Self-dual and dual-containing codes from Group Rings.

Ted Hurley

Cyclic codes are group ring codes...

Cyclic codes are ideals in the group ring of the cyclic group.

Many related codes, such as shortened cyclic and some quasi-cyclic, are modules in the cyclic group ring.

Cyclic codes are group ring codes...

Cyclic codes are ideals in the group ring of the cyclic group.

Many related codes, such as shortened cyclic and some quasi-cyclic, are modules in the cyclic group ring.

Group Ring Codes are constructed from modules, which are sometimes ideals, in general group rings.

Cyclic codes are group ring codes...

Cyclic codes are ideals in the group ring of the cyclic group.

Many related codes, such as shortened cyclic and some quasi-cyclic, are modules in the cyclic group ring.

Group Ring Codes are constructed from modules, which are sometimes ideals, in general group rings.

Matrix representations may be obtained using an isomorphism between a group ring and a ring of matrices.

Cyclic codes are group ring codes...

Cyclic codes are ideals in the group ring of the cyclic group.

Many related codes, such as shortened cyclic and some quasi-cyclic, are modules in the cyclic group ring.

Group Ring Codes are constructed from modules, which are sometimes ideals, in general group rings.

Matrix representations may be obtained using an isomorphism between a group ring and a ring of matrices.

Properties, such as distance, can often be calculated from the group ring construction, and codes with a desired property, such as requiring the code to be *LDPC* or *self-dual*, can be constructed from group rings.

Self-dual, dual-containing ...

This talk presents the method of group rings to the construction of *self-dual* and *dual-containing codes*.

Self-dual, dual-containing ...

This talk presents the method of group rings to the construction of *self-dual* and *dual-containing codes*.

Properties of these codes may be derived directly from the *group ring* properties.

Self-dual, dual-containing ...

This talk presents the method of group rings to the construction of *self-dual* and *dual-containing codes*.

Properties of these codes may be derived directly from the *group ring* properties.

Quantum codes may be constructed from dual-containing codes.

Self-dual, dual-containing ...

This talk presents the method of group rings to the construction of *self-dual* and *dual-containing codes*.

Properties of these codes may be derived directly from the *group ring* properties.

Quantum codes may be constructed from dual-containing codes.

The method is *general* and *particular examples* may be deduced from the general method.

Self-dual, dual-containing ...

This talk presents the method of group rings to the construction of *self-dual* and *dual-containing codes*.

Properties of these codes may be derived directly from the *group ring* properties.

Quantum codes may be constructed from dual-containing codes.

The method is *general* and *particular examples* may be deduced from the general method.

Here examples are shown using group rings of direct products of cyclic groups and group rings of dihedral groups.

Many others are possible.

Cyclic group ring example

In Z_2C_7 it is easy to check that
$(1+g+g^3)(1+g+g^2+g^4)=0$; say $uv=0$.

Cyclic group ring example

In Z_2C_7 it is easy to check that
$(1+g+g^3)(1+g+g^2+g^4)=0$; say $uv=0$.

Now form the circulant matrices with first rows obtained from u, v:

$$\left(\begin{array}{ccccccc} 1 & g & g^2 & g^3 & g^4 & g^5 & g^6 \\ \hline 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array}\right)$$

Cyclic group ring example

In Z_2C_7 it is easy to check that
$(1+g+g^3)(1+g+g^2+g^4)=0$; say $uv=0$.

Now form the circulant matrices with first rows obtained from u, v:

$$\left(\begin{array}{ccccccc} 1 & g & g^2 & g^3 & g^4 & g^5 & g^6 \\ \hline 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array}\right)$$

This gives the following (circulant) matrices U and V:

Produce the matrix

$$U = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$V = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Produce the matrix representation

The last 3 rows of U are dependent on the first 4 rows and the last 4 rows of V are l.d. on the first 3 rows.

Produce the matrix representation

The last 3 rows of U are dependent on the first 4 rows and the last 4 rows of V are l.d. on the first 3 rows.

Thus consider

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Produce the matrix representation

The last 3 rows of U are dependent on the first 4 rows and the last 4 rows of V are l.d. on the first 3 rows.

