Discrete Mathematics 313 (2013) 983–991

Contents lists available at SciVerse ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Structure of repeated-root constacyclic codes of length $3p^s$ and their duals

Hai Q. Dinh

Department of Mathematical Sciences, Kent State University, 4314 Mahoning Avenue, Warren, OH 44483, USA

ARTICLE INFO

Article history:
Received 18 October 2012
Received in revised form 22 January 2013
Accepted 28 January 2013
Available online 24 February 2013

Keywords:
Cyclic codes
Constacyclic codes
Dual codes
Repeated-root codes

ABSTRACT

Let $p \neq 3$ be any prime. A classification of constacyclic codes of length $3p^s$ over the finite field $\mathbb{F}_{p^m}$ is provided. Based on this, the structures in terms of polynomial generators of all such constacyclic codes and their duals are established. Among other results, we show that self-dual cyclic codes of length $3p^s$ exist only when $p = 2$, and in such case, those self-dual codes are listed.

1. Introduction

The classes of cyclic codes in particular, and constacyclic codes in general, play a very significant role in the theory of error-correcting codes. Constacyclic codes can be efficiently encoded using shift registers, which explains their preferred role in engineering. Given a nonzero element λ of the finite field F, λ-constacyclic codes of length n are classified as ideals as the ideals $\langle f(x)\rangle$ of the quotient ring $\frac{F[x]}{\langle x^n-\lambda\rangle}$, where $f(x)$ is a divisor of $x^n - \lambda$. However, classically, most of the research was concentrated on the situation when the code length n is relatively prime to the characteristic of the field F. The case when the code length n is divisible by the characteristic p of the field yields the so-called repeated-root codes, which were first studied since 1967 by Berman [1], and then in the 1970s and 1980s by several authors such as Massey et al. [8], Falkner et al. [5], and Roth and Seroussi [9]. Repeated-root codes were first investigated in the most generality in the 1990s by Castagnoli et al. [2], and van Lint [10], where they showed that repeated-root cyclic codes have a concatenated construction, and are asymptotically bad. Nevertheless, such codes are optimal in a few cases, that motivates researchers to further study this class of codes.

We recently provided the algebraic structure in terms of polynomial generators of all repeated-root constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ [4]. In particular, all self-dual negacyclic codes of length $2p^s$, where $p^m \equiv 1 \pmod 4$ were obtained. It is also shown the non-existence of self-dual negacyclic codes of length $2p^s$, where $p^m \equiv 3 \pmod 4$, and self-dual cyclic codes of length $2p^s$, for any odd prime p. This paper, on the one hand, continues that line of research to investigate repeated-root constacyclic codes of length $3p^s$. On the other hand, we also establish the structure of the duals of all such constacyclic codes, which is a task that was obtained in [4] only for the special cases of cyclic and negacyclic codes.

Hereafter, p is a prime, and $p \neq 3$.[1] The purpose of this paper is to give the algebraic structure in terms of polynomial generators of all repeated-root constacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m}$ and their dual codes. We start in Section 2 by recalling some preliminary concepts about constacyclic codes of any length in general. In Section 3, we classify all such

E-mail address: hdinh@kent.edu.

[1] When $p = 3$, constacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m}$ are just a special case of the situation of constacyclic codes of length a power of p over $\mathbb{F}_{p^m}$, which was covered in our recent paper [3, Section 3].

0012-365X/$ – see front matter
doi:10.1016/j.disc.2013.01.024

constacyclic codes. It will be shown that if $p^m \equiv 2 \pmod 3$ then all λ-constacyclic codes are equivalent to cyclic codes via a ring isomorphism. In the case $p^m \equiv 1 \pmod 3$, λ-constacyclic codes are divided into three distinct classes (constacyclic codes in each of these classes are equivalent via a constructed ring isomorphism). We then give the structure of constacyclic codes in each class in Sections 4 and 5. The structure of all λ-constacyclic codes are summarized in Table 1 in Section 6. Finally, Section 7 provides structure of the duals of all such constacyclic codes.

