



HAL
open science

Geometric Approach to b -Symbol Hamming Weights of Cyclic Codes

Minjia Shi, Ferruh Ozbudak, Patrick Solé

► **To cite this version:**

Minjia Shi, Ferruh Ozbudak, Patrick Solé. Geometric Approach to b -Symbol Hamming Weights of Cyclic Codes. IEEE Transactions on Information Theory, 2021, pp.1 - 1. <10.1109/tit.2021.3069772>. <hal-03189478>

HAL Id: hal-03189478

<https://hal.science/hal-03189478v1>

Submitted on 3 Apr 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

Geometric Approach to b -Symbol Hamming Weights of Cyclic Codes

Minjia Shi¹, Ferruh Özbudak², and Patrick Solé

Abstract—Symbol-pair codes were introduced by Cassuto and Blaum in 2010 to protect pair errors in symbol-pair read channels. Recently Yaakobi, Bruck and Siegel (2016) generalized this notion to b -symbol codes in order to consider consecutive b errors for a prescribed integer $b \geq 2$, and they gave constructions and decoding algorithms. Cyclic codes were considered by various authors as candidates for symbol-pair codes and they established minimum distance bounds on (certain) cyclic codes. In this paper we use algebraic curves over finite fields in order to obtain tight lower and upper bounds on b -symbol Hamming weights of arbitrary cyclic codes over \mathbb{F}_q . Here $b \geq 2$ is an arbitrary prescribed positive integer and \mathbb{F}_q is an arbitrary finite field. We also present a stability theorem for an arbitrary cyclic code C of dimension k and length n : the b -symbol Hamming weight enumerator of C is the same as the k -symbol Hamming weight enumerator of C if $k \leq b \leq n - 1$. Moreover, we give improved tight lower and upper bounds on b -symbol Hamming weights of some cyclic codes related to irreducible cyclic codes. Throughout the paper the length n is coprime to q .

Index Terms—Cyclic code, b -symbol error, algebraic curve, Weil-Serre bound, irreducible cyclic code.

I. INTRODUCTION

SYMBOL-PAIR codes were introduced by Cassuto and Blaum [2], [3] to combat symbol-pair errors in symbol-pair channels. This model was used to address channels with high write resolution but low read resolution, so that individual symbols cannot be read off due to physical limitations. In this new model the errors are no longer individual symbol errors, but rather symbol-error pair errors, where in a symbol-pair error at least one of the symbols is erroneous.

The seminal works [2]–[4] established relationships between the minimum Hamming distance of an error correcting code

and the minimum pair distance, constructed some codes for pair distance and gave decoding algorithms.

The minimum pair distance of linear cyclic codes has been studied by Cassuto and Blaum [3], Kai *et al.* [13], and recently by Yaakobi *et al.* [19]. In particular, Yaakobi *et al.* obtained an elegant result on the pair distance of binary cyclic codes of dimension at least 2: $d_2(C) \geq d_1(C) + \lceil \frac{d_1(C)}{2} \rceil \simeq \frac{3}{2}d_1(C)$, where $d_2(C)$ is the minimum pair distance of C and $d_1(C)$ is the minimum (Hamming) distance of C . Moreover, in [19] they considered the more general problem of consecutive b -symbol errors instead of only 2-symbol errors for a prescribed integer $b \geq 2$. They generalized some results of $b = 2$ to the case of $b \geq 2$.

Let \mathbb{F}_q be an arbitrary finite field. In this paper we use algebraic curves over finite fields (equivalently algebraic function fields over finite fields) in order to study lower and upper bounds on an arbitrary cyclic code C over \mathbb{F}_q of length n , where b is a prefixed integer such that $2 \leq b \leq n - 1$. Our main contributions are:

- We obtain tight lower and upper bounds for b -symbol Hamming weights of arbitrary cyclic codes.
- We give a stability theorem for b -symbol Hamming weights: if C is an arbitrary cyclic code of length n and dimension k , then for any integer b in the range $k \leq b \leq n - 1$ the b -symbol Hamming weight enumerator of C is the same as the k -symbol Hamming weight enumerator of C .
- We obtain improved lower and upper bounds for b -symbol Hamming weights of some cyclic codes related to irreducible cyclic codes.

We also find a connection between maximal and minimal curves over finite fields and the lower and upper bounds of b -symbol Hamming weights of arbitrary cyclic codes. Using this connection and inspired by the important result $d_2(C) \geq \frac{3}{2}d_1(C)$ of Yaakobi *et al.* [19, Theorem 1], we obtain further inequalities between $d_{b+\delta}(C)$ and $d_b(C)$ for some cyclic codes C .

For any code C of length n over \mathbb{F}_q , there is a canonical code $C^{(b)}$ of length n over the alphabet \mathbb{F}_q^b such that the b -symbol Hamming weight enumerator of C is the same as the Hamming weight enumerator of C . This follows naturally from the definition by an explicit \mathbb{F}_q -linear map π_b . We could not find this map in the literature and we explain it in Section 2 below.

The rest of the paper is organized as follows: We give some preliminaries and further notation in Section 2. We present a

Manuscript received September 14, 2019; revised October 31, 2020; accepted March 13, 2021. This work was supported in part by the National Natural Science Foundation of China under Grant 12071001 and Grant 61672036, in part by the Excellent Youth Foundation of Natural Science Foundation of Anhui Province under Grant 1808085J20, in part by the Academic Fund for Outstanding Talents in Universities under Grant gxbjZD03; and in part by the Natural Science Foundation of Anhui Province under Grant 2008085QA04. (Corresponding author: Minjia Shi.)

Minjia Shi is with the Key Laboratory of Intelligent Computing Signal Processing, Ministry of Education, School of Mathematical Sciences, Anhui University, Hefei 230601, China (e-mail: smjwcl.good@163.com).

Ferruh Özbudak is with the Department of Mathematics, Institute of Applied Mathematics, Middle East Technical University, 06800 Ankara, Turkey (e-mail: ozbudak@metu.edu.tr).

Patrick Solé is with I2M, Aix Marseille University, Centrale Marseille, CNRS, 13007, Marseille, France (e-mail: sole@enst.fr).

Communicated by S. Gharpade, Associate Editor for Coding Theory. Digital Object Identifier 10.1109/TIT.2021.3069772

79 trace representation of $C^{(b)}$ in Section 3, that we use in our
80 proofs. We specialize to a subclass of cyclic codes related to
81 irreducible cyclic codes in Section 4. This allows us to present
82 some of our methods in detail and we also get improved
83 bounds on the b -symbol weights in this subclass. We give
84 our results for arbitrary cyclic codes in Section 5. We also
85 have an appendix providing background material on algebraic
86 function fields that we use in Section 4 and 5. We conclude
87 in Section 6.

88 II. PRELIMINARIES

89 We start by fixing a part of our notation:

- 90 • \mathbb{F}_q : finite field with q elements.
- 91 • $n \geq 3$: an integer with $\gcd(n, q) = 1$.
- 92 • $2 \leq b \leq n - 1$: an integer.
- 93 • For a finite set A , let $|A|$ denote its cardinality.
- 94 • C : an \mathbb{F}_q -linear subspace of \mathbb{F}_q^n . We assume that $|C| > 1$
95 omitting the trivial case. C is called a *linear code* of
96 *length n* over \mathbb{F}_q . We also refer C just as *code* throughout
97 this paper. Elements of C are called codewords of C .
- 98 • $k = \dim_{\mathbb{F}_q} C$.

99 We present further notation and preliminaries in the follow-
100 ing subsections.

101 A. Hamming Weight, Hamming Distance and Hamming 102 Weight Enumerator

103 Let \mathbb{A} be a nonempty finite set, which stands for the
104 alphabet to be fixed. Throughout the paper \mathbb{A} becomes \mathbb{F}_q
105 or $\mathbb{F}_q^b = \underbrace{\mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{b \text{ times}}$. Let $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{A}^n$ and
106 $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{A}^n$. The *Hamming weight* $\|\alpha\|$ of α is
107 the nonnegative integer

$$108 \|\alpha\| = |\{1 \leq i \leq n : \alpha_i \neq 0\}|.$$

109 The *Hamming distance* $d(\alpha, \beta)$ between α and β is the
110 nonnegative integer

$$111 d(\alpha, \beta) = |\{1 \leq i \leq n : \alpha_i \neq \beta_i\}|.$$

112 Let $\mathcal{C} \subseteq \mathbb{A}^n$ be a subset with $|\mathcal{C}| \geq 2$. The *minimum Hamming
113 distance* $d(\mathcal{C})$ of \mathcal{C} is the integer

$$114 d(\mathcal{C}) = \min\{d(\alpha, \beta) : \alpha, \beta \in \mathcal{C} \text{ and } \alpha \neq \beta\}.$$

115 If \mathcal{C} is further closed under addition, then it is well known and
116 easy to observe that

$$117 d(\mathcal{C}) = \min\{\|\alpha\| : \alpha \neq \mathbf{0}\}.$$

118 Assume that $\mathcal{C} \subseteq \mathbb{A}^n$ is a subset which is closed under
119 addition. For $0 \leq i \leq n$, let A_i be the nonnegative integer

$$120 A_i = |\{\alpha \in \mathcal{C} : \|\alpha\| = i\}|.$$

121 The polynomial $A(Z) = A_0 + A_1 Z + \cdots + A_n Z^n \in \mathbb{Z}[Z]$ with
122 these nonnegative integer coefficients is called the *Hamming
123 weight enumerator* of \mathcal{C} .

124 B. b -Symbol Hamming Weight, b -Symbol Hamming Minimum 125 Distance and b -Symbol Hamming Weight Enumerator

126 Recall that b is an integer with $2 \leq b \leq n - 1$. Let $\pi_b : \mathbb{F}_q^n \rightarrow (\mathbb{F}_q^b)^n$ the map

$$127 (\alpha_0, \dots, \alpha_i, \dots, \alpha_{n-1}) \mapsto ((\alpha_0, \alpha_1, \dots, \alpha_{b-1}), \dots, \\ 128 (\alpha_i, \alpha_{i+1}, \dots, \alpha_{i+b-1}), \dots, \\ 129 (\alpha_{n-1}, \alpha_0, \dots, \alpha_{n+b-1})), \quad 130$$

131 where the indices are modulo n . It is clear that π_b is an
132 \mathbb{F}_q -linear map.

133 *Example 1:* For $q = 2$, $n = 4$, $b = 3$ and $\alpha =$
134 $(0, 1, 1, 0) \in \mathbb{F}_2^4$ we have

$$135 \pi_3(\alpha) = ((0, 1, 1), (1, 1, 0), (1, 0, 0), (0, 0, 0), (0, 0, 1)) \\ 136 \in (\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2)^5.$$

137 The Hamming weight of $\pi_3(\alpha)$ over the alphabet $\mathbb{A} = \mathbb{F}_2 \times$
138 $\mathbb{F}_2 \times \mathbb{F}_2$ is $1 + 1 + 1 + 0 + 1 = 4$ (see Subsection II-A).

139 Put $\mathbb{A} = \underbrace{\mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{b \text{ times}}$. Recall that $C \subseteq \mathbb{F}_q^n$ is a linear code

140 of length n over \mathbb{F}_q . Let $C^{(b)} = \pi_b(C) \subseteq \mathbb{A}^n$ be the image of
141 C under the \mathbb{F}_q -linear map π_b . Note that $C^{(b)}$ is closed under
142 addition. Using the notation of Subsection II-A, the Hamming
143 weight minimum distance of $C^{(b)}$ and the Hamming weight
144 enumerator of $C^{(b)}$ are well defined. The Hamming weight
145 minimum distance of $C^{(b)}$ is called the *b -symbol Hamming
146 minimum distance* of C . The Hamming weight enumerator
147 of $C^{(b)}$ is called the *b -symbol Hamming weight enumerator*
148 of C . Similarly for a codeword $c \in C$, the Hamming weight
149 of $\pi_b(c) \in \mathbb{A}^n$ is called the *b -symbol Hamming weight* of c .

150 We also denote C as $C^{(1)}$.

151 C. Cyclic Code of Length n Over \mathbb{F}_q and Its Nonzero Set

152 We further fix and assume the following from now on
153 throughout the paper:

- 154 • $r \geq 2$: an integer such that $n \mid (q^r - 1)$.
- 155 • $\eta \in \mathbb{F}_{q^r}^*$: a primitive n -th root of 1.
- 156 • C : an arbitrary (if not stated otherwise) *cyclic* code of
157 length n over \mathbb{F}_q .

158 The existence of r follows by the assumption that
159 $\gcd(n, q) = 1$.

160 We need to introduce some basic facts on cyclic codes.
161 We refer, for example [15], for the details. It is possible
162 to identify an element $(a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_q^n$ with the
163 polynomial $a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} \in \mathbb{F}_q[z]$. Let R be
164 the quotient ring of $\mathbb{F}_q[z]$ given by $R = \mathbb{F}_q[z] / \langle z^n - 1 \rangle$.
165 Using this identification, cyclic codes of length n over \mathbb{F}_q are
166 exactly ideals of R .

167 Let I be the ideal of R corresponding to C . It is well known
168 that the ideals of R are principal. Hence there exists a uniquely
169 determined monic polynomial $g(z) \in \mathbb{F}_q[z]$ of smallest degree
170 such that $g(z) + \langle z^n - 1 \rangle \in I$. This polynomial is called
171 the *generator polynomial* of C . Recall that k is the dimension
172 of C over \mathbb{F}_q . It is well known that $\deg g(z) = n - k$ and
173 $g(z) \mid (z^n - 1)$ in the polynomial ring $\mathbb{F}_q[z]$.

As $n \mid (q^r - 1)$, there is no repeated root of $g(z)$ and $g(z)$ splits into its linear factors over \mathbb{F}_{q^r} . Let $S \subseteq \{0, 1, \dots, n-1\}$ be the subset such that the roots of $g(z)$ are exactly $\{\eta^i : i \in S\}$. Let \tilde{S} be the complement, i.e. $\tilde{S} = \{0, 1, \dots, n-1\} \setminus S$. Let $U \subseteq \{0, 1, \dots, n-1\}$ be the subset of cardinality k defined as $U = \{-j \pmod n : j \in \tilde{S}\}$. We call U the nonzero set of C .

Example 2: Let $q = 4$, $n = 21$ and $r = 3$. Let $\eta \in \mathbb{F}_{4^3}^*$ be a primitive 21-th root of 1. We choose η as a root of $x^6 + x^5 + x^4 + x^2 + 1 \in \mathbb{F}_2[x]$. Let

$$\begin{aligned} g(z) &= (z - \eta^9)(z - \eta^{15})(z - \eta^{18})(z - \eta^5) \\ &\quad (z - \eta^{20})(z - \eta^{17})(z - \eta^{10})(z - \eta^{19}) \\ &\quad (z - \eta^{13})(z - \eta^7). \end{aligned}$$

It turns out that $g(z) \in \mathbb{F}_4[z]$. Namely we have

$$\begin{aligned} g(z) &= z^{10} + \theta z^9 + \theta z^8 + \theta^2 z^7 + z^6 + \theta z^5 \\ &\quad + \theta^2 z^4 + z^2 + \theta z + \theta^2, \end{aligned} \quad (1)$$

where $\theta \in \mathbb{F}_4$ with $\theta^2 + \theta + 1 = 0$. It is clear that $g(z) \mid (z^{21} - 1)$ over \mathbb{F}_4 . Let C be the cyclic code of length 21 over \mathbb{F}_4 generated by $g(z)$. Under notation above we have

$$\begin{aligned} S &= \{5, 7, 9, 10, 13, 15, 17, 18, 19, 20\}, \\ \tilde{S} &= \{0, 1, 2, 3, 4, 6, 8, 11, 12, 14, 16\} \end{aligned}$$

and hence the nonzero set U of C is given by

$$U = \{0, 5, 7, 9, 10, 13, 15, 17, 18, 19, 20\}.$$

We also fix the following from now on throughout the paper:

- $U \subseteq \{0, 1, \dots, n-1\}$: the nonzero set of C .

Note that U and C determine each other uniquely.

D. Trace Representation of a Cyclic Code

In this subsection we present a trace representation of C . We use well known methods, see for example, [16, Chapter 9] and the references therein.

