How many weights can a quasi-cyclic code have ?

Minjia Shi, Alessandro Neri, Patrick Solé

How many weights can a quasi-cyclic code have ?

Minjia Shi[1], Alessandro Neri[2], Patrick Solé[3]
[1]School of Mathematical Sciences, Anhui University, Hefei, 230601, China
[2]Institute for Communications Engineering, Technical University of Munich (TUM), Germany
[3]I2M,(Aix-Marseille Univ., Centrale Marseille, CNRS), Marseilles, France

***Abstract*—We investigate the largest number of nonzero weights of quasi-cyclic codes. In particular, we focus on the function $\Gamma_Q(n,\ell,k,q)$, that is defined to be the largest number of nonzero weights a quasi-cyclic code of index $\gcd(\ell,n)$, length n and dimension k over $\mathbb{F}_q$ can have, and connect it to similar functions related to linear and cyclic codes. We provide several upper and lower bounds on this function, using different techniques and studying its asymptotic behavior. Moreover, we determine the smallest index for which a q-ary Reed-Muller code is quasi-cyclic, a result of independent interest.**

***Index Terms*—Quasi-cyclic codes, weights, q-ary Reed-Muller codes**

I. Introduction

The importance of the number of distinct distances in a code was already pointed out by Delsarte in 1973 in [10]. In that paper, he studied for a given code C, the relations between this value, the number of distinct distances for the dual code $C^\perp$, and the minimum distances of C and $C^\perp$, obtaining interesting results on the weight distributions of cosets of a code. It is easy to see that when one restricts the study to linear codes, then this number coincides with the number of non-zero weights. Further studies on determining the number of weights of a given linear code can be traced back to 1963. In [22], MacWilliams dealt with the problem to establish if, given a finite set of positive integer S, it is possible to construct a code whose set of non-zero weights is precisely S. Also, Assmus and Mattson investigated on the number of non-zero weights of a code in [5], using this value to give a connection between codes and designs. Another useful application deriving from this number can be found in the works of Hill and Lizak [17], [16], who gave conditions on extendability of codes based on the number of their non-zero weights.

More recently, additional results on the number of weights of MDS codes were obtained by Ezerman, Grassl and Solé in [12]. They determined this number for all the MDS codes (assuming that the MDS conjecture is true). Their motivation was due to recent results of Rains ([25]) and Grassl, Röttler and Beth ([13], [26]), who constructed quantum error-correcting codes relying on the existence of codewords of a given weight in a classical block code. New lights on MDS codes without assuming the MDS conjecture were recently shed by Alderson in [2].

A current research topic is to study the maximum number of nonzero weights of codes belonging to some special class of codes. This series of problems in extremal combinatorics started in [28], where Shi, Zhu, Solé and Cohen investigated the class of linear codes. They introduced the functions $L(n,k,q)$ and $L(k,q)$ which represent respectively the maximum number of nonzero weights of an $[n,k]$ code, and the maximum number of nonzero weights of a k-dimensional code, with no restriction on the length. In that paper, some results on these two functions were provided, leaving as on open conjecture that the value $L(k,q)$ is always equal to $\frac{q^k-1}{q-1}$, Such a conjecture was proved to be true in [3], where Alderson and Neri introduced the notion of maximum weight spectrum codes (or MWS codes in short). These codes were studied also by other authors for their combinatorial interest (see [24], [9], [1]). Moreover, the function $L(n,k,q)$ was also studied in

M. Shi is supported by National Natural Science Foundation of China (61672036), Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20), the Academic Fund for Outstanding Talents in Universities (gxbjZD03).

A. Neri is supported by the Swiss National Science Foundation through grant no. 187711.

[28], and new answers were then provided by Alderson in [1]. He defined and studied the combinatorial properties of full weight spectrum codes (or FWS codes in short), which are codes of length n with exactly n nonzero weights. Finally, in [27], Shi, Li, Neri and Solé conducted a study on the weights of cyclic codes, determining upper and lower bounds, and finding the number of weights of all the q-ary Hamming codes, and of many q-ary Reed-Muller codes.

In this paper, we will consider the weights of quasi-cyclic codes, which represent the missing link between linear codes and cyclic codes. This point of view gives interesting results connecting these three families of codes. Concretely, we investigate on the function $\Gamma_Q(n, \ell, k, q)$, which is the maximum number of distinct weights that an $[n, k]$ quasi-cyclic code of index $\gcd(\ell, n)$ can have over the finite field $\mathbb{F}_q$. We derive some upper bounds on this number, analyzing the interplay between the cycle structure of the automorphism group of a quasi-cyclic code and the arithmetic of the underlying finite field. Lower bounds are obtained next, using four different approaches. Firstly, we reduce to lower bounds for linear codes, using the construction of quasi-cyclic codes via direct product. This will result in determining the exact values of $\Gamma_Q(n, \ell, k, q)$ for some set of parameters. A second approach is to study the automorphism group of q-ary Reed -Muller codes. In Theorem 12 we characterize all the possible integers ℓ for which a q-ary Reed-Muller code is quasi-cyclic of index ℓ. Besides its importance as a result in itself, we also use it to determine lower bounds on the function $\Gamma_Q(n, \ell, k, q)$ for some set of parameters. Additional lower bounds are obtained using the connection with cyclic codes and with the covering radius of the dual code via the celebrated Delsarte bound [10]. We also present asymptotic results on this function, which allow us to determine its behavior for long quasi-cyclic codes of fixed rates.

The material is arranged as follows. Section II contains the necessary terminology and definitions on linear codes, quasi-cyclic codes and on the combinatorial functions that we investigate. Section III is dedicated to the upper bounds on the number of weights that a quasi-cyclic code can have. This is done by analyzing the relations between the cycle structure of the automorphism group of a quasi-cyclic code and the arithmetic of the underlying finite field. In Section IV we focus on the lower bounds. We use different approaches for this purpose, exploiting the connections with linear codes and cyclic codes, and using the said Delsarte bound on the covering radius of the dual code. Moreover, in the same section, we study the quasi-cyclicity of q-ary Reed-Muller codes, characterizing the indices for which they are quasi-cyclic. Section V considers an asymptotic approach for the estimate of the maximum number of weights that a quasi-cyclic code can have, producing interesting answers for long quasi-cyclic codes. Section VI contains some numerical values in the case of binary quasi-cyclic codes, leading to a challenging conjecture. Finally, we share our conclusions and some open problems in Section VII.

