Checkable Codes from Group Rings

Somphong Jitman, *Student Member, IEEE*, San Ling, Hongwei Liu, and Xiaoli Xie

***Abstract*—We study codes with a single check element derived from group rings, namely, checkable codes. The notion of a code-checkable group ring is introduced. Necessary and sufficient conditions for a group ring to be code-checkable are given in the case where the group is a finite abelian group and the ring is a finite field. This characterization leads to many good examples, among which two checkable codes and two shortened codes have minimum distance better than the lower bound given in Grassl's online table. Furthermore, when a group ring is code-checkable, it is shown that every code in such a group ring admits a generator, and that its dual is also generated by an element which may be deduced directly from a check element of the original code. These are analogous to the generator and parity-check polynomials of cyclic codes. In addition, the structures of reversible and complementary dual checkable codes are established as generalizations of reversible and complementary dual cyclic codes.**

***Index Terms*—checkable code, group ring, Sylow p-subgroup, zero-divisor code, reversible code, complementary dual code.**

I. Introduction

A group ring code is originally defined to be an ideal in the group ring $\mathbf{F}G$, where $\mathbf{F}$ is a finite field and G is a finite group. When G is cyclic, this concept characterizes the classical cyclic codes over $\mathbf{F}$. In general, when G is abelian, they are called abelian codes and have been studied by many authors (see [2]-[3], [15]-[16], and [5]).

Recently, new techniques for constructing codes have been established for an arbitrary group ring RG in [13], where R is an associative ring with identity $1 \neq 0$ and G is a finite group. For a submodule W of the R-module RG and a zero-divisor u in RG, a *zero-divisor code* generated by u relative to W is defined to be $\mathcal{C} := \{wu \mid w \in W\} = Wu$. Many existing codes coincide with special types of zero-divisor codes (cf. [13]-[14], and [18]).

One of the most interesting is a zero-divisor code determined by a single check element, i.e., there exists v in RG such that $\mathcal{C} = Wu = \{y \in RG \mid yv = 0\}$. Such a code is called a *checkable code* and the element v is called a *check element*. A group ring is said to be *code-checkable* if all its non-trivial ideals are checkable codes. These codes are of interest since they can be viewed as a generalization of the classical cyclic codes. For a finite field $\mathbf{F}$ and a cyclic group G of order n, $\mathbf{F}G \cong \mathbf{F}[X]/\langle X^n - 1\rangle$ is a principal ideal ring, where $\mathbf{F}[X]$ is the ring of polynomials over $\mathbf{F}$. All ideals of $\mathbf{F}G$ are cyclic codes. Every non-trivial ideal is checkable, where the ideal is generated by the generator polynomial and the reciprocal polynomial of the parity-check polynomial acts as a check element. Therefore, $\mathbf{F}G$ is code-checkable.

We extend this study to the group ring $\mathbf{F}G$, where $\mathbf{F}$ is a finite field and G is a finite abelian group. Necessary and sufficient conditions for $\mathbf{F}G$ to be code-checkable are determined. This characterization allows us to find various examples of good codes. Four new codes which have minimum distance better than the lower bound given in Grassl's table [10] are presented. Many other examples found also have minimum distance as good as the best known ones in [10]. Furthermore, it is also shown that, when $\mathbf{F}G$ is a code-checkable group ring, every zero-divisor code in $\mathbf{F}G$ is of the form $\mathbf{F}Gu = \{y \in \mathbf{F}G \mid yv = 0\}$ for some $u, v \in \mathbf{F}G$, and that its dual is given by $\mathbf{F}Gv^{(-1)}$, where $v^{(-1)}$ is defined to be $v^{(-1)} = \sum_{g\in G} v_{g^{-1}} g$ for $v = \sum_{g\in G} v_g g$. As seen above, when G is a cyclic group, i.e., in the case of cyclic codes over $\mathbf{F}$, u and $v^{(-1)}$ may be regarded as the analogs of the generator and parity-check polynomials. In this sense, the class of codes studied in this paper can be regarded as a generalization of cyclic codes. Indeed, when G is a finite abelian group, the group ring $\mathbf{F}G$ is isomorphic to some $\mathbf{F}[X_1, \ldots, X_t]/\langle X_1^{n_1} - 1, \ldots, X_t^{n_t} - 1\rangle$ (cf. [6]), so the elements u and $v^{(-1)}$ may be regarded as the multivariate generator and parity-check polynomials of a checkable abelian code. Moreover, we derive the structures of reversible and complementary dual checkable codes which may have application in certain data storage, computing, and retrieval systems. These codes are generalizations of reversible and complementary dual cyclic codes (cf. [1], [17], and [21]).

The paper is organized as follows. Some basic concepts and necessary terminologies are introduced in Section II. In Section III, we present a characterization of code-checkable group rings together with some related properties. We provide structural characterizations of reversible and complementary dual checkable codes in Section IV. In Section V, some examples from the family of checkable codes and their modifications are discussed, including four new codes and numerous good codes. Finally, we conclude with a summary of results in Section VI.

II. Preliminaries

In order for the exposition in this paper to be self-contained, we introduce some basic concepts and necessary terminologies used later in this paper. The readers may find further details in [7]-[9], [13]-[14], and [19].

S. Jitman, and S. Ling are with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371, Republic of Singapore (emails: pu738241@e.ntu.edu.sg, lingsan@ntu.edu.sg).

S. Jitman is also with the Department of Mathematics, Faculty of Science, Chulalongkorn University, Bangkok 10330, Thailand.

H. Liu, and X. Xie are with the Department of Mathematics, Huazhong Normal University, Wuhan, Hubei 430079, China (emails:{h_w_liu,xiexiaoli_1985}@yahoo.com.cn).

The work of S. Jitman and S. Ling was partially supported by the Singapore Ministry of Education under Research Grant T208B2206. The work of H. Liu and X. Xie was done under the National Natural Science Foundation of China, Grant No. 10871079.

A. Groups and Group Rings

Let G be a finite group and p a prime number. If G is of order $p^a m$, where a is a non-negative integer and m is a positive integer such that $p \nmid m$, then a subgroup of order p^a is called a *Sylow p-subgroup* of G.

Throughout, we assume that G is abelian of order n, written multiplicatively (with identity 1). Let $\mathbf{F}$ denote a finite field of characteristic p and denote by $\mathbf{F}G$ the *group ring* of G over $\mathbf{F}$. The elements in $\mathbf{F}G$ will be written as $\sum_{g\in G} \alpha_g g$, where $\alpha_g \in \mathbf{F}$, and the addition and the multiplication are given by

$$\sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g := \sum_{g\in G} (\alpha_g + \beta_g) g$$

and

$$\left(\sum_{g\in G} \alpha_g g\right)\left(\sum_{h\in G} \beta_h h\right) := \sum_{g,h\in G} (\alpha_g \beta_h) gh.$$

Obviously, $\mathbf{F}G$ is an $\mathbf{F}$-vector space with a basis G, where the scalar multiplication is defined by

$$r \sum_{g\in G} \alpha_g g := \sum_{g\in G} (r\alpha_g) g,$$

for all $r \in \mathbf{F}$ and $\sum_{g\in G} \alpha_g g \in \mathbf{F}G$. As G is abelian, the group ring $\mathbf{F}G$ is commutative.