The cyclic group $\text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ is generated by the Frobenius automorphism $x \mapsto x^q$. There is an action of $\text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ on $\{0, 1, \dots, n-1\}$. The action of the Frobenius automorphism is given as follows: $u \in \{0, 1, \dots, n-1\} \mapsto uq \pmod n \in \{0, 1, \dots, n-1\}$. For any integer $u \in \{0, 1, \dots, n-1\}$, the orbit $\{u^i \pmod n \in \{0, 1, \dots, n-1\} : 0 \leq i \leq r-1\}$ of u under this action is called the q -cyclotomic coset of u modulo n . A subset $A \subseteq \{0, 1, \dots, n-1\}$ is called *closed* if $u \in A$ implies that $uq \pmod n \in A$. A closed set is a disjoint union of q -cyclotomic cosets modulo n .

Recall that U is the nonzero set of the cyclic code C . It is well known that U is a closed set and hence U is a disjoint union of q -cyclotomic cosets modulo n . Note that the disjoint decomposition of U into its disjoint subsets, which are q -cyclotomic cosets modulo n , is uniquely determined. Let U_0 be a subset of U such that there is exactly one element in U_0 for each q -cyclotomic coset modulo n in this disjoint decomposition of U . Note that U_0 is not uniquely determined in general. We call that U_0 is a *basic nonzero set* of C .

We further fix the following from now on throughout the paper:

- $\text{Tr} : \mathbb{F}_{q^r} \rightarrow \mathbb{F}_q$: the trace map defined as $x \mapsto x + x^q + \dots + x^{q^{r-1}}$.

Note that Tr is a surjective and \mathbb{F}_q -linear map.

For $U_0 = \{u_1, u_2, \dots, u_\rho\}$, let $P(U_0)$ denote the \mathbb{F}_{q^r} -linear subspace of $\mathbb{F}_{q^r}[x]$ defined as

$$P(U_0) = \{a_1 x^{u_1} + \dots + a_\rho x^{u_\rho} : a_1, \dots, a_\rho \in \mathbb{F}_{q^r}\}.$$

For $f(x) \in P(U_0)$, we use the short notation $\underline{\text{Tr}(f(x))}$ for the n -tuple

$$\underline{\text{Tr}(f(x))} = (\text{Tr}(f(\eta^0)), \dots, \text{Tr}(f(\eta^{n-1}))) \in \mathbb{F}_q^n.$$

It is well known that we have a *trace representation* for C given by

$$C = \{\underline{\text{Tr}(f(x))} : f \in P(U_0)\},$$

where we are free to choose an arbitrary basic nonzero set U_0 of C . Namely, a generic element $c = (c_0, c_1, \dots, c_{n-1})$ of C is given by

$$c = \underline{\text{Tr}(f(x))} \in \mathbb{F}_q^n \text{ and } f \in P(U_0).$$

Hence for $f \in P(U_0)$, we also use the notation $c(f)$ to denote the codeword

$$c(f) = (\text{Tr}(f(1)), \text{Tr}(f(\eta)), \dots, \text{Tr}(f(\eta^{n-1})))$$

of C .

Example 3: Let $q = 4$, $n = 21$ and $r = 3$. We keep the notation of Example 2. Hence $\eta \in \mathbb{F}_{4^3}^*$ is a primitive 21-th root of 1 as in Example 2.

All 4-cyclotomic cosets modulo 21 are as follows:

$$\begin{aligned} \bar{0} &= \{0\}, \bar{1} = \{1, 4, 16\}, \bar{2} = \{2, 8, 11\}, \\ \bar{3} &= \{3, 12, 6\}, \bar{5} = \{5, 20, 17\}, \bar{7} = \{7\}, \\ \bar{9} &= \{9, 15, 18\}, \bar{10} = \{10, 19, 13\}, \bar{14} = \{14\}. \end{aligned}$$

Let C be the cyclic code of length 21 over \mathbb{F}_4 defined in Example 2. We observe that the nonzero set U of C is a disjoint union of 4-cyclotomic cosets modulo 21 given by

$$\begin{aligned} U &= \{0\} \sqcup \{5, 10, 17\} \sqcup \{7\} \sqcup \{9, 15, 18\} \\ &\quad \sqcup \{10, 19, 13\}, \end{aligned} \quad (2)$$

where \sqcup indicates that the subsets $\{0\}, \dots, \{10, 19, 13\}$ are pairwise disjoint. Hence a basic nonzero set U_0 of C is

$$U_0 = \{0, 5, 7, 9, 10\}.$$

For an arbitrary codeword $\mathbf{c} = (c_0, c_1, \dots, c_{20})$ of $C \subseteq \mathbb{F}_4^{21}$, there exists $f(x) \in P(U_0) = \{a_0 + a_5 x^5 + a_7 x^7 + a_9 x^9 + a_{10} x^{10} : a_0, a_5, a_7, a_9, a_{10} \in \mathbb{F}_{4^3}\}$ such that $\mathbf{c} = c(f)$. Namely there exist $a_0, a_5, a_7, a_9, a_{10} \in \mathbb{F}_{4^3}$ such that

$$c_i = \text{Tr}(a_0 + a_5 \eta^{5i} + a_7 \eta^{7i} + a_9 \eta^{9i} + a_{10} \eta^{10i})$$

for $0 \leq i \leq 20$, where Tr is the trace map from \mathbb{F}_{4^3} onto \mathbb{F}_4 .

III. TRACE REPRESENTATIONS OF $C^{(b)}$

Note that the b -symbol Hamming weights of codewords of C are defined in terms of the Hamming weights of the codewords of $C^{(b)}$ over the alphabets \mathbb{F}_q^b . We refer to Subsection II-B for a definition of the code $C^{(b)}$.

In this section we present a trace representation of $C^{(b)}$, where C is an arbitrary cyclic code over \mathbb{F}_q of length coprime to q . This section is one of the contributions of this paper as we could not find such an approach for the b -symbol Hamming weights of codewords of C in the literature.

First we need a definition.

Definition III.1: For any integer $0 \leq t \leq n-1$ and $f \in P(U_0)$, let $f^{(t)}$ denote the polynomial in $P(U_0)$ given by

$$f^{(t)}(x) = f(\eta^t x).$$

We give our trace representation in the next theorem. We will use this representation in our proofs.

Theorem III.2: Let C be an arbitrary cyclic code over \mathbb{F}_q of length coprime to q . Let $2 \leq b \leq n-1$ be an integer. For the code $C^{(b)}$ of length n over the alphabet \mathbb{F}_q^b we have

$$C^{(b)} = \left\{ \left(\underline{\text{Tr}(f(\eta))}, \dots, \underline{\text{Tr}(f(\eta^{b-1}))} \right) : f \in P(U_0) \right\}.$$

A generic element $(\beta_0, \dots, \beta_{n-1})$ of $C^{(b)}$ is given by

$$\beta_i = \left(\text{Tr}(f(\eta^i)), \text{Tr}(f^{(1)}(\eta^i)), \dots, \text{Tr}(f^{(b-1)}(\eta^i)) \right) \in \mathbb{F}_q^b$$

$f \in P(U_0)$, $0 \leq i \leq n-1$.

Proof: Let $f \in P(U_0)$ and $c(f) \in C$ be the corresponding codeword of the cyclic code C . We have

$$\begin{aligned} c(f) &= (c_0, c_1, \dots, c_{n-1}) \\ &= (\text{Tr}(f(\eta^0)), \text{Tr}(f(\eta^1)), \dots, \text{Tr}(f(\eta^{n-1}))). \end{aligned} \quad (3)$$

Let $c^{(b)}(f) = \pi_b(c(f))$ be the corresponding codeword of $C^{(b)}$. Putting $c^{(b)}(f) = (\beta_0, \beta_1, \dots, \beta_{n-1})$ we obtain that $\beta_i = (c_i, c_{i+1}, \dots, c_{i+b-1}) \in \mathbb{F}_q^b$, where

$$c_{i+\ell} = \text{Tr}(f(\eta^{i+\ell})) \quad (4)$$

for $0 \leq \ell \leq b-1$ and $0 \leq i \leq n-1$. It follows from Definition III.1 that $f^{(\ell)}(x) = f(\eta^\ell x)$ for $0 \leq \ell \leq b-1$. Hence we have that

$$f^{(\ell)}(\eta^i) = f(\eta^\ell \eta^i) = f(\eta^{i+\ell}) \quad (5)$$

for $0 \leq \ell \leq b-1$, and $0 \leq i \leq n-1$. Combining (4) and (5) we complete the proof. \square

Example 4: Let $q = 4$, $n = 21$ and $r = 3$. Let C be the cyclic code of length 21 over \mathbb{F}_4 considered in Examples 2 and 3. We keep the notation of Examples 2 and 3. In particular $\eta \in \mathbb{F}_{4^3}^*$ is a primitive 21-th root of 1. Put $b = 3$.

For an arbitrary element $(\beta_0, \beta_1, \dots, \beta_{20})$ of $C^{(3)} \in (\mathbb{F}_4 \times \mathbb{F}_4 \times \mathbb{F}_4)^{21}$, there exist $a_0, a_5, a_7, a_9, a_{10} \in \mathbb{F}_{4^3}$ such that

$$\begin{aligned} \beta_i &= \left(\text{Tr}(a_0 + a_5 \eta^{5i} + a_7 \eta^{7i} + a_9 \eta^{9i} + a_{10} \eta^{10i}), \right. \\ &\quad \text{Tr}(a_0 + a_5 \eta^{5+5i} + a_7 \eta^{7+7i} + a_9 \eta^{9+9i} + a_{10} \eta^{10+10i}), \\ &\quad \left. \text{Tr}(a_0 + a_5 \eta^{10+5i} + a_7 \eta^{14+7i} + a_9 \eta^{18+9i} + a_{10} \eta^{20+10i}) \right) \end{aligned}$$

for $0 \leq i \leq 20$.

IV. b -SYMBOL WEIGHTS FOR SOME CYCLIC CODES

Throughout this section we assume that C is a cyclic code of length n dividing $q^r - 1$ whose nonzero set is exactly one q -cyclotomic coset U in $\mathbb{Z}/n\mathbb{Z}$. If $U = \{0\}$, then C is a repetition code and any b -symbol Hamming weight of any nonzero codeword c of C is n for any $1 \leq b \leq n-1$. Hence we further assume that there exists an integer $1 \leq u \leq n-1$ such that $u \in U$.

There is a close connection of the codes of this section to irreducible cyclic codes. We explain this connection explicitly after Theorem IV.3 below. It is well known that it is a notoriously difficult open problem to determine the weight distribution of irreducible cyclic codes in general (see, for example, [5]).

First we present a useful stability theorem. We start with some notation.

For $1 \leq t \leq n-1$, let $V(t) = \text{Span}_{\mathbb{F}_q} \{1, \eta^u, \dots, \eta^{(t-1)u}\}$. Note that on the difference of consecutive dimensions we have

$$(\dim_{\mathbb{F}_q} V(t+1) - \dim_{\mathbb{F}_q} V(t)) \in \{0, 1\} \text{ for all } t. \quad (6)$$

The following definition is useful.

Definition IV.1: Let μ be the largest positive integer t such that $\dim_{\mathbb{F}_q} V(t) = t$.

The next lemma gives an alternative definition of μ and it shows that μ is independent from the choice of primitive n -th root of unity and from the choice of $u \in U$.

Lemma IV.2: Under notation above, for μ given in Definition IV.1 we have $\mu = \dim_{\mathbb{F}_q} \mathbb{F}_q(\eta^u)$, where $\mathbb{F}_q(\eta^u)$ is the smallest finite field extension of \mathbb{F}_q containing η^u .

Proof: It follows from (6) and Definition IV.1 that μ is the smallest positive integer t satisfying

$$\eta^{u(t+i)} \in \text{Span}_{\mathbb{F}_q} \{1, \eta^u, \dots, \eta^{u(t-1)}\},$$

for all integers $i \geq 0$. Equivalently μ is the smallest positive integer t such that $\mathbb{F}_q[\eta^u] \in \text{Span}_{\mathbb{F}_q} \{1, \eta^u, \dots, \eta^{u(t-1)}\}$. This means that $\mathbb{F}_q(\eta^u) = \mathbb{F}_q[\eta^u] = \text{Span}_{\mathbb{F}_q} \{1, \eta^u, \dots, \eta^{u(t-1)}\}$. \square

Corollary 1: Under notation above, for μ given in Definition IV.1 the following equivalent characterizations hold:

- $\mu = \dim_{\mathbb{F}_q} \mathbb{F}_q(\eta^u)$.
- $\mu = \dim_{\mathbb{F}_q} C$.
- μ is the multiplicative order of q modulo $\frac{n}{\gcd(n,u)}$.
- μ is the size of the q -cyclotomic coset U (containing u) in $\mathbb{Z}/n\mathbb{Z}$.

Proof: The multiplicative order of η^u is $\frac{n}{\gcd(n,u)}$. Hence we have that $\dim_{\mathbb{F}_q} \mathbb{F}_q(\eta^u) = \mu$ if and only if μ is the smallest integer r such that $\frac{n}{\gcd(n,u)}$ divides $q^r - 1$. In particular this means that μ is the multiplicative order of q modulo $\frac{n}{\gcd(n,u)}$.

Let U be the nonzero set of C . It follows from the definition of the nonzero set (see Subsection II-C) that $\dim_{\mathbb{F}_q} C$ is the size of U . Note that U is the q -cyclotomic coset containing u in $\mathbb{Z}/n\mathbb{Z}$ as the nonzero set of C consists of exactly one q -cyclotomic coset by assumption in this section. The size of U is the smallest integer r such that $q^r u \equiv u \pmod{n}$. This means that the size of U is the smallest integer r such that $\frac{n}{\gcd(n,u)}$ divides $q^r - 1$. Combining the arguments above we complete the proof. \square

First we present our stability theorem in the special case of this section. Basically it says that the b -symbol Hamming weight enumerators of C are the same for all b -symbol Hamming weights if $b \geq \dim_{\mathbb{F}_q}(C)$. There exists a nonempty stability region always except the trivial case that $\dim_{\mathbb{F}_q} C = n - 1$. We generalize the next result to arbitrary cyclic codes in Theorem V.2 below, whose proof is more involved.

Theorem IV.3: Assume that $\gcd(n, q) = 1$. Let C be a cyclic code of length n such that its nonzero set is exactly one q -cyclotomic coset U of $\mathbb{Z}/n\mathbb{Z}$. Assume that $U \neq \{0\}$ and let $u \in U$. Let $k = \dim_{\mathbb{F}_q} C$. For any integer b in the interval $k \leq b \leq n - 1$, the b -symbol Hamming weight enumerator of C is the same as the k -symbol Hamming weight enumerator of C .

Proof: Let $f(x) = ax^u \in \mathbb{F}_{q^r}[x] \setminus \{0\}$ be an arbitrary nonzero polynomial in $P(\{u\})$. Let $c^{(k)}(f) \in C^{(k)}$ and $c^{(b)}(f) \in C^{(b)}$ be the corresponding codewords, where we refer to Theorem III.2 for the explicit descriptions of the codewords. Note that

$$c^{(b)}(f) = \left(\text{Tr}(f(\eta)), \text{Tr}(f^{(1)}(\eta)), \dots, \text{Tr}(f^{(b)}(\eta)) \right).$$

Putting $c^{(b)}(f) = (c_0^{(b)}(f), c_1^{(b)}(f), \dots, c_{n-1}^{(b)}(f)) \in (\mathbb{F}_q^b)^n$, for the symbols of $c^{(b)}(f)$ in the alphabet \mathbb{F}_q^b we observe that

$$c_i^{(b)}(f) = \left(\text{Tr}(a\eta^{ui}), \text{Tr}(\eta^u a\eta^{ui}), \dots, \text{Tr}(\eta^{(b-1)u} a\eta^{ui}) \right). \quad (7)$$

Similarly for the symbols of $c^{(k)}(f)$ in the alphabet \mathbb{F}_q^k we observe that

$$c_i^{(k)}(f) = \left(\text{Tr}(a\eta^{ui}), \text{Tr}(\eta^u a\eta^{ui}), \dots, \text{Tr}(\eta^{(k-1)u} a\eta^{ui}) \right). \quad (8)$$

Using Corollary 1 we get

$$\begin{aligned} Q &:= \text{Span}_{\mathbb{F}_q} \{1, \eta^u, \dots, \eta^{(k-1)u}\} \\ &= \text{Span}_{\mathbb{F}_q} \{1, \eta^u, \dots, \eta^{(b-1)u}\} \end{aligned}$$

Hence if $\alpha \in \mathbb{F}_{q^r}$, then

$$\begin{aligned} 0 &= \text{Tr}(\alpha) = \text{Tr}(\eta^u \alpha) = \dots = \text{Tr}(\eta^{(k-1)u} \alpha) \\ &\iff 0 = \text{Tr}(\alpha) = \text{Tr}(\eta^u \alpha) = \dots = \text{Tr}(\eta^{(b-1)u} \alpha). \end{aligned} \quad (9)$$

Using (7) and (8) this implies that $c_i^{(k)}(f)$ contributes to the Hamming weight of the codeword $c^{(k)}(f)$ of length n over the alphabet \mathbb{F}_q^k if and only if $c_i^{(b)}(f)$ contributes to the Hamming weight of the codeword $c^{(b)}(f)$ of length n over the alphabet \mathbb{F}_q^b . Therefore the values of the Hamming weights (defined over their respective alphabets) of $c^{(k)}(f)$ and $c^{(b)}(f)$ are the same. This completes the proof. \square

Remark 1: We note that Theorem IV.3 (and hence Theorem V.2 below) has useful engineering consequences in applications. For example it implies that increasing b for b -symbol for error correcting does give any further advantage if $b \geq k$ for these codes.