II. Definitions and Notation

In this section we recall some preliminary notions of algebraic coding theory, introducing linear codes, quasi-cyclic codes and the combinatorial functions we are going to study in our paper.

A. Linear codes

A **(linear) code** C of length n over a finite field $\mathbb{F}_q$ is an $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q^n$. The dimension of the code is its dimension as an $\mathbb{F}_q$-vector space, and is denoted by k. A linear code of length n and dimension k over $\mathbb{F}_q$ will be denoted for brevity by $[n, k]_q$ code. The elements of C are called **codewords**.

The **dual** $C^\perp$ of a code C is the orthogonal subspace taken with respect to the standard inner product.

The **(Hamming) weight** of $\mathbf{x} \in \mathbb{F}_q^N$ is the number of indices i where $x_i \neq 0$, and it is denoted by $\mathrm{wt}_H(\mathbf{x})$. Moreover, the **(Hamming) distance** between two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$ is the quantity $d_H(u, v) = \mathrm{wt}_H(u - v)$. The minimum nonzero weight d of a linear code is called the **minimum distance**.

The set of weights of a linear code C (including the 0) is denoted by $\mathrm{wt}(C)$, and the number of nonzero weights of C by $s(C)$, i.e. $\mathrm{wt}(C) = \{\mathrm{wt}_H(c) \mid c \in C\}$ and $s(C) = |\mathrm{wt}(C) \setminus \{0\}| = |\mathrm{wt}(C)| - 1$.

B. Quasi-Cyclic codes

A **quasi-cyclic (QC) code** is a linear code invariant under some positive power α of the cyclic shift ρ. The

smallest such power is called the **index** of the QC code and denoted by ℓ. Let us write $n = Q\ell + R$ with $0 \leq R < \ell$. Since $\rho^n = \mathrm{id}$, then $C = \rho^n(C) = \rho^R(\rho^{Q\ell}(C) = \rho^R(C)$, which by minimality of ℓ implies $R = 0$. Hence, the index ℓ divides the length n of the code. The quotient n/ℓ is called the **co-index**. The **period** t of a codeword $\mathbf{c}$ is the smallest positive power of the shift under which the codeword is invariant, i.e. $\rho^t(\mathbf{c}) = \mathbf{c}$. Furthermore, a quasi-cyclic code of co-index m such that all its nonzero codewords have period m is called **strongly quasi-cyclic**.

A **quasi-cyclic class of index** ℓ of a quasi-cyclic code is the set of all codewords obtained by action of the ℓ-shift ρ^ℓ on a given codeword.

As is well known, QC codes of index ℓ, and co-index m over $\mathbb{F}_q$ are R-submodules of R^ℓ, where $R = \frac{\mathbb{F}_q[x]}{(x^m-1)}$ [20]. When this module has exactly one generator, the code is called **one-generator**.

C. Combinatorial functions

In this subsection we introduce the combinatorial functions we are going to study in this work. We fix a prime power q and two positive integers k, n such that $1 \leq k \leq n$. We recall the following two functions from [27]. We define $\Gamma_C(k, q)$ as the largest number of nonzero weights of a cyclic code of dimension k over $\mathbb{F}_q$. Moreover, we define $\Gamma_C(n, k, q)$ as the largest number of nonzero weights of a cyclic code of fixed length n and dimension k over $\mathbb{F}_q$ if such a code exists, and by zero otherwise.

Let ℓ be an arbitrary positive integer. Define $\Gamma_Q(\ell, k, q)$ to be the largest number of nonzero weights of a QC code of index $\gcd(\ell, n)$ and dimension k over $\mathbb{F}_q$. Clearly, $\Gamma_Q(1, k, q) = \Gamma_C(k, q)$.

Furthermore, we define $\Gamma_Q(n, \ell, k, q)$ as the largest number of nonzero weights of a QC code of fixed length n, index $\gcd(\ell, n)$, and dimension k over $\mathbb{F}_q$, if such a code exists, and by zero otherwise. Thus, $\Gamma_Q(n, 1, k, q) = \Gamma_C(n, k, q)$. The same functions for strongly QC codes are denoted by $\Gamma^0_Q(\ell, k, q)$, and $\Gamma^0_Q(n, \ell, k, q)$, respectively. Note that we have defined these combinatorial functions in such a way they are defined for every integer ℓ and not only for those dividing n.

Moreover, let $\Lambda(m, k, q)$ be the largest number of nonzero weights of a QC code of co-index m, and dimension k, over $\mathbb{F}_q$, if such a code exists, and by zero otherwise. The same function for strongly QC codes is denoted by $\Lambda^0(m, k, q)$. Finally, recall the functions $L(k, q)$ and $L(n, k, q)$ introduced and studied in [28], which are defined respectively to be the maximum number of nonzero weights of a linear code of dimension k over $\mathbb{F}_q$, and the maximum number of nonzero weights of a linear code with length n and dimension k over the same field $\mathbb{F}_q$. These two functions were deeply studied in the last few years. $L(k, q)$ was shown to be equal to $\frac{q^k-1}{q-1}$ in [3], while some partial results on $L(n, k, q)$ were given in [1], [28].

III. Upper bounds

In this section we produce upper bounds on the number of weights of quasi-cyclic codes, depending on the length, the dimension, the index and the underlying finite field. In particular, we will use the interplay of the arithmetic of these parameters in order to derive non-trivial upper bounds.

Recall that $\rho : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ denotes the right shift operator on the vector space $\mathbb{F}_q^n$. We need Lemma 1 from [27], whose proof is omitted.

