal code then each codeword has even weight. Such a code is called an *even* code or a Type I code. If every codeword has weight divisible by 4, then we have a doubly even code or a Type II code.
If d has weight equal to $-1 (mod 4)$, then it is a Type II code.

Self-Dual Unitary Unit Codes

Let $u \in \mathbb{F}_2 D_{2n}$ and let $u = 1 + yd$ where d is a sum of some of the powers of x
(i.e. $d \in \mathbb{F}_2 C_n$ with $C_n = \langle x \rangle$ and
$D_{2n} = \langle x, y | x^n = y^2 = 1, x^y = x^{-1} \rangle$).
Then the group ring matrix of u according to the listing $1, x, .., x^n, y, xy, .., x^n y$ is of the form $\begin{bmatrix} I & A \\ A & I \end{bmatrix}$.

Now $u^2 = 0 \Leftrightarrow (1 + yd)^2 = 0 \Leftrightarrow 1^2 + 2(yd) + ydyd = 0 \Leftrightarrow$
$1 + d^* d = 0 \Leftrightarrow d^* d = 1$.
Thus if $d^* d = 1$ (i.e. d is a unitary unit of $\mathbb{F}_2 C_n$), then u generates a code which is self dual and the code C generated by the group ring element u is self-dual.
Note that if C is a binary self-orthogonal code then each codeword has even weight. Such a code is called an *even* code or a Type I code. If every codeword has weight divisible by 4, then we have a doubly even code or a Type II code.
If d has weight equal to $-1 (mod 4)$, then it is a Type II code.

Self-Dual Unitary Unit Codes

Let $u \in \mathbb{F}_2 D_{2n}$ and let $u = 1 + yd$ where d is a sum of some of the powers of x
(i.e. $d \in \mathbb{F}_2 C_n$ with $C_n = \langle x \rangle$ and
$D_{2n} = \langle x, y | x^n = y^2 = 1, x^y = x^{-1} \rangle$).
Then the group ring matrix of u according to the listing $1, x, .., x^n, y, xy, .., x^n y$ is of the form $\begin{bmatrix} I & A \\ A & I \end{bmatrix}$.

Now $u^2 = 0 \Leftrightarrow (1 + yd)^2 = 0 \Leftrightarrow 1^2 + 2(yd) + ydyd = 0 \Leftrightarrow$
$1 + d^*d = 0 \Leftrightarrow d^*d = 1$.

Thus if $d^*d = 1$ (i.e. d is a unitary unit of $\mathbb{F}_2 C_n$), then u generates a code which is self dual and the code C generated by the group ring element u is self-dual.

Note that if C is a binary self-orthogonal code then each codeword has even weight. Such a code is called an *even* code or a Type I code. If every codeword has weight divisible by 4, then we have a doubly even code or a Type II code.

If d has weight equal to $-1 (mod 4)$, then it is a Type II code

Self-Dual Unitary Unit Codes

Let $u \in \mathbb{F}_2 D_{2n}$ and let $u = 1 + yd$ where d is a sum of some of the powers of x
(i.e. $d \in \mathbb{F}_2 C_n$ with $C_n = \langle x \rangle$ and
$D_{2n} = \langle x, y | x^n = y^2 = 1, x^y = x^{-1} \rangle$).
Then the group ring matrix of u according to the listing $1, x, .., x^n, y, xy, .., x^n y$ is of the form $\begin{bmatrix} I & A \\ A & I \end{bmatrix}$.
Now $u^2 = 0 \Leftrightarrow (1 + yd)^2 = 0 \Leftrightarrow 1^2 + 2(yd) + ydyd = 0 \Leftrightarrow$
$1 + d^* d = 0 \Leftrightarrow d^* d = 1$.
Thus if $d^* d = 1$ (i.e. d is a unitary unit of $\mathbb{F}_2 C_n$), then u generates a code which is self dual and the code C generated by the group ring element u is self-dual.
Note that if C is a binary self-orthogonal code then each codeword has even weight. Such a code is called an *even* code or a Type I code. If every codeword has weight divisible by 4, then we have a doubly even code or a Type II code.
If d has weight equal to $-1 (mod 4)$, then it is a Type II code