Let $\{g_1, g_2, \ldots, g_n\}$ be a fixed list of the elements in G and $M_n(\mathbf{F})$ denote the ring of $n \times n$ matrices over $\mathbf{F}$. For $u = \sum_{i=1}^{n} u_{g_i} g_i \in \mathbf{F}G$, let $U \in M_n(\mathbf{F})$ be defined by

$$U = \begin{pmatrix} u_{g_1^{-1}g_1} & u_{g_1^{-1}g_2} & \cdots & u_{g_1^{-1}g_n} \\ u_{g_2^{-1}g_1} & u_{g_2^{-1}g_2} & \cdots & u_{g_2^{-1}g_n} \\ \vdots & \vdots & \ddots & \vdots \\ u_{g_n^{-1}g_1} & u_{g_n^{-1}g_2} & \cdots & u_{g_n^{-1}g_n} \end{pmatrix}. \tag{II.1}$$

The map $\tau : \mathbf{F}G \to M_n(\mathbf{F})$ given by

$$u \mapsto U^T,$$

where U^T is the transpose of U, is well-known as a *left regular representation* of $\mathbf{F}G$ (cf. [8, Chapter 2], and [19, Example 4.1.6]). This representation plays a vital role in studying the generator and parity-check matrices of codes mentioned later.

An element $a \in \mathbf{F}G$ is called a *unit* if there exists $b \in \mathbf{F}G$ such that $ab = 1$. A non-zero element $u \in \mathbf{F}G$ is called a *zero-divisor* if there exists $0 \neq v \in \mathbf{F}G$ such that $uv = 0$. For a non-empty subset S of $\mathbf{F}G$, the *annihilator* of S is defined to be $Ann(S) = \{x \in \mathbf{F}G \mid xs = 0, \text{ for all } s \in S\}$. Note that $Ann(S)$ is an ideal of $\mathbf{F}G$. When $S = \{s\}$, we simply denote by $Ann(s)$ the annihilator $Ann(S)$. An ideal I of $\mathbf{F}G$ is said to be *non-trivial* if $\{0\} \subsetneq I \subsetneq \mathbf{F}G$ and it is said to be *principal* if it is generated by a single element. We say that $\mathbf{F}G$ is a *principal ideal ring (PIR)* if every ideal of $\mathbf{F}G$ is principal.

In the light of the main result in [9], a characterization of principal ideal group rings is given as follows.

Theorem 2.1 ([9]): Let G be a finite abelian group and $\mathbf{F}$ a finite field of characteristic p. Then $\mathbf{F}G$ is a PIR if and only if a Sylow p-subgroup of G is cyclic.

B. Codes from Group Rings

A zero-divisor code has been introduced for arbitrary group rings in [14]. We recall this concept for a commutative group ring $\mathbf{F}G$ as follows:

Let W be a subspace of the $\mathbf{F}$-vector space $\mathbf{F}G$ and let u be a zero-divisor in $\mathbf{F}G$. The *zero-divisor code* $\mathcal{C}$ generated by u relative to W is defined to be $\mathcal{C} := \{wu \mid w \in W\} = Wu$. The element u is called a *generator element* for $\mathcal{C}$.

Given a zero-divisor code $\mathcal{C} = Wu$, then there exists $0 \neq v \in \mathbf{F}G$ such that $uv = 0$ and hence $cv = 0$ for all $c \in \mathcal{C}$. If there is an element $v \in \mathbf{F}G$ such that $\mathcal{C} = \{y \in \mathbf{F}G \mid yv = 0\} = Ann(v)$, the code $\mathcal{C}$ is said to be *checkable* and the element v is called a *check element* of $\mathcal{C}$. We note that a check element for a code does not need to be unique. The group ring $\mathbf{F}G$ is said to be *code-checkable* if every non-trivial ideal of $\mathbf{F}G$ is a checkable code.

Let u be a zero-divisor in $\mathbf{F}G$ and U its corresponding matrix defined in (II.1). Assume that W is a subspace of $\mathbf{F}G$ with a basis $S \subseteq G$ such that Su is linearly independent. If $|S| = k$, then $\mathrm{rank}(U) = k$ if and only if the code $\mathcal{C} = Wu$ is an ideal of $\mathbf{F}G$, equivalently, $\mathcal{C} = \mathbf{F}Gu$ (see [14, Theorem 7.2]).

To determine whether $\mathbf{F}G$ is code-checkable, it suffices to consider all zero-divisor codes $\mathcal{C}$ where $\mathcal{C} = \mathbf{F}Gu$. From this characterization, a generator matrix for $\mathcal{C}$ can be defined to be any k linearly independent rows of U.

A zero-divisor $u \in \mathbf{F}G$ is called *principal* if there exists $0 \neq v \in \mathbf{F}G$ such that $uv = 0$ and $\mathrm{rank}(V) = n - \mathrm{rank}(U)$, where U and V are the corresponding matrices of u and v, respectively. The following characterization is proved in [14].

Lemma 2.2 ([14, Corollary 4.1]): Let u be a zero-divisor in $\mathbf{F}G$. Then the zero-divisor code $\mathbf{F}Gu$ is checkable if and only if u is principal.

In this case, it is easy to see that the corresponding element v is a check element of $\mathcal{C}$. As $uv = 0$, it follows that $UV = 0$. Hence, by the rank condition, a parity-check matrix for $\mathcal{C}$ can be defined to be any $n-k$ linearly independent columns of V.

For $a = \sum_{g\in G} a_g g$ and $b = \sum_{g\in G} b_g g$ in $\mathbf{F}G$, let $\langle a, b\rangle$ denote the *Euclidean inner product* of the coefficient vectors of a and b, i.e.,

$$\langle a, b\rangle = \sum_{g\in G} a_g b_g.$$

For a code $\mathcal{C} \subseteq \mathbf{F}G$, the *dual code* $\mathcal{C}^\perp$ of $\mathcal{C}$ is defined by

$$\mathcal{C}^\perp = \{a \in \mathbf{F}G \mid \langle a, c\rangle = 0 \text{ for all } c \in \mathcal{C}\}.$$

III. Checkable Codes and Code-Checkable Group Rings

In this section, we present the main results of this paper. A characterization of code-checkable group rings and some relevant properties are given.

Proposition 3.1: Let $\mathbf{F}$ be a finite field and G a finite abelian group. Then $\mathbf{F}G$ is code-checkable if and only if it is a PIR.

Proof: Assume that $\mathbf{F}G$ is code-checkable. Let I be an arbitrary ideal of $\mathbf{F}G$. If I is $\{0\}$ or $\mathbf{F}G$, it is principal. Assume

that I is non-trivial. Then there exists a zero-divisor $v \in \mathbf{F}G$ such that $I = Ann(v)$. Then

$$\mathbf{F}G/Ann(v) \cong \mathbf{F}Gv. \tag{III.1}$$

Next, we show I is principal. Since $\{0\} \subsetneq \mathbf{F}Gv \subsetneq \mathbf{F}G$, there exists $0 \neq u \in \mathbf{F}G$ such that $\mathbf{F}Gv = Ann(u)$. We claim that $\mathbf{F}Gu = Ann(v)$. It is clear that $\mathbf{F}Gu \subseteq Ann(v)$. By (III.1), we have that

$$|\mathbf{F}G/Ann(v)| = |\mathbf{F}Gv| \text{ and } |\mathbf{F}G/Ann(u)| = |\mathbf{F}Gu|.$$

Since $\mathbf{F}G$ is finite, it follows that

$$|\mathbf{F}Gu| = |\mathbf{F}G|/|Ann(u)| = |\mathbf{F}G|/|\mathbf{F}Gv| = |Ann(v)|.$$

Hence, $I = Ann(v) = \mathbf{F}Gu$. Therefore, $\mathbf{F}G$ is a PIR.

Conversely, assume that $\mathbf{F}G$ is a PIR. Let $\mathfrak{J}$ denote the set of all non-trivial ideals of $\mathbf{F}G$. From the finiteness of $\mathbf{F}G$, it follows that $|\mathfrak{J}|$ is finite. Let $\sigma : \mathfrak{J} \to \mathfrak{J}$ be defined by

$$\mathbf{F}Ga \mapsto Ann(a).$$

Clearly, for each $c \in \mathbf{F}G$, we have $Ann(\mathbf{F}Gc) = Ann(c)$. Hence, if $\mathbf{F}Ga = \mathbf{F}Gb$, then

$$Ann(a) = Ann(\mathbf{F}Ga) = Ann(\mathbf{F}Gb) = Ann(b).$$

This implies that the mapping σ is well-defined.

