Checkable Codes from Group Rings

Somphong Jitman,
(joint work with S. Ling, H. Liu, and X. Xie)

MAS-SPMS-NTU

September 23, 2011

Outline

Outline

Outline

Outline

Outline

Motivation

- Various applications of cyclic codes is based on their single generator and check polynomials.
- Checkable codes are introduced to have the similar properties.
- Some special cyclic codes were studied:
  - reversible cyclic codes [Massey'64],
  - complementary-dual cyclic codes [Yang & Massey'94].
- These ideas are generalized for checkable codes.

Motivation

- Various applications of cyclic codes is based on their single generator and check polynomials.
- Checkable codes are introduced to have the similar properties.
- Some special cyclic codes were studied:
  - reversible cyclic codes [Massey'64],
  - complementary-dual cyclic codes [Yang & Massey'94].
- These ideas are generalized for checkable codes.

Motivation

- Various applications of cyclic codes is based on their single generator and check polynomials.
- Checkable codes are introduced to have the similar properties.
- Some special cyclic codes were studied:
  - reversible cyclic codes [Massey'64],
  - complementary-dual cyclic codes [Yang & Massey'94].
- These ideas are generalized for checkable codes.

Motivation

- Various applications of cyclic codes is based on their single generator and check polynomials.
- Checkable codes are introduced to have the similar properties.
- Some special cyclic codes were studied:
  - reversible cyclic codes [Massey'64],
  - complementary-dual cyclic codes [Yang & Massey'94].
- These ideas are generalized for checkable codes.

Group Rings

G – an abelian of order n, written multiplicatively (with identity 1).
$\mathbb{F}$ – a finite field of characteristic p.
$\mathbb{F}G = \{\sum_{g\in G} \alpha_g g \mid \alpha_g \in \mathbb{F}\}$ – the **group ring** of G over $\mathbb{F}$, where

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

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, $\mathbb{F}G$ is an $\mathbb{F}$-vector space with a basis G.
As G is abelian, the group ring $\mathbb{F}G$ is commutative.

Cyclic Codes

If $G = \langle x \rangle$ is cyclic, then $\mathcal{R}_n = \mathbb{F}[X]/\langle X^n - 1 \rangle \cong \mathbb{F}G$ via $X \mapsto x$.

Cyclic Codes in $\mathcal{R}_n$

- For $g(X) \in \mathcal{R}_n$, $\mathcal{C} = \langle g(X) \rangle$ - a cyclic code.
- $g(X)$ - a generator polynomial.
- $\exists h(X) \in R_n$, $\mathcal{C} = \{f(X) \in \mathcal{R}_n \mid f(X)h(X) = 0\}$ ($g(X) \mid (X^N - 1)$ and $h(X) = \frac{X^n - 1}{g(X)}$).
- $h(X)$ - a check polynomial.

Cyclic Codes from $\mathbb{F}G$, $G = \langle x \rangle$

- For a zero-divisor $u \in \mathbb{F}G$, $\mathcal{C} = \mathbb{F}Gu$ - a **zero-divisor code**.
- u - a **generator element**.
- Using $X \mapsto x$, $\exists v \in \mathbb{F}G$,

$$\mathcal{C} = \{y \in \mathbb{F}G \mid yv = 0\} = \mathrm{Ann}(v).$$

- v - a **check element**.

Cyclic Codes

If $G = \langle x \rangle$ is cyclic, then $\mathcal{R}_n = \mathbb{F}[X]/\langle X^n - 1 \rangle \cong \mathbb{F}G$ via $X \mapsto x$.

Cyclic Codes in $\mathcal{R}_n$

- For $g(X) \in \mathcal{R}_n$, $\mathcal{C} = \langle g(X) \rangle$ - a cyclic code.
- $g(X)$ - a generator polynomial.
- $\exists h(X) \in R_n$, $\mathcal{C} = \{f(X) \in \mathcal{R}_n \mid f(X)h(X) = 0\}$

  ($g(X) \mid (X^N - 1)$ and $h(X) = \frac{X^n - 1}{g(X)}$).
- $h(X)$ - a check polynomial.

Cyclic Codes from $\mathbb{F}G$, $G = \langle x \rangle$

- For a zero-divisor $u \in \mathbb{F}G$, $\mathcal{C} = \mathbb{F}Gu$ - a **zero-divisor code**.
- u - a **generator element**.
- Using $X \mapsto x$, $\exists v \in \mathbb{F}G$,

$$\mathcal{C} = \{y \in \mathbb{F}G \mid yv = 0\}$$
$$= \mathrm{Ann}(v).$$

- v - a **check element**.

