On Cyclic Codes of Composite Length and the Minimum Distance

Kwame Ackah Bohulu

December 19, 2018

1 Introduction

The theory of error-correction codes is an important research area, and it has many applications in modern life including the recovery of corrupted information after transmission over an unreliable channel. Till date, the construction of new error-correction codes with good parameters as well as the problem of finding the minimum distance and designing efficient decoding and encoding algorithms is still a major challenge in coding theory. Let $\mathbb{F}_q$ be a finite field of order q. Let n_1, n_2 be two distinct odd primes such that $(n_1 n_2, q) = 1$ and q is a quadratic residue for both n_1 and n_2. In an interesting paper [2], Ding provided a general construction of cyclic codes of length $n_1 n_2$ and dimension $(n_1 n_2 + 1)/2$ over F_q by using generalised cyclotomies of order two in $\mathbb{Z}^*_{n_1 n_2}$ and this construction is similar to that of quadratic residue codes of prime length, which can be defined by using cyclotomy of order two in $\mathbb{Z}^*_n$ when n is a prime number.

For the case when n is a product of two distinct odd primes, there are three different generalised cyclotomies of $\mathbb{Z}^*_n$ and these correspond to Dings first, second and third construction, each of which yields 8 cyclic codes of length n and dimension $(n+1)/2$. The information corresponding to the construction of these cyclic codes is tabulated in Table 1.

In this paper, theory on Dings three constructions that partially explains some of the data in Table 1 is provided (see Theorems 2, 3 and 4 in Section III): first, we prove that under permutation equivalence, there are indeed two codes in each construction; second, we prove an "almost" square-root bound on the minimum distance(i.e. $d_{min} > \sqrt{n_1} or \sqrt{n_2}$ for the codes of length $n_1 n_2$) which is satisfied by all these codes; third, for Dings second and third construction, we illustrate why half of the cyclic codes have relatively small minimum distance. Previously in [2] only lower bounds on the minimum odd-like weight of the codes were obtained but it is well-known that minimum odd-like weight may be much larger than the minimum distance of the codes. This is actually the case for the codes from Dings constructions.

2 Cyclic Codes Of Composite Length

in this section, standard notation ,definitions, theorems and proofs are introduced here

2.1 Notation and Definitions

- $\mathbb{F}_q$ represents the finite field of order q, where q is a prime power.
- A linear $[n, k, d; q]$ code $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum (Hamming) distance $d = d(\mathcal{C})$.
- A linear $[n, k]$ code $\mathcal{C}$ over $\mathbb{F}_q$ is called a cyclic code of length n if any $(c_0, c_1, ..., c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, c_1, ..., c_{n-2}) \in \mathcal{C}$.

– By identifying any vector$(c_0, c_1, ..., c_{n-1}) \in \mathbb{F}_q^n$ with

$$c_0x_0 + c_1x^1 + ... + c_{n-1}x^{n-1} \in \mathbb{R}_n := \mathbb{F}_q[x]/(x^n - 1),$$

$\mathcal{C}$ is a cyclic code of length n over $\mathbb{F}_q$ if and only if the corresponding subset of $\mathbb{R}_n$, (still written as $\mathcal{C}$) is an ideal of the ring $\mathbb{R}_n$.

– Since every ideal of $\mathbb{R}_n$ is principal, there is a monic polynomial $g(x) \in \mathbb{F}_q[x]$ of least degree such that $\mathcal{C} = (g(x)) \subset \mathbb{R}_n$.

– $g(x)$ is unique, satisfying $g(x)|(x^n 1)$ and is called the generator polynomial of C, and $h(x) := (x^n 1)/g(x)$ is called the parity-check polynomial of C.

- Two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are called permutation equivalent, written as $\mathcal{C}_1 \sim \mathcal{C}_2$, if there is a permutation of coordinates that sends $\mathcal{C}_1$ to $\mathcal{C}_2$. The permutation of coordinates is called a permutation equivalence.

- For any $c(x) \in \mathbb{F}_q[x]$, define Supp$(c(x))$ to be the set of integers i such that the term x^i appears in $c(x)$. Define the weight wt$(c(x))$ to be the cardinality of the set Supp$(c(x))$.

2.2 Theorems

The main theorem is the following

Theorem 1: Let $n, r \geq 2$ be positive integers such that $gcd(nr, q) = gcd(n, r) = 1$. Assume that $r|(q1)$. Let θ be a primitive nr-th root of unity in some extension of $\mathbb{F}_q$. Define $\lambda := \theta^n$ and let $\tilde{n}$ be a positive integer such that $n\tilde{n} \equiv 1($ mod $r)$. For any $0 \leq t \leq r - 1$, let $\theta_t := \lambda^{\tilde{n}t}$. We define the map

$$\phi : \frac{\mathbb{F}_q[x]}{(x^{nr} - 1)} \to \Big(\frac{\mathbb{F}_q[x]}{(x^n - 1)}\Big)^r$$

by

$$\phi : c(x) \mapsto \frac{1}{r}\Big(\sum_{t=0}^{r-1} c_t(x)\lambda^{-tk}\Big)_{k=0}^{r-1}$$

here for any $c(x) \in \mathbb{F}_q[x]/(x^{nr} - 1)$ the polynomial $c_t(x) \in \mathbb{F}_q[x]/(x^n - 1)$ is given by

$$c_t(x) \equiv c(x\theta_t)(\mod x^n - 1) \forall 0 \leq t \leq r - 1$$

Then:

1) the map ϕ is a permutation equivalence, and $c(x) = 0$ if and only if $(c_t(x))_{t=0}^{r-1} \neq 0$;

2) if $c(x) \neq 0$, then

$$wt(c(x)) \geq \min\{wt(ct(x)) : c_t(x) \neq 0\}$$

. Moreover,

2.1) if $c_0(x) = c_1(x) = ... = c_{r1}(x)$, then $wt(c(x)) = wt(c_0(x))$;

2.2) if $c_t(x) = 0$for some t, then

$$wt(c(x)) \geq 2\min\{wt(c_t(x)) : c_t(x) \leq 0\}$$

.

Let $\mathcal{C} = (g(x)) \subset \mathbb{F}_q[x]/(x^{nr}1)$ be a cyclic code with the generator polynomial $g(x)$. Then

3) $\mathcal{C}$ is permutation equivalent to $\phi(\mathcal{C})$, which is given by

$$\phi(\mathcal{C}) = \left\{ \Big(\sum_{t=0}^{r-1} c_t(x)\lambda^{-tk} \Big)_{k=0}^{r-1} : c_t(x) \in C_t \forall t \right\},$$

where $\mathcal{C}_t = (gt(x)) \subset \mathbb{F}_q[x]/(x^n - 1)$ is a cyclic code with the generator polynomial $g_t(x)$ given by

$$g_t(x) = gcd(g(x\theta_t), x^n - 1) \forall 0 \leq t \leq r - 1$$

4) If $\mathcal{C} \neq 0$, then

$$d(\mathcal{C}) \geq min\{d(\mathcal{C}_t) : \mathcal{C}_t \neq 0\}$$

. Moreover,

4.1) if $\mathcal{C}_0 = \mathcal{C}_1 = ... = \mathcal{C}_{r-1}$, then $d(\mathcal{C}) = d(\mathcal{C}_0)$;

4.2) if $\mathcal{C}_t = 0$ for some t, then

$$d(\mathcal{C}) \geq 2 \min_t \{d(\mathcal{C}_t) : \mathcal{C}_t \neq 0\}.$$

2.3 Proofs

1) Writing

$$c_t(x) = \sum_{z=0}^{n-1} c_{t,z} x^z$$

$$c(x) = \sum_{i=0}^{nr-1} c_i x^i = \sum_{k=0}^{r-1} \sum_{z=0}^{n-1} c_{kn+z} x^{kn+z}$$

then from $c_t(x) \equiv c(x\theta_t)(\mod x^n - 1)$, we find

$$c_{t,z} = \sum_{k=0}^{r-1} c_{kn+z}\theta_t^{kn+z} \forall t, z$$

since $\theta_t = \lambda^{\tilde{n}t}$ and λ is the r-th root of unity, we can obtain

$$c_{kn+z} = \frac{1}{r}\sum_{t=0}^{r-1} c_{t,z}\theta_t^{-kn-z} \forall t, z$$

Therefore ,

$$c(x) = \frac{1}{r}\sum_{t=0}^{r-1}\sum_{z=0}^{n-1} c_{t,z}x^z \sum_{k=0}^{r-1} x^{nk}\lambda^{-t(k+\tilde{n}z)}$$

For any given$z$, let $k^{'} \equiv k + \tilde{n}z(\mod r)$. Noting that $x^{\tilde{n}k} \equiv x^{n(k^{'}-nz)}(\mod x^{nr} - 1)$ and as $k^{'}$ runs over a complete residue system modulo r , so does $k \equiv k^{'} - \tilde{n}z(\mod r)$., and it is clear that $\psi : x^{nk} \mapsto x^{nk^{'}}$ induces a permutation of coordinates in $\mathbb{F}_q[x]/(x^{nr} - 1)$, thus $c(x)$ is permutation equivalent to

$$\begin{aligned}\psi(c(x)) &= \frac{1}{r}\sum_{t=0}^{r-1}\sum_{z=0}^{n-1} c_{t,z}x^z \sum_{k=0}^{r-1} x^{nk}\lambda^{-tk} \\ &= \frac{1}{r}\sum_{k=0}^{r-1} x^{nk}\sum_{t=0}^{r-1} c_t(x)\lambda^{-tk}\end{aligned} \tag{1}$$

Hence $\psi(c(x))$is permutation equivalent to $\phi(c(x))$, and thus ϕ is a permutation equivalence. Moreover, noting

$$c_t(x) = 0 \iff (x^n 1)|c_t(x) \iff (x^n\lambda^t)|c(x),$$

and

$$x^{nr} - 1 = \prod_{t=0}^{r-1}(x^n - \lambda^t),$$

it is obvious that $c(x) \neq 0$ if and only if $(c_t(x))_{t=0}^{r-1} \neq 0$. This proves 1).