To show that σ is injective, assume that $\sigma(\mathbf{F}Ga) = \sigma(\mathbf{F}Gb)$, i.e., $Ann(a) = Ann(b)$. Since $\mathbf{F}G$ is a PIR, there exists $0 \neq v \in \mathbf{F}G$ such that $Ann(a) = Ann(b) = \mathbf{F}Gv$, and hence $\mathbf{F}Ga = Ann(v) = \mathbf{F}Gb$.

Since $|\mathfrak{J}|$ is finite, σ is bijective. This implies that every non-trivial ideal of $\mathbf{F}G$ is a checkable code. ∎

A characterization of code-checkable group rings follows immediately from Theorem 2.1 and Proposition 3.1.

Theorem 3.2: Let G be a finite abelian group and $\mathbf{F}$ a finite field of characteristic p, where p is a prime number. Then the group ring $\mathbf{F}G$ is code-checkable if and only if a Sylow p-subgroup of G is cyclic.

When $\mathbf{F}G$ is a code-checkable group ring, Proposition 3.1 and its proof also provide a link between a checkable code in $\mathbf{F}G$ and its dual. The following result is found in [14, Theorem 4.6]. Here, we give an alternative proof.

For $v = \sum_{g\in G} v_g g \in \mathbf{F}G$, we define $v^{(-1)} = \sum_{g\in G} v_{g^{-1}} g$.

Corollary 3.3: Let $\mathbf{F}G$ be a code-checkable group ring. Every non-trivial ideal in $\mathbf{F}G$ is of the form $\mathbf{F}Gu = Ann(v)$, for some $u, v \in \mathbf{F}G$. Its dual code is given by $\mathbf{F}Gv^{(-1)}$.

Proof: The fact that every non-trivial ideal in $\mathbf{F}G$ is of the form $\mathcal{C} = \mathbf{F}Gu = Ann(v)$ is already shown in the proof of Proposition 3.1. For such a code $\mathcal{C}$, we now show that $\mathcal{C}^{\perp} = \mathbf{F}Gv^{(-1)}$.

Write $u = \sum_{g\in G} u_g g$ and $v = \sum_{h\in G} v_h h$. Hence

$$0 = uv = \sum_{k\in G} \left(\sum_{g\in G} u_g v_{g^{-1}k} \right) k,$$

which implies that $\sum_{g\in G} u_g v_{g^{-1}k} = 0$ for all $k \in G$.

The typical element in $\mathbf{F}Gu$ is of the form

$$\left(\sum_{h\in G} x_h h \right) \left(\sum_{g\in G} u_g g \right) = \sum_{k\in G} \left(\sum_{g\in G} u_g x_{g^{-1}k} \right) k.$$

We have that

$$\begin{aligned} \sum_{k\in G} \left(\sum_{g\in G} u_g x_{g^{-1}k} \right) v_{k^{-1}} &= \sum_{g\in G} \left(\sum_{k\in G} x_{g^{-1}k} v_{k^{-1}} \right) u_g \\ &= \sum_{k\in G} \left(\sum_{g\in G} u_g v_{g^{-1}k} \right) x_{k^{-1}} \\ &= 0. \end{aligned}$$

This shows that $\mathbf{F}Gv^{(-1)} \subseteq \mathcal{C}^{\perp}$.

It is easy to observe that $v \mapsto v^{(-1)}$ induces an isomorphism of groups $\mathbf{F}Gv \cong \mathbf{F}Gv^{(-1)}$. From the proof of Proposition 3.1, we have that $|\mathbf{F}G|/|\mathbf{F}Gu| = |\mathbf{F}Gv| = |\mathbf{F}Gv^{(-1)}|$. It therefore follows that $\mathbf{F}Gv^{(-1)} = \mathcal{C}^{\perp}$. ∎

Corollary 3.4: If $\mathbf{F}Gu$ is checkable with a check element v, then $|\mathbf{F}Gu| = |\mathbf{F}Gu^{(-1)}|$, $|\mathbf{F}Gv| = |\mathbf{F}Gv^{(-1)}|$, and $|\mathbf{F}G| = |\mathbf{F}Gu| \cdot |\mathbf{F}Gv|$.

Proof: It follows immediately from Corollary 3.3 and its proof. ∎

IV. Some Special Types of Checkable Codes

In this section, we assume that a group ring $\mathbf{F}G$ is code-checkable and study the structure of some special types of checkable codes which may have application in certain data storage, computing, and retrieval systems.

A. Reversible Checkable Codes

For an abelian group G of order n, let $\mathcal{L} = \{g_1, g_2, \ldots, g_n\}$ denote a fixed list of the elements in G. For $w = \sum_{i=1}^{n} w_i g_i$, the reverse of w with respect to $\mathcal{L}$, denote by $\mathrm{r}_{\mathcal{L}}(w)$, is defined to be $\mathrm{r}_{\mathcal{L}}(w) := \sum_{i=1}^{n} w_{n+1-i} g_i$. A code $\mathcal{C} \subseteq \mathbf{F}G$ is said to be *reversible* with respect to $\mathcal{L}$ if $\mathrm{r}_{\mathcal{L}}(w) \in \mathcal{C}$ whenever $w \in \mathcal{C}$. If the list $\mathcal{L}$ satisfies

$$k = g_{n-(i-1)} g_i, \tag{IV.1}$$

for some fixed $k \in G$, and for every $i = 1, 2, \ldots, n$, then $\mathrm{r}_{\mathcal{L}}(w)$ is of the form

$$\begin{aligned} \mathrm{r}_{\mathcal{L}}(w) &= \sum_{i=1}^{n} w_{n+1-i} g_i = \sum_{i=1}^{n} w_i g_{n+1-i} \\ &= \sum_{i=1}^{n} w_i k g_i^{-1} = k \sum_{i=1}^{n} w_i g_i^{-1} = k w^{(-1)}, \end{aligned} \tag{IV.2}$$

for all $w \in \mathbf{F}G$.

Example 4.1: Let $G = C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}$ denote a finite abelian group of order $n = n_1 n_2 \ldots n_r$ written as the product of cyclic groups $C_{n_j} = \langle x_j \rangle$. Define the list $\{g_1, g_2, \ldots, g_n\}$ of G by

$$g_{1+j_1+n_1 j_2+n_1 n_2 j_3+\cdots+n_1 n_2 \ldots n_{r-1} j_r} = x_1^{j_1} x_2^{j_2} \ldots x_r^{j_r}, \tag{IV.3}$$

where $0 \leq j_i < n_i$ for all $1 \leq i \leq r$. Then $g_1 = 1$, the identity of G, and $g_n = g_{n-(i-1)} g_i$ for all $1 \leq i \leq n$. Hence, this list

satisfies (IV.1), where $k = g_n$. Note that if $G = \langle x \rangle$ is cyclic of order n, the list represents $\{1, x, x^2, \ldots, x^{n-1}\}$ which corresponds to the set of monomials $\{1, X, X^2, \ldots, X^{n-1}\}$ in $\mathbf{F}[X]/\langle X^n - 1\rangle$.

Throughout this section, we study reversible checkable codes with respect to a list $\mathcal{L}$ satisfying (IV.1).

To complete a characterization of reversible checkable codes, we need the following lemmas.