Cyclic Codes

If $G = \langle x \rangle$ is cyclic, then $\mathcal{R}_n = \mathbb{F}[X]/\langle X^n - 1\rangle \cong \mathbb{F}G$ via $X \mapsto x$.

Cyclic Codes in $\mathcal{R}_n$

- For $g(X) \in \mathcal{R}_n$,
  $\mathcal{C} = \langle g(X) \rangle$ - a cyclic code.
- $g(X)$ - a generator polynomial.
- $\exists h(X) \in R_n$,
  $\mathcal{C} = \{f(X) \in \mathcal{R}_n \mid f(X)h(X) = 0\}$
  ($g(X) \mid (X^N - 1)$ and $h(X) = \frac{X^n - 1}{g(X)}$).
- $h(X)$ - a check polynomial.

Cyclic Codes from $\mathbb{F}G$, $G = \langle x \rangle$

- For a zero-divisor $u \in \mathbb{F}G$,
  $\mathcal{C} = \mathbb{F}Gu$ - a **zero-divisor code**.
- u - a **generator element**.
- Using $X \mapsto x$, $\exists v \in \mathbb{F}G$,
  $$\mathcal{C} = \{y \in \mathbb{F}G \mid yv = 0\} = \mathrm{Ann}(v).$$
- v - a **check element**.

Cyclic Codes

If $G = \langle x \rangle$ is cyclic, then $\mathcal{R}_n = \mathbb{F}[X]/\langle X^n - 1 \rangle \cong \mathbb{F}G$ via $X \mapsto x$.

Cyclic Codes in $\mathcal{R}_n$

- For $g(X) \in \mathcal{R}_n$,
  $\mathcal{C} = \langle g(X) \rangle$ - a cyclic code.
- $g(X)$ - a generator polynomial.
- $\exists h(X) \in R_n$,
  $\mathcal{C} = \{f(X) \in \mathcal{R}_n \mid f(X)h(X) = 0\}$
  ($g(X) \mid (X^N - 1)$ and $h(X) = \frac{X^n - 1}{g(X)}$).
- $h(X)$ - a check polynomial.

Cyclic Codes from $\mathbb{F}G$, $G = \langle x \rangle$

- For a zero-divisor $u \in \mathbb{F}G$,
  $\mathcal{C} = \mathbb{F}Gu$ - a **zero-divisor code**.
- u - a **generator element**.
- Using $X \mapsto x$, $\exists v \in \mathbb{F}G$,

$$\begin{aligned}\mathcal{C} &= \{y \in \mathbb{F}G \mid yv = 0\} \\ &= \mathrm{Ann}(v).\end{aligned}$$

- v - a **check element**.

Cyclic Codes

If $G = \langle x \rangle$ is cyclic, then $\mathcal{R}_n = \mathbb{F}[X]/\langle X^n - 1 \rangle \cong \mathbb{F}G$ via $X \mapsto x$.

Cyclic Codes in $\mathcal{R}_n$

- For $g(X) \in \mathcal{R}_n$, $\mathcal{C} = \langle g(X) \rangle$ - a cyclic code.
- $g(X)$ - a generator polynomial.
- $\exists h(X) \in R_n$, $\mathcal{C} = \{f(X) \in \mathcal{R}_n \mid f(X)h(X) = 0\}$ ($g(X) \mid (X^N - 1)$ and $h(X) = \frac{X^n - 1}{g(X)}$).
- $h(X)$ - a check polynomial.

Cyclic Codes from $\mathbb{F}G$, $G = \langle x \rangle$

- For a zero-divisor $u \in \mathbb{F}G$, $\mathcal{C} = \mathbb{F}Gu$ - a **zero-divisor code**.
- u - a **generator element**.
- Using $X \mapsto x$, $\exists v \in \mathbb{F}G$,

$$\begin{aligned}\mathcal{C} &= \{y \in \mathbb{F}G \mid yv = 0\} \\ &= \mathrm{Ann}(v).\end{aligned}$$

- v - a **check element**.

Cyclic Codes

If $G = \langle x \rangle$ is cyclic, then $\mathcal{R}_n = \mathbb{F}[X]/\langle X^n - 1 \rangle \cong \mathbb{F}G$ via $X \mapsto x$.