Self-Dual Unitary Unit Codes

Let $u \in \mathbb{F}_2 D_{2n}$ and let $u = 1 + yd$ where d is a sum of some of the powers of x
(i.e. $d \in \mathbb{F}_2 C_n$ with $C_n = \langle x \rangle$ and
$D_{2n} = \langle x, y | x^n = y^2 = 1, x^y = x^{-1} \rangle$).
Then the group ring matrix of u according to the listing $1, x, .., x^n, y, xy, .., x^n y$ is of the form $\begin{bmatrix} I & A \\ A & I \end{bmatrix}$.
Now $u^2 = 0 \Leftrightarrow (1 + yd)^2 = 0 \Leftrightarrow 1^2 + 2(yd) + ydyd = 0 \Leftrightarrow$
$1 + d^* d = 0 \Leftrightarrow d^* d = 1$.
Thus if $d^* d = 1$ (i.e. d is a unitary unit of $\mathbb{F}_2 C_n$), then u generates a code which is self dual and the code C generated by the group ring element u is self-dual.
Note that if C is a binary self-orthogonal code then each codeword has even weight. Such a code is called an *even* code or a Type I code. If every codeword has weight divisible by 4, then we have a doubly even code or a Type II code.
If d has weight equal to $-1 (mod 4)$, then it is a Type II code

The [24,12,8] Golay code

In [Hurley and McLoughlin 2008] these techniques were used to construct the extended binary Golay [24,12,8] code.
This was given as $u = 1 + yd \in F_2D_{24}$, where
$d = 110111101000 = 1 + b + b^3 + b^4 + b^5 + b^6 + b^8 \in F_2C_{12}$
This was found using a computationally "expensive" computer search.

This search can be greatly refined using the following algebraic considerations.

Now $F_2C_{12} \simeq F_2(C_3 \times C_4) \simeq (F_2C_3)C_4 \simeq (F_2 \oplus F_4)C_4$
$\simeq F_2C_4 \oplus F_4C_4$
$\simeq (F_2\langle b^4 \rangle)\langle b^3 \rangle \simeq$
$(F_2\langle b^4 \rangle \hat{b^4} \oplus F_2\langle b^4 \rangle (1 + \hat{b^4}))\langle b^3 \rangle \simeq (F_2\hat{b^4} \oplus F_2\langle b^4 \rangle (1 + \hat{b^4}))\langle b^3 \rangle$.
Note that $F_2\hat{b^4} = \{0, \hat{b^4}\} \simeq F_2$ and
$F_2\langle b^4 \rangle (1 + \hat{b^4}) = \{0, b^4 + b^8, 1 + b^4, 1 + b^8\} \simeq F_4$.

The [24,12,8] Golay code

In [Hurley and McLoughlin 2008] these techniques were used to construct the extended binary Golay [24,12,8] code.
This was given as $u = 1 + yd \in F_2D_{24}$, where
$d = 110111101000 = 1 + b + b^3 + b^4 + b^5 + b^6 + b^8 \in F_2C_{12}$
This was found using a computationally "expensive" computer search.
This search can be greatly refined using the following algebraic considerations.
Now $F_2C_{12} \simeq F_2(C_3 \times C_4) \simeq (F_2C_3)C_4 \simeq (F_2 \oplus F_4)C_4$
$\simeq F_2C_4 \oplus F_4C_4$
$\simeq (F_2\langle b^4 \rangle)\langle b^3 \rangle \simeq$
$(F_2\langle b^4 \rangle \hat{b^4} \oplus F_2\langle b^4 \rangle (1 + \hat{b^4}))\langle b^3 \rangle \simeq (F_2\hat{b^4} \oplus F_2\langle b^4 \rangle (1 + \hat{b^4}))\langle b^3 \rangle$.
Note that $F_2\hat{b^4} = \{0, \hat{b^4}\} \simeq F_2$ and
$F_2\langle b^4 \rangle (1 + \hat{b^4}) = \{0, b^4 + b^8, 1 + b^4, 1 + b^8\} \simeq F_4$.

