Weight Distribution of Cyclic Codes with Several Non-zeroes

Jinquan Luo

Department of Informatics, University of Bergen, Norway

Outline

- Introduction
- Main problem
- Auxiliary tools
- Main result
- Conclusion and further work

Introduction

Linear code An $[n, k, d; q]$ linear code is a k-dimensional $GF(q)$ linear subspace of $GF(q)^n$ with minimum Hamming distance d. For an $[n, k, d; q]$ linear code $\mathcal{C}$, let A_i be the number of codewords in $\mathcal{C}$ with Hamming weight i. The *weight distribution* $\{A_0, A_1, \cdots, A_n\}$ is an important research object in coding theory.

Introduction

Cyclic code In a linear code $\mathcal{C}$, if, for any codeword $(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$, the cyclic shifts $(c_i, c_{i+1}, \cdots, c_{i-1})$ for all i, $1 \leq i \leq n-1$ are codewords in $\mathcal{C}$, then $\mathcal{C}$ is called cyclic code. It is well known that any k-dimensional q-ary cyclic code of length n with $\gcd(n, q) = 1$ is generated by a polynomial $g(x) \in GF(q)[x]$ of degree $n-k$ which is a divisor of $x^n - 1$.

Introduction

The reciprocal polynomial $h(x)$ of $h^*(x) = (x^n - 1)/g(x)$, i.e., $h(x) = x^{\deg(h^*(x))}h^*(x^{-1})$ is called the parity check polynomial of $\mathcal{C}$. The zeroes of $h(x)$ are called the non zeroes of $\mathcal{C}$. We say $\mathcal{C}$ is irreducible if $h(x)$ is irreducible and $\mathcal{C}$ has l non zeroes if $h(x)$ is the product of l irreducible polynomials.

Main Problem

Notations

- Let p an odd prime, $q = p^s$, $r = q^m$, and $GF(p^i)$ be the finite field of order p^i. Let e and h be two integers and $eh \mid q-1$, $\gcd(eh, m) = 1$ and $n = \frac{r-1}{h}$. Let t be an integer coprime to e.

- Let g be a primitive element of $GF(r)$ (that is, g is the generator of the multiplicative group $GF(r)^*$), $\alpha = g^h$ and $\beta = g^{t\frac{r-1}{e}}$.

.

- For $j|i$, let $\mathrm{Tr}_{p^i/p^j} : GF(p^i) \to GF(p^j)$ be the trace mapping defined by $\mathrm{Tr}_{p^i/p^j}(x) = x + x^{p^j} + x^{p^{2j}} + \cdots + x^{p^{j-i}}$.

- Let $\zeta_p = \exp(2\pi\sqrt{-1}/p)$ be a p-th root of unity and $\chi_{p^i}(x) = \zeta_p^{\mathrm{Tr}_{p^i/p}(x)}$ be the canonical additive character on $GF(p^i)$.

Main Problem

In this talk we will give the weight distribution of the cyclic code $\mathcal{C}$ with non zeroes $(\alpha\beta^i)^{-1}$ for $0 \leq i \leq l-1$. Note that for the special case $t = 1$ (then $\beta = g^{(r-1)/e}$) and $l = 2$, the weight distribution of $\mathcal{C}$ has been determined in Ma et al, see

Ma et al, The weight enumerators of a class of cyclic codes, *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 397–402, Jan. 2011.

Main Problem

Thanks to Delsarte's Theorem, the weights of codewords in the above $\mathcal{C}$ can be expressed as

$$c(\mathbf{a}) = (c_0, c_1, \cdots, c_{n-1})$$

for

$$\mathbf{a} = (a_0, \cdots, a_{l-1}) \in GF(q)^l$$

where

$$c_i = \sum_{j=0}^{l-1} \mathrm{Tr}_{r/q}(a_j(\alpha\beta^j)^i) \quad (0 \leq i \leq n-1).$$

For abbreviation, denote by

$$Z(\mathbf{a}) = \sum_{\omega \in GF(q)^*} \sum_{i=0}^{n-1} \chi_r \left(\omega \sum_{j=0}^{l-1} a_j (\alpha \beta^j)^i \right).$$

Then the Hamming weight of $c(\mathbf{a})$ is

$$w_H(c(\mathbf{a})) = n - \frac{n}{q} - \frac{1}{q} Z(\mathbf{a}).$$

In this way, the weight distribution of cyclic code $\mathcal{C}$ can be derived from the explicit evaluating of $Z(\mathbf{a})$.

Auxiliary Tools

Let G be the multiplicative subgroup of $GF(r)^*$ generated by g^h and H be the subgroup of G generated by g^{eh}. Then we have the following coset factorization

$$G = \bigcup_{i=0}^{e-1} g^{hi} H.$$

Auxiliary Tools

Note that $GF(q)^*$ is the multiplicative subgroup of $GF(r)^*$ generated by $g^{(r-1)/(q-1)}$ and $\gcd(eh, m) = 1$.

Lemma 1. *For any $u \in GF(r)^*$, there are exactly $\frac{q-1}{eh}$ pairs $(w, x) \in GF(q)^* \times H$ such that $u = wx$.*

Auxiliary Tools

Note that $\beta = g^{t(r-1)/e}$. The Reed-Solomn code $\mathcal{RS}(\beta, e, l)$ over $GF(r)$ generated by

$$G_{RS}(\beta, e, l) = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \beta & \beta^2 & \cdots & \beta^{e-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \beta^{l-1} & \beta^{2(l-1)} & \ldots & \beta^{(e-1)(l-1)} \end{pmatrix}$$

is an MDS (maximum distance separable) code with parameter $[e, l, e-l+1; r]$.

Auxiliary Tools

The weight distribution of $\mathcal{RS}(\beta, e, l)$ is as follows.

Lemma 2. *Let B_i be the number of codewords in $\mathcal{RS}(\beta, e, l)$ with weight i. Then*

$$B_i = \begin{cases} 1, & \textit{for}\, i = 0 \\ \binom{e}{i}(r-1)\sum_{j=0}^{i-e+l-1}(-1)^j\binom{i-1}{j}r^{i-e+l-j-1}, & \textit{for}\, e-l+1 \le i \le e \\ 0, & \textit{otherwise.} \end{cases}$$

Main Result

Note that G is the cyclic group generated by $\alpha = g^h$. Recall $\beta = g^{t(r-1)/e}$ with $\gcd(t,e) = 1$. Then

$$\begin{aligned} Z(\mathbf{a}) &= \sum_{\omega \in GF(q)^*} \sum_{x \in G} \chi_r \left(\omega \sum_{j=0}^{l-1} a_j x^{1+\frac{t(r-1)}{eh} j} \right) \\ &\qquad \text{(By the factorization } G = \bigcup_{i=0}^{e-1} g^{hi} H\text{)} \\ &= \sum_{\omega \in GF(q)^*} \sum_{i=0}^{e-1} \sum_{y \in H} \chi_r \left(\omega \sum_{j=0}^{l-1} a_j (g^{hi} y)^{1+\frac{t(r-1)}{eh} j} \right) \end{aligned}$$

Main Result

(By $y^{\frac{t(r-1)}{eh}} = 1$ for any $y \in H$)

$$= \sum_{\omega \in GF(q)^*} \sum_{i=0}^{e-1} \sum_{y \in H} \chi_r \left(\sum_{j=0}^{l-1} a_j \beta^{ij} \left(g^{hi} \omega y \right) \right)$$

(By Lemma 1)

$$= \frac{q-1}{eh} \sum_{i=0}^{e-1} \sum_{z \in GF(r)^*} \chi_r \left(\sum_{j=0}^{l-1} a_j \beta^{ij} z \right).$$

Denote by $c_i = \sum_{j=0}^{l-1} a_j \beta^{ij}$. Then

$$c'(\mathbf{a}) = (c_0, c_1, \cdots, c_{e-1}) = (a_0, a_1, \cdots, a_{e-1}) \cdot G_{RS}(\beta, e, l)$$

is a codeword of $\mathcal{RS}(\beta, e, l)$. Note that the inner sum

$$\sum_{z \in GF(r)^*} \chi_r(c_i z) = \begin{cases} r-1 & \text{if } c_i = 0, \\ -1 & \text{if } c_i \neq 0. \end{cases}$$

Therefore

$$\begin{aligned} Z(\mathbf{a}) &= \tfrac{q-1}{eh}\left((r-1)\cdot(e - w_H(c'(\mathbf{a}))) - w_H(c'(\mathbf{a}))\right) \\ &= \tfrac{q-1}{eh}\left((r-1)e - r w_H(c'(\mathbf{a}))\right). \end{aligned}$$

and

$$w_H(c(\mathbf{a})) = \frac{q-1}{q}\frac{r-1}{h} - \frac{1}{q}Z(\mathbf{a}) = \frac{(q-1)q^{m-1}}{eh}w_H(c'(\mathbf{a})).$$

Main Result

From the weight distribution of $\mathcal{RS}(\beta, e, l)$, we obtain the weight enumerator of the code $\mathcal{C}$ with nonzeroes $\alpha\beta^i$ $(0 \le i \le l-1 \le e-1)$.

Theorem 1. *The cyclic code* $\mathcal{C}$ *has parameter* $[\frac{r-1}{h}, lm, \frac{q^{m-1}(q-1)}{eh}(e-l+1); q]$ *and its weight enumerator is*

$$A_{\mathcal{C}}(x) = \sum_{i=e-l+1}^{e} \binom{e}{i} (r-1) \sum_{j=0}^{i-e+l-1} (-1)^j \binom{i-1}{j} r^{i-e+l-j-1} \cdot x^{\frac{q^{m-1}(q-1)}{eh} i}.$$

Main Result

Remarks

(1). When $l = 1$, then the code $\mathcal{C}$ is the Simplex code which has only one nonzero weight.

(2). When $l = 2$ and $t = 1$, the code $\mathcal{C}$ has been studied in Ma et al.

(3). In general, the code $\mathcal{C}$ has l nonzero weights: $\frac{q^{m-1}(q-1)}{eh}i$ for $e - l + 1 \leq i \leq e$.

Main Result

Example When $q = 7$, $m = 2$, $e = l = 3$ and $h = 1$, the code $\mathcal{C}$ has parameters $[48, 6, 14; 7]$. Using Magma, we can calculate the weight enumerator of $\mathcal{C}$

$$A_{\mathcal{C}}(x) = 1 + 144\,x^{14} + 6912\,x^{28} + 117649\,x^{42}$$

which coincides with Theorem 1. The dual of $\mathcal{C}$ is an $[48, 42, 4; 7]$ code.

Conclusion and Further Work

In this talk we discussed the weight distribution of some cyclic codes whose dual has l zeroes, where $l \le e$ and $eh \mid q-1$.

We only focus on the case $\gcd(eh, m) = 1$. For the more general case $\gcd(eh, m) > 1$, the result will become more complicated. For some simple cases, for example $\gcd(eh, m) = 2$ and $l = 3$, we can determine the weight distribution which will be included in an extended version. The general case is still open.

Thanks!