Cyclic Codes in $\mathcal{R}_n$

- For $g(X) \in \mathcal{R}_n$, $\mathcal{C} = \langle g(X) \rangle$ - a cyclic code.
- $g(X)$ - a generator polynomial.
- $\exists h(X) \in R_n$, $\mathcal{C} = \{f(X) \in \mathcal{R}_n \mid f(X)h(X) = 0\}$ ($g(X) \mid (X^N - 1)$ and $h(X) = \frac{X^n - 1}{g(X)}$).
- $h(X)$ - a check polynomial.

Cyclic Codes from $\mathbb{F}G$, $G = \langle x \rangle$

- For a zero-divisor $u \in \mathbb{F}G$, $\mathcal{C} = \mathbb{F}Gu$ - a **zero-divisor code**.
- u - a **generator element**.
- Using $X \mapsto x$, $\exists v \in \mathbb{F}G$,

$$\mathcal{C} = \{y \in \mathbb{F}G \mid yv = 0\} = \mathrm{Ann}(v).$$

- v - a **check element**.

Cyclic Codes

If $G = \langle x \rangle$ is cyclic, then $\mathcal{R}_n = \mathbb{F}[X]/\langle X^n - 1 \rangle \cong \mathbb{F}G$ via $X \mapsto x$.

Cyclic Codes in $\mathcal{R}_n$

- For $g(X) \in \mathcal{R}_n$,
  $\mathcal{C} = \langle g(X) \rangle$ - a cyclic code.
- $g(X)$ - a generator polynomial.
- $\exists h(X) \in R_n$,
  $\mathcal{C} = \{f(X) \in \mathcal{R}_n \mid f(X)h(X) = 0\}$
  ($g(X) \mid (X^N - 1)$ and $h(X) = \frac{X^n - 1}{g(X)}$).
- $h(X)$ - a check polynomial.

Cyclic Codes from $\mathbb{F}G$, $G = \langle x \rangle$

- For a zero-divisor $u \in \mathbb{F}G$,
  $\mathcal{C} = \mathbb{F}Gu$ - a **zero-divisor code**.
- u - a **generator element**.
- Using $X \mapsto x$, $\exists v \in \mathbb{F}G$,
  $$\begin{aligned}\mathcal{C} &= \{y \in \mathbb{F}G \mid yv = 0\} \\ &= \mathrm{Ann}(v).\end{aligned}$$
- v - a **check element**.

Cyclic Codes

If $G = \langle x \rangle$ is cyclic, then $\mathcal{R}_n = \mathbb{F}[X]/\langle X^n - 1 \rangle \cong \mathbb{F}G$ via $X \mapsto x$.

Cyclic Codes in $\mathcal{R}_n$

- For $g(X) \in \mathcal{R}_n$,
  $\mathcal{C} = \langle g(X) \rangle$ - a cyclic code.
- $g(X)$ - a generator polynomial.
- $\exists h(X) \in R_n$,
  $\mathcal{C} = \{f(X) \in \mathcal{R}_n \mid f(X)h(X) = 0\}$
  ($g(X) \mid (X^N - 1)$ and $h(X) = \frac{X^n - 1}{g(X)}$).
- $h(X)$ - a check polynomial.

Cyclic Codes from $\mathbb{F}G$, $G = \langle x \rangle$

- For a zero-divisor $u \in \mathbb{F}G$,
  $\mathcal{C} = \mathbb{F}Gu$ - a **zero-divisor code**.
- u - a **generator element**.
- Using $X \mapsto x$, $\exists v \in \mathbb{F}G$,

$$\begin{aligned}\mathcal{C} &= \{y \in \mathbb{F}G \mid yv = 0\} \\ &= \mathrm{Ann}(v).\end{aligned}$$

- v - a **check element**.

Checkable Codes

Cyclic Codes from $\mathbb{F}G$, $G = \langle x \rangle$

- For a zero-divisor $u \in \mathbb{F}G$, $\mathcal{C} = \mathbb{F}Gu$ - a **zero-divisor code**.
- u - a **generator element**.
- $\exists v \in \mathbb{F}G$,

$$\begin{aligned} \mathcal{C} &= \{y \in \mathbb{F}G \mid yv = 0\} \\ &= \mathrm{Ann}(v). \end{aligned}$$

- v - a **check element**.

