Códigos metacíclicos

Samir Assuena

Tese apresentada
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para
obtenção do título
de
Doutor em Ciências

Programa: Matemática

Orientador: Prof. Dr. Francisco César Polcino Milies

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro do CNPq

São Paulo, outubro de 2013

Códigos metacíclicos

Este exemplar corresponde à redação
final da tese devidamente corrigida
e defendida por Samir Assuena
e aprovada pela Comissão Julgadora.

Banca Examinadora:

- Prof. Dr. Francisco César Polcino Milies (orientador) IME-USP
- Prof. Dr. Raul Antonio Ferraz IME-USP
- Prof^a. Dr^a. Ana Cristina Vieira UFMG
- Prof. Dr. Thierry Petit Lobão UFBA
- Prof. Dr. Antonio Paques UFRGS

Agradecimentos

Agradeço a Deus por ter me dado força para vencer mais este desafio da minha vida mas também por ter me dado os maiores presentes da minha vida meus filhos Mateus e Larissa.

Agradeço minha esposa Elis por todo amor, carinho, compreensão e apoio ao longo de todos esses anos.

Agradeço aos meus pais, João Alberto e Virgínia, por tudo que fizeram por mim e pelos meus irmãos.

Agradeço aos meus irmãos, Jorge e Vinícius e suas respectivas esposas, pela confiança e apoio.

Agradeço a toda minha família tios, tias, primos e primas.

Agradeço ao meu sogro, Eliseu, à minha sogra, Dona Telma.

Agradeço aos meus cunhados Edilson e Edmilson e suas esposas Monise e Fabiana.

Agradeço a UFSCar pela minha formação, ao Prof. Daniel Vendrscolo e aos amigos das turmas de 2000 e 2001.

Agradeço ao Instituto de Matemática e Estatística da USP, principalmente ao Prof. César Polcino Milies pela orientação e pela pessoa extraordinária que é.

Agradeço ao Instituto Mauá de Tecnologia e aos professores Thiago, Anderson, Samira, Marilda, Marim, Ivanildo, Jones, Muller, Paulo, Ana, Airton e Ivete.

Agradeço aos eternos amigos: Betão, Zuaneti, Bigode, Lê, Tica, Ricardo, Felippe e suas respectivas esposas e ainda a todos os outros amigos da CEC.!!!!

Resumo

Neste trabalho, consideramos álgebras de grupo semi-simples $\mathbb{F}_q G$ de grupos metacíclicos não abelianos que cindem sobre corpos finitos. Inicialmente, damos condições para que o número de componentes simples da álgebra $\mathbb{F}_q G$ seja minimal e encontramos os idempotentes centrais primitivos quando a ordem do grupo é igual a $p^m \ell^n$, onde p e ℓ são números primos distintos. Posteriomente, obtemos condições necessárias e suficientes para que o número de componentes simples da álgebra $\mathbb{F}_q G$ seja minimal no caso em que a ordem do grupo é igual a $2n$. Finalmente, quando $G = D_{p^m}$, o grupo diedral de ordem $2p^m$, obtemos duas decomposições da álgebra $\mathbb{F}_q D_{p^m}$ como soma direta de ideais à esquerda minimais, calculamos suas dimensões e pesos e mostramos que, em uma destas decomposições, os códigos à esquerda minimais não são equivalentes a códigos abelianos, dando uma resposta afirmativa para uma conjectura formulada por Sabin e Lomonaco em 1995.

Palavras-chave: Códigos Metacíclicos, Idempotentes Primitivos, Grupos Metacíclicos não Abelianos.

Abstract

We consider semisimple group algebras $\mathbb{F}_q G$ of non abelian split metacyclic groups over a finite field. First we give necessary and suficiente conditions for them to have a minimal number of simple components and find the primitive central idempotents of $\mathbb{F}_q G$ in the case when the order G is equals $p^m \ell^n$, where p and ℓ are different prime numbers. Then, we consider the special case when the order of G is $2n$. Finally, when $G = D_{p^m}$ the dihedral group of order $2p^m$, we obtain two decomposition of the algebra into direct sum of minimal left ideals, compute their dimensions and weights. We show that one of these decompositions gives raise to minimal codes that are not combinatorially equivalent to abelian codes giving an affirmative answer to a conjecture formulated by Sabin and Lomonaco in 1995.

