Convolutional Codes from Group Rings

Jessica OShaughnessy

Prof. Ted Hurley
School of Mathematics, Statistics, and Applied Mathematics
National University of Ireland, Galway
18 May 2010

Outline

1. Background and Definitions
   - Background
   - Group Ring Codes
2. New Construction
   - Main Results
   - Free Distance Properties
3. Results and Future Work
   - Results
   - Future Work

Outline

1. Background and Definitions
   - Background
   - Group Ring Codes
2. New Construction
   - Main Results
   - Free Distance Properties
3. Results and Future Work
   - Results
   - Future Work

Basic Definitions: Group Rings

Definition

Let G be a group, and let R be a ring. The **group ring**, RG, is $RG = \{\sum_{g \in G} \alpha_i g_i | \alpha_i \in R, g_i \in G\}$

- Let $u = \sum_{g \in G} \alpha_g g$ and $v = \sum_{g \in G} \beta_g g$ be elements of the group ring.
- Say u is a **unit** in the group ring if there exists some $v \in RG$ such that $uv = 1$.
- Say u is a **zero divisor** in the group ring if there exists some $v \in RG$, $v \neq 0$, such that $uv = 0$.

Basic Definitions: Group Rings

Definition

Let G be a group, and let R be a ring. The **group ring**, RG, is $RG = \{\sum_{g \in G} \alpha_i g_i | \alpha_i \in R, g_i \in G\}$

- Let $u = \sum_{g \in G} \alpha_g g$ and $v = \sum_{g \in G} \beta_g g$ be elements of the group ring.
- Say u is a **unit** in the group ring if there exists some $v \in RG$ such that $uv = 1$.
- Say u is a **zero divisor** in the group ring if there exists some $v \in RG$, $v \neq 0$, such that $uv = 0$.

Basic Definitions: Group Rings

Definition

Let G be a group, and let R be a ring. The **group ring**, RG, is $RG = \{\sum_{g \in G} \alpha_i g_i | \alpha_i \in R, g_i \in G\}$

- Let $u = \sum_{g \in G} \alpha_g g$ and $v = \sum_{g \in G} \beta_g g$ be elements of the group ring.
- Say u is a **unit** in the group ring if there exists some $v \in RG$ such that $uv = 1$.
- Say u is a **zero divisor** in the group ring if there exists some $v \in RG$, $v \neq 0$, such that $uv = 0$.

Basic Definitions: Convolutional Codes

Definition

An (n, k) convolutional code is a k dimensional subspace of F^n. The code, $\mathscr{C}$, is generated by a generator polynomial,$g(z)$, or a polynomial generator matrix, G, and it is in the solution space of the control polynomial, $f(z)$, or control matrix, F.

- The **free distance**, d_∞, of a convolutional code is the smallest number of places in which any two convolutional codewords differ.
- A generator matrix is said to be **catastrophic** if there is an infinite weight dataword, $d(z)$, such that the corresponding codeword, $c(z)$, has finite weight.

Basic Definitions: Convolutional Codes

Definition

An (n, k) convolutional code is a k dimensional subspace of F^n. The code, $\mathscr{C}$, is generated by a generator polynomial,$g(z)$, or a polynomial generator matrix, G, and it is in the solution space of the control polynomial, $f(z)$, or control matrix, F.

- The **free distance,** d_∞**,** of a convolutional code is the smallest number of places in which any two convolutional codewords differ.
- A generator matrix is said to be **catastrophic** if there is an infinite weight dataword, $d(z)$, such that the corresponding codeword, $c(z)$, has finite weight.

Outline

1. Background and Definitions
   - Background
   - Group Ring Codes
2. New Construction
   - Main Results
   - Free Distance Properties
3. Results and Future Work
   - Results
   - Future Work

Group Matrices

- Let G be a group of order n with listing $\{g_1, g_2, \ldots, g_n\}$.
- The **group matrix**, or G-matrix, is

$$M(G) = \begin{pmatrix} g_1^{-1}g_1 & g_1^{-1}g_2 & \cdots & g_1^{-1}g_n \\ g_2^{-1}g_1 & g_2^{-1}g_2 & \cdots & g_2^{-1}g_n \\ \vdots & \vdots & \ddots & \vdots \\ g_n^{-1}g_1 & g_n^{-1}g_2 & \cdots & g_n^{-1}g_n \end{pmatrix}$$