Lemma 1. *Let C be an $[n, k]_q$ QC code and $c \in C$ be a nonzero codeword of period t. Let moreover $\alpha \in \mathbb{F}_q^*$ and $i \in \{0, \ldots, n-1\}$ such that*

$$\alpha c = \rho^i(c).$$

Then, $\alpha^r = 1$, where $r = \frac{t}{\gcd(t,i)}$. Moreover, α belongs to the unique cyclic subgroup of $\mathbb{F}_q^*$ of order $\gcd(t, q-1)$.

Using Lemma 1, we can prove the following upper bound on the number of nonzero weights in quasi-cyclic codes.

Lemma 2. *If C is an $[n, k]_q$ quasi-cyclic code of index ℓ, then*

$$s(C) \leq \sum_{t|n} \frac{\gcd(\ell, t) B_t}{\mathrm{lcm}(t, q-1)} \leq 1 + \sum_{1<t|n} \frac{\gcd(\ell, t) B_t}{\mathrm{lcm}(t, q-1)},$$

where B_t the number of nonzero codewords of period t contained in C.

Proof: The proof follows the same idea of the one of [27, Lemma 2]. Consider a quasi-cyclic class $\{\rho^{i\ell}(\mathbf{c}) : 0 \leq i \leq \frac{n}{\ell} - 1\}$ of a given codeword c

which has period t. Clearly, we have $\rho^{\mathrm{lcm}(\ell,t)}(\mathbf{c}) = \mathbf{c}$. Moreover, since $\mathrm{lcm}(\ell, t)$ is the first positive multiple of ℓ that is divisible by t, by definition of B_t we also have that all the the elements $\rho^{i\ell}(\mathbf{c})$ for $0 \leq i \leq \frac{n}{\ell} - 1$ are pairwise distinct, and the quasi-cyclic class has exactly $\frac{\mathrm{lcm}(\ell,t}{\ell}$ elements. Therefore, the number of quasi-cyclic classes with index ℓ of codewords of period t is $\frac{B_t \ell}{\mathrm{lcm}(\ell,t)} = \frac{\gcd(\ell,t)B_t}{t}$. All the codewords in the same class share the same weight. Now, we can use Lemma 1. Let $\mathbf{c} \in C$ be a codeword and H be the unique subgroup of $\mathbb{F}_q^*$ of order $\gcd(t, q-1)$. For every representative α of $\mathbb{F}_q^*/H$, the codeword $\alpha\mathbf{c}$ gives a different class that shares the same weight with $\mathbf{c}$. Hence, there are at most $\frac{\gcd(\ell,t)B_t \gcd(t,q-1)}{t(q-1)} = \frac{\gcd(\ell,t)B_t}{\mathrm{lcm}(t,q-1)}$ distinct weights among these codewords, showing the first inequality. Moreover, if a codeword has period 1 then it is necessarily a multiple of the all ones vector, and therefore $B_1 \in \{0, q-1\}$. This proves the second inequality. ∎

Theorem 3. *If C is a $[n,k]_q$ strongly quasi-cyclic code of index ℓ, then*

$$s(C) \leq \frac{\ell(q^k - 1)}{\mathrm{lcm}(q-1, n)}.$$

Thus $\Gamma_Q^0(n, \ell, k, q) \leq \frac{\gcd(\ell,n)(q^k-1)}{\mathrm{lcm}(q-1,n)}$.

Proof: We apply Lemma 2 when $B_t = 0$ for $t \neq \frac{n}{\ell}$, so that the sum in the right hand side contains only one summand. ∎

Remark. Observe that when we have $\ell = 1$, i.e. when we consider cyclic codes, the results above coincide with those obtained in [27]. Moreover, the upper bounds obtained in both Lemma 2 and Theorem 3 are consistent with the fact that any quasi-cyclic code of index ℓ is invariant under the power ℓr of the shift, provided that ℓr divides n. Indeed, in this case, one can easily check that the upper bound for ℓr is always greater or equal than the one for ℓ.

From Lemma 2 we can derive an upper bound also on the function $\Gamma_Q(n, \ell, k, q)$, as shown in the following result.

Theorem 4. *Let C be an $[n,k]_q$ quasi-cyclic code of index ℓ over $\mathbb{F}_q$. Then*

$$s(C) \leq 1 + \left(q^k - 1\right) \left(\sum_{1<t|n} \left(\frac{\gcd(\ell,t)}{\mathrm{lcm}(t, q-1)} \right)^2 \right)^{\frac{1}{2}}.$$

Proof: From Lemma 2, we have

$$(s(C) - 1) \leq \sum_{1<t|n} \frac{\gcd(\ell,t)B_t}{\mathrm{lcm}(t, q-1)}.$$

Applying Cauchy-Schwartz inequality we get

$$s(C) \leq 1 + \left(\sum_{1<t|n} B_t^2 \right)^{\frac{1}{2}} \left(\sum_{1<t|n} \left(\frac{\gcd(\ell,t)}{\mathrm{lcm}(\ell, q-1)} \right)^2 \right)^{\frac{1}{2}}.$$

The result follows by observing that

$$\sum_{1<t|n} B_t^2 \leq \Big(\sum_{1<t|n} B_t \Big)^2 \leq (q^k - 1)^2.$$

∎

A result that differentiates strongly QC codes from QC codes is the following.

Theorem 5. *If C is a $[n,k]_q$ strongly quasi-cyclic code of co-index m, then $s(C) \leq \frac{q^k-1}{m}$. Thus*

$$\Lambda^0(m, k, q) \leq \frac{q^k - 1}{m}.$$

Proof: If C is strongly quasi-cyclic then all cycle classes have size m, and contain codewords of the same weight. The result follows since the total number of nonzero codewords is $q^k - 1$. ∎

IV. Lower bounds

In this section we focus on the lower bounds for the functions $\Gamma_Q(n, \ell, k, q)$ and $\Gamma_Q(\ell, k, q)$. We use four different approaches here. First, we reduce to lower bounds for linear codes, using a well-known construction of quasi-cyclic codes using the direct product with the universe code. This will result in determining the exact values of $\Gamma_Q(n, \ell, k, q)$ for some set of parameters. In particular, we will show in Theorem 8 that whenever $\ell \leq 2^k - 1$, there exist codes of co-index m and dimension mk with all the possible weights. A second approach is to study q-ary Reed-Muller codes. We characterize in Theorem 12 all the possible integers ℓ for which a q-ary Reed-Muller code is quasi-cyclic of index ℓ. Besides the importance of the result *per se*, we also use it to determine lower bounds on the function $\Gamma_Q(n, \ell, k, q)$ for some set of parameters. Additional lower bounds are obtained using the fact that a cyclic code is in particular a quasi-cyclic code of every index ℓ dividing its length. Finally, we relate the function $\Gamma_Q(n, \ell, k, q)$ with the maximum covering radius of an $[n, n-k]_q$ quasi-cyclic code of index ℓ, using the celebrated Delsarte bound [10].