Now we explain the connection of the codes of this section to irreducible cyclic codes. Let $m = \gcd(u, n)$ and put $\bar{n} = n/m$. Note that $\eta^{ui} = \eta^{u(i+\bar{n})}$ for $i \geq 0$ as $\eta^{u\bar{n}} = \eta^{n \frac{u}{m}} = 1$. For a codeword $c = (c_0, c_1, \dots, c_{n-1}) \in C$ and a codeword $c^{(b)} = (c_0^{(b)}, c_1^{(b)}, \dots, c_{n-1}^{(b)}) \in C^{(b)}$, let $\bar{c} \in \mathbb{F}_q^{\bar{n}}$

and $\bar{c}^{(b)} \in (\mathbb{F}_q^{\bar{n}})^{\bar{n}}$ be the corresponding elements defined as the shortenings

$$\bar{c} = (c_0, c_1, \dots, c_{\bar{n}-1}) \text{ and } \bar{c}^{(b)} = (c_0^{(b)}, c_1^{(b)}, \dots, c_{\bar{n}-1}^{(b)}) \quad (10)$$

to the first \bar{n} symbols. Let $\bar{C} \subseteq \mathbb{F}_q^{\bar{n}}$ and $\bar{C}^{(b)} \subseteq (\mathbb{F}_q^{\bar{n}})^{\bar{n}}$ be the codes defined as

$$\bar{C} = \{\bar{c} : c \in C\} \text{ and } \bar{C}^{(b)} = \{\bar{c}^{(b)} : c^{(b)} \in C^{(b)}\}. \quad (11)$$

Using the fact that $\eta^{ui} = \eta^{u(i+\bar{n})}$ for $i \geq 0$ we observe $\pi_b(\bar{C}) = \bar{C}^{(b)}$. Moreover, between the Hamming weights of c , \bar{c} , $c^{(b)}$ and $\bar{c}^{(b)}$ we have the relations

$$w_H(\bar{c}) = \frac{1}{m} w_H(c) \text{ and } w_H(\bar{c}^{(b)}) = \frac{1}{m} w_H(c^{(b)}). \quad (12)$$

Let $\theta = \eta^u \in \mathbb{F}_{q^r}^*$, which is a primitive \bar{n} -th root of 1. We observe that \bar{C} is the irreducible cyclic code of length \bar{n} over \mathbb{F}_q having the trace representation

$$\bar{C} = \{(\text{Tr}(a\theta^0), \text{Tr}(a\theta^1), \dots, \text{Tr}(a\theta^{\bar{n}-1})) : a \in \mathbb{F}_{q^r}\}.$$

These arguments show that C is obtained from \bar{C} via m times replication so that

$$C = \{(\bar{c}, \bar{c}, \dots, \bar{c}) : \bar{c} \in \bar{C}\}.$$

Next we study b -symbol Hamming weights of C for $b \in \{1, 2, \dots, \dim_{\mathbb{F}_q} C\}$, which determine the whole b -symbol Hamming weights profile of all integers $1 \leq b \leq n - 1$ as proved in Theorem IV.3. Recall that 1-symbol Hamming weight corresponds to the usual Hamming weight. First we consider the case of length $n = q^r - 1$.

Theorem IV.4: Assume that $\gcd(n, q) = 1$. Let C be a cyclic code of length $n = q^r - 1$ such that its nonzero set is exactly one q -cyclotomic coset U of $\mathbb{Z}/n\mathbb{Z}$. Assume that $U \neq \{0\}$ and let $u \in U$. Let $k = \dim_{\mathbb{F}_q} C$. Put $N = \gcd(u, q^r - 1)$ and $N_1 = \gcd\left(\frac{q^r - 1}{q - 1}, N\right)$. Let $c \in C$ be an arbitrary nonzero codeword. For $1 \leq b \leq k$, let $w_b(c)$ denote the b -symbol Hamming weight of c . If $N_1 = 1$, then we have

$$w_b(c) = (q^b - 1)q^{r-b}.$$

If $N_1 > 1$, then we have

$$\begin{aligned} &\left\lceil \frac{N(q^b - 1)}{q^{b-1}} \left\lfloor \frac{q^r - \lfloor (N_1 - 1)q^{r/2} \rfloor}{qN} \right\rfloor \right\rceil \\ &\leq w_b(c) \leq \left\lfloor \frac{N(q^b - 1)}{q^{b-1}} \left\lceil \frac{q^r + \lfloor (N_1 - 1)q^{r/2} \rfloor}{qN} \right\rceil \right\rfloor. \end{aligned} \quad (13)$$

Proof: Let $f(x) = ax^u \in \mathbb{F}_{q^r}[x] \setminus \{0\}$ be an arbitrary nonzero polynomial in $P(\{u\})$. Let $c^{(b)}(f) \in C^{(b)}$ be the corresponding codeword.

We use some methods of [12] and further techniques in this proof. We refer to Appendix A for notation and background on algebraic function fields. In Appendix A we provide necessary background on algebraic function fields in order to make the paper self-contained.

As $b \leq k$, it follows from Definition IV.1 and Corollary 1 that $\dim_{\mathbb{F}_q} V(b) = b$. Let $W = \{\alpha \in \mathbb{F}_{q^r} : \text{Tr}(\alpha) = \text{Tr}(\eta^u \alpha) = \dots = \text{Tr}(\eta^{(b-1)u} \alpha) = 0\}$. As $\dim_{\mathbb{F}_q} V(b) = b$, W is an \mathbb{F}_q -linear subspace of codimension b in \mathbb{F}_{q^r} .

Let $A(T) \in \mathbb{F}_{q^r}[T]$ be the monic q -additive polynomial of degree q^b which splits in \mathbb{F}_{q^r} and which satisfies $W = \{A(y) : y \in \mathbb{F}_{q^r}\}$. For some properties, including existence and uniqueness of $A(T)$, we refer to [9] and [12, Section 3].

Let F be the algebraic function field corresponding to the codeword $c^{(b)}(f)$ given by $F = \mathbb{F}_{q^r}(x, y)$ such that $A(y) = ax^u$. Let $V \subseteq \mathbb{F}_{q^r}$ be the subset consisting of the roots of $A(T)$. Note that V is an \mathbb{F}_q -linear subspace of dimension b . Let $P \subseteq V \setminus \{0\}$ be a subset such that each one dimensional \mathbb{F}_q -linear subspace of V contains exactly one nonzero element in V . Then $|P| = (q^b - 1)/(q - 1)$ and let $P = \{\theta_1, \dots, \theta_{(q^b-1)/(q-1)}\}$ be an enumeration of P .

Let j be an integer in the range $1 \leq j \leq (q^b - 1)/(q - 1)$. Let $c(\theta_j f) \in C$ be the codeword corresponding to $\theta_j ax^u$. Let F_j be the algebraic function field corresponding to $c(\theta_j f)$ given by $F_j = \mathbb{F}_{q^r}(x, y_j)$ such that $y_j^q - y_j = \theta_j ax^u$. It is not difficult to observe that F is the compositum of $F_1, F_2, \dots, F_{(q^b-1)/(q-1)}$, that is to say the smallest extension field containing all $F_1, F_2, \dots, F_{(q^b-1)/(q-1)}$.

There exists exactly one rational place of F at infinity, which is the rational place of F over the rational place of the rational function field $\mathbb{F}_{q^r}(x)$ corresponding to the pole of (x) . Let $N^{(\text{aff})}(F)$ denote the number of affine rational places of F .

Consider the i -th symbol $c_i^{(b)}(f) = (\text{Tr}(f(\eta^i)), \text{Tr}(\eta^u f(\eta^i)), \dots, \text{Tr}(\eta^{(b-1)u} f(\eta^i))) \in F_q^{b\epsilon}$ of the codeword $c^{(b)}(f)$ for $0 \leq i \leq n - 1$. This symbol contributes to the Hamming weight $w_H(c^{(b)}(f))$ of $c^{(b)}(f)$ if and only if there are q^b distinct rational places of the covering $F/\mathbb{F}_{q^r}(x)$ over the place of the rational function field $\mathbb{F}_{q^r}(x)$ corresponding to the zero of $(x - \eta^i)$. Also there exist exactly q^b distinct rational places of the covering $F/\mathbb{F}_{q^r}(x)$ over the place of the rational function field $\mathbb{F}_{q^r}(x)$ corresponding to the zero of (x) . Hence we get that

$$(n - w_H(c^{(b)}(f)))q^b + q^b = N^{(\text{aff})}(F).$$

This is equivalent to

$$w_H(c^{(b)}(f)) = q^r - \frac{N^{(\text{aff})}(F)}{q^b}. \quad (14)$$

Recall that j is an integer in the range $1 \leq j \leq (q^b - 1)/(q - 1)$. Again there exists exactly one rational place of F_j at infinity. Let $N^{(\text{aff})}(F_j)$ denote the number of affine rational places of F_j . For the Hamming weight $w_H(c(\theta_j f))$ of $c(\theta_j f)$ using similar arguments we also get that

$$w_H(c(\theta_j f)) = q^r - \frac{N^{(\text{aff})}(F_j)}{q}. \quad (15)$$

Let S and S_j be the integers defined via

$$N^{(\text{aff})}(F) = q^r - S \quad \text{and} \quad N^{(\text{aff})}(F_j) = q^r - S_j. \quad (16)$$

It follows from [6, Corollary 6.7] (see also [10, Proposition 3.6] and [17, Lemma 2.4 and (3)]) that

$$S = \sum_{j=1}^{(q^b-1)/(q-1)} S_j. \quad (17)$$

Here we use the fact that $A(T)$ is a q -additive polynomial splitting in \mathbb{F}_{q^r} . Using (14), (15) and (16) yields

$$\begin{aligned} V &:= q^r - N^{(\text{aff})}(F) \\ &= \sum_{j=1}^{(q^b-1)/(q-1)} (q^r - N^{(\text{aff})}(F_j)) \\ &= \sum_{j=1}^{(q^b-1)/(q-1)} (-(q-1)q^r \\ &\quad + qw_H(c(\theta_j f))) \\ &= -q^{r+b} + q^r \\ &\quad + q \sum_{j=1}^{(q^b-1)/(q-1)} w_H(c(\theta_j f)). \end{aligned} \quad (18)$$

This implies that

$$w_H(c^{(b)}(f)) = \frac{1}{q^{b-1}} \sum_{j=1}^{(q^b-1)/(q-1)} w_H(c(\theta_j f)). \quad (18)$$

Recall that $N = \gcd(u, q^r - 1)$. Put $\bar{n} = \frac{q^r-1}{N}$ and let $\bar{c}(\theta_j f)$ be the shortening of $c(\theta_j f)$ to the first \bar{n} symbols as in (10). Similarly let \bar{C} be the shortening of the code C to the first \bar{n} symbols as in (11). Note that \bar{C} is an irreducible cyclic code of length \bar{n} over \mathbb{F}_q with $N = \frac{q^r-1}{\bar{n}}$.

Assume first that $N_1 = 1$. Using [5, Theorem 15] we have

$$w_H(\bar{c}(\theta_j f)) = \frac{(q-1)q^{r-1}}{N} \quad (19)$$

for each $1 \leq j \leq \frac{q^b-1}{q-1}$. Using (19) and (12) we obtain that

$$w_H(c(\theta_j f)) = (q-1)q^{r-1} \quad (20)$$

for each $1 \leq j \leq \frac{q^b-1}{q-1}$. Combining (20) and (18) we conclude that

$$w_b(c(f)) = w_H(c^{(b)}(f)) = \frac{q^b-1}{q^{b-1}} q^{r-1} = (q^b-1) q^{r-b}$$

which completes the proof of the case that $N_1 = 1$.

Assume next that $N_1 > 1$. Using [5, Theorem 24] we have

$$\begin{aligned} (q-1) \left\lfloor \frac{q^r - \lfloor (N_1-1)q^{r/2} \rfloor}{qN} \right\rfloor &\leq w_H(\bar{c}(\theta_j f)) \\ &\leq (q-1) \left\lfloor \frac{q^r + \lfloor (N_1-1)q^{r/2} \rfloor}{qN} \right\rfloor \end{aligned} \quad (21)$$

for each $1 \leq j \leq \frac{q^b-1}{q-1}$. Using (21) and (12) we obtain that

$$\begin{aligned} N(q-1) \left\lfloor \frac{q^r - \lfloor (N_1-1)q^{r/2} \rfloor}{qN} \right\rfloor &\leq w_H(c(\theta_j f)) \\ &\leq N(q-1) \left\lfloor \frac{q^r + \lfloor (N_1-1)q^{r/2} \rfloor}{qN} \right\rfloor \end{aligned} \quad (22)$$

for each $1 \leq j \leq \frac{q^b-1}{q-1}$. Combining (22) and (18) we conclude that

$$\begin{aligned} N \frac{q^b-1}{q^{b-1}} \left\lfloor \frac{q^r - \lfloor (N_1-1)q^{r/2} \rfloor}{qN} \right\rfloor &\leq w_b(c(f)) \\ &\leq N \frac{q^b-1}{q^{b-1}} \left\lfloor \frac{q^r + \lfloor (N_1-1)q^{r/2} \rfloor}{qN} \right\rfloor. \end{aligned} \quad (23)$$

As $w_b(C(f))$ is an integer, taking the ceiling and the floor integer parts of both sides of (23) we complete the proof. \square

Remark 2: Let u^* be the largest positive divisor t of u such that $\gcd(t, q) = 1$. The genus $g(F)$ of the function field F in the proof of Theorem IV.4 is $g(F) = \frac{(q^b-1)(u^*-1)}{2}$. Hence Serre's improvement on the Hasse-Weil bound [16, Theorem 5.3.1] yields

$$|N^{(\text{aff})}(F)| \leq q^r + \frac{(q^b-1)(u^*-1)}{2} \lfloor 2q^{r/2} \rfloor.$$

For a nonzero codeword $c \in C$, using the arguments in the proof of Theorem IV.4 we arrive at the bounds

$$\begin{aligned} & q^r - q^{r-b} - \left\lfloor \frac{(q^b-1)(u^*-1) \lfloor 2q^{r/2} \rfloor}{2q^b} \right\rfloor \\ & \leq w_b(c) \\ & \leq q^r - q^{r-b} + \left\lfloor \frac{(q^b-1)(u^*-1) \lfloor 2q^{r/2} \rfloor}{2q^b} \right\rfloor. \end{aligned}$$

The bounds of this remark are comparable to the bounds of Theorem IV.4. Nevertheless the bounds of Theorem IV.4 are better in general. We illustrate this in Example 5 below.

It is important to observe that the methods of this remark is valuable in the following sense. If the assumption of Theorem IV.4 that the nonzero set of C is exactly one q -cyclotomic coset of $\mathbb{Z}/n\mathbb{Z}$ does not hold, then we cannot use [5] as in the proof of Theorem IV.4. This corresponds to the general situation of arbitrary cyclic codes. We consider arbitrary cyclic codes in Section V, where we develop and use the methods similar to the methods of this remark.

