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

- (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".

Codes Over Finite Fields

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 **[n,k] linear code** over $\mathbb{F}_q$. This linear code C has q^k codewords.

Generator and Parity Check Matrix of a Linear Code

- 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:

$$x \in C \Leftrightarrow Hx^T = 0$$

- Note that $GH^T = 0$. Thus G, H are in a sense zero-divisors.

Cyclic Codes

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

Table of Contents

Group Rings

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:

$$w = \sum_{i=1}^{n} \alpha_i g_i \to W = \begin{bmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n} \end{bmatrix}$$

Group-Ring Codes

Let RG be a group ring, W a submodule of RG and $u \in RG$.

Definition

- A **right group ring encoding** is a mapping $f : W \to RG$, 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

Checkable Codes

- 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: $y \in C \Leftrightarrow yv = 0$. Then C is called **checkable code.** In other words,

$$C = \{y \in RG : yv = 0\}.$$

Code-Checkable Group Rings

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 $\mathbb{F}$ 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.

Characterization of Code-Checkable Group Algebras

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.

Characterization of Code-Checkable Group Algebras

Theorem (Jitman, 2010)

Let G be a finite abelian group and $\mathbb{F}$ be a finite field of characteristic p. Then the group algebra $\mathbb{F}G$ is code-checkable if and only if a Sylow p-subgroup of G is cyclic.

Definition

Let π be a finite set of primes. A finite group G is called π'-by-cyclic π, if there is a normal subgroup $H \lhd G$ such that:

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

Example

Let $\pi = \{2\}$. Since $A_3 \lhd S_3$, $|A_3| = 3$ and $|S_3/A_3| = 2$. Then S_3 is π'-by-cyclic π.

Characterization of Code-Checkable Group Rings

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 π'-by-cyclic π, where π is the set of noninvertible primes in R.

Characterization of Code-Checkable Group Rings

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 π'-by-cyclic π, where π 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 π the set of noninvertible primes in R. Then the group ring RG is code-checkable if and only if G is π'-by-cyclic π.

Table of Contents

References I

[1] T. J. Dorsey, *Morphic and Principal-Ideal Group Rings*, Journal of Algebra, vol. 318, pp. 393-411, (2007).

[2] J. L. Fisher and S. K. Sehgal, *Principal Ideal Group Rings*, Comm. Algebra, vol. 4, pp. 319-325, (1976).

[3] W. C. Huffman and V. Pless, *Fundamental of Error-Correcting Codes*, Cambridge University Press, New York, (2003).

[4] P. Hurley and T. Hurley, *Module codes in group rings*, Proc. IEEE Int. Symp. on Information Theory, (2007).

[5] P. Hurley and T. Hurley, *Codes from zero-divisors and units in group rings*, Int. J. Information and Coding Theory, pp. 57-87, (2009).

[6] S. Jitman, S. Ling, H. Liu and X. Xie, *Checkable Codes from Group Rings*, CoRR (2011).

[7] T. Y. Lam, *A First course in noncommutative rings*, second ed., Graduate Texts in Mathematics, vol. 131, Springer-Verlag, New York, 2001.

[8] F. J. MacWilliams, *Codes and ideals in group algebras* Combinatorial Mathematics and its Applications, pp. 312-328, (1969).

[9] S. C. Misra, S. Misra and I. Woungang, *Selected topics in information and coding theory*, World Scientific Publishing Co. Pte. Ltd., vol. 7, 2010.

Thank You for Your Time.