A. Reduction to linear codes

In this subsection we explain how to construct quasi-cyclic codes by using the direct product technique. This will produce, as a consequence, lower bounds based on the maximum number of weights of a linear code.

Recall that given an $[n_1, k_1]$ code C_1 and an $[n_2, k_2]$ code C_2 over the same finite field $\mathbb{F}_q$, the **direct product** $C_1 \otimes C_2$ is the $[n_1 n_2, k_1 k_2]$ code over $\mathbb{F}_q$ given by

$$C_1 \otimes C_2 := \{u \otimes v \mid u \in C_1, v \in C_2\},$$

where $u \otimes v$ denotes the Kronecker product of two vectors, and it is defined as $(u \otimes v)_{i,j} = u_i v_j$. See also [23, Chapt. 18] for a more detailed explanation.

Denote by U_m the universe code of parameters $[m, m]$ over $\mathbb{F}_q$. Let C be an $[\ell, k]$ code over $\mathbb{F}_q$. The direct product $C \otimes U_m$ of C and U_m is an $[\ell m, km]$ code. It is clear that it is a QC code of index ℓ, since a valid generator matrix of U_m is the identity matrix of order m, a circulant matrix.

Now, for two sets $A, B \subseteq \mathbb{N}$ and a positive integer r, we define the sets $A \oplus B := \{a + b \mid a \in A, b \in B\}$ and $r \cdot A := \{ra \mid a \in A\}$. With this notation, we have the following result.

Lemma 6. *Let C be an $[\ell, k]$ code and let U_m be the universe code of length m. Then, for every $r_1, \ldots, r_t \in \mathbb{N}$ such that $r_1 + \ldots + r_t \leq m$ we have*

$$\mathrm{wt}(C \otimes U_m) \supseteq r_1 \cdot \mathrm{wt}(C) \oplus \ldots \oplus r_t \cdot \mathrm{wt}(C).$$

In particular

$$\mathrm{wt}(C \otimes U_m) \supseteq \bigcup_{r_1 + \ldots + r_t \leq m} (r_1 \cdot \mathrm{wt}(C) \oplus \ldots \oplus r_t \cdot \mathrm{wt}(C)).$$

Proof: Let $r_1, \ldots, r_t$ be positive integers such that $r_1 + \ldots + r_t \leq m$. For $i = 1, \ldots, t$, choose $v_i \in U_m$ of weight r_i such that $\mathrm{supp}(v_i) \cap \mathrm{supp}(v_j) = \emptyset$ for $i \neq j$. Then, consider the subcode of $C \otimes U_m$, given by the set

$$\left\{ \sum_{i=1}^{t} c_i \otimes v_i \mid c_i \in C \right\}.$$

Since $\mathrm{supp}(v_i) \cap \mathrm{supp}(v_j) = \emptyset$ for $i \neq j$, we also have $\mathrm{supp}(c_i \otimes v_i) \cap \mathrm{supp}(c_j \otimes v_j) = \emptyset$ for every $c_i, c_j \in C$ and $i \neq j$. This implies that

$$\begin{aligned} \mathrm{wt}_H \left(\sum_{i=1}^{t} c_i \otimes v_i \right) &= \sum_{i=1}^{t} \mathrm{wt}_H(c_i \otimes v_i) \\ &= \sum_{i=1}^{t} r_i \mathrm{wt}_H(c_i), \end{aligned}$$

and therefore we conclude. ∎

Theorem 7. *For every prime power q, and positive integer ℓ, k, m such that $0 < k \leq \ell$, we have*

$$\Gamma_Q(\ell m, \ell, km, q) \geq mL(\ell, k, q).$$

Proof: Let C be a code with $L(\ell, k, q)$ nonzero weights. Moreover, by Lemma 6 we have that

$$\mathrm{wt}(C \otimes U_m) \supseteq \bigoplus_{i=1}^{m} \mathrm{wt}(C).$$

By a well-known result in additive combinatorics (see e.g. [14])

$$\left| \bigoplus_{i=1}^{m} \mathrm{wt}(C) \right| \geq m|\mathrm{wt}(C)| - m + 1.$$

We conclude by substituting $|\mathrm{wt}(C)| = L(\ell, k, q) + 1$ in the equation above. ∎

As a consequence, we can completely determine the maximum number of weights of a quasi-cyclic code for some cases. This is done by using the existence of *full weight spectrum (FWS) codes*, first introduced in [1]. An $[n, k]$ FWS code C is a code with all the possible weights, i.e. such that $\mathrm{wt}(C) = \{0, 1, \ldots, n\}$.

Theorem 8. *For every prime power q, and every positive integers ℓ, k, m such that $\ell \leq 2^k - 1$, we have*

$$\Gamma_Q(m\ell, \ell, mk, q) = m\ell.$$

Proof: By Theorem 7, we have $\Gamma_Q(\ell m, \ell, km, q) \geq mL(\ell, k, q)$. However, for $\ell \leq 2^k - 1$, it was proved in [1, Lemma 3.8] that $L(\ell, k, q) = \ell$. Therefore we conclude. ∎

We now recall the notion of *maximum weight spectrum (MWS) code* introduced in [3]. An $[n, k]$ code C over $\mathbb{F}_q$ is said to be MWS if the number of nonzero weights is $\frac{q^k - 1}{q - 1}$. We can deduce the following explicit lower bound again using Theorem 7.