2. Constacyclic codes and their duals

Let F be a finite field. Given an n-tuple $(x_0, x_1, \ldots, x_{n-1}) \in F^n$, the *cyclic shift* τ and *negashift* ν on F^n are defined as usual, i.e.,

$$\tau(x_0, x_1, \ldots, x_{n-1}) = (x_{n-1}, x_0, x_1, \ldots, x_{n-2}),$$

and

$$\nu(x_0, x_1, \ldots, x_{n-1}) = (-x_{n-1}, x_0, x_1, \ldots, x_{n-2}).$$

A code C is called *cyclic* if $\tau(C) = C$, and C is called *negacyclic* if $\nu(C) = C$. More generally, if λ is a nonzero element of F, then the λ-*constacyclic* (λ-twisted) *shift* τ_λ on F^n is the shift

$$\tau_\lambda(x_0, x_1, \ldots, x_{n-1}) = (\lambda x_{n-1}, x_0, x_1, \ldots, x_{n-2}),$$

and a code C is said to be λ-*constacyclic* if $\tau_\lambda(C) = C$, i.e., if C is closed under the λ-constacyclic shift τ_λ. Equivalently, C is a λ-constacyclic code if and only if

$$CS_\lambda \subseteq C,$$

where S_λ is the λ-constacyclic shift matrix given by

$$S_\lambda = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ \lambda & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \\ \lambda & 0 & \cdots & 0 \end{pmatrix} \subseteq F_{n\times n}.$$

In light of this definition, when $\lambda = 1$, λ-constacyclic codes are cyclic codes, and when $\lambda = -1$, λ-constacyclic codes are just negacyclic codes.

Each codeword $c = (c_0, c_1, \ldots, c_{n-1})$ is customarily identified with its polynomial representation $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$, and the code C is in turn identified with the set of all polynomial representations of its codewords. Then in the ring $\frac{F[x]}{\langle x^n-\lambda\rangle}$, the representative of $xc(x)$ corresponds to a λ-constacyclic shift of $c(x)$. From that, the following fact is well known and straightforward (cf. [6,7]).

Proposition 2.1. *A linear code C of length n is λ-constacyclic over F if and only if C is an ideal of $\frac{F[x]}{\langle x^n-\lambda\rangle}$. Moreover, $\frac{F[x]}{\langle x^n-\lambda\rangle}$ is a principal ideal ring, whose ideals are generated by factors of $x^n - \lambda$.*

The dual of a cyclic code is a cyclic code, and the dual of a negacyclic code is a negacyclic code. In general, we have the following implication of the dual of a λ-constacyclic code.

Proposition 2.2 (*Cf. [3, Proposition 2.4]*)**.** *The dual of a λ-constacyclic code is a λ^{-1}-constacyclic code.*

The following fact gives a necessary and sufficient condition for a product of polynomials to be zero over a field.

Proposition 2.3 (*Cf. [4, Proposition 2.3]*)**.** *Let λ be a nonzero element of F and*

$$a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}, \qquad b(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} \in F[x].$$

Then $a(x)b(x) = 0$ in $\frac{F[x]}{\langle x^n-\lambda\rangle}$ if and only if $(a_0, a_1, \ldots, a_{n-1})$ is orthogonal to $(b_{n-1}, b_{n-2}, \ldots, b_0)$ and all its λ^{-1}-constacyclic shifts.

Given a ring R, for a nonempty subset S of R, the *annihilator* of S, denoted by $\mathrm{ann}(S)$, is the set

$$\mathrm{ann}(S) = \{f \mid fg = 0, \text{for all } g \in S\}.$$

Then $\mathrm{ann}(S)$ is also an ideal of R.

Customarily, for a polynomial f of degree k, its reciprocal polynomial $x^k f(x^{-1})$ will be denoted by f^*. Thus, for example, if

$$f(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} + a_kx^k,$$