Example 5: We compare the bounds of Theorem IV.4 and Remark 2 in the following concrete cases.

- Case $q = 3, b = 2, r = 10, u = 11, n = q^r - 1$.

$$\text{Theorem IV.4: } 50336 \leq w_b(c) \leq 54648.$$

$$\text{Remark 2: } 50328 \leq w_b(c) \leq 54648.$$

- Case $q = 3, b = 2, r = 10, u = 61, n = q^r - 1$.

$$\text{Theorem IV.4: } 39528 \leq w_b(c) \leq 65392.$$

$$\text{Remark 2: } 39528 \leq w_b(c) \leq 65448.$$

- Case $q = 2, b = 2, r = 10, u = 11, n = q^r - 1$.

$$\text{Theorem IV.4: } 528 \leq w_b(c) \leq 1006.$$

$$\text{Remark 2: } 528 \leq w_b(c) \leq 1008.$$

- Case $q = 2, b = 2, r = 10, u = 31, n = q^r - 1$.

$$\text{Theorem IV.4: } 93 \leq w_b(c) \leq 1488.$$

$$\text{Remark 2: } 48 \leq w_b(c) \leq 1488.$$

Using the methods in the proof of Theorem IV.4 and (12) we obtain our bounds for the general length $n \mid (q^r - 1)$ in the next corollary.

Corollary 2: Assume that $\gcd(n, q) = 1$. Let C be a cyclic code of length $n \mid (q^r - 1)$ such that its nonzero set is exactly one q -cyclotomic coset U of $\mathbb{Z}/n\mathbb{Z}$. Assume that $U \neq \{0\}$ and let $u \in U$. Let $k = \dim_{\mathbb{F}_q} C$. Put $m = \gcd(u, n)$, $N = \frac{q^r-1}{n}m$ and $N_1 = \gcd\left(\frac{q^r-1}{q-1}, N\right)$. Let $c \in C$ be an arbitrary nonzero

codeword. For $1 \leq b \leq k$, let $w_b(c)$ denote the b -symbol Hamming weight of c . If $N_1 = 1$, then we have

$$w_b(c) = \frac{m}{N} (q^b - 1) q^{r-b}. \quad (24)$$

If $N_1 > 1$, then we have

$$\begin{aligned} & \left\lfloor \frac{m(q^b-1)}{q^{b-1}} \left\lfloor \frac{q^r - \lfloor (N_1-1)q^{r/2} \rfloor}{qN} \right\rfloor \right\rfloor \\ & \leq w_b(c) \leq \left\lceil \frac{m(q^b-1)}{q^{b-1}} \left\lceil \frac{q^r + \lfloor (N_1-1)q^{r/2} \rfloor}{qN} \right\rceil \right\rceil. \end{aligned}$$

Remark 3: If $n = q^r - 1$, then $m = N$ and Corollary 2 coincides with Theorem IV.4.

Remark 4: If $m = 1$ and $b = 1$, then Corollary 2 coincides with [5, Theorem 24].

Remark 5: Note that $k \leq r$ as the nonzero set of C consists of only one q -cyclotomic coset of $\mathbb{Z}/n\mathbb{Z}$ in Corollary 2. Moreover if $N_1 = 1$, then $N \mid (q-1)$. Hence the b -symbol Hamming weight $\frac{m}{N} (q^b - 1) q^{r-b}$ in (24) is an integer.

If $N_1 = 1$, then using also Theorem IV.3 we determine the b -symbol Hamming weight enumerator of C not only for $1 \leq k \leq b$ but for the full range $1 \leq b \leq n-1$ in this case.

Corollary 3: Keeping the notation and assumptions of Corollary 2, assume further that $N_1 = 1$. For integers b in the interval $1 \leq b \leq n-1$, the b -symbol Hamming weight enumerator of C is

$$\begin{cases} 1 + (q^k - 1) Z^{\frac{m(q^b-1)q^{r-b}}{N}} & \text{if } 1 \leq b \leq k, \\ 1 + (q^k - 1) Z^{\frac{m(q^k-1)(q-k)}{N}} & \text{if } k+1 \leq b \leq n-1. \end{cases}$$

Proof: Assume first that $1 \leq b \leq k$. Then we have $w_b(c) = \frac{m}{N} (q^b - 1) q^{r-b}$ using Corollary 2 for any nonzero codeword c of C . For the zero codeword $c = 0$ of C it is clear that $w_b(c) = 0$. These imply that the b -symbol Hamming weight enumerator of C is

$$1 + (q^k - 1) Z^{\frac{m(q^b-1)q^{r-b}}{N}}.$$

In particular if $b = k$, then the b -symbol Hamming weight enumerator of C is

$$1 + (q^k - 1) Z^{\frac{m(q^k-1)q^{r-k}}{N}}. \quad (25)$$

Using Theorem IV.3, the b -symbol Hamming weight enumerator of C is exactly as in (25) if $k+1 \leq b \leq n-1$. \square

Further knowledge on the weight distribution of irreducible cyclic codes combined with the methods of the proof of Theorem IV.4 would immediately imply some improvements on the general bound of Corollary 2. Note that there exists such knowledge on the weight distribution on irreducible cyclic codes only for some very special subcases. We present a collection of such improvements on special subcases in the next corollary.

Corollary 4: Keeping the notation and assumptions of Corollary 2, we obtain improved bounds in the following special subcases. Let $q = p^s$, where p is the characteristic of \mathbb{F}_q . Recall that $k = \dim_{\mathbb{F}_q} C$.

- Assume further that $N_1 = 2$. We have:

$$\begin{aligned} & \left\lceil \frac{m(q^b - 1)(q^r - q^{r/2})}{q^b N} \right\rceil \\ & \leq w_b(c) \\ & \leq \left\lceil \frac{m(q^b - 1)(q^r + q^{r/2})}{q^b N} \right\rceil. \end{aligned}$$

- Assume further that $N_1 = 3$, $p \equiv 2 \pmod{3}$ and $sk \equiv 0 \pmod{4}$. We have:

$$\begin{aligned} & \left\lceil \frac{m(q^b - 1)(q^r - q^{r/2})}{q^b N} \right\rceil \\ & \leq w_b(c) \\ & \leq \left\lceil \frac{m(q^b - 1)(q^r + 2q^{r/2})}{q^b N} \right\rceil. \end{aligned}$$

- Assume further that $N_1 = 3$, $p \equiv 2 \pmod{3}$ and $sk \equiv 2 \pmod{4}$. We have:

$$\begin{aligned} & \left\lceil \frac{m(q^b - 1)(q^r - 2q^{r/2})}{q^b N} \right\rceil \\ & \leq w_b(c) \\ & \leq \left\lceil \frac{m(q^b - 1)(q^r + q^{r/2})}{q^b N} \right\rceil. \end{aligned}$$

- Assume further that $N_1 = 4$ and $p \equiv 3 \pmod{4}$. We have:

$$\begin{aligned} & \left\lceil \frac{m(q^b - 1)(q^r - q^{r/2})}{q^b N} \right\rceil \\ & \leq w_b(c) \\ & \leq \left\lceil \frac{m(q^b - 1)(q^r + 3q^{r/2})}{q^b N} \right\rceil. \end{aligned}$$

Proof: First we assume that $N_1 = 2$. We use the methods in the proof of Theorem IV.4 and we keep its notation. In particular $c^{(b)}$ and $\bar{c}^{(b)}$ denote the corresponding nonzero codewords as in the proof of Theorem IV.4. We have, as in (18), that

$$w_H(c^{(b)}(f)) = \frac{1}{q^{b-1}} \sum_{j=1}^{(q^b-1)/(q-1)} w_H(c(\theta_j f)). \quad (26)$$

Here θ_j for $1 \leq j \leq (q^b - 1)/(q - 1)$ are chosen as in the proof of Theorem IV.4. Using (12) we also have

$$w_H(\bar{c}(\theta_j f)) = \frac{1}{m} w_H(c(\theta_j f)) \quad (27)$$

for $1 \leq j \leq (q^b - 1)/(q - 1)$. Using [5, Theorem 17] we further obtain

$$\begin{aligned} \frac{(q-1)(q^r - q^{r/2})}{qN} & \leq w_H(\bar{c}(\theta_j f)) \\ & \leq \frac{(q-1)(q^r + q^{r/2})}{qN}, \end{aligned} \quad (28)$$

Combining (26), (27) and (28) we conclude that

$$\begin{aligned} \frac{m(q^b - 1)(q^r - q^{r/2})}{q^b N} & \leq w_H(\bar{c}(\theta_j f)) \\ & \leq \frac{(q^b - 1)(q^r + q^{r/2})}{q^b N}. \end{aligned} \quad (29)$$

Taking the ceiling and floor integer parts of both sides of (29) we complete the proof of the case $N_1 = 2$.

Assume next that $N_1 = 3$, $p \equiv 2 \pmod{3}$ and $sk \equiv 0 \pmod{4}$. In this case, using [5, Theorem 19] we obtain

$$\frac{(q-1)(q^r - q^{r/2})}{qN} \leq w_H(\bar{c}(\theta_j f)) \leq \frac{(q-1)(q^r + 2q^{r/2})}{qN}$$

instead of (28) of the case $N_1 = 2$. Using the same arguments with this change we complete the proof of the current case.

Assume next that $N_1 = 3$, $p \equiv 2 \pmod{3}$ and $sk \equiv 2 \pmod{4}$. In this case, using [5, Theorem 19] we obtain

$$\frac{(q-1)(q^r - 2q^{r/2})}{qN} \leq w_H(\bar{c}(\theta_j f)) \leq \frac{(q-1)(q^r + q^{r/2})}{qN}$$

instead of (28) of the case $N_1 = 2$. Using the same arguments with this change we complete the proof of the current case.

Assume next that $N_1 = 3$, $p \equiv 2 \pmod{3}$ and $sk \equiv 2 \pmod{4}$. In this case, using [5, Theorem 20] we obtain

$$\frac{(q-1)(q^r - q^{r/2})}{qN} \leq w_H(\bar{c}(\theta_j f)) \leq \frac{(q-1)(q^r + 3q^{r/2})}{qN}$$

instead of (28) of the case $N_1 = 2$. Using the same arguments with this change we complete the proof of the current case. \square

Now we summarize and compare the bounds of this section. Theorem IV.4 is a special subcase of Corollary 2 with $n = q^r - 1$. In terms of the bounds, Corollary 3 is a special subcase of Corollary 2 with $N_1 = 1$. Corollary 4 improves Corollary 2 in some concrete cases only if $N_1 \in \{2, 3, 4\}$. We present some concrete examples illustrating also these improvements below.

Example 6: We give concrete examples for the bounds of Corollary 3 and Corollary 4.

- Case $q = 2$, $b = 2$, $r = 12$, $u = 11$, $n = 1365$.

$$\text{Corollary 2: } 993 \leq w_b(c) \leq 1056.$$

$$\text{Corollary 4: } 1008 \leq w_b(c) \leq 1056.$$

- Case $q = 2$, $b = 2$, $r = 10$, $u = 5$, $n = 341$.

$$\text{Corollary 2: } 240 \leq w_b(c) \leq 271.$$

$$\text{Corollary 4: } 240 \leq w_b(c) \leq 264.$$

- Case $q = 3$, $b = 2$, $r = 8$, $u = 7$, $n = 1640$.

$$\text{Corollary 2: } 1406 \leq w_b(c) \leq 1512.$$

$$\text{Corollary 4: } 1440 \leq w_b(c) \leq 1512.$$

- Case $q = 9$, $b = 3$, $r = 8$, $u = 47$, $n = 10761680$.

$$\text{Corollary 2: } 10742009 \leq w_b(c) \leq 10751832.$$

$$\text{Corollary 4: } 10745280 \leq w_b(c) \leq 10751832.$$

- Case $q = 2$, $b = 2$, $r = 16$, $u = 17$, $n = 3855$.

$$\text{Corollary 2: } 2712 \leq w_b(c) \leq 3072.$$

Corollary 4 does not work in this case as $N_1 = 17$ in this case.

Remark 6: As we consider cyclic and hence linear codes throughout this paper, our lower and upper bounds on the b -symbol Hamming weights of nonzero codewords mean lower and upper bounds on the b -symbol Hamming distances between distinct codewords. Hence our bounds throughout this paper also correspond to lower and upper bounds on b -symbol Hamming distance of the codes we consider.

V. b -SYMBOL WEIGHTS FOR ARBITRARY CYCLIC CODES

Throughout this section we assume that C is a cyclic code of length n dividing $q^r - 1$. Let U be the nonzero set of C and let U_1, \dots, U_ρ be the distinct q -cyclotomic cosets of $\mathbb{Z}/n\mathbb{Z}$ included in U . Note that $U = U_1 \sqcup U_2 \cdots \sqcup U_\rho$ and $\rho \geq 1$, where \sqcup indicates that the sets U_1, \dots, U_ρ in the union are pairwise disjoint. As in Section IV we assume that $U \neq \{0\}$ in order to avoid the trivial case. Choose $u_j \in U_j$ and put $k_j = |U_j|$ for $1 \leq j \leq \rho$. Note that for the \mathbb{F}_q -dimension k of C we have $k = k_1 + \dots + k_\rho$.

We first generalize our stability theorem (see Theorem IV.3) to arbitrary cyclic codes. Recall that $\eta \in \mathbb{F}_{q^r}^*$ is a primitive n -th root of 1. We introduce some notation. For $0 \leq t \leq n-1$, let \mathbf{v}_t be the vector in $\mathbb{F}_{q^r}^\rho$ defined as

$$\mathbf{v}_t = [\eta^{tu_1}, \eta^{tu_2}, \dots, \eta^{tu_\rho}]. \quad (30)$$

For $1 \leq t \leq n-1$, let $V(t) \subseteq \mathbb{F}_{q^r}^\rho$ be the \mathbb{F}_q -linear subspace defined as

$$V(t) = \text{Span}_{\mathbb{F}_q} \{\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_{t-1}\}.$$

The following lemma is useful.

Lemma V.1: Under the above notation, we have

$$\dim_{\mathbb{F}_q} V(t) = \begin{cases} t & \text{if } 1 \leq t \leq k-1, \\ k & \text{if } k \leq t \leq n-1. \end{cases}$$

Moreover, $\{\mathbf{v}_0, \dots, \mathbf{v}_{t-1}\}$ is an \mathbb{F}_q -basis of $V(t)$ if $1 \leq t \leq k-1$. Also $\{\mathbf{v}_0, \dots, \mathbf{v}_{k-1}\}$ is an \mathbb{F}_q -basis of $V(t)$ if $k \leq t \leq n-1$.

Proof: Recall that $\mathbb{F}_q(\eta^{u_j})$ denotes the smallest finite field extension over \mathbb{F}_q containing η^{u_j} . For the index of this extension we have $[\mathbb{F}_q(\eta^{u_j}) : \mathbb{F}_q] = k_j$. Let $m_j(x) \in \mathbb{F}_q[x]$ be the minimal polynomial of η^{u_j} over \mathbb{F}_q . It is clear that $\deg m_j(x) = k_j$ and the set $\{m_1(x), m_2(x), \dots, m_\rho(x)\}$ consists of irreducible polynomials over \mathbb{F}_q and the elements of this set are pairwise distinct.