Corollary 9. *For every prime power q, and every positive integers ℓ, k, m such that $k \geq 2$ and $\ell \geq \min\{q^{\frac{k^2+k-4}{2}}, \frac{q(q^k-1)(q^{k-1}-1)^2}{2(q-1)^3}\}$, we have*

$$\Gamma_Q(m\ell, \ell, mk, q) \geq m\frac{q^k-1}{q-1}.$$

Proof: For $\ell \geq \min\{q^{\frac{k^2+k-4}{2}}, \frac{q(q^k-1)(q^{k-1}-1)^2}{2(q-1)^3}\}$, it was proved in [3] and [1] that MWS codes exist. Then we conclude by Theorem 7. ∎

B. Reed-Muller codes

In this subsection we study the quasi-cyclic properties of q-ary Reed-Muller codes. In particular, in Theorem 12 we will characterize the set of indices ℓ for which a q-ary Reed-Muller code is quasi-cyclic. This result leads to special lower bounds on the function $\Gamma_Q(n, \ell, k, q)$ for some values of n, k and ℓ.

Let m be a positive integer and consider $R_m := \mathbb{F}_q[x_1, \ldots, x_m]$ the ring of polynomials in m variables over $\mathbb{F}_q$. Moreover, choose an order on the points of $\mathbb{F}_q^m$ and list them as $P_1, \ldots, P_n$, where $n = q^m$. We define the evaluation map

$$\begin{aligned} \mathrm{ev}_m : R_m &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)). \end{aligned}$$

Definition 10. Let r, m be positive integers such that $0 \leq r \leq (q-1)m$. The **q-ary Reed-Muller code of order r in m variables** is the code

$$\mathcal{RM}_q(r, m) := \{\mathrm{ev}_m(f) \mid f \in R_m, \deg(f) \leq r\}.$$

It is well-known (see for instance [7]) that the code $\mathcal{RM}_q(r, m)$ is an $[n(r, m), k(r, m), d(r, m)]_q$ code, with

(1) $n(r, m) = q^m$.
(2) $k(r, m) = \sum_{i=0}^{r} B(q, m, i)$, where $B(q, m, i)$ denotes the coefficient of z^i in the polynomial $(1 + z + \ldots + z^{q-1})^m$.
(3) $d(r, m) = (q - S)q^{m-1-Q}$, where $r = Q(q-1) + S$ with $0 \leq S \leq q-2$.

Observe that the choice of the order of the points P_i of $\mathbb{F}_q^m$ does not matter, since different choices lead to equivalent codes. However, for some special permutations of the points P_i's, the code does not change at all. These permutations are the one induced by the *affine general linear group* $\mathrm{Aff}(m, q)$, the group of linear transformations of the affine space $\mathbb{F}_q^m$. This group is well-studied, and it is given by the set of transformations of the form $M_{A,v}$, acting on $x \in \mathbb{F}_q^m$ via $M_{A,v}(x) = Ax + v$, for any $A \in \mathrm{GL}(m, q)$, $v \in \mathbb{F}_q^m$. Therefore, $\mathrm{Aff}(m, q) \cong \mathrm{GL}(m, q) \rtimes \mathbb{F}_q^m$, where the operation is given by $(A, v)(B, w) = (AB, Aw + v)$. It was indeed proved in [6, Theorem 5] that $\mathrm{Aut}(\mathcal{RM}_q(r, m)) \cong \mathrm{Aff}(m, q)$, whenever $r \geq 1$. The isomorphism is given by considering that every map $M_{A,v}$ applied to the points P_i's induces a permutation of the points.

Proposition 11. *Let q be a power of a prime p and m, i be two non-negative integers. There exists an element $g \in \mathrm{Aff}(m, q)$ of order p^{i+1} such that g^{p^i} has no fixed points if and only if $m \geq p^i$.*

Proof: Let $M_{A,v}$ be the affine map defined as $M_{A,v}(x) = Ax + v$. We want to show that we can construct an element $(A, v) \in \mathrm{GL}(m, q) \rtimes \mathbb{F}_q^m$ such that $(M_{A,v})^{p^{i+1}} = I_m$ and $(M_{A,v})^{p^i}$ has no fixed points, if and only if $m \geq p^i$. Finding a pair (A, v) with such properties is equivalent to require that for every $x \in \mathbb{F}_q^m$ it holds

$$\begin{aligned} (A^{p^{i+1}} - I_m)x &= -\left(\sum_{j=0}^{p^{i+1}-1} A^j\right)v \\ &= -(A - I_m)^{p^{i+1}-1} v, \qquad (1) \\ (A^{p^i} - I_m)x &\neq -\left(\sum_{j=0}^{p^i-1} A^j\right)v \\ &= -(A - I_m)^{p^i-1} v. \qquad (2) \end{aligned}$$

Observe that, since (1) needs to hold for every $x \in \mathbb{F}_q^m$, then in particular it has to be true for $x = 0$. Therefore, we must have that everything is 0, i.e.

$$(A^{p^{i+1}} - I_m) = 0, \quad \text{and} \quad (A - I_m)^{p^{i+1}-1} v = 0.$$

Moreover, (2) needs to hold for every $x \in \mathbb{F}_p^m$, therefore, it is equivalent to the condition that the vector $(A - I_m)^{p^i-1} v \notin \mathrm{colsp}(A^{p^i} - I_m)$.

Now suppose that $m \geq p^i$. We choose a matrix $A \in \mathrm{GL}(m, q)$ with minimal polynomial $\mu_A(x) = (x-1)^{p^i}$, and a vector v such that $(A - I_m)^{p^i-1} v \neq 0$. Note that such a pair (A, v) always exists, since we can for instance take

$$A = \begin{pmatrix} A' & 0 \\ 0 & I_{m-p^i} \end{pmatrix},$$

where

$$A' = \begin{pmatrix} 1 & 1 & & & \\ & 1 & \ddots & 0 & \\ & & \ddots & \ddots & \\ & 0 & & \ddots & 1 \\ & & & & 1 \end{pmatrix} \in \mathbb{F}_q^{p^i \times p^i},$$

and v as the p^i-th standard basis vector. With this choice of A and v, we have that trivially (1) is satisfied, since it is $0 = 0$ for every x, and $(A - I_m)^{p^{i+1}-1}v = 0v = 0$. Moreover, Also (2) is satisfied.

