Galois LCD constacyclic codes over finite commutative chain rings

Samir Assuena

Centro Universiário da FEI

Joint work with André Pereira

samir.assuena@fei.edu.br

EnCoRI

www.fei.edu.br

Constacyclic codes

Let R be a finite commutative chain ring with p^m elements and $\mathcal{C}$ be a linear code over R and let λ a unit element of R. We say that $\mathcal{C}$ is λ-*constacyclic code* if

$$(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C} \Longrightarrow (\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in \mathcal{C}$$

for all $(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$.

Constacyclic codes

When $\lambda = 1$, we have so called *cyclic codes* and, when $\lambda = -1$, we have *negacyclic codes*. Thus, constacyclic codes are generalization of cyclic and negacyclic codes. Also, constacyclic code can be realized as ideals in polinomial factor ring $\dfrac{R[x]}{\langle x^n - \lambda \rangle}$.

Twisted group algebra

Let R be a commutative ring and G be a group. The *twisted group ring $R^\gamma G$ of G over R* is the associative R-algebra with basis $\overline{G} = \{\overline{g},\, g \in G\}$, which is a copy of G, and the multiplication is defined on the basis as

$$\overline{g} \cdot \overline{h} = \gamma(g,h)\overline{gh}$$

where $\gamma(g,h)$ is an element of $\mathcal{U}(R)$, the group of units of R.

Twisted group algebra

The mapping $\gamma : G \times G \longrightarrow \mathcal{U}(R)$ is called *twisting* and there are many different possibilities for $R^{\gamma}G$ depending on the choice of the twisting. For instance, the group ring RG of G over R is a twisted group ring with $\gamma(g, h) = 1$. Furthermore, the associative condition on the multiplication implies that

$$\gamma(g, h)\gamma(gh, k) = \gamma(h, k)\gamma(g, hk)$$

and, for this reason, γ is a 2-cocycle.

Twisted group algebra

It is possible make a *diagonal* change of basis by replacing each $\overline{g}$ by $\widetilde{g} = \delta(g)\overline{g}$ for some $\delta(g) \in \mathcal{U}(R)$ and, with this change of basis, $R^{\gamma}G$ is realized in a second way as a twisted group ring of G over R with twisting

$$\widetilde{\gamma}(g,h) = \delta(g)\delta(h)\delta(gh)^{-1}\gamma(g,h).$$

In this case, we say that γ and $\widetilde{\gamma}$ are *cohomologous*.

Constacyclic codes as ideals in twisted group algebras

Theorem

Let R be a finite field , $C_n = \langle g \mid g^n = 1 \rangle$ a cyclic group of order n and $\mathcal{C}$ be a linear code over R^n. Consider the linear mapping $\varphi : R^n \longrightarrow R^\gamma C_n$ given by $\varphi(c_0, c_1, \cdots, c_{n-1}) = c_0\overline{1} + c_1\overline{g} + \cdots + c_{n-1}\overline{g^{n-1}}$. Then, $\mathcal{C}$ is a λ-constacyclic code if and only if $\varphi(\mathcal{C})$ is an ideal of $\mathbb{F}_q^\gamma C_n$ where

$$\gamma_\lambda(g^j, g^k) = \begin{cases} \lambda, & \text{if } j + k \geq n \\ 1, & \text{if } j + k < n. \end{cases}$$

Twisted group algebras of cyclic groups

Let $C_n = \langle g \mid g^n = 1 \rangle$ be a cyclic group of order n, $\mathbb{F}$ be a field and $R^\gamma C_n$ the twisted group algebra with

$$\gamma_\lambda(g^j, g^k) = \begin{cases} \lambda, & \text{if } j + k \geq n \\ 1, & \text{if } j + k < n \end{cases}$$

where λ is a unit element of R. Thus, $\overline{g}^2 = \overline{g} \cdot \overline{g} = \gamma(g, g)\overline{g^2}$, so we can make a diagonal change of basis and replace $\overline{g^k}$ by $\overline{g}^k$, for all k, $1 \leq k \leq n$. Thus, there exists a non-zero element $a \in \mathbb{F}$ such that $\overline{g}^n = a \cdot 1$ which implies that $R^\gamma C_n$ is a commutative ring.

Galois form

Let R be a finite commutative ring with p^m elements, G be a finite group and $R^\gamma G$ the twisted group ring of G over R. Given $\alpha = \sum_{g \in G} \alpha_g \overline{g}$, $\beta = \sum_{g \in G} \beta_g \overline{g}$ two elements of $R^\gamma G$, for each k, $0 \leq k < m$, we define the *k-Galois form* on $R^\gamma G$ as

$$[\alpha, \beta]_k = \sum_{g \in G} \alpha_g \beta_g^{p^k}.$$

Galois form

It is not difficult to see that k-Galois form is just the Euclidean inner product if $k = 0$. Thus, given a twisted group code $\mathcal{C}$, we can define the *k-Galois dual code of $\mathcal{C}$* as

$$\mathcal{C}^{\perp_k} = \{\beta \in R^\gamma G \mid [\alpha, \beta]_k = 0, \forall\, \alpha \in \mathcal{C}\}.$$

k-Galois dual code

Proposition

Let R be a finite commutative ring with p^m elements, $C_n = \langle g,\, g^n = 1\rangle$ be a cyclic group of order n and $R^{\gamma_\lambda}C_n$ the twisted group algebra of C_n over R where

$$\gamma_\lambda(g^j, g^k) = \begin{cases} \lambda, & \text{if } j+k \geq n \\ 1, & \text{if } j+k < n. \end{cases}$$