Keywords: Metacyclic Codes, Primitive Idempotens, Non Abelian Metacyclic Groups.

Sumário

Introdução

A Teoria dos Códigos Corretores de Erros teve início com o trabalho de Richard Hamming intitulado *Error Detecting and Error Correcting Codes*. Desde então, esta teoria vem sendo aplicada em várias áreas de outras ciências (tais como Engenharia Elétrica, Computação, etc), em telefonia, em DVD, entre outras.

Basicamente, o objetivo da Teoria de Códigos Corretores de Erros é transmitir mensagens através de um canal de uma maneira segura, de tal forma que o código seja capaz de detectar e corrigir o maior número possível de erros que possam ocorrer durante tal transmissão.

Para tanto, tomamos um conjunto finito $\mathcal{A}$ com q elementos o qual chamamos de **alfabeto**. Uma palavra de comprimento n em $\mathcal{A}$ é uma n-upla $(v_0, v_1, \cdots, v_{n-1})$. Um **código de comprimento n** sobre $\mathcal{A}$ é um subconjunto próprio $\mathcal{C}$ do produto cartesiano $\mathcal{A}^n$, para algum $n \geq 1$.

Dados $x = (x_0, x_1, \cdots, x_{n-1})$ e $y = (y_0, y_1, \cdots, y_{n-1})$ duas palavras de $\mathcal{A}^n$, definimos a *distância de Hamming* entre x e y como

$$d(x, y) = |\{i,\ x_i \neq y_i,\ 0 \leq i \leq n-1\}|.$$

Sendo assim, definimos a distância mínima de um código $\mathcal{C}$ como

$$d(\mathcal{C}) = min\ \{d(x, y) \mid x, y \in \mathcal{C},\ x \neq y\}.$$

Se tomarmos $\mathcal{A}$ como sendo $\mathbb{F}_q$, o corpo finito com q elementos, então $\mathbb{F}_q^n$ é um $\mathbb{F}_q$-espaço vetorial. Os $\mathbb{F}_q$-subespaços de $\mathbb{F}_q^n$ são chamados *códigos lineares*. Dentre os códigos lineares, existe uma classe muito importante de códigos chamados *códigos cíclicos*. Mais explicitamente, um código linear diz-se *cíclico* se

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

Sejam $C_n = \langle g,\ g^n = 1 \rangle$ o grupo cíclico de ordem n e $\mathbb{F}_q C_n$ a álgebra do grupo C_n sobre $\mathbb{F}_q$. Prova-se que a imagem de um código cíclico através da função

$$\psi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q C_n$$

$$(x_0, \cdots, x_{n-1}) \longmapsto \textstyle\sum_{i=0}^{n-1} x_i g^i$$

é um ideal de $\mathbb{F}_q C_n$. Sendo assim, define-se um *código de grupo* como um ideal da álgebra $\mathbb{F}_q G$ com G um grupo finito.

Um grupo G diz-se **metacíclico** se G contém um subgrupo normal H cíclico tal que o grupo G/H também é cíclico. Pode-se provar que G, sendo metacíclico finito, possui a seguinte apresentação

$$G = \langle a, b \mid a^m = 1, b^n = a^s, bab^{-1} = a^i \rangle$$

onde a e b são tais que $H = \langle a \rangle$ e $G/H = \langle bH \rangle$. Quando $s = m$, dizemos que G é um grupo *metacíclico que cinde* e, neste caso, G é o produto semi-direto $G = \langle a \rangle \rtimes \langle b \rangle$.

O estudo dos códigos metacíclicos desenvolveu-se através dos seguintes trabalhos

- R. E. Sabin, *On Row-Cyclic Codes with Algebraic Structure* , Designs, Codes and Cryptography, 4, 145-155 (1994)
- R. E. Sabin, S. J. Lomonaco, *Metacyclic Error-Correcting Codes*, AAECC 6 (1995) 191-210.
- F. S. Dutra, R. A. Ferraz, C. Polcino Milies, *Semisimple group codes and dihedral codes*, Algebra and Disc. Math., 3 (2009) 28-4.