The [24,12,8] Golay code

In [Hurley and McLoughlin 2008] these techniques were used to construct the extended binary Golay [24,12,8] code.
This was given as $u = 1 + yd \in F_2D_{24}$, where
$d = 110111101000 = 1 + b + b^3 + b^4 + b^5 + b^6 + b^8 \in F_2C_{12}$
This was found using a computationally "expensive" computer search.
This search can be greatly refined using the following algebraic considerations.
Now $F_2C_{12} \simeq F_2(C_3 \times C_4) \simeq (F_2C_3)C_4 \simeq (F_2 \oplus F_4)C_4$
$\simeq F_2C_4 \oplus F_4C_4$
$\simeq (F_2\langle b^4 \rangle)\langle b^3 \rangle \simeq$
$(F_2\langle b^4 \rangle \hat{b^4} \oplus F_2\langle b^4 \rangle (1 + \hat{b^4}))\langle b^3 \rangle \simeq (F_2\hat{b^4} \oplus F_2\langle b^4 \rangle (1 + \hat{b^4}))\langle b^3 \rangle$.
Note that $F_2\hat{b^4} = \{0, \hat{b^4}\} \simeq F_2$ and
$F_2\langle b^4 \rangle (1 + \hat{b^4}) = \{0, b^4 + b^8, 1 + b^4, 1 + b^8\} \simeq F_4$.

The [24,12,8] Golay code

In [Hurley and McLoughlin 2008] these techniques were used to construct the extended binary Golay [24,12,8] code.
This was given as $u = 1 + yd \in F_2D_{24}$, where
$d = 110111101000 = 1 + b + b^3 + b^4 + b^5 + b^6 + b^8 \in F_2C_{12}$
This was found using a computationally "expensive" computer search.
This search can be greatly refined using the following algebraic considerations.
Now $F_2C_{12} \simeq F_2(C_3 \times C_4) \simeq (F_2C_3)C_4 \simeq (F_2 \oplus F_4)C_4$
$\simeq F_2C_4 \oplus F_4C_4$
$\simeq (F_2\langle b^4 \rangle)\langle b^3 \rangle \simeq$
$(F_2\langle b^4 \rangle \hat{b^4} \oplus F_2\langle b^4 \rangle (1 + \hat{b^4}))\langle b^3 \rangle \simeq (F_2\hat{b^4} \oplus F_2\langle b^4 \rangle (1 + \hat{b^4}))\langle b^3 \rangle$.
Note that $F_2\hat{b^4} = \{0, \hat{b^4}\} \simeq F_2$ and
$F_2\langle b^4 \rangle (1 + \hat{b^4}) = \{0, b^4 + b^8, 1 + b^4, 1 + b^8\} \simeq F_4$.

The [24,12,8] Golay code

In [Hurley and McLoughlin 2008] these techniques were used to construct the extended binary Golay [24,12,8] code.
This was given as $u = 1 + yd \in F_2D_{24}$, where
$d = 110111101000 = 1 + b + b^3 + b^4 + b^5 + b^6 + b^8 \in F_2C_{12}$
This was found using a computationally "expensive" computer search.
This search can be greatly refined using the following algebraic considerations.
Now $F_2C_{12} \simeq F_2(C_3 \times C_4) \simeq (F_2C_3)C_4 \simeq (F_2 \oplus F_4)C_4$
$\simeq F_2C_4 \oplus F_4C_4$
$\simeq (F_2\langle b^4 \rangle)\langle b^3 \rangle \simeq$
$(F_2\langle b^4 \rangle \hat{b^4} \oplus F_2\langle b^4 \rangle (1 + \hat{b^4}))\langle b^3 \rangle \simeq (F_2\hat{b^4} \oplus F_2\langle b^4 \rangle (1 + \hat{b^4}))\langle b^3 \rangle.$
Note that $F_2\hat{b^4} = \{0, \hat{b^4}\} \simeq F_2$ and
$F_2\langle b^4 \rangle (1 + \hat{b^4}) = \{0, b^4 + b^8, 1 + b^4, 1 + b^8\} \simeq F_4.$

