Discrete Mathematics 340 (2017) 3197–3206

Contents lists available at ScienceDirect

Discrete Mathematics

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

A class of minimal cyclic codes over finite fields

Fen Li [a], Xiwang Cao [a,b,*]

[a] Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China
[b] State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences), Beijing 100093, China

ARTICLE INFO

Article history:
Received 21 May 2015
Received in revised form 9 June 2016
Accepted 13 July 2016
Available online 9 August 2016

Keywords:
Irreducible factorization
Primitive idempotent
Irreducible cyclic code

ABSTRACT

Let $\mathbb{F}_q$ be a finite field of odd order q and $n = 2^a p_1^{a_1} p_2^{a_2}$, where a, a_1, a_2 are positive integers, p_1, p_2 are distinct odd primes and $4p_1p_2 | q - 1$. In this paper, we study the irreducible factorization of $x^n - 1$ over $\mathbb{F}_q$ and all primitive idempotents in the ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Moreover, we obtain the dimensions and the minimum Hamming distances of all irreducible cyclic codes of length n over $\mathbb{F}_q$.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of order q. A code C of length n over $\mathbb{F}_q$ is called a *cyclic code* if $(c_{n-1}, c_0, \dots, c_{n-2}) \in C$ for every $(c_0, c_1, \dots, c_{n-1}) \in C$. Cyclic codes over finite fields constitute a remarkable class of linear codes. Any cyclic code of length n over $\mathbb{F}_q$ is identified with exactly one ideal of the quotient algebra $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. A cyclic code is called *minimal* if the corresponding ideal is minimal. In fact, many well known codes, such as BCH and Hamming codes are cyclic codes, and many other famous codes can also be constructed from cyclic codes, for example the Kerdock codes and Golay codes. Cyclic codes also have practical applications, as they can be efficiently encoded by shift registers. It is true that every cyclic code turns out to be a direct sum of some minimal cyclic codes.

Recently, a lot of papers investigate the minimal cyclic code, see e.g. [1,2,4,5,7,10,16,17]. It is well known that minimal cyclic codes and primitive idempotents have a one-to-one correspondence, as every minimal cyclic code can be generated by exactly one primitive idempotent, so it is useful to determine the primitive idempotents in $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. In [3], Arora and Pruthi got the $2n + 2$ minimal cyclic codes of length $2p^n$ over $\mathbb{F}_q$ where q is an odd prime and $\mathrm{ord}_{2p^n}(q) = \varphi(p^n)$, they also got the explicit expression for the primitive idempotents, generating polynomials, minimum distance and dimension of these codes in $\mathbb{F}_q[x]/\langle x^{2p^n} - 1\rangle$. Pruthi and Arora (see [15]) also studied minimal cyclic codes of length p^n over $\mathbb{F}_q$, where q is a primitive root modulo p^n, they described the q-cyclotomic cosets modulo p^n and the primitive idempotents in $\mathbb{F}_q[x]/\langle x^{p^n} - 1\rangle$. Batra and Arora also obtained the primitive idempotents in $\mathbb{F}_q[x]/\langle x^{p^n} - 1\rangle$ with $\mathrm{ord}_{p^n}(q) = \frac{\varphi(p^n)}{2}$ in [2] and [6]. In [7], Batra and Arora got the primitive idempotents in $\mathbb{F}_q[x]/\langle x^{2p^n} - 1\rangle$ where q is odd and $\mathrm{ord}_{2p^n}(q) = \frac{\varphi(p^n)}{2}$ by using the method mentioned in [2]. In [8], Chen et al. studied minimal cyclic codes of length l^m over $\mathbb{F}_q$ where l is a prime divisor of $q - 1$ and m is a positive integer.

This paper is based on [8,9,11,12,14]. First, according to [14] we generally obtain the irreducible factorization of $x^{2^a p_1^{a_1} p_2^{a_2}} - 1$ over $\mathbb{F}_q$, where a, a_1, a_2 are positive integers, p_1, p_2 are odd primes and $4p_1p_2 | q - 1$. Then we can get the primitive idempotents in $\mathbb{F}_q[x]/\langle x^{2^a p_1^{a_1} p_2^{a_2}} - 1\rangle$. In the last part, we provide the check polynomials, minimum Hamming distances and

[*] Corresponding author at: Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China.
E-mail addresses: lifen08001@163.com (F. Li), xwcao@nuaa.edu.cn (X. Cao).

http://dx.doi.org/10.1016/j.disc.2016.07.005
0012-365X/© 2016 Elsevier B.V. All rights reserved.

the dimensions of the codes generated by the primitive idempotents in $\mathbb{F}_q[x]/\langle x^{2^a p_1^{a_1} p_2^{a_2}} - 1\rangle$. In general, we can also get the primitive idempotents in $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ and check polynomials, minimum Hamming distances, the dimensions of the codes generated by the primitive idempotents in $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ with the case $n = 2^a p_1^{a_1} \cdot \cdots \cdot p_e^{a_e}$ where $p_1, \dots, p_e$ are distinct odd primes and $4p_1 \cdot \cdots \cdot p_e | q-1$.