Thus consider

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Then $GH^{\mathsf{T}} = 0$ and thus get the set-up for a code.

This is in fact the *Hamming Code* as a group ring code.

(Basically (linear) Coding Theory is the process of finding two matrices G, H such that $GH^{\mathsf{T}} = 0$ where G is $r \times n$, H^{T} is $n \times (n - r)$, $\operatorname{rank}(G) = r, \operatorname{rank}(H)^{\mathsf{T}} = n - r$.)

Cyclic codes

Cyclic codes are obtained from zero-divisors in a cyclic group ring.

Cyclic codes

Cyclic codes are obtained from zero-divisors in a cyclic group ring.

Matrices that are used in cyclic codes are *circulant matrices* or are derived from circulant matrices in the sense that certain rows of a circulant matrix are used for the generator matrix G and certain columns of a circulant matrix H are used for the check matrix, with $GH^{\mathsf{T}} = 0$.

Cyclic codes

Cyclic codes are obtained from zero-divisors in a cyclic group ring.

Matrices that are used in cyclic codes are *circulant matrices* or are derived from circulant matrices in the sense that certain rows of a circulant matrix are used for the generator matrix G and certain columns of a circulant matrix H are used for the check matrix, with $GH^{\mathsf{T}} = 0$.

Circulant matrices are simply the group ring elements of the cyclic group from the injection of the group ring into a ring of matrices.

Cyclic codes

Cyclic codes are obtained from zero-divisors in a cyclic group ring.

Matrices that are used in cyclic codes are *circulant matrices* or are derived from circulant matrices in the sense that certain rows of a circulant matrix are used for the generator matrix G and certain columns of a circulant matrix H are used for the check matrix, with $GH^{\mathsf{T}} = 0$.

Circulant matrices are simply the group ring elements of the cyclic group from the injection of the group ring into a ring of matrices.

Cyclic codes include such important codes as BCH, Reed-Solomon, (some) Golay and Hamming codes.

Group Rings

RG denotes a group ring with group G and ring R.

An element in a group ring has the form

$$w = \sum_{g \in G} \alpha_g g$$

with $\alpha_g \in R$.

Group Rings

RG denotes a group ring with group G and ring R.

An element in a group ring has the form

$$w = \sum_{g \in G} \alpha_g g$$

with $\alpha_g \in R$.

Thus the group ring is a module over R with basis consisting of the group elements and multiplication determined by the multiplication in the group.

Group Ring Codes

Zero-divisors (and units) in group rings are used to construct Group Ring Codes.

Within a group ring it is possible to construct codes of a particular type with particular properties.

Group Ring Codes

Zero-divisors (and units) in group rings are used to construct Group Ring Codes.

Within a group ring it is possible to construct codes of a particular type with particular properties.

Algebraic group ring constructions of LDPC codes are thus possible as are also Convolutional Codes.

Group Ring Codes

Zero-divisors (and units) in group rings are used to construct Group Ring Codes.

Within a group ring it is possible to construct codes of a particular type with particular properties.

Algebraic group ring constructions of LDPC codes are thus possible as are also Convolutional Codes.

Here we look at the construction of self-dual and dual-containing codes from group rings.

Matrix of group ring code

Going over to a matrix representation, as for example going over to a circulant matrix in case of cyclic codes, enables a matrix representation of the code.

Matrix of group ring code

Going over to a matrix representation, as for example going over to a circulant matrix in case of cyclic codes, enables a matrix representation of the code.

Properties come from the group ring construction.

Matrix of group ring code

Going over to a matrix representation, as for example going over to a circulant matrix in case of cyclic codes, enables a matrix representation of the code.

Properties come from the group ring construction.

The constructions are *algebraic* and the codes can be stored by an algebraic formula.Thus for example they have been found useful when low storage and/or low power are requirements.

Matrix of group ring code

Going over to a matrix representation, as for example going over to a circulant matrix in case of cyclic codes, enables a matrix representation of the code.

Properties come from the group ring construction.

The constructions are *algebraic* and the codes can be stored by an algebraic formula.Thus for example they have been found useful when low storage and/or low power are requirements.