The [24,12,8] Golay code

In [Hurley and McLoughlin 2008] these techniques were used to construct the extended binary Golay [24,12,8] code.
This was given as $u = 1 + yd \in F_2D_{24}$, where
$d = 110111101000 = 1 + b + b^3 + b^4 + b^5 + b^6 + b^8 \in F_2C_{12}$
This was found using a computationally "expensive" computer search.
This search can be greatly refined using the following algebraic considerations.
Now $F_2C_{12} \simeq F_2(C_3 \times C_4) \simeq (F_2C_3)C_4 \simeq (F_2 \oplus F_4)C_4$
$\simeq F_2C_4 \oplus F_4C_4$
$\simeq (F_2\langle b^4\rangle)\langle b^3\rangle \simeq$
$(F_2\langle b^4\rangle\hat{b^4} \oplus F_2\langle b^4\rangle(1 + \hat{b^4}))\langle b^3\rangle \simeq (F_2\hat{b^4} \oplus F_2\langle b^4\rangle(1 + \hat{b^4}))\langle b^3\rangle.$
Note that $F_2\hat{b^4} = \{0, \hat{b^4}\} \simeq F_2$ and
$F_2\langle b^4\rangle(1 + \hat{b^4}) = \{0, b^4 + b^8, 1 + b^4, 1 + b^8\} \simeq F_4.$

The [24,12,8] Golay code

In [Hurley and McLoughlin 2008] these techniques were used to construct the extended binary Golay [24,12,8] code.
This was given as $u = 1 + yd \in F_2D_{24}$, where
$d = 110111101000 = 1 + b + b^3 + b^4 + b^5 + b^6 + b^8 \in F_2C_{12}$
This was found using a computationally "expensive" computer search.
This search can be greatly refined using the following algebraic considerations.
Now $F_2C_{12} \simeq F_2(C_3 \times C_4) \simeq (F_2C_3)C_4 \simeq (F_2 \oplus F_4)C_4$
$\simeq F_2C_4 \oplus F_4C_4$
$\simeq (F_2\langle b^4 \rangle)\langle b^3 \rangle \simeq$
$(F_2\langle b^4 \rangle \hat{b^4} \oplus F_2\langle b^4 \rangle (1 + \hat{b^4}))\langle b^3 \rangle \simeq (F_2\hat{b^4} \oplus F_2\langle b^4 \rangle (1 + \hat{b^4}))\langle b^3 \rangle$.
Note that $F_2\hat{b^4} = \{0, \hat{b^4}\} \simeq F_2$ and
$F_2\langle b^4 \rangle (1 + \hat{b^4}) = \{0, b^4 + b^8, 1 + b^4, 1 + b^8\} \simeq F_4$.

The [24,12,8] Golay code

In [Hurley and McLoughlin 2008] these techniques were used to construct the extended binary Golay [24,12,8] code.
This was given as $u = 1 + yd \in F_2D_{24}$, where
$d = 110111101000 = 1 + b + b^3 + b^4 + b^5 + b^6 + b^8 \in F_2C_{12}$
This was found using a computationally "expensive" computer search.
This search can be greatly refined using the following algebraic considerations.
Now $F_2C_{12} \simeq F_2(C_3 \times C_4) \simeq (F_2C_3)C_4 \simeq (F_2 \oplus F_4)C_4$
$\simeq F_2C_4 \oplus F_4C_4$
$\simeq (F_2\langle b^4 \rangle)\langle b^3 \rangle \simeq$
$(F_2\langle b^4 \rangle \hat{b^4} \oplus F_2\langle b^4 \rangle(1 + \hat{b^4}))\langle b^3 \rangle \simeq (F_2\hat{b^4} \oplus F_2\langle b^4 \rangle(1 + \hat{b^4}))\langle b^3 \rangle.$
Note that $F_2\hat{b^4} = \{0, \hat{b^4}\} \simeq F_2$ and
$F_2\langle b^4 \rangle(1 + \hat{b^4}) = \{0, b^4 + b^8, 1 + b^4, 1 + b^8\} \simeq F_4.$

The [24,12,8] Golay code

In [Hurley and McLoughlin 2008] these techniques were used to construct the extended binary Golay [24,12,8] code.
This was given as $u = 1 + yd \in F_2D_{24}$, where
$d = 110111101000 = 1 + b + b^3 + b^4 + b^5 + b^6 + b^8 \in F_2C_{12}$
This was found using a computationally "expensive" computer search.
This search can be greatly refined using the following algebraic considerations.
Now $F_2C_{12} \simeq F_2(C_3 \times C_4) \simeq (F_2C_3)C_4 \simeq (F_2 \oplus F_4)C_4$
$\simeq F_2C_4 \oplus F_4C_4$
$\simeq (F_2\langle b^4 \rangle)\langle b^3 \rangle \simeq$
$(F_2\langle b^4 \rangle \hat{b^4} \oplus F_2\langle b^4 \rangle(1 + \hat{b^4}))\langle b^3 \rangle \simeq (F_2\hat{b^4} \oplus F_2\langle b^4 \rangle(1 + \hat{b^4}))\langle b^3 \rangle$.
Note that $F_2\hat{b^4} = \{0, \hat{b^4}\} \simeq F_2$ and
$F_2\langle b^4 \rangle(1 + \hat{b^4}) = \{0, b^4 + b^8, 1 + b^4, 1 + b^8\} \simeq F_4$.