We first show that $\dim_{\mathbb{F}_q} V(k) = k$. Assume the contrary, and let $e_0, e_1, \dots, e_{k-1} \in \mathbb{F}_q$ such that

$$e_0 \mathbf{v}_0 + e_1 \mathbf{v}_1 + \dots + e_{k-1} \mathbf{v}_{k-1} = \mathbf{0}. \quad (31)$$

Let $1 \leq j \leq \rho$. Considering the j -th coordinates of the both sides of (31) we get

$$e_0 + e_1 \eta^{u_j} + \dots + e_{k-1} \eta^{(k-1)u_j} = 0. \quad (32)$$

Let $h(x) = e_0 + e_1 x + \dots + e_{k-1} x^{k-1} \in \mathbb{F}_q[x]$, which is a nonzero polynomial of degree at most $k-1$. It follows from (32) that η^{u_j} is a root of $h(x)$. Hence we conclude that

$$h(\eta^{u_j}) = 0 \quad \text{for each } 1 \leq j \leq \rho.$$

As $m_j(x)$ is the minimal polynomial of η^{u_j} over \mathbb{F}_q and $h(x) \in \mathbb{F}_q[x]$ we obtain that

$$m_j(x) \mid h(x) \quad \text{for each } 1 \leq j \leq \rho.$$

Recall that $\{m_1(x), m_2(x), \dots, m_\rho(x)\}$ consists of irreducible polynomials over \mathbb{F}_q and that the elements of this set are pairwise distinct. These arguments yield that the polynomial $\prod_{j=1}^\rho m_j(x)$ divides $h(x)$ and hence

$$\deg h(x) \geq \sum_{j=1}^\rho \deg m_j(x) = \sum_{j=1}^\rho k_j = k.$$

This is a contradiction as $h(x)$ is a nonzero polynomial of degree at most $k-1$.

It is clear that $V(t-1) \subseteq V(t)$ and

$$0 \leq \dim_{\mathbb{F}_q} V(t) - \dim_{\mathbb{F}_q} V(t-1) \leq 1 \quad (33)$$

for each $2 \leq t \leq n-1$. Moreover, $V(1) = \text{Span}_{\mathbb{F}_q} \{[1, \dots, 1]\}$ and hence $\dim_{\mathbb{F}_q} V(1) = 1$. Combining (33), and the facts $\dim_{\mathbb{F}_q} V(1) = 1$, $\dim_{\mathbb{F}_q} V(k) = k$ we conclude that $\dim_{\mathbb{F}_q} V(t) = t$ for each integer t in the range $1 \leq t \leq k$. Moreover, these also imply that

$$\{\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_t\}$$

is a basis of $V(t)$ for each integer t in the range $1 \leq t \leq k$.

It remains to prove that $V(k+i) \subseteq V(k)$ for $1 \leq i \leq n-k-1$. We prove this by induction on i . First we consider the induction step $i=1$. Let $m(x) = m_1(x)m_2(x) \cdots m_\rho(x)$, which is a monic polynomial of degree k . Considering the coefficients of $m(x)$ let

$$m(x) = x^k + e_{k-1}x^{k-1} + \dots + e_1x + e_0,$$

where $e_{k-1}, \dots, e_1, e_0 \in \mathbb{F}_q$. As $m(\eta^{u_j}) = 0$ for each $1 \leq j \leq \rho$, the arguments above in this proof imply that

$$\mathbf{v}_k + e_{k-1} \mathbf{v}_{k-1} + \dots + e_1 \mathbf{v}_1 + e_0 \mathbf{v}_0 = \mathbf{0}.$$

This shows that $\mathbf{v}_k \in V(k)$ and hence $V(k+1) \subseteq V(k)$. Assume the induction hypothesis that $V(k+i) \subseteq V(k)$. Let $h(x) = x^i m(x)$, which is a monic polynomial of degree $k+i$. Considering the coefficients of $h(x)$ let

$$k(x) = x^{k+i} + e_{k+i-1}x^{k+i-1} + \dots + e_1x + e_0,$$

where $e_{k+i-1}, \dots, e_1, e_0 \in \mathbb{F}_q$. Similarly we obtain that

$$\mathbf{v}_{k+i} + e_{k+i-1} \mathbf{v}_{k+i-1} + \dots + e_1 \mathbf{v}_1 + e_0 \mathbf{v}_0 = \mathbf{0}.$$

This yields $\mathbf{v}_{k+i} \in V(k+i)$ and hence $V(k+i+1) \subseteq V(k+i)$. This completes the proof. \square

Next we present our stability theorem for arbitrary cyclic codes. Again it says, but now for arbitrary cyclic codes, that the b -symbol Hamming weight enumerators of C are the same (and hence stable) for all b -symbol Hamming weights if $b \geq \dim_{\mathbb{F}_q} C$ (see also Theorem IV.3). There exists a nonempty stability region for b except the trivial case that $\dim_{\mathbb{F}_q} C = n-1$.

Theorem V.2: Assume that $\gcd(n, q) = 1$. Let C be an arbitrary cyclic code of length n and U be its nonzero set in $\mathbb{Z}/n\mathbb{Z}$. Assume that $U \neq \{0\}$. Let $k = \dim_{\mathbb{F}_q} C$. For any

integer b in the interval $k \leq b \leq n-1$, the b -symbol Hamming weight enumerator of C is the same as the k -symbol Hamming weight enumerator of C .

Proof: We use the notation fixed in this section so that $\{u_1, u_2, \dots, u_\rho\}$ is a basic nonzero set of C . Let $f(x) = a_1 x^{u_1} + a_2 x^{u_2} + \dots + a_\rho x^{u_\rho} \in \mathbb{F}_{q^r}[x] \setminus \{0\}$ be an arbitrary nonzero polynomial in $P(\{u_1, u_2, \dots, u_\rho\})$. Let $c^{(k)}(f) \in C^{(k)}$ and $c^{(b)}(f) \in C^{(b)}$ be the corresponding codewords. Note that

$$c^{(b)}(f) = \left(\underline{\text{Tr}(f(\eta))}, \underline{\text{Tr}(f^{(1)}(\eta))}, \dots, \underline{\text{Tr}(f^{(b)}(\eta))} \right),$$

where $f^{(t)}(x)$ is defined in Definition III.1. Namely we have

$$f^{(t)}(x) = \eta^{tu_1} a_1 x^{u_1} + \eta^{tu_2} a_2 x^{u_2} + \dots + \eta^{tu_\rho} a_\rho x^{u_\rho}. \quad (34)$$

Let i be an integer in the range $0 \leq i \leq n-1$. Let $c_i^{(b)}(f) \in \mathbb{F}_q^b$ be the i -th symbol of the codeword $c^{(b)}(f) \in (\mathbb{F}_q^b)^n$ so that

$$c^{(b)}(f) = \left(c_0^{(b)}(f), c_1^{(b)}(f), \dots, c_{n-1}^{(b)}(f) \right).$$

Let $y_1 = a_1 \eta^{iu_1}$, $y_2 = a_2 \eta^{iu_2}, \dots, y_\rho = a_\rho \eta^{iu_\rho}$ all in $\mathbb{F}_{q^r}^*$. Note that

$$\begin{aligned} c_i^{(b)}(f) &= (\text{Tr}(y_1 + y_2 + \dots + y_\rho), \\ &\quad + \text{Tr}(\eta^{u_1} y_1 + \eta^{u_2} y_2 + \dots + \eta^{u_\rho} y_\rho), \dots, \\ &\quad + \text{Tr}(\eta^{(b-1)u_1} y_1 + \eta^{(b-1)u_2} y_2 + \dots \\ &\quad + \eta^{(b-1)u_\rho} y_\rho)). \end{aligned}$$

Similarly for the i -th symbol $c_i^{(k)}(f) \in \mathbb{F}_q^k$ of the codeword $c^{(k)}(f) \in (\mathbb{F}_q^k)^n$ we have

$$\begin{aligned} c_i^{(k)}(f) &= (\text{Tr}(y_1 + y_2 + \dots + y_\rho), \\ &\quad + \text{Tr}(\eta^{u_1} y_1 + \eta^{u_2} y_2 + \dots + \eta^{u_\rho} y_\rho), \dots, \\ &\quad + \text{Tr}(\eta^{(k-1)u_1} y_1 + \eta^{(k-1)u_2} y_2 + \dots \\ &\quad + \eta^{(k-1)u_\rho} y_\rho)). \end{aligned}$$

Hence $c_i^{(b)}(f)$ does not contribute to the Hamming weight of the codeword $c^{(b)}(f)$ if and only if

$$\begin{aligned} 0 &= \text{Tr}(y_1 + y_2 + \dots + y_\rho) \\ &= \text{Tr}(\eta^{u_1} y_1 + \eta^{u_2} y_2 + \dots + \eta^{u_\rho} y_\rho) \\ &\quad \vdots \\ &= \text{Tr}\left(\eta^{(b-1)u_1} y_1 + \eta^{(b-1)u_2} y_2 + \dots + \eta^{(b-1)u_\rho} y_\rho\right). \end{aligned} \quad (35)$$

Similarly $c_i^{(k)}(f)$ does not contribute to the Hamming weight of the codeword $c^{(k)}(f)$ if and only if

$$\begin{aligned} 0 &= \text{Tr}(y_1 + y_2 + \dots + y_\rho) \\ &= \text{Tr}(\eta^{u_1} y_1 + \eta^{u_2} y_2 + \dots + \eta^{u_\rho} y_\rho) \\ &\quad \vdots \\ &= \text{Tr}\left(\eta^{(k-1)u_1} y_1 + \eta^{(k-1)u_2} y_2 + \dots + \eta^{(k-1)u_\rho} y_\rho\right). \end{aligned} \quad (36)$$

We will prove the following claim at the end of this proof.

Claim 1. The conditions in (35) and (36) are equivalent.

Assume Claim 1 holds. The weight of the contribution of the symbol $c_i^{(b)}(f)$ to the codeword $c^{(b)}(f)$ is 0 or 1, which is identified with the condition in (35). The same holds for the symbol $c_i^{(k)}(f)$ to the codeword $c^{(k)}(f)$ and the condition (36). Using Claim 1 and running through all indices $0 \leq i \leq n-1$ we complete the proof.

Now we prove Claim 1. As $k \leq b$ it is clear that (35) implies (36). Conversely assume that (36) holds. Let t be an integer in the range $k \leq t \leq b-1$. Note that

$$[\eta^{tu_1}, \eta^{tu_2}, \dots, \eta^{tu_\rho}] = \mathbf{v}_t,$$

where \mathbf{v}_t is defined in (30). Using Lemma V.1 we obtain that $\mathbf{v}_t \in V(k)$ and hence there exist $e_0, e_1, \dots, e_{k-1} \in \mathbb{F}_q$ such that

$$\begin{aligned} U &:= [\eta^{tu_1}, \eta^{tu_2}, \dots, \eta^{tu_\rho}] \\ &= e_0 [1, 1, \dots, 1] \\ &\quad + e_1 [\eta^{u_1}, \eta^{u_2}, \dots, \eta^{u_\rho}] \\ &\quad + \dots \\ &\quad + e_{k-1} [\eta^{(k-1)u_1}, \eta^{(k-1)u_2}, \dots, \eta^{(k-1)u_\rho}]. \end{aligned}$$

Multiplying both sides with $[y_1, \dots, y_\rho]$ using the Euclidean inner product in $\mathbb{F}_{q^r}^\rho$ we get

$$\begin{aligned} A &:= \eta^{tu_1} y_1 + \eta^{tu_2} y_2 + \dots + \eta^{tu_\rho} y_\rho \\ &= e_0 (y_1 + y_2 + \dots + y_\rho) \\ &\quad + e_1 (\eta^{u_1} y_1 + \eta^{u_2} y_2 + \dots + \eta^{u_\rho} y_\rho) + \dots \\ &\quad + e_{k-1} (\eta^{(k-1)u_1} y_1 + \eta^{(k-1)u_2} y_2 + \dots + \eta^{(k-1)u_\rho} y_\rho). \end{aligned}$$

Taking trace of both sides and noting $e_0, e_1, \dots, e_{k-1} \in \mathbb{F}_q$ yield

$$\begin{aligned} &\text{Tr}(\eta^{tu_1} y_1 + \eta^{tu_2} y_2 + \dots + \eta^{tu_\rho} y_\rho) \\ &= e_0 \text{Tr}(y_1 + y_2 + \dots + y_\rho) \\ &\quad + e_1 \text{Tr}(\eta^{u_1} y_1 + \eta^{u_2} y_2 + \dots + \eta^{u_\rho} y_\rho) \\ &\quad \vdots \\ &\quad + e_{k-1} \text{Tr}(\eta^{(k-1)u_1} y_1 + \dots + \eta^{(k-1)u_\rho} y_\rho). \end{aligned} \quad (37)$$

As (36) holds by assumption, we have

$$\begin{aligned} 0 &= \text{Tr}(y_1 + y_2 + \dots + y_\rho) \\ &= \text{Tr}(\eta^{u_1} y_1 + \eta^{u_2} y_2 + \dots + \eta^{u_\rho} y_\rho) \\ &\quad \vdots \\ &= \text{Tr}(\eta^{(k-1)u_1} y_1 + \dots + \eta^{(k-1)u_\rho} y_\rho). \end{aligned}$$

for these terms in the right hand side of (37). Therefore using (37) we conclude that

$$\text{Tr}(\eta^{tu_1} y_1 + \eta^{tu_2} y_2 + \dots + \eta^{tu_\rho} y_\rho) = 0.$$

This conclusion holds for each integer t in the range $k \leq t \leq b-1$, which completes the proof of Claim 1. \square

Theorem V.2 implies that it is enough to study b -symbol Hamming weights of an arbitrary cyclic code C of dimension k only for $1 \leq b \leq k$ instead of the much larger integral interval $1 \leq b \leq n-1$ in general.

Next we present our bounds on b -symbol Hamming weights on arbitrary cyclic codes for $1 \leq b \leq k$. We will need the following condition if q is not a prime.

Condition V.3: Assume that $\gcd(n, q) = 1$ and let $1 \leq u \leq n - 1$. Let \bar{u} be the q -cyclotomic coset of $\mathbb{Z}/n\mathbb{Z}$ containing u , namely $\bar{u} = \{uq^i \bmod n : 0 \leq i \leq n - 1\}$. Let $S(u)$ be the subset of \bar{u} given by $S(u) = \{v \in \bar{u} : \gcd(v, q) = 1\}$. If $u \neq 0$, then we say that u satisfies Condition V.3 if both of the followings are satisfied:

- $S(u)$ is not empty.
- $u = \min S(u)$.

If $u = 0$, then we say that u satisfies Condition V.3.

Remark 7: If q is a prime, then u satisfies Condition V.3 if u is the smallest element in \bar{u} . Hence if q is a prime then Condition V.3 is satisfied automatically as we are free to choose any element from \bar{u} in considering C .

Remark 8: If q is not a prime, then there may be some q -cyclotomic cosets which do not satisfy Condition V.3. However, there is a rich collection of nontrivial C such that Condition V.3 is satisfied and q is not prime so that we present our results for arbitrary q . Now we give some toy examples in order to illustrate why Condition V.3 is needed in some cases. Let $q = 4$, $r = 2$, $n = q^r - 1$. The q -cyclotomic cosets $\{10\}$ and $\{2, 8\}$ have no element u such that u satisfies Condition V.3. For the q -cyclotomic coset $Z_1 = \{1, 4\}$, the element $u = 1$ satisfies Condition V.3 and it is the smallest element of Z_1 as in the case that q is a prime. However, for the q -cyclotomic coset $Z_2 = \{6, 9\}$, the element $u = 9$ satisfies Condition V.3 but 9 is not the smallest element of Z_2 . This is different from the case that q is a prime (see Remark 7).

Remark 9: In our proofs in the rest of this section we apply Hasse Weil bound to Artin-Schreier type curves

$$A(y) = a_1 x^{u_1} + a_2 x^{u_2} + \cdots + a_\rho x^{u_\rho}, \quad (38)$$

over \mathbb{F}_{q^r} , where $A(y)$ are certain additive polynomials. Condition V.3 guarantees that the curve in (38) is absolutely irreducible over \mathbb{F}_{q^r} . This is automatically satisfied by choosing the smallest choice of u_i in each q -cyclotomic coset of C if q is a prime. If q is not a prime and Condition V.3 is not satisfied, then we need to consider further methods. For example, if the curve in (38) has irreducible components, then applying Hasse-Weil bound to all of the irreducible components gives similar bounds on the weight of the cyclic code. However, this would be very complicated depending on $\{u_1, u_2, \dots, u_\rho\}$ as we need to consider all $(a_1, a_2, \dots, a_\rho) \in \mathbb{F}_{q^r}^\rho \setminus \{(0, 0, \dots, 0)\}$. There is a general method presented in [11] that uses involved symbolic computations and tools from algebra for studying all possible irreducible components in order to get such bounds on the weight of the cyclic code. If $\rho = 1$, then all these are simple and implicitly used in Remark 2.

