Complete b-Symbol Weight Distribution of Some Irreducible Cyclic Codes

Ferruh Özbudak

Faculty of Engineering and Natural Sciences, Sabancı University, Tuzla, 34956, İstanbul, Turkey
ferruh.ozbudak@sabanciuniv.edu

May 31, 2023

based on some joint works with P. Sole, M. Shi and H. Zhu

Preliminaries

- $\mathbb{F}_q$: finite field with q elements.
- $\mathbb{F}_q^*$: $\mathbb{F}_q \backslash \{0\}$.
- $q = p^e$, $p = \mathcal{char}\ \mathbb{F}_q$ and p is odd.
- $r \geq 2$: an *even* integer.
- $nN = q^r - 1$, where n, N are positive integers.
- $\gcd\left(\frac{q^r-1}{q-1}, N\right) = 2$.
- $2 \leq b \leq n-1$: an integer.
- $\eta \in \mathbb{F}_{q^r}$: a primitive $(q^r - 1)$-th root of 1, or equivalently a primitive element of $\mathbb{F}_{q^r}$.
- $\mathcal{Tr} : \mathbb{F}_{q^r} \to \mathbb{F}_q$: the trace map defined as $x \mapsto x + x^q + \cdots + x^{q^{r-1}}$.
- $w(\mathbf{x})$ or $w_H(\mathbf{x})$: the Hamming weight of $\mathbf{x} \in \mathbb{F}_q^N$.

- The b-symbol Hamming weight $w_b(\mathbf{x})$ of $\mathbf{x} = (x_0, \dots, x_{N-1}) \in \mathbb{F}_q^N$ is defined as the Hamming weight of $\pi_b(\mathbf{x})$, where

$$\pi_b(\mathbf{x}) = ((x_0, \dots, x_{b-1}), (x_1, \dots, x_b), \cdots, (x_{N-1}, \dots, x_{b+N-2(\bmod N)})) \tag{1}$$

  is in $(\mathbb{F}_q^b)^N$. When $b = 1$, $w_1(\mathbf{x})$ is exactly the Hamming weight of $\mathbf{x}$.
- For any $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^N$, we have $\pi_b(\mathbf{x} + \mathbf{y}) = \pi_b(\mathbf{x}) + \pi_b(\mathbf{y})$, and the b-symbol distance (b-distance for short) $d_b(\mathbf{x}, \mathbf{y})$ between $\mathbf{x}$ and $\mathbf{y}$ is defined as $d_b(\mathbf{x}, \mathbf{y}) = w_b(\mathbf{x} - \mathbf{y})$.
- Let $A_i^{(b)}$ denote the number of codewords with b-symbol Hamming weight i in a code C of length n. The b-symbol Hamming weight enumerator of C is defined by

$$1 + A_1^{(b)} T + A_2^{(b)} T + \cdots + A_N^{(b)} T^n.$$

Motivation

- Ding *et al.* established a Singleton-type bound for b-symbol codes.
- Let $q \geq 2$ and $b \leq d_b(C) \leq n$. If C is an $(n, M, d_b(C))_q$ b-symbol code, then we have $M \leq q^{n-d_b(C)+b}$.
- An $(n, M, d_b(C))_q$ b-symbol code $\mathbb{C}$ with $M = q^{n-d_b(C)+b}$ is called a maximum distance separable (MDS for short) b-symbol code.
- For $a \in \mathbb{F}_{q^r}$, let $c(a) \in \mathbb{F}_q^n$ be the codeword defined as

$$c(a) = \left(\mathcal{Tr}(a\eta^{0\cdot N}), \mathcal{Tr}(a\eta^{1\cdot N}), \ldots, \mathcal{Tr}(a\eta^{j\cdot N}), \ldots, \mathcal{Tr}(a\eta^{(n-1)\cdot N})\right),$$

where $0 \leq j \leq n-1$.

Definition

Let $2 \leq b \leq r$ be an integer. It follows from [13, Corollary 4.1] that the set $\left\{1, \eta^N, \eta^{2N}, \ldots, \eta^{(b-1)N}\right\}$ is linearly independent over $\mathbb{F}_q$. Let $\mathcal{P}(b)$ be the subset of cardinality $(q^b - 1)/(q-1)$ in $\mathbb{F}_{q^r}^*$ defined as

$$\begin{aligned} \mathcal{P}(b) &= \bigcup_{j=1}^{b-1} \left\{\eta^{(j-1)N} + x_1\eta^{jN} + \cdots + x_{b-j}\eta^{(b-1)N} : x_1, \cdots, x_j \in \mathbb{F}_q\right\} \\ &\quad \cup \left\{\eta^{(b-1)N}\right\}. \end{aligned}$$

Definition

For $2 \leq b \leq r$, let

$$\mu(b) = \left|\left\{x \in \mathcal{P}(b) : x \text{ is a square in } \mathbb{F}_{q^r}^*\right\}\right|.$$

Example

Here are some numerical examples about $\mu(b)$ which computed by Magma.

p	q	r	N	b	$\mu(b)$
3	3	2	2	2	$2 = \frac{q^r-1}{2(q-1)}$
3	3	4	2	2	3
3	3	4	2	3	8
3	3	4	2	4	$20 = \frac{q^r-1}{2(q-1)}$
5	5	2	2	2	$3 = \frac{q^r-1}{2(q-1)}$
5	5	4	2	2	4
5	5	4	2	3	18
5	5	4	2	4	$78 = \frac{q^r-1}{2(q-1)}$
3	9	2	2	2	$5 = \frac{q^r-1}{2(q-1)}$
3	9	4	2	2	4
3	9	4	2	3	50
3	9	4	2	4	$410 = \frac{q^r-1}{2(q-1)}$
3	9	6	2	2	4
3	9	6	2	3	51
3	9	6	2	4	401
3	9	6	2	5	3728
3	9	6	2	6	$33215 = \frac{q^r-1}{2(q-1)}$
5	25	2	2	2	$13 = \frac{q^r-1}{2(q-1)}$
5	25	4	2	2	11
5	25	4	2	3	338
5	25	4	2	4	$8138 = \frac{q^r-1}{2(q-1)}$

Open Problem

Determine the invariant $\mu(b)$ when $2 \leq b < r$ or give *good* lower and upper bounds to $\mu(b)$.

The Main Results

Theorem

Let $a \in \mathbb{F}_{q^r}^*$. *Assume that* $2 \leq b < r$. *Then we determine* $w_b(c(a))$ *explicitly as follows:*

- *If* $p \equiv 1 \mod 4$ *and* a *is a square in* $\mathbb{F}_{q^r}^*$, *then*

$$\begin{aligned} w_b(c(a)) &= \frac{q^b - 1}{N(q-1)q^{b-1}} \left(q^r - \frac{q^r + (q-1)q^{r/2}}{q} \right) \\ &\quad + \frac{2\mu(b)(q-1)q^{r/2}}{Nq^b}. \end{aligned}$$

- *If* $p \equiv 1 \mod 4$ *and* a *is a non-square in* $\mathbb{F}_{q^r}^*$, *then*

$$\begin{aligned} w_b(c(a)) &= \frac{q^b - 1}{N(q-1)q^{b-1}} \left(q^r - \frac{q^r - (q-1)q^{r/2}}{q} \right) \\ &\quad - \frac{2\mu(b)(q-1)q^{r/2}}{Nq^b}. \end{aligned}$$

Theorem (Continue...)

- *If* $p \equiv 3 \mod 4$ *and* a *is a square in* $\mathbb{F}_{q^r}^*$, *then*

$$w_b(c(a)) = \frac{q^b-1}{N(q-1)q^{b-1}}\left(q^r - \frac{q^r+(-1)^{er/2}(q-1)q^{r/2}}{q}\right) + \frac{2\mu(b)(-1)^{er/2}(q-1)q^{r/2}}{Nq^b}.$$

- *If* $p \equiv 3 \mod 4$ *and* a *is a non-square in* $\mathbb{F}_{q^r}^*$, *then*

$$w_b(c(a)) = \frac{q^b-1}{N(q-1)q^{b-1}}\left(q^r - \frac{q^r-(-1)^{er/2}(q-1)q^{r/2}}{q}\right) - \frac{2\mu(b)(-1)^{er/2}(q-1)q^{r/2}}{Nq^b}.$$

Remark

The Hamming weight distribution of the above cyclic codes has been considered in [9], and C is a wto-weight code under the Hamming metric. In this paper we consider b-symbol weight distribution of such codes. Using the map π_b in (1), the problem becomes Hamming weight distribution of some 2-weight cyclic codes over the alphabet $\mathbb{F}_q \times \cdots \mathbb{F}_q = F_q^b$, which is not a field. We remark that two-weight irreducible cyclic codes *over finite fields* were characterized in [12], and it would be interesting to obtain such a characterization over the alphabet $\mathbb{F}_q^b$. We think that this would be related to Open Problem above.

Theorem

Let $a \in \mathbb{F}_{q^r}^*$. For $r \leq b < n$ we have

$$w_b(c(a)) = n.$$

Corollary

For $2 \leq b \leq r-1$, the b-symbol Hamming weight enumerator of C is

$$A(T) = 1 + \frac{q^r - 1}{2}\left(T^{u_1} + T^{u_2}\right),$$

where

$$u_1 = \begin{cases} \frac{q^b-1}{N(q-1)q^{b-1}}\left(q^r - \frac{q^r+(q-1)q^{r/2}}{q}\right) + \frac{2\mu(b)(q-1)q^{r/2}}{Nq^b} & \text{if } p \equiv 1 \mod 4, \\ \frac{q^b-1}{N(q-1)q^{b-1}}\left(q^r - \frac{q^r+(-1)^{er/2}(q-1)q^{r/2}}{q}\right) + \frac{2\mu(b)(-1)^{er/2}(q-1)q^{r/2}}{Nq^b} & \text{if } p \equiv 3 \mod 4, \end{cases}$$

and

$$u_2 = \begin{cases} \frac{q^b-1}{N(q-1)q^{b-1}}\left(q^r - \frac{q^r-(q-1)q^{r/2}}{q}\right) - \frac{2\mu(b)(q-1)q^{r/2}}{Nq^b} & \text{if } p \equiv 1 \mod 4, \\ \frac{q^b-1}{N(q-1)q^{b-1}}\left(q^r - \frac{q^r-(-1)^{er/2}(q-1)q^{r/2}}{q}\right) - \frac{2\mu(b)(-1)^{er/2}(q-1)q^{r/2}}{Nq^b} & \text{if } p \equiv 3 \mod 4. \end{cases}$$

For $r \leq b < n-1$, the b-symbol Hamming weight enumerator of C is

$$A(T) = 1 + (q^r - 1)T^n.$$

Moreover, C is an MDS b-symbol code when $b = r$.

References

1. Y. Cassuto and M. Blaum: Codes for symbol-pair read channels, in Proc. Int. Symp. Inf. Theory, Austin, TX, USA, Jun. (2010), pp. 988–992
2. Y. Cassuto and M. Blaum: Codes for symbol-pair read channels, IEEE Trans. Inform. Theory 57 (2011), no. 12, pp. 8011–8020.
3. Y. Cassuto and S. Litsyn: Symbol-pair codes: Algebraic constructions and asymptotic bounds, in Proc. Int. Symp. Inf. Theory, St. Petersburg, Russia, Jul./Aug. (2011), pp. 2348–2352.
4. Y.M. Chee, L. Ji, H.M. Kiah, C. Wang and J. Yin: Maximum distance separable codes for symbol pair read channels, IEEE Trans. Inform. Theory, 59 (2013), no. 11, pp. 7259–7267.
5. Y.M. Chee, H.M. Kiah, C. Wang and J. Yin: Maximum distance separable symbol-pair codes, In: Proc. IEEE Int. Symp. Inf. Theory, Cambridge, MA, USA, (2012), 2886–2890.
6. B. Chen, L. Lin and H. Liu: Constacyclic symbol-pair codes: lower bounds and optimal constructions, IEEE Trans. Inform. Theory 63 (2017) no. 12, pp. 7661–7666.
7. B. Ding, G. Ge, J. Zhang, T. Zhang and Y. Zhang: New constructions of MDS symbol-pair codes. Des. Codes Cryptogr., 86 (2018) no. 4, pp. 841–859.
8. B. Ding, T. Zhang and G. Ge: Maximum distance separable codes for b-symbol read channels, Finite Fields Appl., 49 (2018), pp. 180–197.

9. C. Ding and J. Yang: Hamming weights in irreducible cyclic codes, Discrete Math. 313 (2013), no. 4, pp. 434–446.
10. X. Kai, S. Zhu, and P. Li: A construction of new MDS symbol-pair codes, IEEE Trans. Inform. Theory 61 (2015), no. 11, pp. 5828–5834.
11. R. Lidl and H. Niederreiter: Finite Fields, Second Edition, Encyclopedia of Mathematics and its Applications, 20, Cambridge University Press, Cambridge, 1997.
12. B. Schmidt and C. White, All two-weight irreducible cyclic codes?, Finite Fields Appl. 8 (2002), no. 1, pp. 1–17.
13. M. Shi, F. ¨Ozbudak and P. Sol´e : Geometric Approach to b-Symbol Hamming Weights of Cyclic Codes, IEEE Trans. Inform. Theory, accepted, 2021.
14. Z. Sun, S. Zhu and L. Wang: The symbol-pair distance distribution of a class of repeated-root cyclic codes over Fpm, Cryptogr. Commun.,10 (2018), no. 4, pp. 643–653.
15. E. Yaakobi, J. Bruck and P. H. Siegel: Constructions and Decoding of Cyclic Codes Over b-Symbol Read Channels, IEEE Trans. Inform. Theory 62 (2016), no. 4, pp. 1541–1551.

Lastly...

Thank you!