On self-dual constacyclic codes of length $p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

Hai Q. Dinh $^{a,b,c}$, Yun Fan $^d$, Hualu Liu $^{d,e,*}$, Xiusheng Liu $^e$, Songsak Sriboonchitta $^f$

$^a$ Division of Computational Mathematics and Engineering, Institute for Computational Science, Ton Duc Thang University, Ho Chi Minh City, Viet Nam
$^b$ Faculty of Mathematics and Statistics, Ton Duc Thang University, Ho Chi Minh City, Viet Nam
$^c$ Department of Mathematical Sciences, Kent State University, 4314 Mahoning Avenue, Warren, OH 44483, USA
$^d$ School of Mathematics and Statistics, Central China Normal University, Wuhan, Hubei 430079, China
$^e$ School of Mathematics and Physics, Hubei Polytechnic University, Huangshi, Hubei 435003, China
$^f$ Faculty of Economics, Chiang Mai University, Chiang Mai 52000, Thailand

A R T I C L E   I N F O
Article history:
Received 26 April 2017
Received in revised form 28 August 2017
Accepted 30 August 2017
Available online xxxx

Keywords:
Cyclic codes
Constacyclic codes
Self-dual codes
Repeated-root codes
Codes over rings

A B S T R A C T
The aim of this paper is to establish all self-dual $\lambda$-constacyclic codes of length $p^s$ over the finite commutative chain ring $\mathbb{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, where $p$ is a prime and $u^2 = 0$. If $\lambda = \alpha + u\beta$ for nonzero elements $\alpha, \beta$ of $\mathbb{F}_{p^m}$, the ideal $(u)$ is the unique self-dual $(\alpha + u\beta)$-constacyclic codes. If $\lambda = \gamma$ for some nonzero element $\gamma$ of $\mathbb{F}_{p^m}$, we consider two cases of $\gamma$. When $\gamma = \gamma^{-1}$, i.e., $\gamma = 1$ or $-1$, we first obtain the dual of every cyclic code, a formula for the number of those cyclic codes and identify all self-dual cyclic codes. Then we use the ring isomorphism $\varphi$ to carry over the results about cyclic accordingly to negacyclic codes. When $\gamma \neq \gamma^{-1}$, it is shown that $(u)$ is the unique self-dual $\gamma$-constacyclic code. Among other results, the number of each type of self-dual constacyclic code is obtained.

© 2017 Elsevier B.V. All rights reserved.

1. Introduction

Constacyclic codes over finite fields play a very significant role in algebraic coding theory. The most important class of these codes is the class of cyclic codes, which has been well studied since the late 1950s. Constacyclic codes also have practical applications as they can be efficiently encoded with simple shift registers. This family of codes is therefore interesting for both theoretical and practical reasons.

Given a unit $\lambda$ of a finite field $\mathbb{F}$, $\lambda$-constacyclic codes of length $n$ over $\mathbb{F}$ are ideals of the quotient ring $\mathbb{F}[x]/(x^n - \lambda)$. In the literature, most of the research was concentrated on the situation where the code length $n$ is relatively prime to the characteristic of $\mathbb{F}$. The case where the code length $n$ is not relatively prime to the characteristic of $\mathbb{F}$ yields the so-called repeated-root codes, which were first studied since 1967 by Berman [4], and then in the 1970s and 1980s by several authors such as Massey et al. [27], Falkner et al. [19], Roth and Seroussi [32]. However, repeated-root codes were investigated in the most generality in the 1990s by Castagnoli et al. [9], and van Lint [37], where they showed that repeated-root cyclic codes have a concatenated construction, and are asymptotically bad. Nevertheless, it turns out that such codes are optimal in a few cases, which motivates researchers to further study this class of codes (see, for example, [11,23,29,35,38]).

After the realization in the 1990s [7,20,28] that many important yet seemingly non-linear binary codes such as Kerdock and Preparata codes are actually closely related to linear codes over the ring of integers modulo four via the Gray map, codes

* Corresponding author at: School of Mathematics and Physics, Hubei Polytechnic University, Huangshi, Hubei 435003, China
E-mail addresses: dinhquanghai@tdt.edu.vn (H.Q. Dinh), yfan@mail.ccnu.edu.cn (Y. Fan), hwlulu@aliyun.com (H. Liu), lxs6682@163.com (X. Liu), songsakecon@gmail.com (S. Sriboonchitta).

http://dx.doi.org/10.1016/j.disc.2017.08.044
0012-365X/© 2017 Elsevier B.V. All rights reserved.
over finite rings have received a great deal of attention. Since 2003, special classes of repeated-root codes over certain classes of finite chain rings have been studied by many authors (see, for example, [1,5,8,18,30]).

The class of finite rings of the form \(F_p^{m} + uF_p^{m}\), where \(u^2 = 0\), has been widely used as alphabets of certain constacyclic codes. For example, the structure of \(F_2 + uF_2\) is interesting. It can be considered as algebraically lying between \(F_4\) and \(Z_4\) in the sense that it is additively analogous to \(F_4\), and multiplicatively analogous to \(Z_4\). Linear codes over \(F_2 + uF_2\) have been studied by a lot of researchers (see, for example, [2,3,6,21,33,36]). All constacyclic codes of length \(2^s\) over the Galois extension rings of \(F_2 + uF_2\) are classified and their detailed structures are established in [13]. In [14], Dinh classified and gave the detailed structures of all constacyclic codes of length \(p^s\) over \(F_p^{m} + uF_p^{m}\). Recently, Dinh et al. studied negacyclic and constacyclic codes of length \(2p^s\) over the ring \(F_p^{m} + uF_p^{m}\) in [17] and [10]. The purpose of this paper is to continue this line of research. We identify all the self-dual \(\lambda\)-constacyclic codes of length \(p^s\) over \(F_p^{m} + uF_p^{m}\), where \(\lambda\) is an arbitrary unit of the ring \(F_p^{m} + uF_p^{m}\), \(p\) is a prime number and \(u^2 = 0\).