Lemma 4.2 ([11, Lemma 1.1]): Given $a \in \mathbf{F}G$, then the set of generators of $\mathbf{F}Ga$ is $\mathcal{U}(\mathbf{F}G)a$, where $\mathcal{U}(\mathbf{F}G)$ is the set of units in $\mathbf{F}G$.

Lemma 4.3: Let a and b be elements in $\mathbf{F}G$. Then $\mathbf{F}Ga = \mathbf{F}Gb$ if and only if $a = fb$ for some unit f in $\mathbf{F}G$.

Proof: Assume that $\mathbf{F}Ga = \mathbf{F}Gb$. Note that a is a generator of $\mathbf{F}Gb$. Then, by Lemma 4.2, $a \in \mathcal{U}(\mathbf{F}G)b$ which implies that $a = fb$ for some unit $f \in \mathbf{F}G$.

Conversely, assume that $a = fb$ for some unit f in $\mathbf{F}G$. Then $\mathbf{F}Ga = \mathbf{F}Gfb \subseteq \mathbf{F}Gb = \mathbf{F}Gf^{-1}a \subseteq \mathbf{F}Ga$. Therefore, $\mathbf{F}Ga = \mathbf{F}Gb$ as desired. ∎

Theorem 4.4: Let $\mathcal{L}$ be a fixed list of G satisfying (IV.1). Let $\mathbf{F}Gu$ be a checkable code with a check element v. Then the following statements are equivalent:

$i)$ $\mathbf{F}Gu$ is reversible with respect to $\mathcal{L}$.
$ii)$ $\mathbf{F}Gu = \mathbf{F}Gu^{(-1)}$.
$iii)$ $u = au^{(-1)}$ for some unit a in $\mathbf{F}G$.
$iv)$ $v = bv^{(-1)}$ for some unit b in $\mathbf{F}G$.
$v)$ $\mathbf{F}Gv = \mathbf{F}Gv^{(-1)}$.
$vi)$ $\mathbf{F}Gv$ is reversible with respect to $\mathcal{L}$.

Proof: We prove $i) \Rightarrow ii) \Rightarrow iii) \Rightarrow i)$, $iii) \Leftrightarrow iv)$, and $iv) \Rightarrow v) \Rightarrow vi) \Rightarrow iv)$. To prove $i) \Rightarrow ii)$, assume that $\mathbf{F}Gu$ is reversible with respect to $\mathcal{L}$. Since $\mathbf{F}G$ contains 1, $ku^{(-1)} = \mathrm{r}_{\mathcal{L}}(u) \in \mathbf{F}Gu$. Then $u^{(-1)} = k^{-1}\mathrm{r}_{\mathcal{L}}(u) \in \mathbf{F}Gu$, i.e. $\mathbf{F}Gu^{(-1)} \subseteq \mathbf{F}Gu$. Since, by Corollary 3.4, they have the same cardinality, we conclude that $\mathbf{F}Gu^{(-1)} = \mathbf{F}Gu$.

The proof of $ii) \Rightarrow iii)$ is immediate from Lemma 4.3.

To prove $iii) \Rightarrow i)$, assume that there exists a unit $a \in \mathbf{F}G$ such that $u = au^{(-1)}$. Let $wu \in \mathbf{F}Gu$. Then

$$\begin{aligned}\mathrm{r}_{\mathcal{L}}(wu) &= k(wu)^{(-1)} = kw^{(-1)}u^{(-1)} \\ &= (kw^{(-1)}a^{-1})u \in \mathbf{F}Gu.\end{aligned}$$

This shows that $\mathbf{F}Gu$ is reversible.

Next, we prove $iii) \Leftrightarrow iv)$. Assume that $u = au^{(-1)}$ for some unit a in $\mathbf{F}G$. Since $0 = uv = au^{(-1)}v = u^{(-1)}(av)$ and $v^{(-1)}$ is a check element of $\mathbf{F}Gu^{(-1)}$, we have $av \in \mathbf{F}Gv^{(-1)}$. As a is a unit, $v \in \mathbf{F}Gv^{(-1)}$. Then, by Corollary 3.4, $\mathbf{F}Gv = \mathbf{F}Gv^{(-1)}$. Therefore, by Lemma 4.3, there exists a unit b in $\mathbf{F}G$ such that $v = bv^{(-1)}$. The converse is proved using similar arguments.

The equivalence $iv) \Rightarrow v) \Rightarrow vi) \Rightarrow iv)$ is proved similar to $iii) \Rightarrow ii) \Rightarrow i) \Rightarrow iii)$. ∎

Remark 4.5: To verify whether $\mathbf{F}Gu$ is reversible, by the condition $ii)$, it is equivalent to checking if $u^{(-1)} \in \mathbf{F}Gu$.

When $G = \langle x \rangle$, we know that any non-trivial cyclic code corresponds to some checkable code in $\mathbf{F}G$. According to [17], a cyclic code is said to be *reversible* if its corresponding checkable code is reversible with respect to the list $\{1, x, x^2, \ldots, x^{n-1}\}$.

For a polynomial $f(X) = f_0 + f_1X + \cdots + X^t \in \mathbf{F}[X]$ with $f_0 \neq 0$, the *reciprocal polynomial* of $f(X)$ is defined to be $f^*(X) := f_0^{-1}X^t f(\frac{1}{X})$. The polynomial $f(X)$ is said to be self-reciprocal if $f(X) = f^*(X)$. Then the following corollary is immediate from Theorem 4.4.

Corollary 4.6 ([17, Theorem 1]): The cyclic code generated by a monic polynomial $g(X)$ is reversible if and only if $g(X)$ is self-reciprocal.

B. Complementary Dual Checkable Codes

In this subsection, we study the structure of a checkable code $\mathbf{F}Gu$ with $\mathbf{F}Gu \cap (\mathbf{F}Gu)^{\perp} = \{0\}$, namely, a *complementary dual code* (cf. [21]). We focus on the case where the characteristic p of $\mathbf{F}$ does not divide the order n of G which is a common restriction as in the study of simple root cyclic codes.

Under this restriction, the group ring $\mathbf{F}G$ is always code-checkable since the Sylow p-subgroup of G is trivial. Moreover, $p \nmid n$ if and only if $\mathbf{F}G$ is semi-simple (cf. [20, Chapter 2: Theorem 4.2]). See [19] and [20] for further details.

We recall a special ideal of $\mathbf{F}G$ which is key to characterizing the structure of complementary dual checkable codes. An ideal A of $\mathbf{F}G$ is called a *nil ideal* if, for each $a \in A$, there exists a positive integer r such that $a^r = 0$. By the finiteness of $\mathbf{F}G$ and [19, Theorem 2.7.14 and Theorem 2.7.16], the nil ideal characterizes semi-simplicity of $\mathbf{F}G$ as follows.

Lemma 4.7: A finite group ring $\mathbf{F}G$ is semi-simple if and only if it has no non-zero nil ideals.

Corollary 4.8: If $\mathbf{F}Gu$ is checkable with a check element v, then $\mathbf{F}Gu \cap \mathbf{F}Gv = \{0\}$.

Proof: Let $w \in \mathbf{F}Gu \cap \mathbf{F}Gv$. Then $w = au = bv$ for some $a, b \in \mathbf{F}G$. Hence, $w^2 = aubv = (ab)(uv) = 0$ which implies that $\mathbf{F}Gu \cap \mathbf{F}Gv$ is a nil ideal. As $\mathbf{F}G$ is semi-simple, $\mathbf{F}Gu \cap \mathbf{F}Gv = \{0\}$ by Lemma 4.7. ∎

Theorem 4.9: Let $\mathbf{F}Gu$ be checkable with a check element v and $\mathcal{L}$ a list of G satisfying (IV.1). Then the following statements are equivalent.