Properties such as distance can be proved *algebraically*.

Group rings ... Convolution etc.

When R is a field, RG is often called a *group algebra*.

However group rings where the ring is not a field are useful and indeed a group ring where the ring is actually a group ring itself is useful for constructing and analysing Convolutional Codes.

Group rings ... Convolution etc.

When R is a field, RG is often called a *group algebra*.

However group rings where the ring is not a field are useful and indeed a group ring where the ring is actually a group ring itself is useful for constructing and analysing Convolutional Codes.

Group ring RG can be considered as the module (= vector space when R is a field) over R with basis consisting of the elements of G and with a multiplication determined by the *convolutional type multiplication* of the elements of G.

Group rings ... Convolution etc.

When R is a field, RG is often called a *group algebra*.

However group rings where the ring is not a field are useful and indeed a group ring where the ring is actually a group ring itself is useful for constructing and analysing Convolutional Codes.

Group ring RG can be considered as the module (= vector space when R is a field) over R with basis consisting of the elements of G and with a multiplication determined by the *convolutional type multiplication* of the elements of G.

The word *convolution* is the 'multiplication' used by Engineers in digital signal processing (DSP); the convolution they use in DSP is exactly the group ring multiplication when the group is the cyclic group.

Group rings ... Convolution etc.

When R is a field, RG is often called a *group algebra*.

However group rings where the ring is not a field are useful and indeed a group ring where the ring is actually a group ring itself is useful for constructing and analysing Convolutional Codes.

Group ring RG can be considered as the module (= vector space when R is a field) over R with basis consisting of the elements of G and with a multiplication determined by the *convolutional type multiplication* of the elements of G.

The word *convolution* is the 'multiplication' used by Engineers in digital signal processing (DSP); the convolution they use in DSP is exactly the group ring multiplication when the group is the cyclic group.

Group Rings are also proving useful in constructing paraunitary matrices which are then used to construct Filter Banks.

References on group rings

Many survey papers and books as well as a huge number of research articles have appeared on group rings over the years.

References on group rings

Many survey papers and books as well as a huge number of research articles have appeared on group rings over the years.

Particularly worth mentioning is the recent book by Milies and Sehgal *'Introduction to group rings'* as well as previous books by Passman and Sehgal.

References on group rings

Many survey papers and books as well as a huge number of research articles have appeared on group rings over the years.

Particularly worth mentioning is the recent book by Milies and Sehgal *'Introduction to group rings'* as well as previous books by Passman and Sehgal.

Details on Group Rings Codes may now be obtained in two chapters of book:

'Selected Topics in Information and Coding Theory', April 2010, published by Inderscience, editors I. Woungang & S. Misra.

This is suitable for graduate students and has exercises and research problems.

Zero-divisors and units

A *unit* is an element u such that there exists v with $uv = 1$. A *zero-divisor* is an element $z \neq 0$ such that $zt = 0$ for some non-zero t.

For example, matrices have *lots of* zero-divisors = singular matrices, and *lots of* units = non-singular matrices.

Group rings are rich sources of zero-divisors and units. They also have the advantage of a **rich structure**.

Transpose and rank

Transpose in group rings corresponds to taking inverses of each group element in the group ring element.

Transpose and rank

Transpose in group rings corresponds to taking inverses of each group element in the group ring element.

Thus suppose $w = 1 - g^3 + g^6 + g^{11}$ in RC_{12}. Then $w^{\mathsf{T}} = 1 - g^9 + g^6 + g$.

The notation w^{-1} is also used.

Transpose and rank

Transpose in group rings corresponds to taking inverses of each group element in the group ring element.

Thus suppose $w = 1 - g^3 + g^6 + g^{11}$ in RC_{12}. Then $w^{\mathsf{T}} = 1 - g^9 + g^6 + g$.

The notation w^{-1} is also used.

If w has matrix W then $w^{\mathsf{T}} = w^{-1}$ has matrix W^{T}.

Transpose and rank

Transpose in group rings corresponds to taking inverses of each group element in the group ring element.

Thus suppose $w = 1 - g^3 + g^6 + g^{11}$ in RC_{12}. Then $w^{\mathsf{T}} = 1 - g^9 + g^6 + g$.