RG Matrices

- Let G be a group of order n with listing $\{g_1, g_2, \ldots, g_n\}$.
- Let RG be a group ring.
- Let u be a unit in the group ring such that

$$u = \alpha_{g_1} g_1 + \cdots + \alpha_{g_n} g_n$$

- The RG matrix of u is

$$U = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix}$$

Group Matrix

Example

Let $G = C_4 = < a >$. Let $\{1, a, a^2, a^3\}$ be a listing of G.
Then, the group matrix of G is

$$\begin{pmatrix} 1\cdot 1 & 1\cdot a & 1\cdot a^2 & 1\cdot a^3 \\ a^3\cdot 1 & a^3\cdot a & a^3\cdot a^2 & a^3\cdot a^3 \\ a^2\cdot 1 & a^2\cdot a & a^2\cdot a^2 & a^2\cdot a^3 \\ a\cdot 1 & a\cdot a & a\cdot a^2 & a\cdot a^3 \end{pmatrix} = \begin{pmatrix} 1 & a & a^2 & a^3 \\ a^3 & 1 & a & a^2 \\ a^2 & a^3 & 1 & a \\ a & a^2 & a^3 & 1 \end{pmatrix}.$$

RG Matrix

Example

Let $G = C_4 = < a >$, and $RG = \mathbb{Z}_2 C_4$. Let $\{1, a, a^2, a^3\}$ be a listing of G. Take $u = 1 + a + a^3$. Then the RG matrix of u is

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

Convolutional Codes from Group Rings

- RGC_∞
- Take unit, u, in RGC_∞
- RG matrix of u built around RG
- Choose first k rows for A.
- $U = \begin{pmatrix} A \\ B \end{pmatrix}$, $V = \begin{pmatrix} C & D \end{pmatrix}$
- $UV = \begin{pmatrix} A \\ B \end{pmatrix} \begin{pmatrix} C & D \end{pmatrix} = \begin{pmatrix} AC & AD \\ BC & BD \end{pmatrix} = \begin{pmatrix} I_k & 0_{k\times(n-k)} \\ 0_{(n-k)\times k} & I_k \end{pmatrix}$
- Generator is A
- Control is D

Convolutional Codes from Group Rings

- RGC_∞
- Take unit, u, in RGC_∞
- RG matrix of u built around RG

- Choose first k rows for A.
- $U = \begin{pmatrix} A \\ B \end{pmatrix}$, $V = \begin{pmatrix} C & D \end{pmatrix}$
- $UV = \begin{pmatrix} A \\ B \end{pmatrix} \begin{pmatrix} C & D \end{pmatrix} = \begin{pmatrix} AC & AD \\ BC & BD \end{pmatrix} = \begin{pmatrix} I_k & 0_{k\times(n-k)} \\ 0_{(n-k)\times k} & I_k \end{pmatrix}$

- Generator is A
- Control is D

Convolutional Codes from Group Rings

- RGC_∞
- Take unit, u, in RGC_∞
- RG matrix of u built around RG

- Choose first k rows for A.
- $U = \begin{pmatrix} A \\ B \end{pmatrix}$, $V = \begin{pmatrix} C & D \end{pmatrix}$
- $UV = \begin{pmatrix} A \\ B \end{pmatrix} \begin{pmatrix} C & D \end{pmatrix} = \begin{pmatrix} AC & AD \\ BC & BD \end{pmatrix} = \begin{pmatrix} I_k & 0_{k\times(n-k)} \\ 0_{(n-k)\times k} & I_k \end{pmatrix}$

- Generator is A
- Control is D

Convolutional Codes from Group Rings: Generator

- Let $G = C_2 = < a >$, and $RG = \mathbb{Z}_2 C_2 C_\infty$.
- $u = (1+a) + z + (1+a)z^2 + (1+a)z^4$
- $U = \begin{pmatrix} 1+z+z^2+z^4 & 1+z^2+z^4 \\ 1+z^2+z^4 & 1+z+z^2+z^4 \end{pmatrix}$
- $u = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} z + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} z^2 + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} z^4$
- $a = \begin{pmatrix} 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \end{pmatrix} z + \begin{pmatrix} 1 & 1 \end{pmatrix} z^2 + \begin{pmatrix} 1 & 1 \end{pmatrix} z^4$
- $b = \begin{pmatrix} 1 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \end{pmatrix} z + \begin{pmatrix} 1 & 1 \end{pmatrix} z^2 + \begin{pmatrix} 1 & 1 \end{pmatrix} z^4$