$i)$ $\mathbf{F}Gu$ is a complementary dual code.
$ii)$ $\mathbf{F}Gu$ is a reversible code with respect to $\mathcal{L}$.
$iii)$ $\mathbf{F}Gv$ is a complementary dual code.

Proof: To prove $i) \Rightarrow ii)$, assume that $\mathbf{F}Gu$ is a complementary dual code. Applying Corollary 3.3, we obtain $\{0\} = \mathbf{F}Gu \cap (\mathbf{F}Gu)^{\perp} = \mathbf{F}Gu \cap \mathbf{F}Gv^{(-1)}$ which implies $\mathbf{F}G = \mathbf{F}Gu \oplus \mathbf{F}Gv^{(-1)}$. Since, by Corollary 4.8, $\mathbf{F}Gu \cap \mathbf{F}Gv = \{0\}$, we have

$$\begin{aligned}\mathbf{F}Gv &= \mathbf{F}G \cap \mathbf{F}Gv \\ &= (\mathbf{F}Gu \cap \mathbf{F}Gv) \oplus (\mathbf{F}Gv^{(-1)} \cap \mathbf{F}Gv) \\ &= \mathbf{F}Gv^{(-1)} \cap \mathbf{F}Gv.\end{aligned}$$

Thus, $\mathbf{F}Gv \subseteq \mathbf{F}Gv^{(-1)}$. Since, by Corollary 3.4, they have the same cardinality, it follows that $\mathbf{F}Gv = \mathbf{F}Gv^{(-1)}$. Therefore, $\mathbf{F}Gu$ is reversible by Theorem 4.4.

To prove $ii) \Rightarrow i)$, assume that $\mathbf{F}Gu$ is reversible with respect to $\mathcal{L}$. Let $w \in \mathbf{F}Gu \cap (\mathbf{F}Gu)^{\perp}$. Then, by Corollary 3.3 and Theorem 4.4, $w \in \mathbf{F}Gu \cap \mathbf{F}Gv^{(-1)} = \mathbf{F}Gu \cap \mathbf{F}Gv$.

We have $w = 0$ by Corollary 4.8. Therefore, $\mathbf{F}Gu$ is a complementary dual code.

By Theorem 4.4, $ii)$ holds if and only if $\mathbf{F}Gv$ is reversible, which is equivalent to that $\mathbf{F}Gv$ is a complementary dual code. This proves $ii) \Leftrightarrow iii)$. ∎

Corollary 4.10 ([21, Corollary]): Let $\mathbf{F}$ be a finite field of characteristic p, and n a positive integer such that $p \nmid n$. Then a cyclic code of length n over $\mathbf{F}$ is a complementary dual code if and only if it is reversible.

V. Examples

Many different interesting examples arise from the family of checkable codes from group rings. In this section, we discuss some of these examples based on Theorem 3.2. We show that various *Maximum Distance Separable (MDS) codes*, $[n, k, d]$ linear codes attaining the Singleton bound $d \leq n - k + 1$, are checkable. Moreover, numerous good checkable codes and new codes are illustrated as well.

A. Some MDS Checkable Codes

Given a positive integer n, we show that $[n, 1, n]$ and $[n, n-1, 2]$ MDS codes can be constructed as zero-divisor codes. In many cases, they are checkable.

Lemma 5.1: Given a finite field $\mathbf{F}$ and a finite abelian group G, then the element $\sum_{g\in G} g$ is always a zero-divisor in the group ring $\mathbf{F}G$.

Proof: This follows since $(1 - g') \sum_{g\in G} g = 0$, for all $g' \in G \setminus \{1\}$, where 1 is the group identity in G. ∎

Corollary 5.2: Given a finite field $\mathbf{F}$ and a finite abelian group G of order n, then there exists an $[n, 1, n]$ zero-divisor MDS code constructed from the group ring $\mathbf{F}G$.

Proof: From Lemma 5.1, $\sum_{g\in G} g$ is a zero divisor in $\mathbf{F}G$. It is easy to see that the associated U of $u = \sum_{g\in G} g$ is the all 1's $n \times n$-matrix. Therefore, the code generated by u is obviously $\{\lambda(11\ldots1) \mid \lambda \in \mathbf{F}\}$, an $[n, 1, n]$ MDS code over $\mathbf{F}$. ∎

Corollary 5.3: Let $\mathbf{F}$ be a finite field of characteristic p and let G be a finite abelian group of order n. If a Sylow p-subgroup of G is cyclic, then there exist checkable $[n, 1, n]$ and $[n, n-1, 2]$ MDS codes from the group ring $\mathbf{F}G$.

Proof: By Corollary 5.2, the code $\mathcal{C}$ generated by $\sum_{g\in G} g$ is an $[n, 1, n]$ MDS code. Assume that a Sylow p-subgroup of G is cyclic. From Theorem 3.2, it follows that $\mathcal{C}$ and its dual $\mathcal{C}^\perp$ are checkable. Since $\mathcal{C}$ is MDS, $\mathcal{C}^\perp$ is again MDS with parameters $[n, n-1, 2]$. ∎

Remark 5.4: Since $(\sum_{g\in G} g)^{(-1)} = (\sum_{g\in G} g)$, the $[n, 1, n]$ MDS code generated by $\sum_{g\in G} g$ and its dual are reversible by Theorem 4.4. Moreover, if the characteristic of $\mathbf{F}$ does not divide n, then, by Theorem 4.9, they are complementary dual.

B. Good Codes from Code-Checkable Group Rings

We illustrate some good examples of checkable codes. Let $\mathbf{F}_q$ denote the finite field of order q with characteristic p and let G be an abelian group of order n. When G is a cyclic group, we know that checkable codes from the group ring $\mathbf{F}_qG$ are the classical cyclic codes. Hence, we consider examples only in the case where G is a non-cyclic abelian group such that a Sylow p-subgroup of G is cyclic, i.e., $\mathbf{F}G$ is code-checkable.

With the help of the computer algebra system MAGMA [4], generator elements, check elements, and the actual minimum distances of checkable codes from $\mathbf{F}_qG$ are computed in many cases for $q \in \{2, 3, 4, 5\}$ and G is a non-cyclic abelian group decomposed as a product of two cyclic groups. In numerous cases, the parameters of these codes are as good as the best known ones in [10]. We call such codes *good codes*. In particular, an optimal $[36, 28, 6]$ code and a $[72, 62, 6]$ code over $\mathbf{F}_5$ with minimum distances improving by 1 upon [10] are found. These are called *new codes* presented in the next subsection.

In Tables I-IV, a group $G = C_r \times C_s$ of order $n = rs$ denotes the product of cyclic groups $C_r = \langle x \rangle$ and $C_s = \langle y \rangle$. A vector $u = (u_0u_1u_2\ldots u_{n-1}) \in \mathbf{F}_q^n$ represents the element $u(x, y) \in \mathbf{F}_qG$ with respect to the list $\mathcal{L}$ defined in (IV.3), i.e., u is the coefficients of

$$u(x, y) = \sum_{j=0}^{s-1} \sum_{i=0}^{r-1} u_{jr+i} x^i y^j \text{ in } \mathbf{F}_qG.$$

Given positive integers n and k, the minimum distance of the $[n, k, d]$ codes displayed in the tables achieve the best known distances [10], except for the two codes with asterisk in Table IV, where the distance improves upon that of the best known ones by 1. Based on the characterizations in Section IV, the subscripts $_{\mathrm{R}}$ and $_{\mathrm{C}}$ indicate the reversibility and complementary duality of the codes, respectively. To save space, codes with small length, $[n, 1, n]$ and $[n, n-1, 2]$ MDS codes guaranteed by Corollary 5.3, and codes with minimum distance 2 will be omitted.