The notation w^{-1} is also used.

If w has matrix W then $w^{\mathsf{T}} = w^{-1}$ has matrix W^{T}.

rank (u) is defined to be rank (U) where U is the matrix corresponding to u.

Self-dual codes in group rings

General method:

Form self-dual codes in RG as follows:

Suppose $|G| = n = 2m$.

Self-dual codes in group rings

General method:

Form self-dual codes in RG as follows:

Suppose $|G| = n = 2m$.

Let $u \in RG$ satisfy:

1. $u^2 = 0$.
2. $u = u^{\mathsf{T}}$ so that $uu^{\mathsf{T}} = 0$.
3. u and its corresponding matrix U have rank m.

Self-dual codes in group rings

General method:

Form self-dual codes in RG as follows:

Suppose $|G| = n = 2m$.

Let $u \in RG$ satisfy:

1. $u^2 = 0$.
2. $u = u^{\mathsf{T}}$ so that $uu^{\mathsf{T}} = 0$.
3. u and its corresponding matrix U have rank m.

Then u generates a self-dual code.

Self-dual codes in group rings

General method:

Form self-dual codes in RG as follows:

Suppose $|G| = n = 2m$.

Let $u \in RG$ satisfy:

1. $u^2 = 0$.
2. $u = u^{\mathsf{T}}$ so that $uu^{\mathsf{T}} = 0$.
3. u and its corresponding matrix U have rank m.

Then u generates a self-dual code.

The 'generator' element here is u and the 'control' element is $u = u^{\mathsf{T}}$.

To get the matrix representation go from the group ring element u to the corresponding matrix element U.

An example

Consider $\mathbb{Z}_2(C_2 \times C_4)$, the group ring of the direct product of the cyclic group of order 2 with the cyclic group of order 4 over the field of two elements.

An example

Consider $\mathbb{Z}_2(C_2 \times C_4)$, the group ring of the direct product of the cyclic group of order 2 with the cyclic group of order 4 over the field of two elements.

Let C_4 be generated by a and let C_2 be generated by h.

Consider $u = 1 + h(a + a^2 + a^3)$ in the group ring.

Now indeed $u^2 = 0$, $u^{\mathsf{T}} = u$ and u and its corresponding matrix has rank 4.

An example

Consider $\mathbb{Z}_2(C_2 \times C_4)$, the group ring of the direct product of the cyclic group of order 2 with the cyclic group of order 4 over the field of two elements.

Let C_4 be generated by a and let C_2 be generated by h.

Consider $u = 1 + h(a + a^2 + a^3)$ in the group ring.

Now indeed $u^2 = 0$, $u^{\mathsf{T}} = u$ and u and its corresponding matrix has rank 4.

It is ensured that u is symmetric in the construction by having the same coefficient for each group element g in u as for its inverse g^{-1} in u.

Matrix

The matrix of u is

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

where

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

The matrix of the code is then:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right)$$

Matrix

The matrix of u is

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

where

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

The matrix of the code is then:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right)$$

which is easily recognisable!

Extend this

The above example may be extended:

Consider $G = C_2 \times C_4 \times C_4$ and the group ring $\mathbb{Z}_2 G$.

Suppose the C_4 are generated by a_1, a_2 and that C_2 is generated by h.

Consider $u = 1 + h(a_1 + a_2 + a_3)(a_2 + a_2^2 + a_2^3)$.

Then: $u^2 = 0$, $u^{\mathsf{T}} = u$ and the rank of u is 16.

This gives a $(32, 16, 6)$ self-dual code; the distance may be proved directly from the group ring construction.

Note: The code may be stored by an algebraic formula.

More general

Using $G = C_2 \times C_4 \times \ldots \times C_4 = C_4^m \times C_2$ self-dual codes of the form $(2 \times 4^m, 4^m, 2 \times 3^{\frac{m}{2}})$ for m even and of the form $(2 \times 4^m, 4^m, 4 \times 3^{\frac{m-1}{2}})$ for m odd may be formed.

The distances may be proved algebraically and the codes stored by algebraic formulae.