The [24,12,8] Golay code

In [Hurley and McLoughlin 2008] these techniques were used to construct the extended binary Golay [24,12,8] code.
This was given as $u = 1 + yd \in F_2D_{24}$, where
$d = 110111101000 = 1 + b + b^3 + b^4 + b^5 + b^6 + b^8 \in F_2C_{12}$
This was found using a computationally "expensive" computer search.
This search can be greatly refined using the following algebraic considerations.
Now $F_2C_{12} \simeq F_2(C_3 \times C_4) \simeq (F_2C_3)C_4 \simeq (F_2 \oplus F_4)C_4$
$\simeq F_2C_4 \oplus F_4C_4$
$\simeq (F_2\langle b^4\rangle)\langle b^3\rangle \simeq$
$(F_2\langle b^4\rangle\hat{b^4} \oplus F_2\langle b^4\rangle(1 + \hat{b^4}))\langle b^3\rangle \simeq (F_2\hat{b^4} \oplus F_2\langle b^4\rangle(1 + \hat{b^4}))\langle b^3\rangle.$
Note that $F_2\hat{b^4} = \{0, \hat{b^4}\} \simeq F_2$ and
$F_2\langle b^4\rangle(1 + \hat{b^4}) = \{0, b^4 + b^8, 1 + b^4, 1 + b^8\} \simeq F_4.$

The [24,12,8] Golay code

Note also that $e_1 = \hat{b^4}$ and $e_2 = b^4 + b^8 = 1 + \hat{b^4}$ are symmetric idempotents
(i.e. $e_i^2 = e_i$ and $e_i^* = e_i$ for $i = 1, 2$)
Let $c = b^3$ (an element of order 4). Now in this format,

$$d = (1+b^4+b^8)+(b^1+b^5)+b^3+b^6 = \hat{b^4}+b^9(b^4+b^8)+c^1+c^2$$

$$= c^0\hat{b^4} + c^3(b^4 + b^8) + (c^1 + c^2)(1 + \hat{b^4} + \hat{b^4})$$

$$= c^0\hat{b^4} + c^3(b^4 + b^8) + (c^1 + c^2)(\hat{b^4}) + (c^1 + c^2)(b^4 + b^8)$$

$$= (c^0 + c^1 + c^2)\hat{b^4} \oplus (c^1 + c^2 + c^3)(b^4 + b^8)$$

$$= (c^3 + \hat{c})\hat{b^4} \oplus (1 + \hat{c})(1 + \hat{b^4})$$

The [24,12,8] Golay code

So $d = (c^3 + \hat{c})\hat{b^4} \oplus (1 + \hat{c})(1 + \hat{b^4})$.

Note that $(c^3 + \hat{c})$ and $(1 + \hat{c})$ are unitary units and $\hat{b^4}$ and $(1 + \hat{b^4})$ are symmetric orthogonal idempotents.Now

$$d^2 = c^2\hat{b^4} \oplus c^0(b^4 + b^8)$$

$$\Rightarrow d^4 = c^0\hat{b^4} \oplus c^0(b^4 + b^8) = 1.$$

Also

$$dd^* = (c^3 + \hat{c})\hat{b^4}(c^1 + \hat{c})\hat{b^4} \oplus (1 + \hat{c})^2(b^4 + b^8)^2$$

$$= c^0\hat{b^4} \oplus c^0(b^4 + b^8) = 1$$

Hence d is a unitary unit of order 4.
Note the ease with which the above calculations were performed due to the direct decomposition of the group ring.