Convolutional Codes from Group Rings: Generator

- Let $G = C_2 = < a >$, and $RG = \mathbb{Z}_2 C_2 C_\infty$.
- $u = (1+a) + z + (1+a)z^2 + (1+a)z^4$
- $U = \begin{pmatrix} 1+z+z^2+z^4 & 1+z^2+z^4 \\ 1+z^2+z^4 & 1+z+z^2+z^4 \end{pmatrix}$
- $u = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} z + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} z^2 + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} z^4$
- $a = \begin{pmatrix} 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \end{pmatrix} z + \begin{pmatrix} 1 & 1 \end{pmatrix} z^2 + \begin{pmatrix} 1 & 1 \end{pmatrix} z^4$
- $b = \begin{pmatrix} 1 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \end{pmatrix} z + \begin{pmatrix} 1 & 1 \end{pmatrix} z^2 + \begin{pmatrix} 1 & 1 \end{pmatrix} z^4$

Convolutional Codes from Group Rings:Control

- $v = (1+a)z^{-2} + z^{-1} + (1+a) + (1+a)z^2$
- $V = \begin{pmatrix} z^{-2}+z^{-1}+1+z^2 & z^{-2}+1+z^2 \\ z^{-2}+1+z^2 & z^{-2}+z^{-1}+1+z^2 \end{pmatrix}$
- $v = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} z^{-2} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} z^{-1} + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} z^2$
- $c = \begin{pmatrix} 1 \\ 1 \end{pmatrix} z^{-2} + \begin{pmatrix} 1 \\ 0 \end{pmatrix} z^{-1} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} z^2$
- $d = \begin{pmatrix} 1 \\ 1 \end{pmatrix} z^{-2} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} z^{-1} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} z^2$

Convolutional Codes from Group Rings:Control

- $v = (1+a)z^{-2} + z^{-1} + (1+a) + (1+a)z^2$
- $V = \begin{pmatrix} z^{-2}+z^{-1}+1+z^2 & z^{-2}+1+z^2 \\ z^{-2}+1+z^2 & z^{-2}+z^{-1}+1+z^2 \end{pmatrix}$
- $v = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} z^{-2} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} z^{-1} + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} z^2$
- $c = \begin{pmatrix} 1 \\ 1 \end{pmatrix} z^{-2} + \begin{pmatrix} 1 \\ 0 \end{pmatrix} z^{-1} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} z^2$
- $d = \begin{pmatrix} 1 \\ 1 \end{pmatrix} z^{-2} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} z^{-1} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} z^2$

Outline

1. Background and Definitions
   - Background
   - Group Ring Codes
2. New Construction
   - Main Results
   - Free Distance Properties
3. Results and Future Work
   - Results
   - Future Work

New Construction Basic Idea

- $|G| = n$
- n must be even
- $k = \frac{n}{2}$

- Take unit, u, in Z_2G.
- $U = \begin{pmatrix} A \\ B \end{pmatrix}$, $V = \begin{pmatrix} C & D \end{pmatrix}$
- $UV = \begin{pmatrix} A \\ B \end{pmatrix} \begin{pmatrix} C & D \end{pmatrix} = \begin{pmatrix} AC & AD \\ BC & BD \end{pmatrix} = \begin{pmatrix} I_k & 0_{k\times k} \\ 0_{k\times k} & I_k \end{pmatrix}$

- Generator is $g(z) = A + Bz$
- Control is $f(z) = D + Cz$
- $g(z)f(z) = (A+Bz)(D+Cz) = (AD + ACz + BDz + BCz^2) = 0_{k\times k} + I_k z + I_k z + 0_{k\times k} z^2 = 0_{k\times k}$

New Construction Basic Idea

- $|G| = n$
- n must be even
- $k = \frac{n}{2}$
- Take unit, u, in Z_2G.
- $U = \begin{pmatrix} A \\ B \end{pmatrix}$, $V = \begin{pmatrix} C & D \end{pmatrix}$
- $UV = \begin{pmatrix} A \\ B \end{pmatrix} \begin{pmatrix} C & D \end{pmatrix} = \begin{pmatrix} AC & AD \\ BC & BD \end{pmatrix} = \begin{pmatrix} I_k & 0_{k\times k} \\ 0_{k\times k} & I_k \end{pmatrix}$
- Generator is $g(z) = A + Bz$
- Control is $f(z) = D + Cz$
- $g(z)f(z) = (A+Bz)(D+Cz) = (AD + ACz + BDz + BCz^2) = 0_{k\times k} + I_k z + I_k z + 0_{k\times k} z^2 = 0_{k\times k}$