Checkable Codes from $\mathbb{F}G$, G is abelian

- For a zero-divisor $u \in \mathbb{F}G$, $\mathcal{C} = \mathbb{F}Gu$ - a **zero-divisor code**.
- u - a **generator element**.
- If there exists $v \in \mathbb{F}G$

$$\begin{aligned} \mathcal{C} &= \{y \in \mathbb{F}G \mid yv = 0\} \\ &= \mathrm{Ann}(v), \text{ then} \end{aligned}$$

v - a **check element** and $\mathcal{C}$ - a **checkable code**.

Checkable Codes

Cyclic Codes from $\mathbb{F}G$, $G = \langle x \rangle$

- For a zero-divisor $u \in \mathbb{F}G$, $\mathcal{C} = \mathbb{F}Gu$ - a **zero-divisor code**.
- u - a **generator element**.
- $\exists v \in \mathbb{F}G$,

$$\begin{aligned}\mathcal{C} &= \{y \in \mathbb{F}G \mid yv = 0\}\\ &= \mathrm{Ann}(v).\end{aligned}$$

- v - a **check element**.

Checkable Codes from $\mathbb{F}G$, G is abelian

- For a zero-divisor $u \in \mathbb{F}G$, $\mathcal{C} = \mathbb{F}Gu$ - a **zero-divisor code**.
- u - a **generator element**.
- If there exists $v \in \mathbb{F}G$

$$\begin{aligned}\mathcal{C} &= \{y \in \mathbb{F}G \mid yv = 0\}\\ &= \mathrm{Ann}(v), \text{ then}\end{aligned}$$

v - a **check element** and C - a **checkable code**.

Checkable Codes

Cyclic Codes from $\mathbb{F}G$, $G = \langle x \rangle$

- For a zero-divisor $u \in \mathbb{F}G$, $\mathcal{C} = \mathbb{F}Gu$ - a **zero-divisor code**.
- u - a **generator element**.
- $\exists v \in \mathbb{F}G$,
$$\mathcal{C} = \{y \in \mathbb{F}G \mid yv = 0\} = \mathrm{Ann}(v).$$
- v - a **check element**.

Checkable Codes from $\mathbb{F}G$, G is abelian

- For a zero-divisor $u \in \mathbb{F}G$, $\mathcal{C} = \mathbb{F}Gu$ - a **zero-divisor code**.
- u - a **generator element**.
- If there exists $v \in \mathbb{F}G$
$$\mathcal{C} = \{y \in \mathbb{F}G \mid yv = 0\} = \mathrm{Ann}(v), \text{ then}$$
v - a **check element** and
C - a **checkable code**.

Checkable Codes

Cyclic Codes from $\mathbb{F}G$, $G = \langle x \rangle$

- For a zero-divisor $u \in \mathbb{F}G$, $\mathcal{C} = \mathbb{F}Gu$ - a **zero-divisor code**.
- u - a **generator element**.
- $\exists v \in \mathbb{F}G$,

$$\mathcal{C} = \{y \in \mathbb{F}G \mid yv = 0\} = \mathrm{Ann}(v).$$

- v - a **check element**.

Checkable Codes from $\mathbb{F}G$, G is abelian

- For a zero-divisor $u \in \mathbb{F}G$, $\mathcal{C} = \mathbb{F}Gu$ - a **zero-divisor code**.
- u - a **generator element**.
- If there exists $v \in \mathbb{F}G$

$$\mathcal{C} = \{y \in \mathbb{F}G \mid yv = 0\} = \mathrm{Ann}(v), \text{ then}$$

v - a **check element** and
C - a **checkable code**.

$\mathbb{F}G$ is **code-checkable** if every non-trivial ideal of $\mathbb{F}G$ is a checkable code.

Given a finite abelian group G and a finite field $\mathbb{F}$ of characteristic p, we have the following results.

Proposition

$\mathbb{F}G$ is code-checkable if and only if it is a principal ideal ring (PIR).

Theorem (Fisher & Sehgal'76)

$\mathbb{F}G$ is a PIR if and only if a Sylow p-subgroup of G is cyclic.

Theorem

$\mathbb{F}G$ is code-checkable if and only if a Sylow p-subgroup of G is cyclic.

Given a finite abelian group G and a finite field $\mathbb{F}$ of characteristic p, we have the following results.

Proposition

$\mathbb{F}G$ is code-checkable if and only if it is a principal ideal ring (PIR).