The [24,12,8] Golay code

So $d = (c^3 + \hat{c})\hat{b^4} \oplus (1 + \hat{c})(1 + \hat{b^4})$.
Note that $(c^3 + \hat{c})$ and $(1 + \hat{c})$ are unitary units and $\hat{b^4}$ and $(1 + \hat{b^4})$ are symmetric orthogonal idempotents.Now

$$d^2 = c^2\hat{b^4} \oplus c^0(b^4 + b^8)$$

$$\Rightarrow d^4 = c^0\hat{b^4} \oplus c^0(b^4 + b^8) = 1.$$

Also

$$dd^* = (c^3 + \hat{c})\hat{b^4}(c^1 + \hat{c})\hat{b^4} \oplus (1 + \hat{c})^2(b^4 + b^8)^2$$

$$= c^0\hat{b^4} \oplus c^0(b^4 + b^8) = 1$$

Hence d is a unitary unit of order 4.
Note the ease with which the above calculations were performed due to the direct decomposition of the group ring.

The [24,12,8] Golay code

So $d = (c^3 + \hat{c})\hat{b^4} \oplus (1 + \hat{c})(1 + \hat{b^4})$.
Note that $(c^3 + \hat{c})$ and $(1 + \hat{c})$ are unitary units and $\hat{b^4}$ and $(1 + \hat{b^4})$ are symmetric orthogonal idempotents.Now

$$d^2 = c^2\hat{b^4} \oplus c^0(b^4 + b^8)$$

$$\Rightarrow d^4 = c^0\hat{b^4} \oplus c^0(b^4 + b^8) = 1.$$

Also

$$dd^* = (c^3 + \hat{c})\hat{b^4}(c^1 + \hat{c})\hat{b^4} \oplus (1 + \hat{c})^2(b^4 + b^8)^2$$

$$= c^0\hat{b^4} \oplus c^0(b^4 + b^8) = 1$$

Hence d is a unitary unit of order 4.
Note the ease with which the above calculations were performed due to the direct decomposition of the group ring.

The [24,12,8] Golay code

So $d = (c^3 + \hat{c})\hat{b^4} \oplus (1 + \hat{c})(1 + \hat{b^4})$.
Note that $(c^3 + \hat{c})$ and $(1 + \hat{c})$ are unitary units and $\hat{b^4}$ and $(1 + \hat{b^4})$ are symmetric orthogonal idempotents.Now

$$d^2 = c^2\hat{b^4} \oplus c^0(b^4 + b^8)$$

$$\Rightarrow d^4 = c^0\hat{b^4} \oplus c^0(b^4 + b^8) = 1.$$

Also

$$dd^* = (c^3 + \hat{c})\hat{b^4}(c^1 + \hat{c})\hat{b^4} \oplus (1 + \hat{c})^2(b^4 + b^8)^2$$

$$= c^0\hat{b^4} \oplus c^0(b^4 + b^8) = 1$$

Hence d is a unitary unit of order 4.
Note the ease with which the above calculations were performed due to the direct decomposition of the group ring.

The [24,12,8] Golay code

So $d = (c^3 + \hat{c})\hat{b^4} \oplus (1 + \hat{c})(1 + \hat{b^4})$.
Note that $(c^3 + \hat{c})$ and $(1 + \hat{c})$ are unitary units and $\hat{b^4}$ and $(1 + \hat{b^4})$ are symmetric orthogonal idempotents.Now

$$d^2 = c^2\hat{b^4} \oplus c^0(b^4 + b^8)$$

$$\Rightarrow d^4 = c^0\hat{b^4} \oplus c^0(b^4 + b^8) = 1.$$

Also

$$dd^* = (c^3 + \hat{c})\hat{b^4}(c^1 + \hat{c})\hat{b^4} \oplus (1 + \hat{c})^2(b^4 + b^8)^2$$

$$= c^0\hat{b^4} \oplus c^0(b^4 + b^8) = 1$$

Hence d is a unitary unit of order 4.
Note the ease with which the above calculations were performed due to the direct decomposition of the group ring.

Generalisations

Lemma

Let K be any commutative ring and G any group. Suppose KG decomposes as $KGe_1 \oplus KGe_2$ where e_1 is a symmetric central idempotent and $e_2 = 1 - e_1$. $\alpha = \beta e_1 + \gamma e_2$ is a unitary unit if and only if $\beta\beta^* e_1 = e_1$ and $\gamma\gamma^* e_2 = e_2$.
In particular, if β and γ are unitary units (i.e. in $V_*(KG)$) then $\alpha = \beta e_1 + \gamma e_2$ is a unitary unit.