More general

Using $G = C_2 \times C_4 \times \ldots \times C_4 = C_4^m \times C_2$ self-dual codes of the form $(2 \times 4^m, 4^m, 2 \times 3^{\frac{m}{2}})$ for m even and of the form $(2 \times 4^m, 4^m, 4 \times 3^{\frac{m-1}{2}})$ for m odd may be formed.

The distances may be proved algebraically and the codes stored by algebraic formulae.

This gives
$(8, 4, 4), (32, 16, 6), (128, 64, 12), (512, 256, 18), (2048, 1024, 36)$.
etc. self-dual codes.

More general

Using $G = C_2 \times C_4 \times \ldots \times C_4 = C_4^m \times C_2$ self-dual codes of the form $(2 \times 4^m, 4^m, 2 \times 3^{\frac{m}{2}})$ for m even and of the form $(2 \times 4^m, 4^m, 4 \times 3^{\frac{m-1}{2}})$ for m odd may be formed.

The distances may be proved algebraically and the codes stored by algebraic formulae.

This gives
$(8, 4, 4), (32, 16, 6), (128, 64, 12), (512, 256, 18), (2048, 1024, 36)$.
etc. self-dual codes.

These extend the Hamming $(8, 4, 4)$ self-dual code to an infinite sequence of self-dual codes with known distance and algebraic structure.

More general

Using $G = C_2 \times C_4 \times \ldots \times C_4 = C_4^m \times C_2$ self-dual codes of the form $(2 \times 4^m, 4^m, 2 \times 3^{\frac{m}{2}})$ for m even and of the form $(2 \times 4^m, 4^m, 4 \times 3^{\frac{m-1}{2}})$ for m odd may be formed.

The distances may be proved algebraically and the codes stored by algebraic formulae.

This gives
$(8, 4, 4), (32, 16, 6), (128, 64, 12), (512, 256, 18), (2048, 1024, 36)$.
etc. self-dual codes.

These extend the Hamming $(8, 4, 4)$ self-dual code to an infinite sequence of self-dual codes with known distance and algebraic structure.

A best $(32, 16, 8)$ self-dual code may be produced by the group ring method but is not part of an infinite sequence as above.

More general

Using $G = C_2 \times C_4 \times \ldots \times C_4 = C_4^m \times C_2$ self-dual codes of the form $(2 \times 4^m, 4^m, 2 \times 3^{\frac{m}{2}})$ for m even and of the form $(2 \times 4^m, 4^m, 4 \times 3^{\frac{m-1}{2}})$ for m odd may be formed.

The distances may be proved algebraically and the codes stored by algebraic formulae.

This gives
$(8, 4, 4), (32, 16, 6), (128, 64, 12), (512, 256, 18), (2048, 1024, 36)$.
etc. self-dual codes.

These extend the Hamming $(8, 4, 4)$ self-dual code to an infinite sequence of self-dual codes with known distance and algebraic structure.

A best $(32, 16, 8)$ self-dual code may be produced by the group ring method but is not part of an infinite sequence as above.

Another advantage is that the codes can be algebraically stored and the matrices constructed algebraically as required, thus saving storage and power.

Others ..

Many other self-dual codes may be produced in this way.

For example using $C_6^m \times C_2$ produces $(2 \times 6^m, 6^4, 2^{m+1})$ self-dual binary codes.

This gives $(12, 6, 4), (72, 36, 8), (432, 216, 16), (2592, 1296, 32)$ etc. self-dual codes. $(12, 6, 4)$ is best possible although $(72, 36, 8)$ is not.

Others ..

Many other self-dual codes may be produced in this way.

For example using $C_6^m \times C_2$ produces $(2 \times 6^m, 6^4, 2^{m+1})$ self-dual binary codes.

This gives $(12, 6, 4), (72, 36, 8), (432, 216, 16), (2592, 1296, 32)$ etc. self-dual codes. $(12, 6, 4)$ is best possible although $(72, 36, 8)$ is not.

Examples of this type beyond $(72, 36)$ with described generator and check matrices and known distances do not seem to be known. Again the codes can be stored by an algebraic formula and the matrices can be constructed algebraically as required.