Theorem (Fisher & Sehgal'76)

$\mathbb{F}G$ is a PIR if and only if a Sylow p-subgroup of G is cyclic.

Theorem

$\mathbb{F}G$ is code-checkable if and only if a Sylow p-subgroup of G is cyclic.

Given a finite abelian group G and a finite field $\mathbb{F}$ of characteristic p, we have the following results.

Proposition

$\mathbb{F}G$ is code-checkable if and only if it is a principal ideal ring (PIR).

Theorem (Fisher & Sehgal'76)

$\mathbb{F}G$ is a PIR if and only if a Sylow p-subgroup of G is cyclic.

Theorem

$\mathbb{F}G$ is code-checkable if and only if a Sylow p-subgroup of G is cyclic.

Dual of Checkable Codes

For $f(X) = f_0 + f_1 X + \cdots + X^t \in \mathbb{F}[X]$ with $f_0 \neq 0$, the **reciprocal polynomial** of $f(X)$ is defined to be $f^*(X) := f_0^{-1} X^t f(\frac{1}{X})$.

Proposition

Let $g(X)h(X) = X^n - 1$. Then $\langle g(X) \rangle^\perp = \langle h^*(X) \rangle = \langle h(X^{-1}) \rangle$.

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

Proposition

Let $\mathbb{F}Gu$ be checkable with a check element v. Then $(\mathbb{F}Gu)^\perp = \mathbb{F}Gv^{(-1)}$.

Corollary

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

Dual of Checkable Codes

For $f(X) = f_0 + f_1X + \cdots + X^t \in \mathbb{F}[X]$ with $f_0 \neq 0$, the **reciprocal polynomial** of $f(X)$ is defined to be $f^*(X) := f_0^{-1}X^t f(\frac{1}{X})$.

Proposition

Let $g(X)h(X) = X^n - 1$. Then $\langle g(X)\rangle^\perp = \langle h^*(X)\rangle = \langle h(X^{-1})\rangle$.

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

Proposition

Let $\mathbb{F}Gu$ be checkable with a check element v. Then $(\mathbb{F}Gu)^\perp = \mathbb{F}Gv^{(-1)}$.

Corollary

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

Dual of Checkable Codes

For $f(X) = f_0 + f_1X + \cdots + X^t \in \mathbb{F}[X]$ with $f_0 \neq 0$, the **reciprocal polynomial** of $f(X)$ is defined to be $f^*(X) := f_0^{-1}X^t f(\frac{1}{X})$.

Proposition

Let $g(X)h(X) = X^n - 1$. Then $\langle g(X)\rangle^{\perp} = \langle h^*(X)\rangle = \langle h(X^{-1})\rangle$.

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

Proposition

Let $\mathbb{F}Gu$ be checkable with a check element v. Then $(\mathbb{F}Gu)^{\perp} = \mathbb{F}Gv^{(-1)}$.

Corollary

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

Dual of Checkable Codes

For $f(X) = f_0 + f_1X + \cdots + X^t \in \mathbb{F}[X]$ with $f_0 \neq 0$, the **reciprocal polynomial** of $f(X)$ is defined to be $f^*(X) := f_0^{-1}X^t f(\frac{1}{X})$.

Proposition

Let $g(X)h(X) = X^n - 1$. Then $\langle g(X)\rangle^\perp = \langle h^*(X)\rangle = \langle h(X^{-1})\rangle$.

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

Proposition

Let $\mathbb{F}Gu$ be checkable with a check element v. Then $(\mathbb{F}Gu)^\perp = \mathbb{F}Gv^{(-1)}$.

Corollary

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

Reversible Cyclic Codes

A code $\mathcal{C}$ is **reversible** if $(c_n, c_{n-1}, \ldots, c_1) \in \mathcal{C}$ whenever $(c_1, c_2, \ldots, c_n) \in \mathcal{C}$.

Note that the reversibility of cyclic codes are corresponding to the fixed list of monomials $\{1, X, X^2, \ldots, X^{n-1}\}$.

$f(X)$ is said to be **self-reciprocal** if $f(X) = f^*(X)$.

Corollary (Massey'64)

The cyclic code generated by a monic polynomial $g(X)$ is reversible if and only if $g(X)$ is self-reciprocal.

Reversible Cyclic Codes

A code $\mathcal{C}$ is **reversible** if $(c_n, c_{n-1}, \dots, c_1) \in \mathcal{C}$ whenever $(c_1, c_2, \dots, c_n) \in \mathcal{C}$.