Proof.

Suppose α is a unitary unit. Then
$1 = \alpha\alpha^* = (\beta e_1 + \gamma e_2)(\beta e_1 + \gamma e_2)^* = (\beta e_1 + \gamma e_2)(e_1^*\beta^* + e_2^*\gamma^*) = (\beta e_1 + \gamma e_2)(e_1\beta^* + e_2\gamma^*) = \beta e_1^2\beta^* + \gamma e_2^2\gamma^* = \beta\beta^* e_1 + \gamma\gamma^* e_2$.
Hence $\beta\beta^* e_1 + \gamma\gamma^* e_2 = 1 = e_1 + e_2$ and so $\beta\beta^* e_1 = e_1$ and $\gamma\gamma^* e_2 = e_2$ since it is a direct decomposition of rings.
Conversely, suppose $\beta\beta^* e_1 = e_1$ and $\gamma\gamma^* e_2 = e_2$. Then
$\alpha\alpha^* = (\beta e_1 + \gamma e_2)(\beta e_1 + \gamma e_2)^* = (\beta e_1 + \gamma e_2)((\beta e_1)^* + (\gamma e_2)^*) = (\beta e_1 + \gamma e_2)(e_1^*\beta^* + e_2^*\gamma^*) = (\beta e_1 + \gamma e_2)(e_1\beta^* + e_2\gamma^*) = \beta e_1 e_1\beta^* + \gamma e_2 e_2\gamma^* = \beta e_1\beta^* + \gamma e_2\gamma^* = \beta\beta^* e_1 + \gamma\gamma^* e_2 = e_1 + e_2 = 1$ as required. □

Generalisations

Definition

Let F be a finite field of characteristic p.
Define $\odot : FG \to FG$ by $\odot(\sum a_i g_i) = \sum a_i^p g_i^{-1}$
(the classical involution on FG followed by the Frobenius automorphism on F)

Lemma

$\odot$ defines a (non-classical) involution on $F_4C_{2^n}$ given by $\odot(\sum a_i g_i) = \sum a_i^2 g_i^{-1}$

Generalisations

Definition

Let F be a finite field of characteristic p.
Define $\odot : FG \to FG$ by $\odot(\sum a_i g_i) = \sum a_i^p g_i^{-1}$
(the classical involution on FG followed by the Frobenius automorphism on F)

Lemma

$\odot$ defines a (non-classical) involution on $F_4 C_{2^n}$ given by $\odot(\sum a_i g_i) = \sum a_i^2 g_i^{-1}$

Generalisations

Let π_1 denote the projection of $F_2C_{3(2^n)} \simeq F_2C_{2^n} \oplus F_4C_{2^n}$ onto the left summand and let π_2 denote the projection onto the right summand.

Theorem

π_1 commutes with $*$
(i.e. $\pi_1(\alpha^*) = (\pi_1(\alpha))^*$ for all $\alpha \in F_2C_{3(2^n)}$.
However, π_2 does not commute with $*$.
In fact $\pi_2(\alpha^*) = (\pi_2(\alpha))^{\odot}$ for all $\alpha \in F_2C_{3(2^n)}$.

So $*$ restricts to the non-classical involution $\odot$ on $F_4C_{2^n}$. Hence $(\alpha e_2)(\alpha e_2)^* = e_2$ implies that αe_2 corresponds to a unitary unit in $F_2C_{2^n}$ under the non-classical involution $\odot$, i.e.
$\alpha e_2 \in U_{\odot}(F_4C_{2^n}) = \{u \in U(F_4C_{2^n}) | uu^{\odot} = 1\}$.

Generalisations

To find all the classical unitary units and test to find their minimum distance, it previously required a search of $F_2C_{3(2^n)}$ (containing $2^{3(2^n)}$ elements).

Now it requires a search of the classical unitary units of $F_2C_{2^n}$ (containing 2^{2^n} elements) and a search of the non-classical $\odot$-unitary units of $F_4C_{2^n}$ (containing $4^{2^n} = 2^{2^{n+1}}$ elements).