2). Since $c_t(x) \equiv c(x\theta_t)(\mod x^n - 1)$ we have

$$wt(c(x)) = wt(c(x\theta_t)) \geq wt(c_t(x)) \quad \forall 0 \leq t \leq r-1.$$

Taking $c_0(x) = ... = c_{r-1}(x)$ in (1), and using

$$\sum_{t=0}^{r-1}\lambda^{-}tk = \begin{cases} r :, & \text{if } r|k \\ 0 :, & r \nmid k \end{cases}$$

we find easily that $\psi(c(x)) = c_0(x)$. This proves 2) and 2.1).

For

2.2) , let

$$A = \{0 \le t \le r-1 : c_t(x) \neq 0\}, \quad \mathbf{I} = \bigcup_{t \in A} \mathrm{Supp}(c_t(x))$$

from (1) we find that

$$\mathrm{wt}(c(x)) = \sum_{z \in \mathbf{I}} \sum_{k=0}^{r-1} \mathrm{wt}\Big(\sum_{t \in A} c_{t,z} \lambda^{-tk} \Big)$$

for each k and z, write

$$h_{k,z} := \sum_{t \in A} c_{t,z} \lambda^{-tk}$$

and for each z write $\underline{\mathrm{h}}_z := (h_{k,z})_{k=0}^{r-1}$ and $\underline{\mathrm{c}}_z := (c_{t,z})_{t \in A}$ as column vectors. Assume that $A = \{t_1, t_2, ..., t_u\}$ Then we have

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \lambda^{-t_1} & \lambda^{-t_2} & \cdots & \lambda^{-t_u} \\ \vdots & \vdots & \vdots & \vdots \\ \lambda^{-(r-1)t_1} & \lambda^{-(r-1)t_2} & \cdots & \lambda^{-(r-1)t_u} \end{bmatrix} \cdot \underline{\mathrm{c}}_z = \underline{\mathrm{h}}_z \tag{2}$$

and

$$\mathrm{wt}(c(x)) = \sum_{z \in \mathbf{I}} \mathrm{wt}(\underline{\mathrm{h}}_z)$$

Noting that for any $z \in I$, we have $c_z \neq 0$, and the matrix on the left side of the equation (2) is a Vandermond matrix of size $r \times u$ where $1 \le u < r$, we find $\mathrm{wt}(\underline{\mathrm{h}}_z) \ge 2$. Thus

$$\mathrm{wt}(c(x)) \ge \sum_{z \in \mathbf{I}} 2 \ge 2 \min\{\mathrm{wt}(c(x)) : c_t(x)\}$$

This proves 2.2).

3) . For any $0 \le t \le r-1$ define maps, $\phi_t, \ f_t$

$$\frac{\mathbb{F}_q[x]}{(x^{nr}-1)} \to^{\phi_t} \frac{\mathbb{F}_q[x]}{(x^n - \lambda^t)} \to^{f_t} \frac{\mathbb{F}_q[x]}{(x^n-1)}$$

by

$$\phi_t : c(x) \mapsto c(x) \pmod{x^n - \lambda^t}, \quad f_t : x \mapsto x\theta_t$$

Let $\Psi_t := f_t \circ \phi_t and \Psi = (\Psi)_{t=0}^{r-1}$. The isomorphism from the Chinese Remainder Theorem

$$\Psi : \frac{\mathbb{F}_q[x]}{(x^{nr}-1)} \to \prod_{t=0}^{r-1} \frac{\mathbb{F}_q[x]}{(x^n-1)}$$

induces an isomorphism $\Psi(\mathcal{C}) \cong \prod_{t=0}^{r-1} \Psi_t(\mathcal{C})$. Since clearly $\mathcal{C}_t = \Psi_t(\mathcal{C})$, 3) is proved.

4) Suppose $c(x) \in \mathcal{C}$ is a codeword with the minimum distance. The corresponding $(c_t(x))_{t=0}^{r-1} \neq 0$. Since $c_t(x) \in \mathcal{C}_t$ for each $t, \text{if} c_t(x) \neq 0$, then $\text{wt}(c_t(x)) \geq d(\mathcal{C}_t)$. Hence

$$\text{wt}(c(x)) \geq \min_t \{\text{wt}(c_t(x)) : c_t(x) \neq 0\} \geq \min\{d(\mathcal{C}_t) : \mathcal{C}_t\}$$

On the other hand, if $\mathcal{C}_0 = ... = \mathcal{C}_{r-1} \neq 0$ we may take a codeword $\bar{c}(x) \in \mathcal{C}_0$ with the minimum distance and let $c_t(x) = \bar{c}(x) \forall t$. The corresponding codeword $c(x) \in \mathcal{C}$ satisfies the property that $\text{wt}(c(x)) = \text{wt}(\bar{c}(x))$. So $d(\mathcal{C}) = d(\mathcal{C}_0)$. This proves 4) and 4.1). The proof of 4.2) is similar.