Note that the reversibility of cyclic codes are corresponding to the fixed list of monomials $\{1, X, X^2, \dots, X^{n-1}\}$.

$f(X)$ is said to be **self-reciprocal** if $f(X) = f^*(X)$.

Corollary (Massey'64)

The cyclic code generated by a monic polynomial $g(X)$ is reversible if and only if $g(X)$ is self-reciprocal.

Reversible Checkable Codes

Let $\mathcal{L} = \{g_1, g_2, \dots, g_n\}$ denote a fixed list of the elements in G.
For $w = \sum_{i=1}^{n} w_i g_i$, the reverse $\mathrm{r}_{\mathcal{L}}(w)$ of w is $\mathrm{r}_{\mathcal{L}}(w) := \sum_{i=1}^{n} w_{n+1-i} g_i$.
A code $\mathcal{C} \subseteq \mathbb{F}G$ 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

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

for some fixed $k \in G$, and for every $i = 1, 2, \dots, n$, then

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

Example

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

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

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 (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 $\mathbb{F}[X]/\langle X^n - 1 \rangle$.

Theorem

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

i) $\mathbb{F}Gu$ *is reversible with respect to* $\mathcal{L}$.

ii) $\mathbb{F}Gu = \mathbb{F}Gu^{(-1)}$.

iii) $u = au^{(-1)}$ *for some unit* a *in* $\mathbb{F}G$.

iv) $v = bv^{(-1)}$ *for some unit* b *in* $\mathbb{F}G$.

v) $\mathbb{F}Gv = \mathbb{F}Gv^{(-1)}$.

vi) $\mathbb{F}Gv$ *is reversible with respect to* $\mathcal{L}$.

Remark

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

Theorem

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

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

Remark

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

Theorem

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

i) $\mathbb{F}Gu$ *is reversible with respect to* $\mathcal{L}$.

ii) $\mathbb{F}Gu = \mathbb{F}Gu^{(-1)}$.

iii) $u = au^{(-1)}$ *for some unit* a *in* $\mathbb{F}G$.

iv) $v = bv^{(-1)}$ *for some unit* b *in* $\mathbb{F}G$.

v) $\mathbb{F}Gv = \mathbb{F}Gv^{(-1)}$.

vi) $\mathbb{F}Gv$ *is reversible with respect to* $\mathcal{L}$.

Corollary (Massey'64)

The cyclic code generated by a monic polynomial $g(X)$ is reversible if and only if $g(X)$ is self-reciprocal.

Theorem

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

i) $\mathbb{F}Gu$ *is reversible with respect to* $\mathcal{L}$.

ii) $\mathbb{F}Gu = \mathbb{F}Gu^{(-1)}$.

iii) $u = au^{(-1)}$ *for some unit* a *in* $\mathbb{F}G$.

iv) $v = bv^{(-1)}$ *for some unit* b *in* $\mathbb{F}G$.

v) $\mathbb{F}Gv = \mathbb{F}Gv^{(-1)}$.

vi) $\mathbb{F}Gv$ *is reversible with respect to* $\mathcal{L}$.

Corollary (Massey'64)

The cyclic code generated by a monic polynomial $g(X)$ *is reversible if and only if* $g(X)$ *is self-reciprocal.*

Complementary-Dual Checkable Codes

$\mathbb{F}Gu$ is **complementary dual** if $\mathbb{F}Gu \cap (\mathbb{F}Gu)^{\perp} = \{0\}$. Assume that $p \nmid n$. Then $\mathbb{F}G$ is code-checkable since the Sylow p-subgroup of G is trivial.

Theorem

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

i) $\mathbb{F}Gu$ *is a complementary dual code.*

ii) $\mathbb{F}Gu$ *is a reversible code with respect to* $\mathcal{L}$*.*

iii) $\mathbb{F}Gv$ *is a reversible code with respect to* $\mathcal{L}$*.*

iv) $\mathbb{F}Gv$ *is a complementary dual code.*

Corollary (Yang & Massey'94)

Then a cyclic code of length n over $\mathbb{F}$ is a complementary dual code if and only if it is reversible.

Complementary-Dual Checkable Codes

$\mathbb{F}Gu$ is **complementary dual** if $\mathbb{F}Gu \cap (\mathbb{F}Gu)^{\perp} = \{0\}$. Assume that $p \nmid n$. Then $\mathbb{F}G$ is code-checkable since the Sylow p-subgroup of G is trivial.