The remainder of the paper is organized as follows. Preliminary concepts and results are presented in Section 2. The units of the ring \(R = F_p^{m} + uF_p^{m}\) are of the forms \(\alpha + u\beta\) and \(\gamma\), where \(\alpha\), \(\beta\) and \(\gamma\) are nonzero elements of \(F_p^{m}\), which provides \(p^m(p^m - 1)\) such constacyclic codes. First, we study the self-dual \((\alpha + u\beta)\)-constacyclic code of length \(p^s\) over \(R\) and show that the ideal \((u)\) is the unique self-dual code in Section 3. Section 4 addresses the cyclic codes of length \(p^s\) over \(R\). These cyclic codes are completely classified by categorizing the ideals of the local ring \(R[x]/(x^{p^s} - 1)\) into four distinct types. After exhibiting the dual of each type of such cyclic codes, we then identify all self-dual cyclic codes. Finally, in Section 5, we use a one-to-one correspondence between cyclic and \(\gamma\)-constacyclic codes via the ring isomorphism \(\phi\), which allows us to apply the results about cyclic codes in Section 4 to \(\gamma\)-constacyclic codes except for the results about self-dual codes, since the dual of a \(\gamma\)-constacyclic code is a \(\gamma^{-1}\) constacyclic code. To investigate self-dual constacyclic codes, we consider two cases of \(\gamma\), namely, \(\gamma = \gamma^{-1}\) and \(\gamma \neq \gamma^{-1}\). When \(\gamma = \gamma^{-1}\), i.e., \(\gamma = 1\) or \(-1\), the results about cyclic codes hold true with negacyclic codes by replacing \(x\) by \(-x\) and writing \(h(x)\) more explicitly. When \(\gamma \neq \gamma^{-1}\), \((u)\) is the unique self-dual \(\gamma\)-constacyclic code of length \(p^s\) over \(R\).

2. Preliminaries

Let \(R\) be a finite commutative ring. An ideal \(I\) of the ring \(R\) is called principal if it is generated by one element. If all the ideals of \(R\) are principal, then \(R\) is called a principal ideal ring. \(R\) is called a local ring if \(R\) has a unique maximal ideal. Furthermore, \(R\) is said to be a chain ring if the set of all ideals of \(R\) is a chain under set-theoretic inclusion. The following result is well known (cf. [15, Proposition 2.1]).

**Proposition 2.1.** Let \(R\) be a finite commutative ring. Then the following conditions are equivalent:

(i) \(R\) is a local ring and the maximal ideal \(M\) of \(R\) is principal, i.e., \(M = (I^i)\) for some \(I^i \in R\),

(ii) \(R\) is a local principal ideal ring,

(iii) \(R\) is a chain ring whose ideals are \(\{I^i\}, 0 \leq i \leq e\), where \(e\) is the nilpotency index of \(I^i\).

Moreover, if \(R\) is a finite chain ring with the unique maximal ideal \((I^i)\) and the nilpotency index of \(I^i\) is \(e\), then the cardinality of the ideal \((I^i)^n\) is \(|R/(I^i)^n|\) for \(n = 0, 1, \ldots, e - 1\).

A code \(C\) of length \(n\) over \(R\) is a nonempty subset of \(R^n\) and the ring \(R\) is referred to as the alphabet of \(C\). If, in addition, that \(C\) is an \(R\)-submodule of \(R^n\), then \(C\) is said to be linear. For a unit \(\lambda\) of \(R\), the \(\lambda\)-constacyclic (\(\lambda\)-twisted) shift \(\tau_\lambda\) on \(R^n\) is the shift

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

A linear code \(C\) is said to be \(\lambda\)-constacyclic if \(\tau_\lambda(C) = C\), i.e., if \(C\) is closed under the \(\lambda\)-constacyclic shift \(\tau_\lambda\). If \(\lambda = -1\), then \(\lambda\)-constacyclic codes are called cyclic codes.

Each codeword \(c = (c_0, c_1, \ldots, c_{n-1}) \in C\) 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 \(R[x]/(x^{n} - \gamma)\), \(xc(x)\) corresponds to a \(\lambda\)-constacyclic shift of \(c(x)\). From that, the following fact is well known (cf. [22,26]) and straightforward:

**Proposition 2.2.** A linear code \(C\) of length \(n\) over \(R\) is \(\lambda\)-constacyclic if and only if \(C\) is an ideal of \(R[x]/(x^n - \gamma)\).

Given \(n\)-tuples \(x = (x_0, x_1, \ldots, x_{n-1}), y = (y_0, y_1, \ldots, y_{n-1}) \in R^n\), their inner product or dot product is defined as usual

\[x \cdot y = x_0y_0 + x_1y_1 + \cdots + x_{n-1}y_{n-1}\]

evaluated in \(R\). Two \(n\)-tuples \(x, y\) are called orthogonal if \(x \cdot y = 0\). For a linear code \(C\) over \(R\), its dual code \(C^\perp\) is the set of \(n\)-tuples over \(R\) that are orthogonal to all codewords of \(C\), i.e.,

\[C^\perp = \{x | x \cdot y = 0, \text{ for any } y \in C\}\]

A code \(C\) is called self-orthogonal if \(C \subseteq C^\perp\), and it is called self-dual if \(C = C^\perp\). The following result is well known (cf. [12,22,26,31]).
دریافت فوری متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات