Codes from Group Rings

Ted Hurley
Intro

*Group ring codes* have many applications.
Group ring codes have many applications. 
Sorry about the applications!
Group ring codes have many applications.
Sorry about the applications!
However: There are many nice theorems involved.
Group ring codes have many applications.

Sorry about the applications!

However: There are many nice theorems involved.

However again: To describe in detail one of the theorems would take up most of the time.
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 modules, sometimes ideals, in (general) group rings. An isomorphism between a group ring and a ring of matrices gives matrix representations and implementations of the codes.
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 modules, sometimes ideals, in (general) group rings. An isomorphism between a group ring and a ring of matrices gives matrix representations and implementations of the codes. Properties, such as distance, can often be calculated from the group ring construction, and codes with a desired property can be obtained using group ring properties and constructions.
Cyclic example

In $\mathbb{Z}_2C_7$ it is easy to check that
$$(1 + g + g^3)(1 + g + g^2 + g^4) = 0; \text{ say } uv = 0.$$
Cyclic example

In $\mathbb{Z}_2 C_7$ it is easy to check that
$$(1 + g + g^3)(1 + g + g^2 + g^4) = 0; \text{ say } uv = 0.$$ 

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

$$
\begin{pmatrix}
1 & g & g^2 & g^3 & g^4 & g^5 & g^6 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\end{pmatrix}
$$
Cyclic example

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

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

$$
\begin{pmatrix}
1 & g & g^2 & g^3 & g^4 & g^5 & g^6 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots 
\end{pmatrix}
$$

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

\[ U = \begin{pmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 1
\end{pmatrix} \]

\[ V = \begin{pmatrix}
1 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 1
\end{pmatrix} \]
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

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

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

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

This is in fact the Hamming Code as a group ring code.
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 $GH^T = 0$ and thus get the set-up for a code.

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

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

Thus $G, H$ are in a sense zero-divisors.
Basic codes

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

Thus $G, H$ are in a sense zero-divisors.
Basic codes

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

Thus $G, H$ are in a sense zero-divisors.

A check matrix is an $(n - r) \times n$ matrix $H$, of rank $(n - r)$, such that $GH^T = 0_{r \times (n-r)}$ or equivalently that $HG^T = 0_{(n-r) \times r}$. 
Basic codes

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

Thus $G, H$ are in a sense zero-divisors.

A check matrix is an $(n - r) \times n$ matrix $H$, of rank $(n - r)$, such that $GH^T = 0_{r \times (n-r)}$ or equivalently that $HG^T = 0_{(n-r) \times r}$.

Then $y$ is a codeword iff $Hy^T = 0$. 
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 presently used in cyclic codes and some others 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 $GH^T = 0$. Circulant matrices are simply the group ring elements of the cyclic group from the injection of the cyclic group ring onto the ring of circulant matrices. Cyclic codes include such important codes as BCH, Reed-Solomon, (some) Golay and Hamming codes. Example: The (famous) Golay self-dual code $(24, 12, 8)$ is not a cyclic (group ring) code but is a dihedral (group ring) code.
Cyclic codes

Cyclic codes are obtained from zero-divisors in a cyclic group ring. Matrices that are presently used in cyclic codes and some others 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 $GH^T = 0$.

Circulant matrices are simply the group ring elements of the cyclic group from the injection of the cyclic group ring onto the ring of circulant matrices.
Cyclic codes

Cyclic codes are obtained from zero-divisors in a cyclic group ring. Matrices that are presently used in cyclic codes and some others 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 $GH^T = 0$.

Circulant matrices are simply the group ring elements of the cyclic group from the injection of the cyclic group ring onto the ring of circulant matrices.

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

Cyclic codes are obtained from zero-divisors in a cyclic group ring. Matrices that are presently used in cyclic codes and some others 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 $GH^T = 0$.

Circulant matrices are simply the group ring elements of the cyclic group from the injection of the cyclic group ring onto the ring of circulant matrices.

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

Example: The (famous) Golay self-dual code $(24, 12, 8)$ is not a cyclic (group ring) code but is a dihedral (group ring) code.
Zero-divisors and units

Why not use other group rings?

Group Ring codes can be produced from zero-divisors in a group ring and also from constructions from within units.

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.
Group ring codes: Zero-divisor case

Zero-divisors and units are used to construct Group Ring Codes.
Group ring codes: Zero-divisor case

Zero-divisors and units are used to construct Group Ring Codes.

Zero-divisor codes:

In $RG$ suppose $uv = 0$. Then $u$ is the generator of the code and $v$ is the check of the code. From this get matrix code with generator matrix $U$ and check matrix $V^T$ where $U$ is the matrix corresponding to $u$ and $V$ is the matrix corresponding to $v$. Of course not all of $U$ or $V$ are used as these do not have full rank. 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.
Zero-divisors and units are used to construct Group Ring Codes. Zero-divisor codes:

In $RG$ suppose $uv = 0$. Then $u$ is the generator of the code and $v$ is the check of the code. From this get matrix code with generator matrix $U$ and check matrix $V^T$ where $U$ is the matrix corresponding to $u$ and $V$ is the matrix corresponding to $v$. Of course not all of $U$ or $V$ are used as these do not have full rank.
Group ring codes: Zero-divisor case

Zero-divisors and units are used to construct Group Ring Codes.

Zero-divisor codes:
In $RG$ suppose $uv = 0$. Then $u$ is the generator of the code and $v$ is the check of the code. From this get matrix code with generator matrix $U$ and check matrix $V^T$ where $U$ is the matrix corresponding to $u$ and $V$ is the matrix corresponding to $v$. Of course not all of $U$ or $V$ are used as these do not have full rank. 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.
Group ring codes: Zero-divisor case

Zero-divisors and units are used to construct Group Ring Codes. Zero-divisor codes:

In $RG$ suppose $uv = 0$. Then $u$ is the generator of the code and $v$ is the check of the code. From this get matrix code with generator matrix $U$ and check matrix $V^T$ where $U$ is the matrix corresponding to $u$ and $V$ is the matrix corresponding to $v$.

Of course not all of $U$ or $V$ are used as these do not have full rank. 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.
Units

Since conference here only allows units of group rings (doesn’t mention zero-divisors!) it is necessary to explain how to obtain codes from units....
Units

Since conference here only allows units of group rings (doesn’t mention zero-divisors!) it is necessary to explain how to obtain codes from units....

Suppose we have an invertible matrix $U$ with $UU^{-1} = I$.

Divide $U = \begin{pmatrix} A \\ B \end{pmatrix}$ into block matrices where $A$ is $r \times n$ and $B$ is $(n - r) \times n$. Similarly, let $U^{-1} = \begin{pmatrix} C & D \end{pmatrix}$ where $C$ is $n \times r$ and $D$ is $n \times (n - r)$. 

Need a theorem here to show that $D$ is actually a check matrix – left as exercise!
Units

Since conference here only allows units of group rings (doesn’t mention zero-divisors!) it is necessary to explain how to obtain codes from units....

Suppose we have an invertible matrix $U$ with $UU^{-1} = I$.

Divide $U = \begin{pmatrix} A \\ B \end{pmatrix}$ into block matrices where $A$ is $r \times n$ and $B$ is $(n - r) \times n$. Similarly, let $U^{-1} = \begin{pmatrix} C & D \end{pmatrix}$ where $C$ is $n \times r$ and $D$ is $n \times (n - r)$.

Then $UU^{-1} = I$ gives $\begin{pmatrix} A \\ B \end{pmatrix} \times \begin{pmatrix} C & D \end{pmatrix} = \begin{pmatrix} AC & AD \\ BC & BD \end{pmatrix} = I$. 

In particular this gives $AD = 0$. Now rank (A) = r and rank (D) = (n - r).

We have the set-up for a linear-code! $A$ is the generator matrix and $D^T$ is a check matrix.

Need a theorem here to show that $D$ is actually a check matrix – left as exercise!
Units

Since conference here only allows units of group rings (doesn’t mention zero-divisors!) it is necessary to explain how to obtain codes from units....

Suppose we have an invertible matrix $U$ with $UU^{-1} = I$.

Divide $U = \begin{pmatrix} A \\ B \end{pmatrix}$ into block matrices where $A$ is $r \times n$ and $B$ is $(n - r) \times n$. Similarly, let $U^{-1} = \begin{pmatrix} C & D \end{pmatrix}$ where $C$ is $n \times r$ and $D$ is $n \times (n - r)$.

Then $UU^{-1} = I$ gives $\begin{pmatrix} A \\ B \end{pmatrix} \times \begin{pmatrix} C & D \end{pmatrix} = \begin{pmatrix} AC & AD \\ BC & BD \end{pmatrix} = I$.

In particular this gives $AD = 0$. Now $\text{rank}(A) = r$ and $\text{rank}(D) = (n - r)$.

We have the set-up for a linear-code!

$A$ is the generator matrix and $D^T$ is a check matrix.
Units

Since conference here only allows units of group rings (doesn’t mention zero-divisors!) it is necessary to explain how to obtain codes from units....

Suppose we have an invertible matrix $U$ with $UU^{-1} = I$.

Divide $U = \begin{pmatrix} A \\ B \end{pmatrix}$ into block matrices where $A$ is $r \times n$ and $B$ is $(n-r) \times n$. Similarly, let $U^{-1} = \begin{pmatrix} C & D \end{pmatrix}$ where $C$ is $n \times r$ and $D$ is $n \times (n-r)$.

Then $UU^{-1} = I$ gives $\begin{pmatrix} A \\ B \end{pmatrix} \times \begin{pmatrix} C & D \end{pmatrix} = \begin{pmatrix} AC & AD \\ BC & BD \end{pmatrix} = I$.

In particular this gives $AD = 0$. Now rank $(A) = r$ and rank $(D) = (n-r)$.

We have the set-up for a linear-code!

$A$ is the generator matrix and $D^T$ is a check matrix.

Need a theorem here to show that $D$ is actually a check matrix – left as exercise!
Most used and useful codes

Codes most commonly used and causing excitement at the moment seem to be:

- LDPC (Low density parity check) codes.
- Convolutional Codes
- Self-dual (and dual-containing) codes.

Methods for producing and analysing these have essentially been computer methods; these are now in many cases at the limit of the power of the computer and algebraic methods are needed.

Can group rings be used?
Most used and useful codes

Codes most commonly used and causing excitement at the moment seem to be:

- LDPC (Low density parity check) codes.
- Convolutional Codes
- Self-dual (and dual-containing) codes.
Most used and useful codes

Codes most commonly used and causing excitement at the moment seem to be:

- LDPC (Low density parity check) codes.
- Convolutional Codes
- Self-dual (and dual-containing) codes.

Methods for producing and analysing these have essentially been computer methods; these are now in many cases at the limit of the power of the computer and algebraic methods are needed.
Codes most commonly used and causing excitement at the moment seem to be:

- LDPC (Low density parity check) codes.
- Convolutional Codes
- Self-dual (and dual-containing) codes.

Methods for producing and analysing these have essentially been computer methods; these are now in many cases at the limit of the power of the computer and algebraic methods are needed.

Can group rings be used?
Convolutional codes are widely used in satellite, GSM, and digital signals.
Convolutional codes are widely used in satellite, GSM, and digital signals.

The group ring $RGC_{\infty}$ can be used to construct convolutional codes and analyse the constructions.
Convolutional codes are widely used in satellite, GSM, and digital signals. The group ring $RGC_\infty$ can be used to construct convolutional codes and analyse the constructions. It transpires that many convolutional codes constructed (such as QLI, ‘Quick look in’) are special cases of such group ring codes. The group ring method expands these greatly and puts them on an algebraic footing.
Convolutional codes are widely used in satellite, GSM, and digital signals.

The group ring $RGC_\infty$ can be used to construct convolutional codes and analyse the constructions.

It transpires that many convolutional codes constructed (such as QLI, ‘Quick look in’) are special cases of such group ring codes. The group ring method expands these greatly and puts them on an algebraic footing.

On a related issue, group rings are also proving useful in constructing paraunitary matrices which are then used to construct Filter Banks.
Low density parity check (LDPC) codes

LDPC codes are code where the number of elements in each row and column of the check is small compared to the length.
Low density parity check (LDPC) codes

LDPC codes are code where the number of elements in each row and column of the check is small compared to the length. LDPC codes with no short cycles are known to perform well.
Low density parity check (LDPC) codes

LDPC codes are code where the number of elements in each row and column of the check is small compared to the length. LDPC codes with no short cycles are known to perform well. Low Density Parity Check (LDPC) codes have an easy interpretation as group ring codes. It is required to find a zero-divisor code or unit code where the check element is ‘short’ or equivalently where the check matrix has ‘few’ non-zero elements in each row and column compared to the size of the matrix.
Low density parity check (LDPC) codes

LDPC codes are code where the number of elements in each row and column of the check is small compared to the length. LDPC codes with no short cycles are known to perform well. Low Density Parity Check (LDPC) codes have an easy interpretation as group ring codes. It is required to find a zero-divisor code or unit code where the check element is ‘short’ or equivalently where the check matrix has ‘few’ non-zero elements in each row and column compared to the size of the matrix.

*This means that the check group ring element has small support as a group ring element.* Easy ....
Short cycles in group rings?

What about no short cycles?

To say a group ring element has a short cycle can be interpreted as a group ring property.

**Theorem**

A group ring element has no short cycles if and only if (certain condition on the difference set of the group elements of the group ring element.

Thus LDPC codes with no short cycles may be constructed from group ring elements fairly readily - choose your element appropriately.
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. $u = u^T$ so that $uu^T = 0$.
3. $u$ and its corresponding matrix $U$ have rank $m$.

Then $u$ generates a self-dual code.
General method: Form self-dual codes in $RG$ as follows:

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

Let $u \in RG$ satisfy:

1. $u^2 = 0$.
2. $u = u^T$ so that $uu^T = 0$.
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 $u = u^T$.

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 $u^2 = 0$, $u^\top = u$ 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 $u^2 = 0$, $u^T = u$ and $u$ and its corresponding matrix has rank 4.

It is ensured that $u$ is symmetric by making sure that each group element $g$ and its inverse $g^{-1}$ appear in $u$ with the same coefficient.
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:
\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0
\end{pmatrix}
\]
which is easily recognisable!
Go large

Large examples of all of the above types can be constructed.
Large examples of all of the above types can be constructed. Using \textit{dihedral group rings} and related groups have proved particularly useful and often (almost always) give better codes than cyclic codes.