Finite Fields and Their Applications 38 (2016) 93–115

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Concatenated structure of left dihedral codes

Yonglin Cao [a,*], Yuan Cao [b], Fang-Wei Fu [c]

[a] School of Sciences, Shandong University of Technology, Zibo, Shandong 255091, China
[b] College of Mathematics and Econometrics, Hunan University, Changsha 410082, China
[c] Chern Institute of Mathematics and LPMC, Nankai University, Tianjin 300071, China

A R T I C L E I N F O

Article history:
Received 6 March 2015
Received in revised form 26 November 2015
Accepted 3 January 2016
Available online 11 January 2016
Communicated by W. Cary Huffman

MSC:
94B05
94B15
11T71

Keywords:
Left dihedral code
Skew cyclic code
Concatenated structure
Cyclic code
Dual code
Self-dual code

A B S T R A C T

Let D_{2n} be the dihedral group of order n. Left ideals of the group algebra $\mathbb{F}_q D_{2n}$ are known as left dihedral codes over $\mathbb{F}_q$ of length $2n$, and abbreviated as left D_{2n}-codes. In this paper, a system theory for left D_{2n}-codes is developed only using finite field theory and basic theory of cyclic codes and skew cyclic codes. First, we prove that any left D_{2n}-code is a direct sum of concatenated codes with inner codes $\mathcal{A}_i$ and outer codes C_i, where $\mathcal{A}_i$ is a minimal self-reciprocal cyclic code over $\mathbb{F}_q$ of length n and C_i is a skew cyclic code of length 2 over an extension field or principal ideal ring of $\mathbb{F}_q$. Then for the case of $\gcd(n, q) = 1$, we give a precise description for outer codes in the concatenated codes, provide the dual code for any left D_{2n}-code and determine all self-dual left D_{2n}-codes. Moreover, all 1995 binary left dihedral codes and all 255 binary self-dual left dihedral codes of length 30 are given, and a class of left D_{2p^n}-codes over $\mathbb{F}_q$ is investigated.

* Corresponding author. Fax: +86 0533 2782308.
E-mail addresses: ylcao@sdut.edu.cn (Y. Cao), yuan_cao@hnu.edu.cn (Y. Cao), fwfu@nankai.edu.cn (F.-W. Fu).

http://dx.doi.org/10.1016/j.ffa.2016.01.001
1071-5797/

1. Introduction

Let $\mathbb{F}_q$ be a finite field of cardinality q and $D_{2n} = \langle x, y \mid x^n = 1, y^2 = 1, yxy = x^{-1}\rangle$ the dihedral group of order n. The group algebra $\mathbb{F}_q D_{2n}$ is a vector space over $\mathbb{F}_q$ with basis D_{2n}. In addition, multiplication with scalars $c \in \mathbb{F}_q$ and multiplication are defined by: for any $a_g, b_g \in \mathbb{F}_q$ where $g \in D_{2n}$,

$$\sum_{g\in D_{2n}} a_g g + \sum_{g\in D_{2n}} b_g g = \sum_{g\in D_{2n}} (a_g + b_g)g, \; c(\sum_{g\in D_{2n}} a_g g) = \sum_{g\in D_{2n}} c a_g g,$$
$$(\sum_{g\in D_{2n}} a_g g)(\sum_{g\in D_{2n}} b_g g) = \sum_{g\in D_{2n}} (\sum_{uv=g} a_u b_v) g.$$

Then $\mathbb{F}_q D_{2n}$ is an associative and noncommutative $\mathbb{F}_q$-algebra with identity $1 = 1_{\mathbb{F}_q} 1_{D_{2n}}$ where $1_{\mathbb{F}_q}$ and $1_{D_{2n}}$ are the identity elements of $\mathbb{F}_q$ and D_{2n} respectively. Readers are referred to [12] for more details on group algebra.

For any $\mathbf{a} = (a_{0,0}, a_{1,0}, \ldots, a_{n-1,0}, a_{0,1}, a_{1,1}, \ldots, a_{n-1,1}) \in \mathbb{F}_q^{2n}$, we define

$$\Psi(\mathbf{a}) = (1, x, \ldots, x^{n-1}) M_{\mathbf{a}} \begin{pmatrix} 1 \\ y \end{pmatrix}, \text{ where } M_{\mathbf{a}} = \begin{pmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \\ \ldots & \ldots \\ a_{n-1,0} & a_{n-1,1} \end{pmatrix}.$$

Then Ψ is an $\mathbb{F}_q$-linear isomorphism from $\mathbb{F}_q^{2n}$ onto $\mathbb{F}_q D_{2n}$. As in [8], a nonempty subset C of $\mathbb{F}_q^{2n}$ is called a *left dihedral code* (or *left D_{2n}-code* more precisely) over $\mathbb{F}_q$ if $\Psi(C)$ is a left ideal of the $\mathbb{F}_q$-algebra $\mathbb{F}_q D_{2n}$. As usual, we will identify C with $\Psi(C)$ in this paper.

Dutra et al. [7] investigated codes that are given as two-sided ideals in a semisimple finite group algebra $\mathbb{F}_q G$ defined by idempotents constructed from subgroups of a finite group G, and gave a criterion to decide when these ideals are all the minimal two-sided ideals of $\mathbb{F}_q G$ in the case when G is a dihedral group. McLoughlin [11] provided a new construction of the self-dual, doubly-even and extremal $[48, 24, 12]$ binary linear block code using a zero divisor in the group ring $\mathbb{F}_2 D_{48}$.

Recently, Brochero Martínez [6] showed explicitly all central irreducible idempotents and their Wedderburn decomposition of the dihedral group algebra $\mathbb{F}_q D_{2n}$, in the case when every divisor of n divides $q - 1$. This characterization depends to the relation of the irreducible idempotents of the cyclic group algebra $\mathbb{F}_q C_n$ and the central irreducible idempotents of the group algebras $\mathbb{F}_q D_{2n}$. Gabriela and Inneke [8] provided algorithms to construct minimal left group codes. These are based on results describing a complete set of orthogonal primitive idempotents in each Wedderburn component of a semisimple finite group algebra $\mathbb{F}_q G$ for a large class of groups G.

More importantly, Bazzi and Mitter [1] showed that for infinitely many block lengths a random left ideal in the binary group algebra of the dihedral group is an asymptotically