For example, for the Golay [24,12,8] code, McLoughlin and Hurley searched F_2C_{12} containing 2^{12} elements, whereas this new technique requires us to only search $2^{2^2} + 2^{2^3} = 2^4 + 2^8$ elements.

Similarly, for the extremal [48,24,12] code, McLoughlin searched F_2C_{24} containing 2^{24} elements, but this new technique requires us to only search $2^{2^3} + 2^{2^4} = 2^8 + 2^{16}$ elements.

Generalisations

To find all the classical unitary units and test to find their minimum distance, it previously required a search of $F_2C_{3(2^n)}$ (containing $2^{3(2^n)}$ elements).
Now it requires a search of the classical unitary units of $F_2C_{2^n}$ (containing 2^{2^n} elements) and a search of the non-classical $\odot$-unitary units of $F_4C_{2^n}$ (containing $4^{2^n} = 2^{2^{n+1}}$ elements).
For example, for the Golay [24,12,8] code, McLoughlin and Hurley searched F_2C_{12} containing 2^{12} elements, whereas this new technique requires us to only search $2^{2^2} + 2^{2^3} = 2^4 + 2^8$ elements.
Similarly, for the extremal [48,24,12] code, McLoughlin searched F_2C_{24} containing 2^{24} elements, but this new technique requires us to only search $2^{2^3} + 2^{2^4} = 2^8 + 2^{16}$ elements.

Generalisations

To find all the classical unitary units and test to find their minimum distance, it previously required a search of $F_2C_{3(2^n)}$ (containing $2^{3(2^n)}$ elements).
Now it requires a search of the classical unitary units of $F_2C_{2^n}$ (containing 2^{2^n} elements) and a search of the non-classical $\odot$-unitary units of $F_4C_{2^n}$ (containing $4^{2^n} = 2^{2^{n+1}}$ elements).
For example, for the Golay [24,12,8] code, McLoughlin and Hurley searched F_2C_{12} containing 2^{12} elements, whereas this new technique requires us to only search $2^{2^2} + 2^{2^3} = 2^4 + 2^8$ elements.
Similarly, for the extremal [48,24,12] code, McLoughlin searched F_2C_{24} containing 2^{24} elements, but this new technique requires us to only search $2^{2^3} + 2^{2^4} = 2^8 + 2^{16}$ elements.

Generalisations

To find all the classical unitary units and test to find their minimum distance, it previously required a search of $F_2C_{3(2^n)}$ (containing $2^{3(2^n)}$ elements).
Now it requires a search of the classical unitary units of $F_2C_{2^n}$ (containing 2^{2^n} elements) and a search of the non-classical $\odot$-unitary units of $F_4C_{2^n}$ (containing $4^{2^n} = 2^{2^{n+1}}$ elements).
For example, for the Golay [24,12,8] code, McLoughlin and Hurley searched F_2C_{12} containing 2^{12} elements, whereas this new technique requires us to only search $2^{2^2} + 2^{2^3} = 2^4 + 2^8$ elements.
Similarly, for the extremal [48,24,12] code, McLoughlin searched F_2C_{24} containing 2^{24} elements, but this new technique requires us to only search $2^{2^3} + 2^{2^4} = 2^8 + 2^{16}$ elements.

What next?

- The next step (for codes of length 96) will be to search F_2C_{48}. Searching all 2^{48} elements was computationally prohibitive, but with this new technique we need "only" test $2^{2^4} + 2^{2^5} = 2^{16} + 2^{32}$ elements.
- Note that we have been looking at codes of length $3(2^n)$. If we apply this technique to codes of length $m(2^n)$, where m is an odd number > 3 then the gains will be even greater. In particular, it may be very useful in hunting for an extremal [72,36,16] code (or determining that none exist).

What next?

- The next step (for codes of length 96) will be to search F_2C_{48}. Searching all 2^{48} elements was computationally prohibitive, but with this new technique we need "only" test $2^{2^4} + 2^{2^5} = 2^{16} + 2^{32}$ elements.
- Note that we have been looking at codes of length $3(2^n)$. If we apply this technique to codes of length $m(2^n)$, where m is an odd number > 3 then the gains will be even greater. In particular, it may be very useful in hunting for an extremal [72,36,16] code (or determining that none exist).

Thank You!