2. Factorization of $x^{2^a}p_1^{a_1}p_2^{a_2} - 1$

In this section, we will give the factorization of $x^n - 1$ over $\mathbb{F}_q$ with $n = 2^a p_1^{a_1} p_2^{a_2}$, where p_1, p_2 are distinct odd primes, a, a_1, a_2 are positive integers and $4p_1p_2 | q-1$.

There is a criterion for irreducibility of non-linear binomials over $\mathbb{F}_q$, which was given by Serret in 1866 (e.g. see [13], Theorem 3.75 or [18], Theorem 10.7).

Lemma 1. *Assume that $k \geq 2$, $k \in N^*$. For any $\gamma \in \mathbb{F}_q^*$, with $\mathrm{ord}(\gamma) = e$, the binomial $x^k - \gamma$ is irreducible over $\mathbb{F}_q$ if and only if both the following two conditions are satisfied:*

(1) *Every prime divisor of k divides e, but does not divide $\frac{q-1}{e}$;*
(2) *If $4|k$, then $4|(q-1)$.*

Let $\mathbb{F}_q$ be a finite field of odd order q. We denote all the non-zero elements of $\mathbb{F}_q$ by $\mathbb{F}_q^*$, i.e. the multiplicative group of $\mathbb{F}_q$. For $\beta \in \mathbb{F}_q^*$, we denote $\mathrm{ord}(\beta)$ the order of β in $\mathbb{F}_q^*$, then $\mathrm{ord}(\beta)$ is a divisor of $q-1$, and β is called a primitive $\mathrm{ord}(\beta)$th root of unity. It is well known that $\mathbb{F}_q^*$ is a cyclic group of order $q-1$, if $\mathbb{F}_q^* = \langle \xi \rangle$ for some ξ, i.e., $\mathrm{ord}(\xi) = q-1$, then ξ is a *primitive element* of $\mathbb{F}_q$. We also denote $v_p(m)$ the degree of p in the standard decomposition of the positive integer m. In this paper, we assume that $v_2(q-1) = u$, $v_{p_1}(q-1) = u_1$ and $v_{p_2}(q-1) = u_2$, where $2, p_1, p_2$ are distinct primes and u, u_1, u_2 are positive integers. Then $q - 1 = 2^u p_1^{u_1} p_2^{u_2} c$, where $\gcd(2p_1p_2, c) = 1$. In the following, we will give the irreducible factorization of $x^{2^a p_1^{a_1} p_2^{a_2}} - 1$ over $\mathbb{F}_q$. By Division Algorithm, we assume that

$$a = mu + r;\ a_1 = m_1u_1 + r_1;\ a_2 = m_2u_2 + r_2,$$
$$0 \leq r < u, 0 \leq r_1 < u_1, 0 \leq r_2 < u_2.$$

For convenience, we just assume that $m \leq 1$, $m_1 \leq 1$ and $m_2 \leq 1$ here. In this paper, we denote ζ_k be a primitive kth root of unity over $\mathbb{F}_q^*$. When $m = m_1 = m_2 = 0$, the factorization of $x^{2^a p_1^{a_1} p_2^{a_2}} - 1$ over $\mathbb{F}_q$ is given as follows:

$$x^{2^r p_1^{r_1} p_2^{r_2}} - 1 = \prod_{i=0}^{2^r p_1^{r_1} p_2^{r_2} - 1} (x - \alpha^i),$$

where $\alpha = \xi^{2^{u-r} p_1^{u_1 - r_1} p_2^{u_2 - r_2} c}$ is a primitive $2^r p_1^{r_1} p_2^{r_2}$th root of unity. By symmetry, we discuss the factorization of $x^{2^a p_1^{a_1} p_2^{a_2}} - 1$ in three cases when $(m, m_1, m_2) \neq (0, 0, 0)$ as follows. Since the results below (Theorems 1–3) are special cases of [14], the proof of which are thus omitted.

Theorem 1. *When $m = 1$, $m_1 = m_2 = 0$, there is a factorization over $\mathbb{F}_q$:*

$$x^{2^{u+r} p_1^{r_1} p_2^{r_2}} - 1 = \prod_{i=0}^{2^u p_1^{r_1} p_2^{r_2} - 1} (x^{2^r} - \beta^i),$$

where $\beta = \xi^{p_1^{u_1 - r_1} p_2^{u_2 - r_2} c}$ is a primitive $2^u p_1^{r_1} p_2^{r_2}$th root of unity. Moreover, we suppose that $i = 2^t k$, $\gcd(2, k) = 1$.

(1) *When $t = 0$, the polynomial $x^{2^r} - \beta^i$ is irreducible over $\mathbb{F}_q$;*
(2) *When $t < r$, the factorization of $x^{2^r} - \beta^i$ over $\mathbb{F}_q$ is given as follows:*

$$x^{2^r} - \beta^i = \prod_{j=0}^{2^t - 1} (x^{2^{r-t}} - \zeta_{2^t}^j \beta^k); \tag{1}$$

(3) *When $t \geq r$, the factorization of $x^{2^r} - \beta^i$ over $\mathbb{F}_q$ is given as follows:*

$$x^{2^r} - \beta^i = \prod_{j=0}^{2^r - 1} (x - \zeta_{2^r}^j \beta^{2^{t-r} k}). \tag{2}$$