Dihedral

Using *dihedral group rings* and related groups have proved particularly useful and often give better codes than cyclic codes.

Dihedral

Using *dihedral group rings* and related groups have proved particularly useful and often give better codes than cyclic codes.

Dihedral groups could be considered as the next class after abelian groups. These groups and their group rings have a beautiful structure.

Dihedral

Using *dihedral group rings* and related groups have proved particularly useful and often give better codes than cyclic codes.

Dihedral groups could be considered as the next class after abelian groups. These groups and their group rings have a beautiful structure.

The most famous, probably, self-dual code is the Golay $(24, 12, 8)$ code. It is not a cyclic code.

This has also been constructed by the group ring method as a self-dual (zero-divisor) code in the group ring of the *dihedral group*.

Dihedral Self-Dual Codes

Series of binary self-dual codes are also obtained by considering dihedral group ring codes and generalised dihedral group ring codes.

These dihedral-type codes show particular promise.

Dihedral Self-Dual Codes

Series of binary self-dual codes are also obtained by considering dihedral group ring codes and generalised dihedral group ring codes.

These dihedral-type codes show particular promise.

By specifying certain *difference sets*, self-dual $(8m-2, 4m-1)$ codes are obtained when $(4m-1)$ is a power of a prime and m odd.

Dihedral Self-Dual Codes

Series of binary self-dual codes are also obtained by considering dihedral group ring codes and generalised dihedral group ring codes.

These dihedral-type codes show particular promise.

By specifying certain *difference sets*, self-dual $(8m-2, 4m-1)$ codes are obtained when $(4m-1)$ is a power of a prime and m odd.

Difference sets are related to group rings.

Dihedral examples

Binary $(22, 11, 6)$, $(38, 19, 8)$ and $(54, 27, 10)$ self-dual codes are obtained in this way from the
$(11, 5, 2), (19, 9, 4), (27, 13, 6)$ difference sets.

Dihedral examples

Binary $(22, 11, 6)$, $(38, 19, 8)$ and $(54, 27, 10)$ self-dual codes are obtained in this way from the
$(11, 5, 2), (19, 9, 4), (27, 13, 6)$ difference sets.

Now $(22, 11, 6)$ and $(38, 19, 8)$ are best possible for self-dual binary codes.

Dihedral examples

Binary $(22, 11, 6)$, $(38, 19, 8)$ and $(54, 27, 10)$ self-dual codes are obtained in this way from the
$(11, 5, 2), (19, 9, 4), (27, 13, 6)$ difference sets.

Now $(22, 11, 6)$ and $(38, 19, 8)$ are best possible for self-dual binary codes.

In general the distance d of the $(8m - 2, 4m - 1)$ self-dual dihedral code is either $m + 1$ or $m + 3$.

Dihedral examples

Binary $(22, 11, 6)$, $(38, 19, 8)$ and $(54, 27, 10)$ self-dual codes are obtained in this way from the
$(11, 5, 2), (19, 9, 4), (27, 13, 6)$ difference sets.

Now $(22, 11, 6)$ and $(38, 19, 8)$ are best possible for self-dual binary codes.

In general the distance d of the $(8m - 2, 4m - 1)$ self-dual dihedral code is either $m + 1$ or $m + 3$.

This gives a series of good self-dual $(8m - 2, 4m - 1, \geq m + 1)$ codes in which the distance over length approaches $\frac{1}{8}$.

Difference sets

Briefly with flavour:

Suppose D is a difference set (v, k, λ) in $G = C_v$.

Thus $DD^{-1} = \lambda G + n1$, where $n = k - \lambda$.

Difference sets

Briefly with flavour:

Suppose D is a difference set (v, k, λ) in $G = C_v$.

Thus $DD^{-1} = \lambda G + n1$, where $n = k - \lambda$.

Now construct your group ring to ensure $DD^{-1} = 0$ or $DD^{-1} = 1$ or whatever is required in other characteristics ..

Difference sets

Briefly with flavour:

Suppose D is a difference set (v, k, λ) in $G = C_v$.

Thus $DD^{-1} = \lambda G + n1$, where $n = k - \lambda$.

Now construct your group ring to ensure $DD^{-1} = 0$ or $DD^{-1} = 1$ or whatever is required in other characteristics ..

In $\mathbb{Z}_2 G$, $DD^{-1} = 1$ when n is odd and λ is even as for example in $(11, 5, 2)$.

So in D_{2v} let $w = 1 + aD$ where
$D_{2v} = \langle a, b | a^2 = 1 = b^v, ab = b^{-1}a \rangle$.

Difference sets

Briefly with flavour:

Suppose D is a difference set (v, k, λ) in $G = C_v$.

Thus $DD^{-1} = \lambda G + n1$, where $n = k - \lambda$.

Now construct your group ring to ensure $DD^{-1} = 0$ or $DD^{-1} = 1$ or whatever is required in other characteristics ..

In $\mathbb{Z}_2 G$, $DD^{-1} = 1$ when n is odd and λ is even as for example in $(11, 5, 2)$.

So in D_{2v} let $w = 1 + aD$ where
$D_{2v} = \langle a, b | a^2 = 1 = b^v, ab = b^{-1}a \rangle$.

Then $w^2 = 0$, $w = w^{\mathsf{T}}$ and w generates a self-dual code.

Dual-containing codes

A *dual-containing code* $\mathcal{C}$ is a code such that its dual, $\mathcal{C}'$, satisfies $\mathcal{C}' \subset \mathcal{C}$.

Dual-containing codes may be used to construct *quantum codes*, as noted in papers by Calderbank, MacKay and others.

Dual-containing codes

A *dual-containing code* $\mathcal{C}$ is a code such that its dual, $\mathcal{C}'$, satisfies $\mathcal{C}' \subset \mathcal{C}$.

Dual-containing codes may be used to construct *quantum codes*, as noted in papers by Calderbank, MacKay and others.

Using a similar technique in the group rings as for the self-dual codes, dual-containing codes of various (good) rates may be obtained.

Dual-containing codes of rate $\frac{3}{4}$

General set-up. Consider RG with $|G| = m = 4q$ and suppose G has an element u such that:

1. $u^4 = 0$.
2. u is symmetric, $u^{\mathsf{T}} = u$.
3. u and U have rank $= 3q$.

Since u has rank $3q$ it will follow that u^3 has rank q.

Dual-containing codes of rate $\frac{3}{4}$

General set-up. Consider RG with $|G| = m = 4q$ and suppose G has an element u such that:

1. $u^4 = 0$.
2. u is symmetric, $u^{\mathsf{T}} = u$.
3. u and U have rank $= 3q$.

Since u has rank $3q$ it will follow that u^3 has rank q.

Then u will generate a dual-containing code $(4q, 3q)$ of rate $\frac{3}{4}$.

u is the generating element of the code and u^3 is the check element.

Dual-containing codes of rate $\frac{3}{4}$

General set-up. Consider RG with $|G| = m = 4q$ and suppose G has an element u such that:

1. $u^4 = 0$.
2. u is symmetric, $u^{\mathsf{T}} = u$.
3. u and U have rank $= 3q$.

Since u has rank $3q$ it will follow that u^3 has rank q.

Then u will generate a dual-containing code $(4q, 3q)$ of rate $\frac{3}{4}$.

u is the generating element of the code and u^3 is the check element.

The generator matrix of the equivalent matrix code is the matrix U corresponding to the group ring element u and only the first three-quarters of the rows of U need be used.

U^3 is the check matrix and only the first quarter of its rows need be used as the check matrix.

Specific example of rate $\frac{3}{4}$

Let $G = C_8 \times C_2$ with C_8 generated by a and C_2 generated by h.

Let $u = 1 + h(a + a^4 + a^7)$ in $\mathbb{Z}_2 G$.

Then $u^4 = 0, u^{\mathsf{T}} = u$, $\operatorname{rank} u = 12$, $\operatorname{rank} u^3 = 4$.

Thus u generates a dual-containing code with generator u and check u^3.

This gives a $(16, 12, 2)$ dual-containing code which is best possible distance for a $(16, 12)$ code.