We first consider the case of length $n = q^r - 1$ as we use methods from algebraic function fields (see also [18]). We extend our results to arbitrary length $n \mid (q^r - 1)$ in Remark 14 below.

In the next theorem we present our bound in the case $b \leq \min\{k_1, k_2, \dots, k_\rho\}$. Note that this case is much more

general than the case of Section IV. Indeed it is possible, for example, that $k_1 = k_2 = \dots = k_\rho$ and ρ is a large positive integer.

Theorem V.4: Let C be an arbitrary cyclic code of length $n = q^r - 1$ over \mathbb{F}_q . Let $U_0 = \{u_1, u_2, \dots, u_\rho\}$ be a basic nonzero set of C . Assume that $U_0 \neq \{0\}$ and each element of U_0 satisfies Condition V.3. Put $u^* = \max\{u_1, u_2, \dots, u_\rho\}$. Let $\eta \in \mathbb{F}_{q^r}^*$ be a primitive n -th root of 1. For $1 \leq j \leq \rho$, let k_j be the index $[\mathbb{F}_q(\eta^{u_j}) : \mathbb{F}_q]$ of the field extension $\mathbb{F}_q(\eta^{u_j})/\mathbb{F}_q$. Let $c \in C$ be an arbitrary nonzero codeword. For $1 \leq b \leq \min\{k_1, k_2, \dots, k_\rho\}$, let $w_b(c)$ denote the b -symbol Hamming weight of c . We have

$$\begin{aligned} & q^r - q^{r-b} - \left\lfloor \frac{(q^b - 1)(u^* - 1) \lfloor 2q^{r/2} \rfloor}{2q^b} \right\rfloor \\ & \leq w_b(c) \\ & \leq q^r - q^{r-b} + \left\lfloor \frac{(q^b - 1)(u^* - 1) \lfloor 2q^{r/2} \rfloor}{2q^b} \right\rfloor. \end{aligned}$$

Proof: Let $f(x) = a_1 x^{u_1} + a_2 x^{u_2} + \cdots + a_\rho x^{u_\rho} \in \mathbb{F}_{q^r}[x] \setminus \{0\}$ be an arbitrary nonzero polynomial in $P(\{u_1, \dots, u_\rho\})$. Let $c^{(b)}(f) \in C^{(b)}$ be the corresponding codeword. Recall that

$$f^{(t)}(x) = \eta^{tu_1} a_1 x^{u_1} + \eta^{tu_2} a_2 x^{u_2} + \cdots + \eta^{tu_\rho} a_\rho x^{u_\rho} \quad (39)$$

for $0 \leq t \leq b - 1$, where $f^{(0)}(x) = f(x)$. Let $L \subseteq \mathbb{F}_{q^r}[x]$ be the \mathbb{F}_q -linear subspace of polynomials defined as

$$L = \text{Span}_{\mathbb{F}_q} \{f(x), f^{(1)}(x), \dots, f^{(b-1)}(x)\}.$$

First we show that $\dim_{\mathbb{F}_q} L = b$. Indeed assume the contrary that there exists $(e_0, e_1, \dots, e_{b-1}) \in \mathbb{F}_q^n \setminus \{(0, 0, \dots, 0)\}$ such that

$$e_0 f(x) + e_1 f^{(1)}(x) + \cdots + e_{b-1} f^{(b-1)}(x) = 0. \quad (40)$$

Note that the polynomial in the left hand side of (40) has monomials with possibly nonzero coefficients only at $x^{u_1}, x^{u_2}, \dots, x^{u_\rho}$. As $f(x) \neq 0$, there exists at least one coefficient a_{j_0} such that $a_{j_0} \neq 0$. Using (39), (40) and the coefficient of the monomial $x^{u_{j_0}}$ in the left hand side of (40) we obtain that

$$e_0 + e_1 \eta^{u_{j_0}} + e_2 \eta^{2u_{j_0}} + \cdots + \eta^{(b-1)u_{j_0}} = 0. \quad (41)$$

Let $e(x) \in \mathbb{F}_q[x]$ be the nonzero polynomial of degree at most $b - 1$ such that

$$e(x) = e_0 + e_1 x + \cdots + e_{b-1} x^{b-1}.$$

Let $m_{j_0}(x) \in \mathbb{F}_q[x]$ be the minimal polynomial of $\eta^{u_{j_0}}$ over \mathbb{F}_q . Let $k_{j_0} = \deg m_{j_0}(x)$. Note that $b \leq k_{j_0}$ by the assumption $b \leq \min\{k_1, k_2, \dots, k_\rho\}$. Using (41) we obtain that $e(\eta^{u_{j_0}}) = 0$ and hence $m_{j_0}(x) \mid e(x)$. However, this is a contradiction as $\deg e(x) \leq b - 1 < k_{j_0}$. This completes the proof of the statement that $\dim_{\mathbb{F}_q} L = b$.

For $0 \leq \ell \leq b - 1$, let F_ℓ be the algebraic function field $F_\ell = \mathbb{F}_{q^r}(x, y_\ell)$ such that $y_\ell^q - y_\ell = f(x)$. Let $g(F_\ell)$ denote the genus of F_ℓ . Using Condition V.3 it follows from [16, Proposition 3.2.8] that $g(F_\ell) \leq \frac{(q-1)(u^*-1)}{2}$.

Let F be the algebraic function field $F = \mathbb{F}_{q^r}(x, y_0, y_1, \dots, y_{b-1})$, which is the compositum of the function fields F_0, F_1, \dots, F_{b-1} . Let $g(F)$ denote the genus of F . As $\dim_{\mathbb{F}_q} L = b$, it follows from [6, Corollary 6.7] (see also [10, Proposition 3.6] and [17, Lemma 2.4 and (3)]) that

$$g(F) \leq \frac{(q^b - 1)(u^* - 1)}{2}. \quad (42)$$

Let $N^{(\text{aff})}(F)$ denote the number of affine rational places of F . As in the proof of Theorem IV.4, for the Hamming weight $w_H(c^{(b)}(f))$ of $c^{(b)}(f)$ we have

$$w_H(c^{(b)}(f)) = q^r - \frac{N^{(\text{aff})}(F)}{q^b}. \quad (43)$$

Moreover, there is only one rational place of F at infinity. Hence using (42) and Serre's improvement on the Hasse-Weil bound [16, Theorem 5.3.1] yields

$$|N^{(\text{aff})}(F)| \leq q^r + \frac{(q^b - 1)(u^* - 1)}{2} [2 q^{r/2}]. \quad (44)$$

Combining (43) and (44) we complete the proof. \square

Remark 10: There is a codeword of C such that the genus bound (42) is tight. Indeed let $f(x) = a_1 x^{u_1} + a_2 x^{u_2} + \dots + a_\rho x^{u_\rho} \in \mathbb{F}_{q^r}[x] \setminus \{0\}$ such that the coefficient a^* corresponding to x^{u^*} is nonzero. Then the genus bound in (42) becomes equality. This always holds if $\rho = 1$ and we have equality $g(F) = \frac{(q^b - 1)(u^* - 1)}{2}$ in Remark 2 instead of the inequality in (42).

In the next remark we explain how Theorem V.4 generalizes an important result of Yaakobi et. al., namely [19, Theorem 1], to arbitrary b and arbitrary q for some cyclic codes.

First we recall that an algebraic function field F with full constant field \mathbb{F}_q is called a *maximal* function field if it attains the upper bound of Hasse-Weil inequality. Namely if $N(F)$ denotes the rational places of F and $g(F)$ denotes the genus of F , then F is a maximal function field if and only if

$$N(F) = 1 + q^r + 2g(F)q^{r/2}.$$

It is a difficult open problem to characterize all maximal function fields (see, for example, [8], [9], [16]).

For $1 \leq b \leq n - 1$, let $d_b(C)$ denote the minimum b -symbol Hamming weight $w_b(c)$ of codewords as c runs through all nonzero elements of C . Note that $d_b(C)$ is the b -symbol Hamming minimum distance of C . Similarly let $D_b(C)$ denote the maximum b -symbol Hamming weight $w_b(c)$ of codewords as c runs through all nonzero elements of C .

Remark 11: For any fixed b , there are cyclic codes satisfying the conditions of Theorem V.4 such that the lower bound on $w_b(c)$ of Theorem V.4 is tight. For instance these codes can be constructed using some maximal algebraic function fields as follows. Note that there are various examples of algebraic functions fields $F = \mathbb{F}_{q^r}(x, y)$ of the form $A(y) = f(x)$, where $A(y)$ is a given q -additive polynomial of degree q^b splitting over \mathbb{F}_{q^r} and $f(x) \in \mathbb{F}_{q^r}[x]$ is a suitable polynomial. For example if we choose m and put $r = 2m$, then for any divisor $u \mid (q^m + 1)$ we obtain a maximal function field as a subcover of the Hermitian function field $H = \mathbb{F}_{q^{2m}}(x, y)$ given by $y^{q^m} + y = x^{q^{m+1}}$. We refer, for example,

to [1], [8], [9], for the details. Hence if u_1, u_2, \dots, u_ρ are chosen so that u^* becomes a divisor of $(q^m + 1)$, then there is a codeword of C corresponding to a maximal function field of the form $A(y) = a_1 x^{u_1} + a_2 x^{u_2} + \dots + a_\rho x^{u_\rho}$ with full constant field \mathbb{F}_{q^r} for some coefficients $a_1, \dots, a_\rho \in \mathbb{F}_{q^r}$, not all zero. This implies that the lower bound of Theorem V.4 is tight.

For a given $1 \leq b < \min\{k_1, k_2, \dots, k_\mu\}$, let C be a cyclic code such that the lower bound of Theorem V.4 is tight for b . Then for the minimum distance $d_b(C)$ of C we have

$$d_b(C) = q^r - q^{r-b} - \frac{q^b - 1}{q^b} (u^* - 1) q^{r/2}. \quad (45)$$

For $\delta \geq 1$ and assume that $b + \delta \leq \min\{k_1, k_2, \dots, k_\rho\}$ and hence we are in the range for application of Theorem V.4. For $(b + \delta)$ -symbol minimum distance $d_{b+\delta}(C)$ using Theorem V.4 we obtain

$$d_{b+\delta}(C) \geq q^r - q^{r-b-\delta} - \frac{(q^{b+\delta} - 1)}{q^{b+\delta}} (u^* - 1) q^{r/2}. \quad (46)$$

Using (45) and (46) we obtain that

$$d_{b+\delta}(C) \geq \frac{(q^{b+\delta} - 1)}{(q^b - 1)q^\delta} d_b(C). \quad (47)$$

For $q = 2$ and $b = \delta = 1$, then the inequality in (47) coincides with [19, Theorem 1], which holds for arbitrary binary cyclic codes of dimension at least 2. We have many further inequalities in (47) for various values of b, δ and q . For $q = 2$ and some small values of b and δ , the inequality in (47) gives

$$d_2(C) \geq \frac{3}{2} d_1(C), \quad d_3(C) \geq \frac{7}{4} d_1(C), \quad d_3(C) \geq \frac{7}{6} d_2(C).$$

Here if $q = 2$, and $b = \delta = 1$, then we get the constant $3/2$ above, which corresponds to [19, Theorem 1]. For $q = 3$ and some small values of b and δ , the inequality in (47) gives

$$d_2(C) \geq \frac{4}{3} d_1(C), \quad d_3(C) \geq \frac{13}{9} d_1(C), \quad d_3(C) \geq \frac{13}{12} d_2(C).$$

In the next corollary we show that if $d_b(C)$ is tight for some $1 < b \leq \min\{k_1, k_2, \dots, k_\rho\}$ in Theorem V.4, then all $d_\ell(C)$ are tight for $1 \leq \ell \leq b$. Note that there exist C and b such that $d_b(C)$ is tight (see Remark 11).

Corollary 5: We keep the notation and assumptions of Theorem V.4. Assume that there exists an integer b such that $1 < b \leq \min\{k_1, k_2, \dots, k_\rho\}$ such that

$$d_b(C) = q^r - q^{r-b} - \frac{(q^b - 1)(u^* - 1)q^{r/2}}{q^b}.$$

Then for any integer $1 \leq \ell \leq b$ we have

$$d_\ell(C) = q^r - q^{r-\ell} - \frac{(q^\ell - 1)(u^* - 1)q^{r/2}}{q^\ell}.$$

Proof: It follows from the proof of Theorem V.4, there exists $f(x) \in P(\{u_1, u_2, \dots, u_\rho\})$ such that the function field $F = \mathbb{F}_{q^r}(x, y_0, y_1, \dots, y_{b-1})$, where $y_i^q - y_i = f^{(i)}(x)$ for $1 \leq i \leq b - 1$, is a maximal function field. For $1 \leq \ell \leq b - 1$, let F_ℓ be the subfield of F defined as $F_\ell = \mathbb{F}_{q^r}(x, y_0, y_1, \dots, y_{\ell-1})$. It is well known that subcovers of maximal function fields are maximal as well [14]. Hence F_ℓ is a maximal function field (of

a different genus in general). The proof of Theorem V.2 (see also Remark 11) implies that its bound on $d_\ell(C)$ is tight. \square

Remark 12: Note that in Corollary 5, if the equality on $d_b(C)$ holds for some $1 < b \leq \min\{k_1, \dots, k_\rho\}$, then all equalities on the minimum distances $d_\ell(C)$ hold and these values decrease as ℓ decreases. However, in the other direction there is a natural bound by Theorem V.2 and it is important to assume that $b + \delta \leq \min\{k_1, \dots, k_\rho\}$. Indeed if the bound of Theorem V.2 on $d_b(C)$ is tight for an integer $1 \leq b \leq \min\{k_1, k_2, \dots, k_\rho\}$, then $d_{b+\delta} \geq \frac{(q^{b+\delta}-1)}{(q^b-1)q^\delta} d_b(C)$ if $b + \delta \leq \min\{k_1, k_2, \dots, k_\rho\}$. However, it follows from Theorem V.2 that $d_{b+\delta+1}(C) = d_{b+\delta}(C)$ if $b + \delta \geq k_1 + k_2 \dots + k_\rho$.

We also recall that an algebraic function field F with full constant field \mathbb{F}_q is called a *minimal* function field if it attains the lower bound of Hasse-Weil inequality. Namely if $N(F)$ denotes the rational places of F and $g(F)$ denotes the genus of F , then F is a minimal function field if and only if

$$N(F) = 1 + q^r - 2g(F)q^{r/2}.$$

Again characterization of all minimal function fields is a difficult open problem and we have minimal function fields in the form of maximum function fields mentioned above. Therefore considering minimal function fields instead of maximal function fields we have analogous results of Remark 11 and Corollary 5 on the maximum distances $D_b(C)$.

Remark 13: For any fixed b , there are cyclic codes satisfying the conditions of Theorem V.4 such that the upper bound on $w_b(c)$ of Theorem V.4 is tight. For existence we use similar arguments as in Remark 11 and minimal algebraic function fields instead of maximal algebraic function fields.

For a given $1 \leq b < \min\{k_1, k_2, \dots, k_\mu\}$, let C be a cyclic code such that the upper bound of Theorem V.4 is tight for b . Then for the maximal distance $D_b(C)$ of C we have

$$D_b(C) = q^r - q^{r-b} + \frac{q^b - 1}{q^b} (u^* - 1) q^{r/2}. \quad (48)$$

For $\delta \geq 1$ and assume that $b + \delta \leq \min\{k_1, k_2, \dots, k_\rho\}$. For $(b+\delta)$ -symbol minimum distance $d_{b+\delta}(C)$ using Theorem V.4 we obtain

$$D_{b+\delta}(C) \leq q^r - q^{r-b-\delta} + \frac{(q^{b+\delta} - 1)}{q^{b+\delta}} (u^* - 1) q^{r/2}. \quad (49)$$

Using (48) and (49) yield

$$D_{b+\delta}(C) \leq \frac{(q^{b+\delta} - 1)}{(q^b - 1)q^\delta} D_b(C).$$

We present the next corollary on maximum distances, which is an analog of Corollary 5. Its proof follows using similar arguments together with minimal function fields instead of maximal function fields. Note that it is also well known that a subcover of a minimal function field is minimal [14].

