Checkable Codes form Group Algebras to Group Rings

Noha Abdelghany

Department of Mathematics, Faculty of Science, Cairo University.

Lens, NCRA IV

June 11, 2015
Table of Contents

History

Group-Ring Codes

Code-Checkable Group Rings

References
History

- (MacWilliams, 1969)  
  "Codes and ideals in group algebras".
- (Hurley, 2007)  
  "Module codes over group rings".
- (Hurley, 2009)  
  "Codes from zero-divisors and units in group rings".
- (Jitman, 2010)  
  "Checkable Codes from group rings".
Let $\mathbb{F}_q^n$ denote the vector space of all $n$-tuples over the finite field $\mathbb{F}_q$.

- An $(n,M)$ code $C$ over $\mathbb{F}_q$ is a subset of $\mathbb{F}_q^n$ of size $M$.
- If $C$ is a $k$-dimensional vector subspace of $\mathbb{F}_q^n$, then $C$ will be called a $[n,k]$ linear code over $\mathbb{F}_q$. This linear code $C$ has $q^k$ codewords.
A **generator matrix** for an \([n, k]\) linear code \(C\) is any \(k \times n\) matrix \(G\) whose rows form a basis for the code \(C\). \(C\) is written as:

\[
C = \{xG : x \in \mathbb{F}_q^k\}
\]

A **parity check matrix** \(H\) for an \([n, k]\) linear code \(C\) is an \((n - k) \times n\) matrix defined by:

\[
x \in C \iff Hx^T = 0
\]

Note that \(GH^T = 0\). Thus \(G, H\) are in a sense zero-divisors.
The class of cyclic codes is one of the most important classes of codes. In fact almost all codes used for practical issues, like BCH and Reed-Solomon codes, are cyclic codes. This is due to the existence of fast encoding and decoding algorithms.

**Definition**

A linear code $C$ is a **cyclic code** if $C$ satisfies:

$$(c_1, c_2, \ldots, c_{n-1}, c_n) \in C \Rightarrow (c_n, c_1, \ldots, c_{n-1}) \in C,$$

For every $c \in \mathbb{F}_q^n$. 

Cyclic Codes
Table of Contents

History

Group-Ring Codes

Code-Checkable Group Rings

References
Definition
Given a group $G$ and a ring $R$ the **group ring** $RG$ is the ring consisting of the set of all formal finite sums $\sum_{g \in G} \alpha_g g$, where $\alpha_g \in R$.

For $u = \sum_{g \in G} \alpha_g g$, $v = \sum_{g \in G} \beta_g g \in RG$ and $\alpha \in R$, define:

- $u + v = \sum_{g \in G} (\alpha_g + \beta_g) g$,
- $uv = (\sum_{g \in G} \alpha_g g)(\sum_{h \in G} \beta_h h) = \sum_{g \in G}(\sum_{h \in G} \alpha_h \beta_{h^{-1}} g) g$,
- $\alpha u = \sum_{g \in G} (\alpha u_g) g$. 
Basic Properties of Group Rings

- The group ring $RG$ is a ring.
- The group ring $RG$ is a left $R$-module.
- When $R$ is a field, the group ring $RG$ is an algebra over $R$ and it is called group algebra.

**Theorem**

*For a fixed listing of elements of a finite group $G = \{g_1, g_2, \ldots, g_n\}$ there is a one-to-one correspondence between $RG$ and a subring of the matrix ring $M_n(R)$, given by:*

$$w = \sum_{i=1}^{n} \alpha_i g_i \rightarrow W = \begin{bmatrix}
\alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n}
\end{bmatrix}$$
Let $RG$ be a group ring, $W$ a submodule of $RG$ and $u \in RG$.

**Definition**

- A **right group ring encoding** is a mapping $f : W \rightarrow RG$, such that $f(x) = xu$.
- The **group-ring code** $C$ generated by $u$ relative to $W$ is the image of the group ring encoding: $C = \{ xu : x \in W \}$.