More examples

Using $C_8 \times C_8 \times C_2$ gives $(128, 96, 4)$ dual-containing code.

More examples

Using $C_8 \times C_8 \times C_2$ gives $(128, 96, 4)$ dual-containing code.

Generally $C_8^m \times C_2$ will give $(4 \times 8^m, 3 \times 8^m, 2^{m+1})$ rate $\frac{3}{4}$ dual-containing codes.

Get $(16, 12, 2), (128, 96, 4), (1024, 768, 8), (8192, 7168, 16)$ etc. dual-containing codes of rate $\frac{3}{4}$.

More examples

Using $C_8 \times C_8 \times C_2$ gives $(128, 96, 4)$ dual-containing code.

Generally $C_8^m \times C_2$ will give $(4 \times 8^m, 3 \times 8^m, 2^{m+1})$ rate $\frac{3}{4}$ dual-containing codes.

Get $(16, 12, 2), (128, 96, 4), (1024, 768, 8), (8192, 7168, 16)$ etc. dual-containing codes of rate $\frac{3}{4}$.

Using $C_8 \times C_4$ gives $(32, 24, 4)$ dual-containing which is best possible for $(32, 24)$ code.

Using $C_8^m \times C_4$ gives $(4 \times 8^m, 3 \times 8^m, 2^{m+1})$ dual-containing codes.

This gives $(32, 24, 4), (256, 192, 8), (2048, 1536, 16)$ etc. dual-containing codes of rate $\frac{3}{4}$.

More examples

Using $C_8 \times C_8 \times C_2$ gives $(128, 96, 4)$ dual-containing code.

Generally $C_8^m \times C_2$ will give $(4 \times 8^m, 3 \times 8^m, 2^{m+1})$ rate $\frac{3}{4}$ dual-containing codes.

Get $(16, 12, 2), (128, 96, 4), (1024, 768, 8), (8192, 7168, 16)$ etc. dual-containing codes of rate $\frac{3}{4}$.

Using $C_8 \times C_4$ gives $(32, 24, 4)$ dual-containing which is best possible for $(32, 24)$ code.

Using $C_8^m \times C_4$ gives $(4 \times 8^m, 3 \times 8^m, 2^{m+1})$ dual-containing codes.

This gives $(32, 24, 4), (256, 192, 8), (2048, 1536, 16)$ etc. dual-containing codes of rate $\frac{3}{4}$.

There are others ... Make up your own ...

The generator and check matrices for these codes are immediately obtained from the group ring elements.

More general..

Rate $\frac{7}{8}$ dual-containing codes are similarly obtained.

Need an element $u \in RG$ where $|G| = m = 8q$ with

(i) $u^8 = 0$ and

(ii)rank $u = 7q$.

Here get $(32, 28, 2), (512, 448, 4)$ etc. dual-containing codes from direct products of cyclic groups.

More general..

Rate $\frac{7}{8}$ dual-containing codes are similarly obtained.

Need an element $u \in RG$ where $|G| = m = 8q$ with

(i) $u^8 = 0$ and

(ii)rank $u = 7q$.

Here get $(32, 28, 2), (512, 448, 4)$ etc. dual-containing codes from direct products of cyclic groups.

Get the picture??

More general..

Rate $\frac{7}{8}$ dual-containing codes are similarly obtained.

Need an element $u \in RG$ where $|G| = m = 8q$ with

(i) $u^8 = 0$ and

(ii)rank $u = 7q$.

Here get $(32, 28, 2), (512, 448, 4)$ etc. dual-containing codes from direct products of cyclic groups.

Get the picture??

Rate $\frac{15}{16}$ dual-containing codes, etc. are possible.

Over other rings

The general techniques described can be applied to obtain self-dual and dual-containing codes over fields of other characteristics, and over $\mathbb{Z}_4$.

Over other rings

The general techniques described can be applied to obtain self-dual and dual-containing codes over fields of other characteristics, and over $\mathbb{Z}_4$.

The end.

Over other rings

The general techniques described can be applied to obtain self-dual and dual-containing codes over fields of other characteristics, and over $\mathbb{Z}_4$.

The end. Or is it just the beginning?