New Construction Basic Idea

- $|G| = n$
- n must be even
- $k = \frac{n}{2}$
- Take unit, u, in Z_2G.
- $U = \begin{pmatrix} A \\ B \end{pmatrix}$, $V = \begin{pmatrix} C & D \end{pmatrix}$
- $UV = \begin{pmatrix} A \\ B \end{pmatrix} \begin{pmatrix} C & D \end{pmatrix} = \begin{pmatrix} AC & AD \\ BC & BD \end{pmatrix} = \begin{pmatrix} I_k & 0_{k\times k} \\ 0_{k\times k} & I_k \end{pmatrix}$
- Generator is $g(z) = A + Bz$
- Control is $f(z) = D + Cz$
- $g(z)f(z) = (A+Bz)(D+Cz) = (AD + ACz + BDz + BCz^2) = 0_{k\times k} + I_k z + I_k z + 0_{k\times k} z^2 = 0_{k\times k}$

New Construction Extended

- Generator is $g(z) = Az^j + \sum_i \delta_i Bz^i$
- Control is $f(z) = Dz^j + \sum_i \delta_i Cz^i$
- $i \in \mathbb{N}_0$
- $\delta_i \in \{0, 1\}$

Outline

1. Background and Definitions
   - Background
   - Group Ring Codes
2. New Construction
   - Main Results
   - Free Distance Properties
3. Results and Future Work
   - Results
   - Future Work

Free Distance Properties

Theorem

Let u be a unit in the group ring, RG, with group ring matrix $U = \begin{pmatrix} A \\ B \end{pmatrix}$, $|G| = n$, and $k = \frac{n}{2}$, $n \in \{\mathbb{N} \cup 0\}$, n even, and $R = \mathbb{Z}_2$. Let $\mathscr{C}$ be an (n,k) convolutional code generated by $g(z) = A + Bz + \cdots + Bz^m$. Then the free distance is

$$d_\infty = min \begin{cases} d(A) + d(B) + d(A+B) \\ d(A) + md(B) \end{cases}$$

Free Distance Properties

Theorem

Let u be a unit in the group ring, RG, with group ring matrix $U = \begin{pmatrix} A \\ B \end{pmatrix}$, $|G| = n$, and $k = \frac{n}{2}$. Let $g(z) = A + Bz + \cdots + Bz^{m-2} + Bz^m$. Then $g(z)$ has free distance

$$d_\infty = min \begin{cases} d(A) + d(A+B) + 3d(B) \\ d(A) + (m-1)d(B) \end{cases}$$

Free Distance Properties

Example

$u = 1 + a^2 + a^3$, a unit in $\mathbb{Z}_2 C_6$.

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

Taking $g(z) = A + Bz + Bz^2 + Bz^3 + Bz^4 + Bz^5$ gives a free distance of $8 = d(A) + d(B) + d(A + B)$
Taking $g(z) = A + Bz + Bz^2 + Bz^3 + Bz^5$ gives a free distance of 14, which is $d(A) + 3d(B) + d(A + B)$.

Outline

1. Background and Definitions
   - Background
   - Group Ring Codes
2. New Construction
   - Main Results
   - Free Distance Properties
3. Results and Future Work
   - Results
   - Future Work

Results

- Construct all $(2,1)$ systematic convolutional codes
- Construct LDPC convolutional codes
- Construct optimal $(2,1)$ convolutional codes

Outline

1. Background and Definitions
   - Background
   - Group Ring Codes
2. New Construction
   - Main Results
   - Free Distance Properties
3. Results and Future Work
   - Results
   - Future Work

Future Work

- Consider removing short cycles in LDPC convolutional codes
- Further free distance results

For Further Reading I


R.J. McEliece
The Algebraic Theory of Convolutional Codes
The Handbook of Coding Theory. 1:1065–1138, 1983.


T. Hurley
Convolutional Codes from Units in Matrix and Group Rings
Inter. J. Pure & Appl. Mathematics. 50(3):431–463, 2009.