Finite Fields and Their Applications 52 (2018) 301–318

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Extremal quasi-cyclic self-dual codes over finite fields

Hyun Jin Kim [a,*,1], Yoonjin Lee [b,2]

[a] University College, Yonsei University, 85 Songdogwahak-ro, Yeonsu-gu, Incheon 21983, South Korea

[b] Department of Mathematics, Ewha Womans University, 52, Seodaemun-Gu, Seoul, 03760, South Korea

A R T I C L E   I N F O

Article history:
Received 20 November 2017
Received in revised form 25 April 2018
Accepted 26 April 2018
Available online xxxx
Communicated by W. Cary Huffman

MSC:
primary 94B05
secondary 11T71

Keywords:
Quasi-cyclic code
Self-dual code
Extremal code
Finite field

A B S T R A C T

We study self-dual codes over a factor ring $\mathcal{R} = \mathbb{F}_q[X]/(X^m - 1)$ of length ℓ, equivalently, ℓ-quasi-cyclic self-dual codes of length $m\ell$ over a finite field $\mathbb{F}_q$, provided that the polynomial $X^m - 1$ has exactly three distinct irreducible factors in $\mathbb{F}_q[X]$, where $\mathbb{F}_q$ is the finite field of order q. There are two types of the ring $\mathcal{R}$ depending on how the conjugation map acts on the minimal ideals of $\mathcal{R}$. We show that every self-dual code over the ring $\mathcal{R}$ of the first type with length ≥ 6 has free rank ≥ 2. This implies that every ℓ-quasi-cyclic self-dual code of length $m\ell \geq 6m$ over $\mathbb{F}_q$ can be obtained by the *building-up construction*, where m corresponds to the ring $\mathcal{R}$ of the first type. On the other hand, there exists a self-dual code of free rank ≤ 1 over the ring $\mathcal{R}$ of the second type. We explicitly determine the forms of generator matrices of all self-dual codes over $\mathcal{R}$ of free rank ≤ 1. For the case that $m = 7$, we find 9828 binary 10-quasi-cyclic self-dual codes of length 70 with minimum weight 12, up to equivalence, which are constructed from self-dual codes over the ring $\mathcal{R}$ of the second type. These codes are all new codes. Furthermore,

* Corresponding author.
E-mail addresses: guswls41@yonsei.ac.kr (H.J. Kim), yoonjinl@ewha.ac.kr (Y. Lee).

[1] The author was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (NRF-2017R1D1A1B03028251).

[2] The author was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2009-0093827) and also by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (NRF-2017R1A2B2004574).

https://doi.org/10.1016/j.ffa.2018.04.013

for the case that $m = 17$, we find 1566 binary 4-quasi-cyclic self-dual codes of length 68 with minimum weight 12, up to equivalence, which are constructed from self-dual codes over the ring $\mathcal{R}$ of the first type.

1. Introduction

There has been active development on self-dual codes and quasi-cyclic codes over finite fields and finite rings. Self-dual codes are connected with other combinatorial structures as lattices [7,9], invariant theory [25], designs [1], and so forth. Quasi-cyclic codes are among the most commonly used linear codes. In fact, quasi-cyclic codes can be considered as modules over a group algebra of a cyclic group. There is a one-to-one correspondence between ℓ-quasi-cyclic codes over a finite field $\mathbb{F}_q$ of length ℓm and linear codes over a factor ring $\mathcal{R} = \mathbb{F}_q[X]/(X^m - 1)$ of length ℓ [22]. Ling and Solé [22,24] studied quasi-cyclic codes over a finite field $\mathbb{F}_q$ by considering linear codes over the ring $\mathcal{R}$, where m is a positive integer coprime to q. There is a bijective correspondence between quasi-cyclic codes over $\mathbb{F}_q$ and linear codes over $\mathcal{R}$. We call quasi-cyclic codes over $\mathbb{F}_q$ *cubic*, *quintic*, or *septic* codes depending on $m = 3, 5$, or 7, respectively. Binary cubic self-dual codes were studied by Bonnecaze et. al. [3] and binary quintic self-dual codes by Bracco et. al. [5]. Recently, Han et al. [12] worked on the case that $X^m - 1$ has exactly two distinct irreducible factors in $\mathbb{F}_q[X]$; in this case, they proved that every ℓ-quasi-cyclic self-dual code of length $m\ell$ over a finite field $\mathbb{F}_q$ can be obtained by the *building-up* construction. Every quasi-cyclic codes over $\mathbb{F}_q$ in this paper has a permutation automorphism of order m without fixed points. There is well-known closely related theory, for example [4,16,17,30], which is applicable to these codes.

According to our computation, the case that the number of distinct irreducible factors of $X^m - 1$ in $\mathbb{F}_2[X]$ (respectively, $\mathbb{F}_3[X]$) is two occurs in 40 percentage (respectively, 41 percentage) and three occurs in 30 percentage (respectively, 30 percentage) for $2 \leq m \leq 1000$. As a matter of fact, for a fixed finite field $\mathbb{F}_q$, there are infinitely many polynomials $X^m - 1$ which have exactly three distinct irreducible factors in $\mathbb{F}_q[X]$ according to Artin's conjecture. Motivated by this fact, we are interested in working on the case that $X^m - 1$ has exactly three distinct irreducible factors in $\mathbb{F}_q[X]$.

In this paper, we study self-dual codes over a ring $\mathcal{R} = \mathbb{F}_q[X]/(X^m - 1)$ of length ℓ, equivalently, ℓ-quasi-cyclic self-dual codes of length $m\ell$ over a finite field $\mathbb{F}_q$, provided that the polynomial $X^m - 1$ has exactly three distinct irreducible factors in $\mathbb{F}_q[X]$, where $\mathbb{F}_q$ is the finite field of order q. In fact, for a fixed prime power q, there are infinitely many polynomials $X^m - 1$ which have exactly three distinct irreducible factors in $\mathbb{F}_q[X]$ (Remark 3.4). We point out that there are two types of the ring $\mathcal{R}$ depending