C. New Codes from Code-Checkable Group Rings

A checkable code is determined by a check element. We give the check elements of the two new checkable codes in Table IV. In addition, generator elements and the standard generator matrices of these codes are also provided. Moreover, other two optimal codes with minimum distances improving by 1 upon [10] are found by shortening a new checkable code.

The $[36, 28, 6]$ code $\mathcal{C}_{36}$ over $\mathbf{F}_5$ in Table IV improves the lower bound on the minimum distance given in [10] by 1 and it is optimal. The code $\mathcal{C}_{36}$ derived from $\mathbf{F}_5(C_6 \times C_6)$ is generated by

$$u_{36} = (021242402043131423014123232100132334)$$

with check element

$$v_{36} = (100004000410431304002224330013242110).$$

The standard generator matrix of $\mathcal{C}_{36}$ is given by

$$\mathcal{G}_{36} = \begin{pmatrix} & 323044040 \\ & 221030034 \\ & 400021324 \\ & 040013243 \\ & 004023041 \\ & 122034033 \\ & 120024112 \\ & 012030244 \\ & 312033000 \\ & 342022220 \\ & 340021142 \\ & 034030442 \\ & 330022241 \\ I_{27} & 033041113 \\ & 242002413 \\ & 330041333 \\ & 033021300 \\ & 242033210 \\ & 210021311 \\ & 021041020 \\ & 430011312 \\ & 043034414 \\ & 243040132 \\ & 213013421 \\ & 122043340 \\ & 323023204 \\ & 221044011 \\ \mathbf{0}_{1\times 27} & 000111111 \end{pmatrix}.$$

By shortening $\mathcal{C}_{36}$ at the $1st$ position, we obtain a optimal $[35, 27, 6]$ code over $\mathbf{F}_5$. Similarly, a optimal $[34, 26, 6]$ code over $\mathbf{F}_5$ can be obtained by shortening $\mathcal{C}_{36}$ at the $1st$ and $2nd$ positions. The minimum distances of these codes are improved by 1 from the lower bound given in [10].

The $[72, 62, 6]$ code $\mathcal{C}_{72}$ over $\mathbf{F}_5$ in Table IV improves the lower bound on the minimum distance given in [10] by 1. The code $\mathcal{C}_{72}$ derived from $\mathbf{F}_5(C_6 \times C_{12})$ is generated by u_{72} with check element v_{72}.

The standard generator matrix of $\mathcal{C}_{72}$ is given by

$$\mathcal{G}_{72} = \begin{pmatrix} & 30003323330 12 \\ & 30001203122 04 \\ & 30004403320 31 \\ & 30004220340 14 \\ & 30001340323 04 \\ & 30003142102 20 \\ & 40004304420 22 \\ & 40002324421 30 \\ & 40004214202 33 \\ & 40003131342 22 \\ & 40000112332 13 \\ & 40003221100 20 \\ & 30003401021 41 \\ & 30004120110 20 \\ & 30001331300 00 \\ & 30002322312 24 \\ & 30001100020 20 \\ & 30004444010 13 \\ & 30003444014 41 \\ & 30003304021 34 \\ & 30004113410 24 \\ & 30000014242 34 \\ & 30000104320 00 \\ & 30004344440 11 \\ & 30001323024 13 \\ & 30001004144 44 \\ & 30004433422 20 \\ & 30002132024 41 \\ I_{59} & 30002403434 13 \\ & 30004022301 02 \\ & 10002434242 44 \\ & 10001210114 04 \\ & 10004003420 33 \\ & 10003011313 20 \\ & 10004234040 20 \\ & 10001441144 32 \\ & 00001322203 34 \\ & 00002221001 20 \\ & 00002312431 04 \\ & 00001000131 31 \\ & 00000101013 13 \\ & 00000013101 31 \\ & 30000120020 01 \\ & 30001432341 03 \\ & 30002330411 34 \\ & 30002421223 32 \\ & 30001113411 31 \\ & 30000211242 40 \\ & 10004142313 30 \\ & 10002202314 34 \\ & 10003332202 10 \\ & 10001301410 01 \\ & 10003244112 22 \\ & 10002114044 23 \\ & 40002442034 33 \\ & 40001314344 00 \\ & 40003343301 44 \\ & 40001400421 21 \\ & 40002033021 40 \\ & 01004234112 34 \\ \mathbf{0}_{3\times 59} & 00103332130 31 \\ & 00013244432 11 \end{pmatrix}.$$

$$u_{72} = (312411232330313143111221222301122414030013401133430420133323011301020100),$$
$$v_{72} = (100000000441004102234010043124424101300211324012401114201004023203011413).$$

TABLE I
GOOD CHECKABLE CODES FROM $\mathbf{F}_2G$

n	Code $\mathcal{C}$	Group G	Generator Element u and Check Element v
25	$[25, 16, 4]_{\mathrm{R,C}}$	$C_5 \times C_5$	$u = (0111000101010111000101010)$, $v = (1000000001101010111010101)$
	$[25, 17, 4]_{\mathrm{R,C}}$	$C_5 \times C_5$	$u = (1110001101100000111000100)$, $v = (1000000001000100010010111)$
27	$[27, 18, 4]_{\mathrm{R,C}}$	$C_3 \times C_9$	$u = (011100010001110110000111011)$, $v = (010001001001111111111010010)$
45	$[45, 28, 8]$	$C_3 \times C_{15}$	$u = (011101000001100011101100111101011000010000001)$, $v = (110000000000000011001010000001010111000010111)$
	$[45, 29, 7]$	$C_3 \times C_{15}$	$u = (001010010100011101100110011101000100110011111)$, $v = (100000000000000010001100101111101111011100100)$
	$[45, 31, 6]$	$C_3 \times C_{15}$	$u = (010101110110100011110110001010110010100110001)$, $v = (110000000000100110010100001101111001110111000)$
	$[45, 32, 6]$	$C_3 \times C_{15}$	$u = (000000100011011100100110111001001010000000001)$, $v = (110000000000010001001110100100110011100101001)$
	$[45, 37, 4]_{\mathrm{R,C}}$	$C_3 \times C_{15}$	$u = (010000110101111010010111010001001110011000001)$, $v = (100011011011011011100011100100011011100100011)$
	$[45, 38, 4]$	$C_3 \times C_{15}$	$u = (000010010011100011011001100110010011010001110)$, $v = (100001001010011110010001011100111111010001)$
	$[45, 39, 3]$	$C_3 \times C_{15}$	$u = (100011010001011010000111100001010011110011111)$, $v = (101000000011110101101110110110000101110101000)$
49	$[49, 30, 8]$	$C_7 \times C_7$	$u = (011000110111100111000010001001101111000100110011011)$, $v = (000110000000000000111001111111101001100111101100)$
	$[49, 33, 6]$	$C_7 \times C_7$	$u = (100001101100011111111101101000011001100010010010 0)$, $v = (110000000001000000010000110001010000101101111010 1)$
	$[49, 34, 6]$	$C_7 \times C_7$	$u = (000000111101001000001010100000101001011011010011 0)$, $v = (001100000000000001010000010111101111010011011001 1)$
	$[49, 39, 4]$	$C_7 \times C_7$	$u = (000100110101000011110111101010111010001010001110 0)$, $v = (100000000010111000000101011101001010100101101 0111)$
	$[49, 40, 4]$	$C_7 \times C_7$	$u = (001100011100111111010010010101001010000100000010 1)$, $v = (011000000010101110100011011011101110101101010001 0)$
	$[49, 42, 4]$	$C_7 \times C_7$	$u = (001000001000000100000101000100100110101110110110 1)$, $v = (010001100011011111111000110101000110011010011001 0)$
	$[49, 43, 3]$	$C_7 \times C_7$	$u = (000010100100011010010000011100001000111010101001 1)$, $v = (100000101010000001111001001011001100110101111101 1)$
50	$[50, 40, 4]_{\mathrm{R}}$	$C_5 \times C_{10}$	$u = (000100001001010110001100100110101111001001111110 10)$, $v = (100000000010000010011011001111111110111110110010 01)$

TABLE II
GOOD CHECKABLE CODES FROM $\mathbf{F}_3G$

n	Code $\mathcal{C}$	Group G	Generator Element u and Check Element v
20	$[20, 14, 4]_{\mathrm{R,C}}$	$C_2 \times C_{10}$	$u = (02101221221212221102)$, $v = (21010201020121202120)$
24	$[24, 18, 4]_{\mathrm{R}}$	$C_2 \times C_{12}$	$u = (112221001100010121120021)$, $v = (210202020202212102100221)$
	$[24, 19, 3]_{\mathrm{R}}$	$C_2 \times C_{12}$	$u = (111120120021120102022202)$, $v = (100201020120222022111011)$
32	$[32, 18, 8]$	$C_4 \times C_8$	$u = (000101211012221212101210220000 01)$, $v = (100000020002000202220021011211 02)$
	$[32, 21, 6]$	$C_4 \times C_8$	$u = (100021121212010211002020202211 00)$, $v = (110000000002112222010021020012 12)$
	$[32, 25, 4]$	$C_4 \times C_8$	$u = (102222202112212110220211012220 02)$, $v = (210000000210212100212121221100 00)$
	$[32, 26, 4]$	$C_4 \times C_8$	$u = (102021001010201101212100200100 12)$, $v = (210000112210002221002200110211 00)$
	$[32, 27, 3]$	$C_4 \times C_8$	$u = (102100220200021221200101022102 10)$, $v = (100100220110001121120022122111 22)$
40	$[40, 33, 4]$	$C_2 \times C_{20}$	$u = (020022112202102021011102120120112211 1221)$, $v = (100101010101101022100101100110010122222 2)$
	$[40, 34, 4]$	$C_2 \times C_{20}$	$u = (220020010021012021122102110212001011010 1)$, $v = (210102010201212010200201210121010210212 1012)$
44	$[44, 36, 4]$	$C_2 \times C_{22}$	$u = (101202002020101201210010110101110221001100 01)$, $v = (210102010201022002122120101210121012212 20220)$
	$[44, 37, 4]$	$C_2 \times C_{22}$	$u = (201022121212010222020000212222202220210122 00)$, $v = (010201020102101101201020222022202211102002 11)$
48	$[48, 41, 4]_{\mathrm{R}}$	$C_4 \times C_{12}$	$u = (110121102110110111001110110220020112122022220 001)$, $v = (210000110122221110220011120011001022112201221 100)$
	$[48, 40, 4]_{\mathrm{R}}$	$C_4 \times C_{12}$	$u = (120122000210012211010202001020120012101002100 02)$, $v = (121000020001222120212221000100021210222111122 221)$

TABLE III
GOOD CHECKABLE CODES FROM $\mathbf{F}_4G$, WHERE $\mathbf{F}_4 = \{0, 1, a, a^2 = 1 + a\}$

n	Code $\mathcal{C}$	Group G	Generator Element u and Check Element v
18	$[18, 14, 3]$	$C_3 \times C_6$	$u = (a^2aa01011a^20a^2a^2aaa^2a^211)$, $v = (a1a^2111a^2a10a^2100001a)$
25	$[25, 16, 6]_{\mathrm{R,C}}$	$C_5 \times C_5$	$u = (1a^2001a11a0a0a^2a0a^2110111a^2aa^2)$, $v = (a1111111001a^2010a^210aa^2a100a)$
	$[25, 19, 4]_{\mathrm{R,C}}$	$C_5 \times C_5$	$u = (01a^2001a0aaa^200a^2111a^20001a^2a0)$, $v = (a^2111a11a^20a^20a^2a^2aa1a1a0a^2a^2000)$
	$[25, 20, 4]_{\mathrm{R,C}}$	$C_5 \times C_5$	$u = (0a^2a^211aa^2a0aa^20a^211a0010a^2a11a^2)$, $v = (a^211a^2a11a^2aa^2a0a^2a^201a100a^20a0a^2)$
	$[25, 21, 3]_{\mathrm{R,C}}$	$C_5 \times C_5$	$u = (1101000aa^2aaa^2a0a^2111a^20a^20011)$, $v = (a11a011a0aa^2a^2101a^20a^2aa1a^2a^210)$
45	$[45, 38, 4]$	$C_3 \times C_{15}$	$u = (0010aa^2aa^211aaa11aaa^200a01a^2010aa0100a^2a0aa00a0a00)$, $v = (a1111a^211a10a^2a^20a^2a^2111aa0a^20aa^2aa0aa^2a^21a00a^21a^2100a^2a^20)$
	$[45, 39, 4]$	$C_3 \times C_{15}$	$u = (1a1aaaaa^210a^2a^21aaaaaa^2aa^21a01a1a^21a^20a^21a0a^2a0a^211011a^20)$, $v = (a^21111011a^2a00a^2a^2a11a^20aaaaa^200aa00aaa^2aa0a^211a^2a^2a00a)$
	$[45, 34, 6]$	$C_3 \times C_{15}$	$u = (a^2aa0aa^2aaa^21110a01aa0111a^2aa0110a^21aa^2aa^2a^2a0a^2aa^2a1a^2a^2)$, $v = (1111111111100a^2a^210a011a0011aa^21a^20aa0a010a1aaa^211)$
	$[45, 35, 6]$	$C_3 \times C_{15}$	$u = (1a^2111a000aa^2a^21a^2a1aaaa^21000aa^2a10aaa^21a^20a^21a^2aa1a^210a^2)$, $v = (a^21111111a^211a^211aa1a000aa^2000100aa^2a1a10a^2a^20101a11)$
	$[45, 40, 3]$	$C_3 \times C_{15}$	$u = (101a^211a^21aa1a1a^200a^2a^2a1aa^20a00a0a0aa^20aaa^2aaa^20a1a^21a)$, $v = (a1a^21101aa^2a^2a^20a^2a11aa^20aa0a^2a^2a^21aa^2a^200a^2a^2aa^21a1a^2a^2a1a^21a)$
	$[45, 41, 3]$	$C_3 \times C_{15}$	$u = (0a^20011a^211aa^201a1a^20a^2aa^2101a0100a^2a^2a00aa^2a0a^20aaa^21aa^2)$, $v = (a1a^210a^21a^2aa^20a01aa01a1a^201a0aa^20a^2110a^2a010a^21aa^201a^2a)$
49	$[49, 42, 4]$	$C_7 \times C_7$	$u = (a^21a^2a^2011a^20111a^21a^20a^2aa^21a^2a^2a^21000010a^2a^2aa^21a^2110aaaaa0a11a)$, $v = (a111a1a111a1aa1a1aa11aaaaaaa11a1aa1aa111a1a1aa111)$
50	$[50, 43, 4]_{\mathrm{R}}$	$C_5 \times C_{10}$	$u = (01a^2aaaaa^2a^200010a^21a^2a^20aa110a11aaa^21a01a11a^2111a^210a1a^2110)$, $v = (a^211a^20111111a^2a^21a11111a^211a^2000000a00a1aaaaaa00a100000)$
	$[50, 44, 4]_{\mathrm{R}}$	$C_5 \times C_{10}$	$u = (a^2a^20a0aa1aa01aa^210a1a^21a^20a^2aa001aa^21a00a^2a^2a^210aa0001aa^2a^2a^2a)$, $v = (a1111110aa^2a1aa^201a^201aa01a^2a1aaaaaaa^2101a10a^2a0a^2a11a^2a01)$

TABLE IV
GOOD CHECKABLE CODES FROM $\mathbf{F}_5G$

n	Code $\mathcal{C}$	Group G	Generator Element u and Check Element v
18	$[18, 10, 6]_{\mathrm{R,C}}$	$C_3 \times C_6$	$u = (304442010212124112)$, $v = (100000004013203240)$
	$[18, 13, 4]_{\mathrm{R,C}}$	$C_3 \times C_6$	$u = (111444121401433042)$, $v = (100011044233322344)$
20	$[20, 15, 4]_{\mathrm{R}}$	$C_2 \times C_{10}$	$u = (12410122413003142121)$, $v = (10010401103443404334)$
24	$[24, 19, 4]$	$C_2 \times C_{12}$	$u = (223203242014333100004101)$, $v = (110103043433032211332104)$
32	$[32, 26, 4]$	$C_4 \times C_8$	$u = (121133310012442043022133110322 03)$, $v = (141400310043031042422203110442 04)$
	$[32, 28, 3]$	$C_4 \times C_8$	$u = (221111224033442430123221001424 31)$, $v = (412003240231421324032041134231 02)$
36	$[36, 27, 6]_{\mathrm{R,C}}$	$C_6 \times C_6$	$u = (320132303303034041221304303442323 43)$, $v = (100001000434001100141404131131141404)$
	$\mathbf{[36, 28, 6]}^*_{\mathrm{R,C}}$	$C_6 \times C_6$	$u = (021242402043131423014123232100132334)$, $v = (100004000410431304002224330013242110)$
	$[36, 30, 4]_{\mathrm{R,C}}$	$C_6 \times C_6$	$u = (430221420433120003111301342330403142)$, $v = (100011024142020141102014233433232434)$
	$[36, 31, 4]_{\mathrm{R,C}}$	$C_6 \times C_6$	$u = (414212431211114001024430113141242220)$, $v = (100001244134331320112211023133431442)$
40	$[40, 34, 4]$	$C_2 \times C_{20}$	$u = (101424144044434024131422131040010310 2403)$, $v = (010401040131331342312404240424224 03322)$
	$[40, 36, 3]$	$C_2 \times C_{20}$	$u = (340444242043041442344312421041240 1010024)$, $v = (100404212121430432433232431021100 4321043)$
45	$[45, 38, 4]_{\mathrm{R}}$	$C_3 \times C_{15}$	$u = (422214114313301102020432222411013144100033133)$, $v = (100000011322000344433444011433222122322444122)$
48	$[48, 37, 6]$	$C_4 \times C_{12}$	$u = (022401214232343132104344424140031221030041132043)$, $v = (100000000003314304224422430430220301424142443412)$
	$[48, 41, 4]$	$C_4 \times C_{12}$	$u = (033110404424400223213444240314124301040420320311)$, $v = (010001410400041412112313101143034044120221221020)$
	$[48, 42, 4]$	$C_4 \times C_{12}$	$u = (200421304403101244441432224311111011301122004343)$, $v = (410000230302113004421310322332142021210224312422)$
	$[48, 44, 3]$	$C_4 \times C_{12}$	$u = (034043422131413332341002234213011122220221033211)$, $v = (100401314123303424134222412344431004422200323034)$
72	$\mathbf{[72, 62, 6]}^*$	$C_6 \times C_{12}$	$u = (312411232330313143111221222301122414030013401133430420133323011301020100)$, $v = (100000000441004102234010043124424101300211324012401114201004023203011413)$

VI. Conclusion

We have studied checkable codes derived from the group ring $\mathbf{F}G$, where $\mathbf{F}$ is a finite field and G is a finite abelian group. We have introduced a notion of code-checkable group rings and determined necessary and sufficient conditions for a group ring $\mathbf{F}G$ to be code-checkable. Based on this characterization, we obtained two new codes which have minimum distance better than the lower bound given in Grassl's table [10]. Various codes with minimum distance as good as the best known ones in [10] are also found. By shortening a new checkable code, we obtain other two optimal codes which have minimum distance better than the lower bound in [10]. In addition, we have proved that many $[n, 1, n]$ and $[n, n-1, 2]$ MDS codes can be constructed as checkable codes. Furthermore, when $\mathbf{F}G$ is a code-checkable group ring, the dual of a code in $\mathbf{F}G$ may be described via a check element of the code. This property generalizes the notions of the generator and parity-check polynomials of cyclic codes to the multivariate case. Moreover, we have characterized the structures of reversible and complementary dual checkable codes which are generalizations of reversible and complementary dual cyclic codes, respectively.

It would be interesting to study possible generalizations of other properties of cyclic codes to this new class of codes.

References

[1] T. Abualrub, A. Ghrayeb, and X. N. Zeng, "Construction of cyclic codes over $\mathrm{GF}(4)$ for DNA computing," *J. Franklin Inst.*, vol. 343, pp. 448-457, 2006.

[2] S. D. Berman, "On the theory of group codes," *Kibernetika*, vol. 3, pp. 31–39, 1967.

[3] S. D. Berman, "Semi-simple cyclic and abelian codes," *Kibernetika*, vol. 3, pp. 21–30, 1967.

[4] W. Bosma, J. J. Cannon, and C. Playoust, "The Magma algebra system I: the user language," *J. Symbolic Comput.*, vol. 24, pp. 235–266, 1997.

[5] H. Chabanne, "Permutation decoding of abelian codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1826–1829, 1992.

[6] C. Ding, D. R. Kohel, and S. Ling, "Split group codes," *IEEE Trans. Inform. Theory*, vol. 46, pp. 485–495, 2000.

[7] D. S. Dummit, and R. M. Foote, *Abstract Algebra*. John Wiley & Sons, 3rd edition, 2004.

[8] D. R. Farenick, *Algebras of Linear Transformations*. Springer, 2001.

[9] J. L. Fisher and S. K. Sehgal, "Principal ideal group rings," *Comm. Algebra*, vol. 4, pp. 319–325, 1976.

[10] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," Online available at http://www.codetables.de, accessed on 2010-09-29.

[11] M. Greferath, and S. E. Schmidt, "Finite-ring combinatorics and MacWilliams Equivalence Theorem," *J. Combin. Theory Ser. A*, vol. 92, pp. 17–28, 2000.

[12] T. Hurley, "Group ring and rings of matrices," *Inter. J. Pure and Appl. Math.*," vol. 31, pp. 319–335, 2006.

[13] P. Hurley, and T. Hurley, "Module codes in group rings," in *Proc. IEEE Int. Symp. Information Theory*, Nice, France, Jul. 2007, pp. 1981–1985.

[14] P. Hurley, and T. Hurley, "Codes from zero-divisors and units in group rings," *Int. J. Information and Coding Theory*, vol. 1, pp. 57–87, 2009.

[15] F. J. MacWilliams, "Codes and ideals in group algebras," *Combinatorial Mathematics and its Applications*, pp. 312–328, 1969.

[16] F. J. MacWilliams, "Binary codes which are ideals in the group algebra of an abelian group," *Bell Syst. Tech. J.*, vol. 49, pp. 987–1011, 1970.

[17] J. L. Massey, "Reversible codes," *Inform. and control*, vol. 7, pp. 369–380, 1964.

[18] I. McLoughlin, and T. Hurley, "A group ring construction of the extended binary Golay code," *IEEE Trans. Inform. Theory*, vol. 54, pp. 4381–4383, 2008.

[19] C. P. Milies, and S. K. Sehgal, *An Introduction to Group Rings*. London: Kluwer Academic Publishes, 2002.

[20] D. S. Passman, *The Algebraic Structure of Group Rings*. New York: Wiley, 1977.

[21] X. Yang, and J. L. Massey, "The condition for a cyclic code to have a complementary dual," *Discrete Math.*, vol. 126, pp. 391–393, 1994.