On the other hand, if $m < p^i$, requiring that $(A - I_m)^{p^{i+1}} = 0$ means that the minimal polynomial of A is equal to $(x-1)^s$ for some $s \leq m$. Therefore, $s \leq p^i - 1$ and

$$\begin{aligned} -(A - I_m)^{p^i-1}v &= -(A - I_m)^s(A - I_m)^{p^i-1-s}v \\ &= 0 = (A - I_m)^{p^i}x \\ &= (A^{p^i} - I_m)x \end{aligned}$$

for every $x, v \in \mathbb{F}_q^m$. Hence, the second inequality cannot be satisfied. ∎

The next result characterizes the possible indexes of a q-ary Reed-Muller code.

Theorem 12. *Let $q = p^h$ be a power of a prime p, and let r and m two positive integers. A q-ary Reed-Muller code of degree r in m variables $\mathcal{RM}_q(r, m)$ is (permutation-equivalent to) a quasi-cyclic code of index $\frac{q^m}{p^{t+1}} = p^{hm-t-1}$ where $t := \max\{i \mid m \geq p^i\}$. Moreover, $\mathcal{RM}_q(r, m)$ is not permutation-equivalent to a quasi-cyclic code of index $\frac{q^m}{p^{j+1}} = p^{hm-j-1}$, for any $j > t$.*

Proof: By definition, we have that a code C of length n is equivalent to a quasi-cyclic code of index r if and only if $\mathrm{Aut}(C)$ seen as a subgroup of $\mathcal{S}_n$ contains an element g which is the product of r disjoint s-cycles, where $s := \frac{n}{r}$. Moreover, an element g has this property if and only if $g^s = \mathrm{id}$ and for every prime p' dividing s, the element $g^{\frac{s}{p'}}$ has no fixed points.

By [6, Theorem 5], we have that the automorphism group of $\mathcal{RM}_q(r, m)$ is $\mathrm{Aff}(m, q)$. Since $n = q^m$, the only possible indices for $\mathcal{RM}_q(r, m)$ being a quasi-cyclic code are powers of the prime p. Furthermore by Proposition 11, we have that there exists an element $g \in \mathrm{Aut}(\mathcal{RM}_q(r, m))$ such that $g^{p^{i+1}} = \mathrm{id}$ and g^{p^i} has no fixed points if and only if $p^i \geq m$. In particular, g acts on $\mathbb{F}_q^m$ as a product of

$$\frac{q^m}{p^{j+1}} = p^{hm-j-1}$$

disjoint p^{i+1}-cycles. This concludes the proof. ∎

Example. Consider $q = 2$ and the code $\mathcal{RM}_2(2, 4)$. A computation in Magma [8] shows that its permutation group contains a permutation of order 8 with the cycle decomposition

$$(1, 12, 14, 6, 2, 11, 13, 5)(3, 9, 16, 7, 4, 10, 15, 8).$$

But that group does not contain any permutation of order 16. The code $\mathcal{RM}_2(2, 4)$ is doubly circulant, but not cyclic.

Remark. Observe that we can summarizes Theorem 12 by saying that any p^h-ary Reed-Muller code $\mathcal{RM}_q(r, m)$, with $r, m \geq 1$ is a Quasi-Cyclic code of index $p^{hm-\lfloor \log_p(m) \rfloor - 1}$ but not a QC code for any smaller index.

The following result summarizes all the cases in which a Reed-Muller code is permutation equivalent to a cyclic code.

Corollary 13. *The Reed-Muller code $\mathcal{RM}_q(r, m)$ is permutation equivalent to a cyclic code if and only if one of the following holds*

1) *$r = 0$, for any m and q.*
2) *$r \geq 1$, $m = 1$ and any q.*
3) *$r \geq 1$, $m = 2$ and $q = 2$.*

Corollary 14. *Let $q = p^h$ be a power of a prime p. For every positive integers r, t such that $0 \leq r \leq \frac{q-3}{2}$, and $0 \leq t \leq \log_p m$, we have*

$$\Gamma_Q\left(q, p^{hm-t-1}, \sum_{i=0}^{(q-1)m-r-1} B(q, m, i), q\right) \geq q^m - r - 1.$$

Proof: The number of nonzero weights of q-ary Reed-Muller codes $\mathcal{RM}_q((q-1)m - r - 1, m)$ for $0 \leq r \leq \frac{q-3}{2}$ is equal to $q^m - r - 1$, by [27, Theorem 26]. Then we conclude by Theorem 12. ∎

Corollary 15. *With the notations above, we have the*

following results.

$$\Gamma_Q\left(2^m, 2^{m-t-1}, 2^m-m-1, 2\right) \geq 2^m-2 \quad \textit{for} \quad m \geq 3, t \leq \log_2 m;$$

$$\Gamma_Q\left(2^m, 2^{m-t-1}, \sum_{i=0}^{m-3}\binom{m}{i}, 2\right) \geq 2^m-8 \quad \textit{for} \quad m \geq 6, t \leq \log_2 m;$$

$$\Gamma_Q\left(3^m, 3^{m-t-1}, \sum_{i=0}^{2m-2} B(3,m,i), 3\right) \geq 3^m-2 \quad \textit{for} \quad m \geq 1, t \leq \log_3 m;$$

$$\Gamma_Q\left(3^m, 3^{m-t-1}, \sum_{i=0}^{2m-3} B(3,m,i), 3\right) \geq 3^m-6 \quad \textit{for} \quad m \geq 3, t \leq \log_3 m;$$

$$\Gamma_Q\left(5^m, 5^{m-t-1}, \sum_{i=0}^{4m-3} B(5,m,i), 5\right) \geq 5^m-3 \quad \textit{for} \quad m \geq 1, t \leq \log_5 m.$$

Proof: The number of nonzero weights of q-ary Reed-Muller codes for these sets of parameters has been determined in [27], and we conclude using Theorem 12. ∎

C. Reduction to cyclic codes

In this subsection, we develop some lower bounds based on some results on cyclic codes that have been found in [27]. Note that a cyclic code of length ab is, in particular, a QC code of index a. The following bound is then immediate. The proof is omitted.