Corollary 6: We keep the notation and assumptions of Theorem V.4. Assume that there exists an integer b such that $1 < b \leq \min\{k_1, k_2, \dots, k_\rho\}$ such that

$$D_b(C) = q^r - q^{r-b} + \frac{(q^b - 1)(u^* - 1)q^{r/2}}{q^b}.$$

Then for any integer $1 \leq \ell \leq b$ we have

$$D_\ell(C) = q^r - q^{r-\ell} + \frac{(q^\ell - 1)(u^* - 1)q^{r/2}}{q^\ell}.$$

We can assume that

$$k_1 \leq k_2 \leq \dots \leq k_\rho \quad (50)$$

without loss of generality. It follows from Theorem V.2 that there is no need to consider b -symbol weights if $k_1 + k_2 \dots + k_\rho < b \leq n - 1$. Hence there are exactly $\rho + 1$ regions given below to consider for the full b -symbol weight profile of C :

$$\begin{aligned} \text{Region 0:} & \quad 1 \leq b \leq k_1, \\ \text{Region 1:} & \quad k_1 < b \leq k_2, \\ & \quad \vdots \\ \text{Region } \rho - 1: & \quad k_{\rho-1} < b \leq k_\rho, \\ \text{Region } \rho: & \quad k_\rho < b \leq k_1 + k_2 + \dots + k_\rho. \end{aligned} \quad (51)$$

It follows from (50) that Region 0 corresponds to Theorem V.4. Next we consider the remaining ρ regions. We need the following notation in order to present our results for the remaining regions neatly. For integers $b, u \in \overline{N}$, let $L, U : \overline{N} \times \overline{N} \rightarrow \overline{N}$ be the functions defined as

$$L(b, u) = q^r - q^{r-b} - \left\lfloor \frac{(q^b - 1)(u^* - 1) [2q^{r/2}]}{2q^b} \right\rfloor,$$

and

$$U(b, u) = q^r - q^{r-b} + \left\lfloor \frac{(q^b - 1)(u^* - 1) [2q^{r/2}]}{2q^b} \right\rfloor.$$

Note that the functions L and U depend also on q and r , which we consider to be fixed. Moreover, these functions correspond to the lower and upper bounds of Theorem V.4. It is easy to observe that as the second parameter u increases (and the first parameter b is fixed), $L(b, u)$ is a decreasing function and $U(b, u)$ is an increasing function.

We are ready to present our bounds for Region 1 in the next theorem.

Theorem V.5: We keep the notation and assumptions of Theorem V.4. We also assume that (50) holds without loss of generality. Recall that $u^* = \max\{u_1, \dots, u_\rho\}$ and $w_b(c)$ denotes b -symbol Hamming weight of a nonzero codeword c of C . If b is an integer in Region 1, i.e. $k_1 < b \leq k_2$, then we have

$$\begin{aligned} & \min\{L(b, u^*), L(k_1, u_1)\} \\ & \leq w_b(c) \\ & \leq \max\{U(b, u^*), U(k_1, u_1)\} \end{aligned}$$

Proof: Let $f(x)$ be an arbitrary nonzero polynomial in $P(\{u_1, u_2, \dots, y_\rho\})$. Let $f_1(x)$ and $g(x)$ be the uniquely determined polynomials in $P(\{u_1, u_2, \dots, y_\rho\})$ such that $f_1(x) = a_1 x^{u_1}$, $g(x) = a_2 x^{u_2} + \dots + a_\rho x^{u_\rho}$ and $f(x) = f_1(x) + g(x)$. At least one of the polynomials $f_1(x)$ and $g(x)$ is nonzero.

If $g(x) \neq 0$, then, as $b \leq k_2 = \min\{k_2, k_3, \dots, k_\rho\}$, we have

$$\dim_{\mathbb{F}_q} \text{Span}\{f(x), f^{(1)}(x), \dots, f^{(b-1)}(x)\} = b.$$

1184 Moreover, using the methods of the proof of Theorem V.4 we
1185 obtain that

$$1186 \quad L(b, u^*) \leq w_b(c) \leq U(b, u^*). \quad (52)$$

1187 If $g(x) = 0$ and $f_1(x) \neq 0$, then it follows from Theorem V.2
1188 that $w_b(c) = w_{k_1}(c)$ as $k_1 < b$. Using Theorem V.4 for k_1 ,
1189 we obtain that

$$1190 \quad L(k_1, u_1) \leq w_b(c) \leq U(k_1, u_1). \quad (53)$$

1191 Combining (52) and (53) we complete the proof. \square

1192 These methods apply for all regions in (51). It becomes
1193 more complicated to state these bounds for Region j as j
1194 increases. Next we consider Region 2.

1195 *Theorem V.6:* We keep the notation and assumptions of
1196 Theorem V.4. We also assume that (50) holds without loss
1197 of generality. Recall that $u^* = \max\{u_1, \dots, u_\rho\}$ and $w_b(c)$
1198 denotes b -symbol Hamming weight of a nonzero codeword c
1199 of C . Let b be an integer in Region 2, i.e. $k_2 < b \leq k_3$. Our
1200 bounds in this region is presented depending on two cases as
1201 follows:

1202 **Case $b \leq k_1 + k_2$:** We have

$$1203 \quad \min\{L(b, u^*), L(b, \max\{u_1, u_2\}), L(k_2, u_1), L(k_1, u_1)\} \\ 1204 \quad \leq w_b(c) \leq \\ 1205 \quad \max\{U(b, u^*), U(b, \max\{u_1, u_2\}), U(k_2, u_1), U(k_1, u_1)\}.$$

1206 **Case $k_1 + k_2 < b$:** We have

$$1207 \quad \min\{L(b, u^*), L(k_1 + k_2, \max\{u_1, u_2\}), \\ 1208 \quad L(k_2, u_2), L(k_1, u_1)\} \leq w_b(c) \leq \max\{U(b, u^*), \\ 1209 \quad U(k_1 + k_2, \max\{u_1, u_2\}), U(k_2, u_2), U(k_1, u_1)\}.$$

1210 *Proof:* Let $f_1(x) = a_1x^{u_1}$, $f_2(x) = a_2x^{u_2}$ and $g(x) =$
1211 $a_3x^{u_3} + \dots + a_\rho x^{u_\rho}$ be the polynomials with coefficients from
1212 \mathbb{F}_{q^r} so that their sum $f(x) = f_1(x) + f_2(x) + g(x)$ is not the
1213 zero polynomial.

1214 If $g(x) \neq 0$, then we have that $\dim_{\mathbb{F}_q} \text{Span}$
1215 $\{f(x), f^{(1)}(x), \dots, f^{(b-1)}(x)\} = b$ as $b \leq \min\{k_3, \dots, k_\rho\}$.
1216 Using Theorem V.4 we obtain that

$$1217 \quad L(b, u^*) \leq w_b(c) \leq U(b, u^*). \quad (54)$$

1218 Assume that $g(x) = 0$ and $b \leq k_1 + k_2$. If $a_2 \neq 0$, then using
1219 Theorem V.2 and considering the subcases $a_1 \neq 0$ and $a_1 = 0$
1220 we obtain

$$1221 \quad \min\{L(b, \max\{u_1, u_2\}), L(k_2, u_2)\} \\ 1222 \quad \leq w_b(c) \leq \max\{U(b, \max\{u_1, u_2\}), U(k_2, u_2)\}. \quad (55)$$

1223 If $a_2 = 0$, then $a_1 \neq 0$ and using Theorem V.2 we get

$$1224 \quad L(k_1, u_1) \leq w_b(c) \leq U(k_1, u_1). \quad (56)$$

1225 Combining (54), (55) and (56) we complete the proof of the
1226 case $b \leq k_1 + k_2$.

1227 Next we assume that $g(x) = 0$ and $k_1 + k_2 < b$. If $a_1 \neq 0$
1228 and $a_2 \neq 0$, then using Theorem V.2 we get

$$1229 \quad L(k_1 + k_2, \max\{u_1, u_2\}) \leq w_b(c) \quad (57) \\ 1230 \quad \leq U(k_1 + k_2, \max\{u_1, u_2\})$$

If $a_2 \neq 0$ and $a_1 = 0$, then similarly we have

$$L(k_2, u_2) \leq w_b(c) \leq U(k_2, u_2). \quad (58)$$

1231 Finally if $a_2 = 0$ and $a_1 \neq 0$, then we have

$$L(k_1, u_1) \leq w_b(c) \leq U(k_1, u_1). \quad (59)$$

1232 Combining (54), (57), (58) and (59) we complete the proof of
1233 the case $b < k_1 + k_2$. \square

1234 *Example 7:* Let $q = 2$, $r = 12$, $n = 4095$, $\rho = 2$,
1235 $u_1 = 3$ and $u_2 = 5$ under notation of Theorem V.6. Using
1236 Theorem V.6 we obtain that

$$1237 \quad 2880 \leq w_2(c) \leq 3264, \quad 1240$$

$$1238 \quad 3360 \leq w_3(c) \leq 3808, \quad 1241$$

$$1239 \quad 3600 \leq w_4(c) \leq 4080. \quad 1242$$

1243 Theorems V.4, V.5 and V.6 present a method to obtain
1244 explicit formulas for the bounds on $w_b(c)$ for Region i with
1245 $i \geq 3$ in (51). It is clear that presenting explicit formulas
1246 like in these theorems becomes more involved as the region
1247 number i increases. We refrain ourselves from presenting
1248 explicit formulas for Region i if $3 \leq i \leq \rho$ as they just use
1249 the same ideas and only become more complicated to state.
1250 Nevertheless the proofs of Theorems V.2, V.4, V.5 and V.6 give
1251 a method to derive lower and upper bounds on the b -symbol
1252 Hamming weights of arbitrary nonzero codewords of C using
1253 algebraic curves. Hence we solve this problem for all regions
1254 in (51) implicitly. For any practical situation, and Region i
1255 with $3 \leq i \leq \rho$, the methods of this section would be enough
1256 to obtain explicit formulas as in Theorems V.4, V.5 and V.6.

1257 Next we extend all of our previous bounds in this section
1258 to cyclic codes of length $n \mid (q^r - 1)$. Let C be a cyclic code
1259 of length $n \mid (q^r - 1)$ over \mathbb{F}_q . Let $U_0 = \{u_1, u_2, \dots, u_\rho\}$ be
1260 a basic nonzero set of C . Assume that $U_0 \neq \{0\}$ and each
1261 element of U_0 satisfies Condition V.3. Let $N = \frac{q^r - 1}{n}$. For
1262 integers $0 \leq i$ and $0 \leq u \leq n - 1$, it is easy to observe that

$$1263 \quad uq^i \equiv u \pmod{n} \iff uNq^i \equiv uN \pmod{(q^r - 1)}. \quad (60)$$

1264 Let $\hat{U} = \{u_1 N, u_2 N, \dots, u_\rho N\}$. Using (60) we get that
1265 \hat{U}_0 is a basic nonzero set for a cyclic code \hat{C} of length
1266 $nN = q^r - 1$ over \mathbb{F}_q . Moreover, each element of \hat{U}_0 satisfies
1267 Condition V.3 for the length $q^r - 1$. Let $f(x) = a_1x^{u_1} +$
1268 $a_2x^{u_2} + \dots + a_\rho x^{u_\rho} \in P(U_0)$ be a nonzero polynomial.
1269 Let $c(f) \in C$ be the codeword corresponding to $f(x)$. Put
1270 $\hat{f}(x) = a_1x^{u_1 N} + a_2x^{u_2 N} + \dots + a_\rho x^{u_\rho N} \in P(\hat{U}_0)$. Let
1271 $\hat{c}(\hat{f}) \in \hat{C}$ be the codeword corresponding to $\hat{f}(x)$. As in
1272 the proof of Theorem IV.4 we conclude that for any integer
1273 $1 \leq b \leq n - 1$ we have

$$1274 \quad w_b(c(f)) = \frac{1}{N} w_b(\hat{c}(\hat{f})),$$

1275 where $w_b(c)$ and $w_b(\hat{c})$ denote the b -symbol Hamming weight
1276 of $c(f)$ and $\hat{c}(\hat{f})$, respectively. These arguments yield the
1277 following theorem, which generalizes Theorem V.4.

1278 *Theorem V.7:* Let n be a divisor of $q^r - 1$. Let C be
1279 an arbitrary cyclic code of length n over \mathbb{F}_q . Let $U_0 =$
1280 $\{u_1, u_2, \dots, u_\rho\}$ be a basic nonzero set of C . Assume that
1281 $U_0 \neq \{0\}$ and each element of U_0 satisfies Condition V.3.

Put $N = \frac{q^r - 1}{n}$ and $u^* = \max\{u_1, u_2, \dots, u_\rho\}$. Let $\eta \in \mathbb{F}_{q^r}^*$ be a primitive n -th of 1. For $1 \leq j \leq \rho$ let k_j be the index $[\mathbb{F}_q(\eta^{u_j}) : \mathbb{F}_q]$ of the field extension $\mathbb{F}_q(\eta^{u_j})/\mathbb{F}_q$. Let $c \in C$ be an arbitrary nonzero codeword. For $1 \leq b \leq \min\{k_1, k_2, \dots, k_\rho\}$, let $w_b(c)$ denote the b -symbol Hamming weight of c . We have

$$\frac{1}{N} \left(q^r - q^{r-b} - \left\lfloor \frac{(q^b - 1)(u^*N - 1) \lfloor 2q^{r/2} \rfloor}{2q^b} \right\rfloor \right) \leq w_b(c) \leq \frac{1}{N} \left(q^r - q^{r-b} + \left\lfloor \frac{(q^b - 1)(u^*N - 1) \lfloor 2q^{r/2} \rfloor}{2q^b} \right\rfloor \right).$$

In the following remark we explain how we obtain our bounds for length $n \mid (q^r - 1)$ using our earlier bounds in this section.

Remark 14: Note that the bounds of Theorem V.7 are obtained from the bounds of Theorem V.4 after applying the following two simple operations in order:

- i) change u^* to u^*N and get the numbers L' and U' in place of the lower bound L and the upper bound U of Theorem V.4,
- ii) divide the numbers L' and U' obtained in step i) by $N = \frac{q^r - 1}{n}$ in order to get the lower and the upper bounds of Theorem V.7.

This method applies to all our bounds in Theorems V.4, V.5 and V.6 and we obtain explicit lower and upper bounds for Regions 0, 1 and 2 in (51) for any n dividing $q^r - 1$. Also our arguments after Theorem V.6 regarding the remaining regions, Region i with $3 \leq i \leq \rho$, hold for any length n dividing $q^r - 1$. Therefore we implicitly solve the problem of obtaining formulas on lower and upper bounds of b -symbol weights for these regions if n is an arbitrary positive number dividing $q^r - 1$.

VI. CONCLUSION

Let C be an arbitrary cyclic code of length n over \mathbb{F}_q with $\gcd(n, q) = 1$. Let b be an integer with $1 \leq b \leq n - 1$. We gave tight lower and upper bounds for b -symbol weights of nonzero codewords of C using algebraic curves over finite fields. We obtained a stability theorem for arbitrary cyclic codes so that the weight enumerator of b -symbol Hamming weights of C is the same as the weight enumerator of k -symbol Hamming weight of C if $k \leq b \leq n - 1$. We improved our lower and upper bounds on b -symbol weights of codewords of general cyclic codes for some special subclasses of cyclic codes.

There are still many open problems which require further work in this subject. It is a natural open problem to compute b -symbol Hamming weight enumerators of cyclic codes. Construction of explicit classes of optimal cyclic codes for prescribed b -symbol would also be interesting. Moreover, generalizing our bounds to the repeated root case, i.e. $\gcd(n, q) \neq 1$ is open.

APPENDIX

In this appendix we provide necessary background on algebraic function fields in order to make the paper

self-contained. For further details we refer, for example, to [7], [16].

Let \mathbb{K} be a finite field. An *algebraic function field* F over \mathbb{K} is a finite extension of the rational function field $\mathbb{K}(x)$ such that any element of F that is algebraic over \mathbb{K} is in \mathbb{K} . Here \mathbb{K} is called the *constant field* of F . If $[F : \mathbb{K}(x)] = m$, then there exists a polynomial $h(T) = h_0 + h_1T + \dots + h_mT^m \in \mathbb{K}(x)[T]$ of degree m such that $F = \mathbb{K}(x, y)$ and the minimal polynomial of y over $\mathbb{K}(x)$ is $h(T)$. We also call F as an algebraic function field without mentioning \mathbb{K} if it is clear that the constant field is \mathbb{K} from the context.