Theorem

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

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

Corollary (Yang & Massey'94)

Then a cyclic code of length n over $\mathbb{F}$ is a complementary dual code if and only if it is reversible.

Complementary-Dual Checkable Codes

$\mathbb{F}Gu$ is **complementary dual** if $\mathbb{F}Gu \cap (\mathbb{F}Gu)^{\perp} = \{0\}$. Assume that $p \nmid n$. Then $\mathbb{F}G$ is code-checkable since the Sylow p-subgroup of G is trivial.

Theorem

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

i) $\mathbb{F}Gu$ is a complementary dual code.

ii) $\mathbb{F}Gu$ is a reversible code with respect to $\mathcal{L}$.

iii) $\mathbb{F}Gv$ is a reversible code with respect to $\mathcal{L}$.

iv) $\mathbb{F}Gv$ is a complementary dual code.

Corollary (Yang & Massey'94)

Then a cyclic code of length n over $\mathbb{F}$ is a complementary dual code if and only if it is reversible.

Trivial MDS Checkable Codes

Lemma

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

Corollary

If a Sylow p-subgroup of G is cyclic, then there exist checkable $[n,1,n]$ and $[n,n-1,2]$ MDS codes from $\mathbb{F}G$.

Remark

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.
Moreover, if $p \nmid n$, then they are complementary dual.

Trivial MDS Checkable Codes

Lemma

Given a finite field $\mathbb{F}$ and a finite abelian group G, then the element $\sum\limits_{g\in G} g$ is always a zero-divisor in the group ring $\mathbb{F}G$.

Corollary

If a Sylow p-subgroup of G is cyclic, then there exist checkable $[n,1,n]$ and $[n,n-1,2]$ MDS codes from $\mathbb{F}G$.

Remark

Since $(\sum\limits_{g\in G} g)^{(-1)} = (\sum\limits_{g\in G} g)$, the $[n,1,n]$ MDS code generated by $\sum\limits_{g\in G} g$ and its dual are reversible.
Moreover, if $p \nmid n$, then they are complementary dual.

Trivial MDS Checkable Codes

Lemma

Given a finite field $\mathbb{F}$ and a finite abelian group G, then the element $\sum\limits_{g\in G} g$ is always a zero-divisor in the group ring $\mathbb{F}G$.

Corollary

If a Sylow p-subgroup of G is cyclic, then there exist checkable $[n,1,n]$ and $[n,n-1,2]$ MDS codes from $\mathbb{F}G$.

Remark

Since $(\sum\limits_{g\in G} g)^{(-1)} = (\sum\limits_{g\in G} g)$, the $[n,1,n]$ MDS code generated by $\sum\limits_{g\in G} g$ and its dual are reversible.
Moreover, if $p \nmid n$, then they are complementary dual.

Good Checkable Codes

1. Many Good Codes
2. 4 New Codes

The code $\mathcal{C}_{36}$ derived from $\mathbb{F}_5(C_6 \times C_6)$ is generated by

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

with check element

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

$\mathcal{C}_{36}$ is an optimal $[36, 28, 6]_5$ code.

Shortening $\mathcal{C}_{36}$ at the $1st$ position, we obtain an optimal $[35, 27, 6]_5$ code.

Shortening $\mathcal{C}_{36}$ at the $1st$ and $2nd$ positions, we obtain an optimal $[34, 26, 6]_5$ code

Good Checkable Codes

1. Many Good Codes
2. 4 New Codes

   The code $\mathcal{C}_{36}$ derived from $\mathbb{F}_5(C_6 \times C_6)$ is generated by

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

   with check element

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

   $\mathcal{C}_{36}$ is an optimal $[36, 28, 6]_5$ code.

   Shortening $\mathcal{C}_{36}$ at the $1st$ position, we obtain an optimal $[35, 27, 6]_5$ code.

   Shortening $\mathcal{C}_{36}$ at the $1st$ and $2nd$ positions, we obtain an optimal $[34, 26, 6]_5$ code

The code $\mathcal{C}_{72}$ derived from $\mathbb{F}_5(C_6 \times C_{12})$ is generated by

$$u_{72} = (312411232330313143111221222301122414030013401133430420133323011301020100),$$

with check element

$$v_{72} = (100000000441004102234010043124424101300211324012401114201004023203011413).$$

The $\mathcal{C}_{72}$ is an $[72, 62, 6]_5$ code.