Proposition 16. *For all integers a, b we have*

$$\Gamma_Q(ab, a, k, q) \quad \geq \quad \Gamma_C(ab, k, q). \tag{3}$$

We combine this result with some lower bounds in [27]. The following bound is inspired by [27, Theorem 12].

Theorem 17. *Let m be a positive integer and a be any divisor of 2^m-1. Then*

$$\Gamma_Q(2^m-1, a, 2^m-m-1, 2) \geq 2^m-5.$$

Proof: We combine Proposition 16 with the fact that the number of weights in the cyclic Hamming code of length n is 2^m-5 [23, Chapt. 6, Ex. (E2)]. ∎

The following bound is based on [27, Theorem 13].

Theorem 18. *Let $q>2$ be a prime power and $r \geq 2$ such that $\gcd(r, q-1)=1$. We have the bound*

$$\Gamma_Q\left(\frac{q^r-1}{q-1}, a, \frac{q^r-1}{q-1}-r, q\right) \geq \frac{q^r-1}{q-1}-2,$$

for every integer a dividing $\frac{q^r-1}{q-1}$.

The following bound is based on [27, Theorem 14].

Theorem 19. *For every positive integer m, we have*

$$\Gamma_Q\left(2^m-1, a, \sum_{i=0}^{m-3}\binom{m}{i}, 2\right) \geq 2^m-9 \quad \textit{for} \quad m \geq 6 \textit{ and } a \mid 2^m-1;$$

$$\Gamma_Q\left(3^m-1, a, \sum_{i=0}^{2m-2} B(3,m,i), 3\right) \geq 3^m-3 \quad \textit{for} \quad m \geq 1 \textit{ and } a \mid 3^m-1;$$

$$\Gamma_Q\left(3^m-1, a, \sum_{i=0}^{2m-3} B(3,m,i), 3\right) \geq 3^m-7 \quad \textit{for} \quad m \geq 3 \textit{ and } a \mid 3^m-1;$$

$$\Gamma_Q\left(5^m-1, a, \sum_{i=0}^{4m-3} B(5,m,i), 5\right) \geq 5^m-4 \quad \textit{for} \quad m \geq 1 \textit{ and } a \mid 5^m-1;$$

$$\Gamma_Q\left(q^m-1, a, \sum_{i=0}^{(q-1)m-r-1} B(q,m,i), q\right) \geq q^m-r-2 \quad \textit{for} \quad 0 \leq r \leq \frac{q-3}{2} \textit{ and } a \mid q^m-1.$$

The next result relies on [27, Theorem 15].

Theorem 20. *For all integers $m \geq 3$, we have*

$$\Gamma_Q(2^m-1, a, 2m, 2) \geq \lceil 2^{m/2} \rceil,$$

for any positive integer a such that $a \mid 2^m-1$, and

$$\Gamma_Q(2^m+1, a, 2m, 2) \geq \lceil 2^{m/2} \rceil,$$

for any positive integer a dividing 2^m+1.

A ternary analogue, based on [27, Theorem 16] is as follows.

Theorem 21. *For all integers $m \geq 2$, we have $\Gamma_Q(3^m-1, a, 2m, 3) \geq \lceil 2 \times 3^{\frac{m-2}{2}} \rceil$, for any positive integer a dividing 3^m-1.*

D. Covering radius

Now we give lower bounds based on the covering radius of a code, using Delsarte bound. Recall that the **covering radius** of a code C is the smallest integer t such that every point in $\mathbb{F}_q^n$ has Hamming

distance at most t from some codeword of C, and it is denoted by $\rho(C)$. Consider the combinatorial function $T[n,\ell,k,q]$, which represent the largest covering radius of a QC code of length n, index $\gcd(\ell,n)$, and dimension k over $\mathbb{F}_q$. The Delsarte bound [10] asserts that for a given linear code C we have $\rho(C^\perp)\leq s(C)$ (see also [23, Chap. 6, Theorem 21]). With the above definitions, we can state the following result.

Proposition 22. *For all integers n,k with $1\leq k\leq n$, we have*

$$\Gamma_Q(n,\ell,k,q)\geq T[n,\ell,n-k,q].$$

Proof: Let C be an $[n,n-k]_q$ quasi-cyclic code of index ℓ with covering radius $\rho(C)=T[n,\ell,n-k,q]$. Then $C^\perp$ is an $[n,k]_q$ quasi-cyclic code of index ℓ with $s(C^\perp)\geq\rho(C)=T[n,\ell,n-k,q]$. ∎

V. Asymptotics

In this section we give asymptotic estimate on the number of weights of QC codes. More specifically, in order to consider the number of weights of long QC codes of given rate R, and normalized index λ, we study the behavior of the function $\gamma_q(\lambda,R)$ defined for $0<R<1$ as

$$\gamma_q(\lambda,R)=\limsup_{n\to\infty}\frac{1}{n}\Gamma_Q(n,\lfloor\lambda n\rfloor,\lfloor Rn\rfloor,q).$$

Before studying the properties of $\gamma_q(\lambda,R)$, we recall the function $\mathcal{L}_q$ already introduced in [28]. It is defined for values $0<R<1$ as

$$\mathcal{L}_q(R)=\limsup_{n\to\infty}\frac{1}{n}\left(L(n,\lfloor Rn\rfloor,q)\right).$$

However, using the results of [1], we can determine completely the function $\mathcal{L}_q$.

Theorem 23. *For every prime power q and every rate $0<R<1$, we have*

$$\mathcal{L}_q(R)=1.$$

Proof: By [1, Lemma 3.8], whenever $n\leq 2^k-1$, we have $L(n,k,q)=n$. Now, there exists $n_0\in\mathbb{N}$ such that $n\leq 2^{\lfloor Rn\rfloor}-1$ for every $n\geq n_0$. For n going to infinity we then get $\mathcal{L}_q(R)=\limsup_{n\to\infty}\frac{1}{n}\left(L(n,\lfloor Rn\rfloor,q)\right)=1$. ∎

We are now ready to study the function $\gamma_q\left(\lambda,R\right)$.