If $u$ is a zero-divisor (resp. unit), $C$ is called zero-divisor (resp. unit-derived) code.
Table of Contents

History

Group-Ring Codes

Code-Checkable Group Rings

References
Suppose that \( u \) is a zero-divisor in \( RG \) and let \( v \) be a non-zero element such that \( uv = 0 \).

Let \( C = \{ xu : x \in W \} = Wu \) be a code generated by \( u \) relative to \( W \). Then

\[
y \in C \Rightarrow yv = 0.
\]

If the zero-divisor code \( C \) satisfies: \( y \in C \iff yv = 0 \). Then \( C \) is called checkable code. In other words,

\[
C = \{ y \in RG : yv = 0 \}.
\]
$C$ is said to be checkable if $C = \{ y \in RG : yv = 0 \}$ for some $v \in RG$.

**Definition (Jitman, 2010)**

A group ring $RG$ is said to be **code-checkable** if every ideal in $RG$ is a checkable code.
Characterization of Code-Checkable Group Algebras

Let $G$ be a finite abelian group and $F$ be a finite field of characteristic $p$.

**Proposition (Jitman, 2010)**

*The group algebra $FG$ is code-checkable if and only if it is a PIR.*

**Theorem (Fisher and Sehgal, 1976)**

*The group algebra $FG$ is a PIR if and only if a Sylow $p$-subgroup of $G$ is cyclic.*
Let $G$ be a finite abelian group and $\mathbb{F}$ be a finite field of characteristic $p$.

**Proposition (Jitman, 2010)**

*The group algebra $\mathbb{F}G$ is code-checkable if and only if it is a PIR.*

**Theorem (Fisher and Sehgal, 1976)**

*The group algebra $\mathbb{F}G$ is a PIR if and only if a Sylow $p$-subgroup of $G$ is cyclic.*
Theorem (Jitman, 2010)

Let $G$ be a finite abelian group and $F$ be a finite field of characteristic $p$. Then the group algebra $F G$ is code-checkable if and only if a Sylow $p$-subgroup of $G$ is cyclic.
Definition
Let $\pi$ be a finite set of primes. A finite group $G$ is called $\pi'$-by-cyclic $\pi$, if there is a normal subgroup $H \triangleleft G$ such that:

- $|H|$ is coprime with each prime in $\pi$.
- The quotient group $G/H$ is cyclic and a $\pi$-group.

Example
Let $\pi = \{2\}$. Since $A_3 \triangleleft S_3$, $|A_3| = 3$ and $|S_3/A_3| = 2$. Then $S_3$ is $\pi'$-by-cyclic $\pi$. 
Lemma
Let $R$ be a finite commutative ring and $G$ a finite group. Then $RG$ is code-checkable if and only if $RG$ is a principal ideal group ring.

Theorem (Dorsey, 2006)
Let $R$ be a finite semisimple ring and $G$ a finite group. Then $RG$ is PIR if and only if $G$ is $\pi'$-by-cyclic $\pi$, where $\pi$ is the set of noninvertible primes in $R$. 
Lemma
Let $R$ be a finite commutative ring and $G$ a finite group. Then $RG$ is code-checkable if and only if $RG$ is a principal ideal group ring.

Theorem (Dorsey, 2006)
Let $R$ be a finite semisimple ring and $G$ a finite group. Then $RG$ is PIR if and only if $G$ is $\pi'$-by-cyclic $\pi$, where $\pi$ is the set of noninvertible primes in $R$. 
Characterization of Code-Checkable Group Rings

Theorem
Let $G$ be a finite group, $R$ a finite commutative semisimple ring and $\pi$ the set of noninvertible primes in $R$. Then the group ring $RG$ is code-checkable if and only if $G$ is $\pi'$-by-cyclic $\pi$. 
Table of Contents

History

Group-Ring Codes

Code-Checkable Group Rings

References
References I


Thank You for Your Time.