Conclusion and Open Problems

Conclusion

1. a notion of checkable codes and code-checkable group rings.
2. necessary and sufficient conditions for a group ring $\mathbb{F}G$ to be code-checkable.
3. the dual of checkable codes.
4. reversible and complementary dual checkable codes.
5. many good codes and 4 new codes.

Open Problems

1. generalize other properties of cyclic codes to codes in $\mathbb{F}G$.
2. study self-orthogonal codes.
3. extend this concept to RG, where R is a finite commutative ring and G is a finite group.

Conclusion and Open Problems

Conclusion

1. a notion of checkable codes and code-checkable group rings.
2. necessary and sufficient conditions for a group ring $\mathbb{F}G$ to be code-checkable.
3. the dual of checkable codes.
4. reversible and complementary dual checkable codes.
5. many good codes and 4 new codes.

Open Problems

1. generalize other properties of cyclic codes to codes in $\mathbb{F}G$.
2. study self-orthogonal codes.
3. extend this concept to RG, where R is a finite commutative ring and G is a finite group.

Conclusion and Open Problems

Conclusion

1. a notion of checkable codes and code-checkable group rings.
2. necessary and sufficient conditions for a group ring $\mathbb{F}G$ to be code-checkable.
3. the dual of checkable codes.
4. reversible and complementary dual checkable codes.
5. many good codes and 4 new codes.

Open Problems

1. generalize other properties of cyclic codes to codes in $\mathbb{F}G$.
2. study self-orthogonal codes.
3. extend this concept to RG, where R is a finite commutative ring and G is a finite group.

Conclusion and Open Problems

Conclusion

1. a notion of checkable codes and code-checkable group rings.
2. necessary and sufficient conditions for a group ring $\mathbb{F}G$ to be code-checkable.
3. the dual of checkable codes.
4. reversible and complementary dual checkable codes.
5. many good codes and 4 new codes.

Open Problems

1. generalize other properties of cyclic codes to codes in $\mathbb{F}G$.
2. study self-orthogonal codes.
3. extend this concept to RG, where R is a finite commutative ring and G is a finite group.

Conclusion and Open Problems

Conclusion

1. a notion of checkable codes and code-checkable group rings.
2. necessary and sufficient conditions for a group ring $\mathbb{F}G$ to be code-checkable.
3. the dual of checkable codes.
4. reversible and complementary dual checkable codes.
5. many good codes and 4 new codes.

Open Problems

1. generalize other properties of cyclic codes to codes in $\mathbb{F}G$.
2. study self-orthogonal codes.
3. extend this concept to RG, where R is a finite commutative ring and G is a finite group.

Conclusion and Open Problems

Conclusion

1. a notion of checkable codes and code-checkable group rings.
2. necessary and sufficient conditions for a group ring $\mathbb{F}G$ to be code-checkable.
3. the dual of checkable codes.
4. reversible and complementary dual checkable codes.
5. many good codes and 4 new codes.

Open Problems

1. generalize other properties of cyclic codes to codes in $\mathbb{F}G$.
2. study self-orthogonal codes.
3. extend this concept to RG, where R is a finite commutative ring and G is a finite group.

Conclusion and Open Problems

Conclusion

1. a notion of checkable codes and code-checkable group rings.
2. necessary and sufficient conditions for a group ring $\mathbb{F}G$ to be code-checkable.
3. the dual of checkable codes.
4. reversible and complementary dual checkable codes.
5. many good codes and 4 new codes.

Open Problems

1. generalize other properties of cyclic codes to codes in $\mathbb{F}G$.
2. study self-orthogonal codes.
3. extend this concept to RG, where R is a finite commutative ring and G is a finite group.

Conclusion and Open Problems

Conclusion

1. a notion of checkable codes and code-checkable group rings.
2. necessary and sufficient conditions for a group ring $\mathbb{F}G$ to be code-checkable.
3. the dual of checkable codes.
4. reversible and complementary dual checkable codes.
5. many good codes and 4 new codes.

Open Problems

1. generalize other properties of cyclic codes to codes in $\mathbb{F}G$.
2. study self-orthogonal codes.
3. extend this concept to RG, where R is a finite commutative ring and G is a finite group.

Reference

S. Jitman, S. Ling, H. Liu, and X. Xie, "Checkable codes from group rings", available online : http://arxiv.org/pdf/1012.5498, 2010.

Thank You!