The simplest algebraic function field is $F = \mathbb{K}(x)$, where $[F : \mathbb{K}(x)] = 1$.

A valuation ring of F is a ring $\mathcal{O} \subseteq F$ such that

- i) $\mathbb{K} \subsetneq \mathcal{O} \subsetneq F$, and
- ii) for any $z \in F \setminus \{0\}$ we have that either $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

Example 8: Assume that $F = \mathbb{K}(x)$, the rational function field. Let $r(x) \in \mathbb{K}[x]$ be an irreducible polynomial. Then the set

$$\mathcal{O}_{r(x)} = \left\{ \frac{a(x)}{b(x)} : a(x), b(x) \in \mathbb{K}[x], r(x) \nmid b(x) \right\}$$

is a valuation ring of F .

Let \mathcal{O} be a valuation ring of F . The group of units of \mathcal{O} is

$$\mathcal{O}^\times = \{u \in \mathcal{O} : \text{there exists } v \in \mathcal{O} \text{ such that } uv = 1\}.$$

It is well known that \mathcal{O} is a local ring, that there exists a unique maximal ideal P of \mathcal{O} , which is given by $P = \mathcal{O} \setminus \mathcal{O}^\times$.

A *place* P of F is the maximal ideal of a valuation ring \mathcal{O} of F . Conversely the valuation ring \mathcal{O} is also uniquely determined by its place P as follows: $\mathcal{O} = \{z \in F \setminus \{0\} : z^{-1} \notin P\} \cup \{0\}$. We denote it \mathcal{O}_P and call it the valuation ring of P .

Let P be a place of F . There exists an element $t \in P$ such that $P = t\mathcal{O}$. This element is not necessarily unique. Such an element is called a local parameter of P . As P is the maximal ideal of its valuation ring \mathcal{O}_P , the quotient ring $F_P = \mathcal{O}_P/P$ is a field. F_P is called the residue field of P . It is well known that F_P is a finite extension of \mathbb{K} and the extension degree $[F_P : \mathbb{K}]$ is called the *degree* of P . If the degree of P is one, then we also call that P is a *rational place*.

Example 9: Assume that $\mathbb{K} = \mathbb{F}_q$ and $F = \mathbb{F}_q(x)$, the rational function field over \mathbb{F}_q . There are exactly $q + 1$ rational places (degree one places) of F and they are given as follows:

- i) For $\alpha \in \mathbb{F}_q$, let

$$P_\alpha = \left\{ \frac{a(x)}{b(x)} : a(\alpha) = 0, b(\alpha) \neq 0 \right\}, \quad (61)$$

where $a(x)$ and $b(x) \in \mathbb{F}_q[x]$. These form q (affine) rational places of F .

- ii) There is one rational place at infinity of F . It is defined as

$$P_\infty = \left\{ \frac{a(x)}{b(x)} : \deg a(x) < \deg b(x) \right\}, \quad (62)$$

where $a(x)$ and $b(x) \in \mathbb{F}_q[x]$.

In general, for $m \geq 1$, an arbitrary place of $\mathbb{F}_q(x)$ of degree m , different from P_∞ , is obtained as follows. Let $r(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m . Then

$$P_{r(x)} = \left\{ \frac{a(x)}{b(x)} : r(x) \mid a(x), r(x) \nmid b(x) \right\}, \quad (63)$$

where $a(x)$ and $b(x) \in \mathbb{F}_q[x]$. is a degree m place of F . The notation in (61) and (63) coincide for degree one places: $P_\alpha = P_{x-\alpha}$ if $\alpha \in \mathbb{F}_q$.

Let P be a place of F . Let \mathcal{O}_P be its valuation ring and \mathcal{O}_P^\times be the group of units in \mathcal{O}_P . We choose a local parameter t of P . The discrete valuation v_P is a map corresponding to P , which is defined as

$$v_P : F \rightarrow \mathbb{Z} \cup \{\infty\}$$

$$z \mapsto \begin{cases} n & \text{if there exists } n \in \mathbb{Z} \\ & \text{and } u \in \mathcal{O}_P^\times \text{ such that } z = t^n u, \\ \infty & \text{otherwise (or equivalently if } z = 0) \end{cases}$$

It is well known that v_P is independent from the choice of the local parameter.

Assume that E and F are algebraic function fields with the same full constant field \mathbb{K} . Assume further that E is a finite extension of F . Let P be a place of E . Then $P' = P \cap F$ is a place of F . Moreover the residue field F_P is a finite extension of the residue field $F_{P'}$. The extension degree $[F_P : F_{P'}]$ is called the inertia degree of $P|P'$ and its is denoted as $f(P|P')$. In particular P is a rational place of E if and only if P' is a rational place of F and $f(P|P') = 1$. Moreover there exists an integer e such that

$$v_P(z) = e v_{P'}(z) \text{ for all } z \in F.$$

This integer is called the ramification index of $P|P'$ and it is denoted as $e(P|P')$. Conversely if Q is a place of F , then there are a finite number of places Q_1, \dots, Q_ℓ in E such that $Q_i \cap F = Q$ for $1 \leq i \leq \ell$. A fundamental fact is that

$$\sum_{i=1}^{\ell} e(Q_i|Q) f(Q_i|Q) = [E : F].$$

Let $s \geq 1$ be an integer. Let F be an algebraic function field with full constant field \mathbb{F}_q . Let $F \cdot \mathbb{F}_{q^s}$ be the smallest extension of F containing \mathbb{F}_{q^s} . Note that for $s = 1$ we have $F = F \cdot \mathbb{F}_q$. Let $N(F \cdot \mathbb{F}_{q^s})$ denote the number of rational places of $F \cdot \mathbb{F}_{q^s}$. The Hasse-Weil bound [16, Theorem 5.2.3] states that there exists a nonnegative integer $g(F)$, which depends only on F , such that for each positive s integer we have

$$|N(F \cdot \mathbb{F}_{q^s}) - (q^s + 1)| \leq 2g(F)q^{s/2}. \quad (64)$$

The integer $g(F)$ in (64) is called the *genus* of F . The definition of genus using (64) is not very common, which is an arithmetic method of definition. This definition requires the presentation of the Hasse-Weil bound for all constant field extension $F \cdot \mathbb{F}_{q^s}$ with $s \geq 1$. When we state the Hasse-Weil bound, we usually refer to the version of (64) with $s = 1$ only. Alternative definitions of genus would require further background like Riemann-Roch Theorem and ramification theory, which we do not need in this paper.

There is an improvement of the Hasse-Weil bound, which is Serre's improvement (see [16, Theorem 5.3.1]). It states that

if F is an algebraic function field with full constant field \mathbb{F}_q , then

$$|N(F) - (q + 1)| \leq g(F) \left[2 q^{1/2} \right]. \quad (65)$$

Let F be an algebraic function field with full constant field \mathbb{F}_q . Assume that F is an extension of the rational function field $\mathbb{F}_q(x)$. Let P be a rational place of F . Recall that $\mathbb{F}_q(x)$ has exactly $q + 1$ rational places. The affine rational places of $\mathbb{F}_q(x)$ are P_α ; where $\alpha \in \mathbb{F}_q$, and P_α defined in (61) in Example 9 above.

In general we call that P is an *affine rational place* of F if $P \cap F = P_\alpha$ for an $\alpha \in \mathbb{F}_q$. Otherwise we call that P is a place of F *at infinity*.

Example 10: Let $r \geq 2$ be an integer. Let $a(x) \in \mathbb{F}_{q^r}[x]$ be a polynomial of degree coprime to q . Let $\mathbb{F}_{q^r}(x)[y]/\langle y^q - y - a(x) \rangle$. Then $F/\mathbb{F}_{q^r}(x)$ is a field extension of degree q and the full constant field of F is \mathbb{F}_{q^r} .

As in Example 9, for $\alpha \in \mathbb{F}_{q^r}$, let P_α be an affine rational place of \mathbb{F}_{q^r} , which corresponds to the irreducible polynomial $x - \alpha \in \mathbb{F}_{q^r}[x]$. Let P_∞ denote the remaining rational place of $\mathbb{F}_{q^r}(x)$, which corresponds to the pole of $x \in \mathbb{F}_{q^r}(x)$.

The following characterization of all rational places of F is known. Recall that $\text{Tr} : \mathbb{F}_{q^r} \rightarrow \mathbb{F}_q$ is the trace map $x \mapsto x + x^q + \dots + x^{q^{r-1}}$. For $\alpha \in \mathbb{F}_{q^r}$ and the affine place P_α of $\mathbb{F}_{q^r}(x)$ we have two cases to consider:

- **Case** $\text{Tr}(a(\alpha)) = 0$: In this case there are exactly q rational places $Q_{\alpha,1}, Q_{\alpha,2}, \dots, Q_{\alpha,q}$ of F such that $Q_{\alpha,i} \cap F = P_\alpha$ for each $1 \leq i \leq q$.
- **Case** $\text{Tr}(a(\alpha)) \neq 0$: In this case there is no rational place Q of F such that $Q \cap F = P_\alpha$.

Moreover there is a unique rational place Q_∞ of F such that $Q_\infty \cap F = P_\infty$.

Let $N^{(\text{aff})}(F)$ denote the number of affine rational places of F . These arguments imply that

$$N^{(\text{aff})}(F) = N(F) - 1$$

and

$$N^{(\text{aff})}(F) = q |\{ \alpha \in \mathbb{F}_{q^r} : \text{Tr}(a(\alpha)) \}|.$$

ACKNOWLEDGMENT

The authors extend thanks to the anonymous reviewers and the associate editor for their valuable comments and suggestions, which improved the quality and presentation of the manuscript.

REFERENCES

- [1] E. Çakçak and F. Özbudak, "Some Artin-Schreier type function fields over finite fields with prescribed genus and number of rational places," *J. Pure Appl. Algebra*, vol. 210, no. 1, pp. 113–135, Jul. 2007.
- [2] Y. Cassuto and M. Blaum, "Codes for symbol-pair read channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, USA, Jun. 2010, pp. 988–992.
- [3] Y. Cassuto and M. Blaum, "Codes for symbol-pair read channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 12, pp. 8011–8020, Dec. 2011.
- [4] Y. Cassuto and S. Litsyn, "Symbol-pair codes: Algebraic constructions and asymptotic bounds," in *Proc. IEEE Int. Symp. Inf. Theory Process.*, St. Petersburg, Russia, Jul. 2011, pp. 2348–2352.

- 1485 [5] C. Ding and J. Yang, "Hamming weights in irreducible cyclic codes," *Discrete Math.*, vol. 313, no. 4, pp. 434–446, Feb. 2013.
- 1486
- 1487 [6] I. Duursma, H. Stichtenoth, and C. Voss, "Generalized Hamming
- 1488 weights for duals of BCH codes, and maximal algebraic function fields,"
- 1489 in *Arithmetic Geometry and Coding Theory*, R. Pellikaan, M. Perret, and
- 1490 S. G. Vlăduț, Eds. 1996, pp. 53–65.
- 1491 [7] A. Garcia and H. Stichtenoth, "Algebraic function fields over finite fields
- 1492 with many rational places," *IEEE Trans. Inf. Theory*, vol. 41, no. 6,
- 1493 pp. 1548–1563, Nov. 1995.
- 1494 [8] A. Garcia, H. Stichtenoth, and C. Xing, "On subfields of the Her-
- 1495 mitian function field," *Compos. Math.*, vol. 120, no. 2, pp. 137–170,
- 1496 2000.
- 1497 [9] A. Garcia and F. Özbudak, "Some maximal function fields and additive
- 1498 polynomials," *Commun. Algebra*, vol. 35, no. 5, pp. 1553–1566,
- 1499 May 2007.
- 1500 [10] C. Găneri and F. Özbudak, "Improvements on generalized Hamming
- 1501 weights of some trace codes," *Des., Codes Cryptogr.*, vol. 39, no. 2,
- 1502 pp. 215–231, May 2006.
- 1503 [11] C. Güneri and F. Özbudak, "Weil-serre type bounds for cyclic
- 1504 codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5381–5395,
- 1505 Dec. 2008.
- 1506 [12] C. Güneri, F. Özbudak, and F. Özdemir, "Hasse–Weil bound for additive
- 1507 cyclic codes," *Des., Codes Cryptogr.*, vol. 82, nos. 1–2, pp. 249–263,
- 1508 Jan. 2017.
- 1509 [13] X. Kai, S. Zhu, and P. Li, "A construction of new MDS symbol-
- 1510 pair codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 5828–5834,
- 1511 Nov. 2015.
- 1512 [14] G. Lachaud, "Sommes d'eisenstein et nombre de points de certaines
- 1513 courbes algébriques sur les corps finis," *CR Acad. Sci. Paris*, vol. 305,
- 1514 pp. 729–732, Oct. 1987.
- 1515 [15] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting*
- 1516 *Codes*. Amsterdam, The Netherlands: North Holland, 1977.
- 1517 [16] H. Stichtenoth, *Algebraic Function Fields and Codes*, vol. 254.
- 1518 New York, NY, USA: Springer, 2009.
- 1519 [17] G. van der Geer and M. van der Vlugt, "Fibre products
- 1520 of Artin-Schreier curves and generalized Hamming weights of
- 1521 codes," *J. Combinat. Theory A*, vol. 70, no. 2, pp. 337–348,
- 1522 May 1995.
- 1523 [18] J. Wolfmann, "New bounds on cyclic codes from algebraic curves," in
- 1524 *Coding Theory and Applications* (Lecture Notes in Computer Science),
- 1525 vol. 70. Toulon, France: Springer, 1988, pp. 47–62.
- 1526 [19] E. Yaakobi, J. Bruck, and P. H. Siegel, "Constructions and decoding
- 1527 of cyclic codes over b -symbol read channels," *IEEE Trans. Inf. Theory*,
- 1528 vol. 62, no. 4, pp. 1541–1551, Apr. 2016.

Minjia Shi received the B.S. degree in mathematics from Anqing Normal University, China, in 2004, the M.S. degree in mathematics from the Hefei University of Technology, China, in 2007, and the Ph.D. degree from the Institute of Computer Network Systems, Hefei University of Technology, China, in 2010. From August 2012 to August 2013, he was a Visiting Researcher with the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. From July 2016 to August 2016, he was a Visiting Researcher with Telecom Paris Tech, Paris, France. Later, he visited the Sobolev Institute of Mathematics, in 2020. He has been teaching with the School of Mathematical Sciences, Anhui University, China, since 2007, where he has been a Master's Supervisor and an Associate Professor, since April 2012, and a Professor, since 2017. He has been a Ph.D. Supervisor, since 2014. He is the author of over 100 journal articles and two books. His research interests include algebraic coding theory and cryptography.

Feruh Özbudak received the B.S. degree in electrical and electronics engineering and the Ph.D. degree in mathematics from Bilkent University, Ankara, Turkey, in 1993 and 1997, respectively. He is currently a Professor with Middle East Technical University, Ankara. His research interests include algebraic curves, codes, sequences, cryptography, finite fields, and finite rings.

Patrick Solé received the Ingénieur and Docteur Ingénieur degrees from the Ecole Nationale Supérieure des Télécommunications, Paris, France, in 1984 and 1987, respectively, and the Habilitation Diriger Des Recherches from the Université de Nice-Sophia Antipolis, Sophia Antipolis, France, in 1993. He has held visiting positions at Syracuse University, Syracuse, NY, USA, from 1987 to 1989, Macquarie University, Sydney, NSW, Australia, from 1994 to 1996, and Lille University, Lille, France, from 1999 to 2000. Since 1989, he has been a Permanent Member of the CNRS and became a Directeur de Recherche, in 1996. He is currently a member of the CNRS lab I2M, Marseilles, France. He is the author of more than 180 journal articles and four books. His research interests include coding theory (codes over rings, quasi-cyclic codes), interconnection networks (graph spectra, expanders), vector quantization (lattices), and cryptography (Boolean functions, pseudo random sequences). He was a co-recipient of the Best Paper Award for Information Theory, in 1995, given by the Information Theory Chapter of the IEEE. He was an Associate Editor of the IEEE TRANSACTIONS ON INFORMATION THEORY, from 1996 to 1999.