No artigo *Metacyclic Error-Correcting Codes*, Sabin e Lomonaco introduziram a noção de *equivalência combinatorial* que é uma bijeção entre álgebras de grupos obtida pela extensão linear de uma bijeção entre dois grupos finitos de mesma ordem. Mais detalhadamente, sejam G e $\mathcal{G}$ dois grupos finitos de mesma ordem e $\mathbb{F}$ um corpo, sejam $\mathbb{F}G$ e $\mathbb{F}\mathcal{G}$ suas correspondentes álgebras de grupo, uma **equivalência combinatorial** é um isomorfismo de espaços vetoriais $\phi : \mathbb{F}G \longrightarrow \mathbb{F}\mathcal{G}$ induzido por uma bijeção $\phi : G \longrightarrow \mathcal{G}$. Os códigos $\mathcal{C} \subset \mathbb{F}G$ e $\widehat{\mathcal{C}} \subset \mathbb{F}\mathcal{G}$ são **combinatorialmente equivalentes** se existe uma equivalência combinatorial $\phi : \mathbb{F}G \longrightarrow \mathbb{F}\mathcal{G}$ tal que $\phi(\mathcal{C}) = \widehat{\mathcal{C}}$.

No caso em que G é um grupo metacíclico, tal que $mdc(q, |G|) = 1$, a álgebra de grupo $\mathbb{F}_qG$ é semissimples, Sabin e Lomonaco, usando Teoria de Representações de Grupos, mostraram que códigos em $\mathbb{F}_qG$, gerados por idempotentes centrais são combinatorialmente equivalentes a códigos abelianos. Isso motivou a procura de códigos minimais à esquerda da álgebra $\mathbb{F}_qG$.

No capítulo 1, apresentamos as noções preliminares que serão utilizadas ao longo deste trabalho.

No capítulo 2, consideramos álgebras de grupos metacíclicos **não abelianos** que cindem sobre corpos finitos e encontramos uma condição necessária para que a álgebra $\mathbb{F}_qG$ tenha número mínimo de componentes simples. Isto acontece quando as álgebras $\mathbb{F}_qG$ e $\mathbb{Q}G$ têm o mesmo número de componentes simples. Finalizamos este capítulo obtendo os idempotentes centrais primitivos da álgebra $\mathbb{F}_qG$, no caso em que $|G| = p^m\ell^n$, sendo p e ℓ números primos.

No capítulo 3, apresentamos uma extensão do [4, Teorema 3.3] feito para grupos diedrais.

No capítulo 4, conhecendo os idempotentes centrais primitivos da álgebra $\mathbb{F}_qD_{p^m}$, onde D_{p^m} é o grupo diedral de ordem p^m, obtivemos duas decomposições da álgebra $\mathbb{F}_qD_{p^m}$ como soma direta de ideais à esquerda minimais, sendo que, em uma destas decomposições, tais ideais minimais são combinatorialmente equivalentes a códigos abelianos mas na outra decomposições, tais ideais minimais **não** são combinatorialmente equivalentes a códigos abelianos.

Capítulo 1

Preliminares

1.1 Grupos Metacíclicos

Definição 1.1.1. *Um grupo G diz-se* ***metacíclico*** *se G contém um subgrupo normal H cíclico tal que o grupo G/H também é cíclico.*

Exemplos de grupos metacíclicos são os grupo diedrais e os grupos cujos subgrupos de Sylow são cíclicos ([18, Teorema 10.1.10]).

Seja G um grupo metacíclico finito, escrevendo $H = \langle a \rangle$, seu subgrupo normal de ordem m, e $G/H = \langle bH \rangle$, podemos provar que G possui a seguinte apresentação

$$G = \langle a, b \mid a^m = 1, b^n = a^s, bab^{-1} = a^i \rangle$$

onde n é $|G/H|$. Além disto, os inteiros n, m, s, i se relacionam da seguinte maneira

$$s \mid m, \quad m \mid s(i-1) \quad , \quad i < m, \quad \text{mdc}(i, m) = 1.$$

Quando $s = m$, dizemos que G é um grupo *metacíclico que cinde* e, neste caso, G é o produto semi-direto $G = \langle a \rangle \rtimes \langle b \rangle$.

Teorema 1.1.2. [2, Teorema 47.10] *Seja G um grupo metacíclico com apresentação acima. Seu subgrupo comutador G' é cíclico, gerado por a^{i-1}. Consequentemente, $|G'| = m/mdc(m, i-1)$.*