Then, if $\mathcal{C}$ is a λ-constacyclic code, its k-Galois dual $\mathcal{C}^{\perp_k}$ is a $\lambda^{-p^{m-k}}$-constacyclic code.

k-Galois LCD codes

Definition

Let $\mathcal{C}$ be a constacyclic code over a finite commutative ring R. We say that $\mathcal{C}$ is a linear complementary k-Galois dual code (k-Galois LCD code for shorty) if $\mathcal{C} \cap \mathcal{C}^{\perp_k} = \{0\}$.

k-Galois LCD codes

Definition

Let $\mathcal{C}$ be a constacyclic code over a finite commutative ring R. We say that $\mathcal{C}$ is a linear complementary k-Galois dual code (k-Galois LCD code for shorty) if $\mathcal{C} \cap \mathcal{C}^{\perp_k} = \{0\}$.

Proposition

If $\lambda^{1+p^{m-k}} \neq 1$, then any λ-constacyclic code $\mathcal{C}$ over R is a k-Galois LCD code.

centro universitário FEI

www.fei.edu.br

The classical involution

Definition

Let R be a commutative ring with identity and let G be a group.

The mapping $^* : R^\gamma G \longrightarrow R^\gamma G$ given by $\left(\sum_{g\in G} \alpha_g \overline{g}\right)^* = \sum_{g\in G} \alpha_g \overline{g}^{-1}$ is called the classical involution of $R^\gamma G$.

k-Galois LCD codes

Lemma

Let R be a finite commutative with p^m elements, $C_n = \langle g,\, g^n = 1\rangle$ be a cyclic group of order n and $\mathbb{F}_q^{\gamma_\lambda} C_n$ the twisted group algebra of C_n over R where Given two arbitrary elements $\alpha = \sum_{i=0}^{n-1} \alpha_i \overline{g}^i$ and $\beta = \sum_{i=0}^{n-1} \beta_i \overline{g}^i$ of $R^{\gamma_\lambda} C_n$, let us denote by $\beta^{(p^k)}$ the element $\sum_{i=0}^{n-1} \beta_i^{p^k} \overline{g}^i$. If $\alpha \left(\beta^{(p^k)}\right)^* = 0$, then $[\alpha, \beta]_k = 0$.

Euclidean Constacyclic LCD codes

Proposition

Let R be a finite commutative ring, $C_n = \langle g,\, g^n = 1\rangle$ be a cyclic group of order n and $R^{\gamma_\lambda}C_n$ the twisted group algebra of C_n over R where

$$\gamma_\lambda(g^j, g^k) = \begin{cases} \lambda, & \text{if } j+k \geq n \\ 1, & \text{if } j+k < n. \end{cases}$$

for some unit $\lambda \in R$. If $\lambda^2 = 1$, then $\mathcal{C}$ is a λ-constacyclic LCD code if, and only if, $\mathcal{C}$ is generated by an idempontent e such that $e = e^*$.

k-Galois constacyclic LCD code

Proposition

Let R be a finite commutative ring with p^m elements,

$C_n = \langle g,\, g^n = 1\rangle$ be a cyclic group of order n and $R^{\gamma_\lambda}C_n$ the

twisted group algebra of C_n over R where

$$\gamma_\lambda(g^j, g^k) = \begin{cases} \lambda, & \text{if } j+k \geq n \\ 1, & \text{if } j+k < n. \end{cases}$$

If $\lambda^2 = 1$, $\mathcal{C}$ is a λ-constacyclic code generated by an idempontent

e such that $e = e(e^{(p^k)})^*$ if and only if $\mathcal{C}$ is k-Galois LCD code.

An example

- $R = \mathbb{Z}_8$

An example

- $R = \mathbb{Z}_8$
- C_3

www.fei.edu.br

An example

- $R = \mathbb{Z}_8$
- C_3
- $\lambda = 3$

www.fei.edu.br

An example

- $R = \mathbb{Z}_8$
- C_3
- $\lambda = 3$
- $e = 3\overline{g}^2 + \overline{g} + 3$

An example

- $R = \mathbb{Z}_8$
- C_3
- $\lambda = 3$
- $e = 3\overline{g}^2 + \overline{g} + 3$
- $\mathcal{C} = (\mathbb{Z}_8 C_3)\, e$

An example

- $R = \mathbb{Z}_8$
- C_3
- $\lambda = 3$
- $e = 3\overline{g}^2 + \overline{g} + 3$
- $\mathcal{C} = (\mathbb{Z}_8 C_3)\, e$
- $\dim\mathcal{C} = 1$

An example

- $R = \mathbb{Z}_8$
- C_3
- $\lambda = 3$
- $e = 3\overline{g}^2 + \overline{g} + 3$
- $\mathcal{C} = (\mathbb{Z}_8 C_3)\, e$
- $\dim\mathcal{C} = 1$
- $w(\mathcal{C}) = 3$

centro universitário FEI

www.fei.edu.br

An example

- $R = \mathbb{Z}_8$
- C_3
- $\lambda = 3$
- $e = 3\overline{g}^2 + \overline{g} + 3$
- $\mathcal{C} = (\mathbb{Z}_8 C_3)\, e$
- $\dim \mathcal{C} = 1$
- $w(\mathcal{C}) = 3$
- $\mathcal{C}$ LCD MDS code.

Than^k you for your attention!!!!!

www.fei.edu.br