Theorem 24. *For all rationals $0<\lambda<1$, and rates $0<R<1$, we have*

$$\gamma_q\left(\lambda,R\right)=1.$$

Proof: It trivially holds that $\gamma_q(\lambda,R)\leq 1$. To derive the opposite inequality, we use Theorem 7. First, we write $\lambda=\frac{a}{b}$ for some $a,b\in\mathbb{N}$, such that $\gcd(a,b)=1$. We take the subsequence $n=\ell b$ for $\ell\in\mathbb{N}$, entailing therefore $k\sim Rn=R\ell b$, and we get

$$\begin{aligned}\gamma_q\left(\frac{a}{b},R\right)&=\limsup_{n\to\infty}\frac{1}{n}\left(\Gamma_Q\left(n,\left\lfloor\frac{na}{b}\right\rfloor,\lfloor Rn\rfloor,q\right)\right)\\&\geq\frac{1}{b}\limsup_{\ell\to\infty}\frac{1}{\ell}(\Gamma_Q(\ell b,\ell a,\lfloor R\ell b\rfloor,q))\\&\overset{(*)}{=}\frac{1}{b}\limsup_{\ell\to\infty}\frac{1}{\ell}(\Gamma_Q(\ell b,\ell,\lfloor R\ell b\rfloor,q))\\&\geq\frac{1}{b}\limsup_{\ell\to\infty}\frac{1}{\ell}(bL(\ell,\lfloor R\ell\rfloor,q))\\&=\limsup_{\ell\to\infty}\frac{1}{\ell}\left(L(\ell,\lfloor R\ell\rfloor,q)\right)\\&=\mathcal{L}_q(R)=1,\end{aligned}$$

where $(*)$ holds because $\gcd(\ell b,\ell a)=\ell$ and hence by definition $\Gamma_Q(\ell b,\ell a,\lfloor R\ell b\rfloor,q)=\Gamma_Q(\ell b,\ell,\lfloor R\ell b\rfloor,q)$. ∎

Remark. This bound does not provide any information when ℓ is fixed like in the case of e.g. cyclic codes or double circulant codes.

More interesting is what happens when we consider the asymptotic behaviour of codes with a fixed rate. Let $\ell>0$ be an integer and $0<R<1$ be a rational number. We define the function

$$\eta_q(\ell,R):=\limsup_{n\to\infty}\frac{1}{n}(\Gamma_Q(n,\ell,\lfloor Rn\rfloor,q)).$$

We could not determine the exact value of η_q, but we can give a lower bound based on Theorem 7.

Theorem 25. *For every positive integer ℓ and every rate $0<R<1$, we have*

$$\eta_q(\ell,R)\geq\frac{L(\ell,\lfloor R\ell\rfloor,q)}{\ell}.$$

Moreover, for all (ℓ,R) satisfying $\lfloor R\ell\rfloor\geq\log_2(\ell+1)$ we have $\eta_q(\ell,R)=1$.

Proof: We take the subsequence $n=\ell n'$ and using Theorem 7 we obtain

$$\begin{aligned}\eta_q\left(\ell,R\right)&=\limsup_{n\to\infty}\frac{1}{n}\left(\Gamma_Q\left(n,\ell,\lfloor Rn\rfloor,q\right)\right)\\&\geq\frac{1}{\ell}\limsup_{n'\to\infty}\frac{1}{n'}(\Gamma_Q(\ell n',\ell,\lfloor R\ell n'\rfloor,q))\\&\geq\frac{1}{\ell}\limsup_{n'\to\infty}\frac{1}{n'}(n'L(\ell,\lfloor R\ell\rfloor,q))\\&=\frac{L(\ell,\lfloor R\ell\rfloor,q)}{\ell}.\end{aligned}$$

Table 1: Values of $s = \Gamma_Q(2n, 2, n, 2)$

n	4	5	6	7	8	9	10
s	5	5	8	8	11	13	≥ 13

Table 2: Values of $s = \Gamma_Q(3n, 3, n, 2)$

n	4	5	6	7	8
s	5	7	10	11	≥ 14

The second statement then follows from the fact that for that set of parameters we have $L(\ell, \lfloor R\ell \rfloor, q) = \ell$, by [1, Lemma 3.8] ■

VI. Numerics

Exhaustive computations in Magma [8] yielded the following values. Table 1 was written by computing all possible generator matrices for a one-generator index 2 QC code of length in the range $[8, 20]$, and Table 2 was written by computing all possible generator matrices for a one-generator index 3 QC code of length in the range $[12, 24]$. In both the cases we can observe that the lower bound obtained by Theorem 7 is not tight for all the parameters. Therefore, it also seems that the asymptotic lower bound given in Theorem 25 could be non-tight. Based on these values, we conjecture the following.

Conjecture: The functions $n \mapsto \Gamma_Q(2n, 2, n, 2)$ and $n \mapsto \Gamma_Q(3n, 3, n, 2)$ are nondecreasing functions of n.

VII. Conclusion and open problems

In this paper we have studied the largest number of distinct nonzero weights a QC code can have. We have introduced a number of combinatorial functions to that effect. Some are relevant to the index of the code; some to the co-index. Combinatorial upper bounds on these quantities have been derived using the cycle structure of the code. Lower bounds have been derived by employing a variety of techniques. Since this is the third in a series of three papers we have been able to make the results of [28] on linear codes and that of [27] on cyclic codes to bear on the problem: see §IV-A and §IV-B respectively. In particular Theorem 7 of §IV-A was very useful in the asymptotic bounds of Section §V. This also leads to the problem of determining the whole behavior of the function η_q, which does not seem to be easy. The section on the representation of q-ary Reed-Muller codes as QC codes has its own interest, and can be read independently of the rest of the paper.

The main open problems are as follows. There is no general arithmetic upper bound on the number of weights that is similar to that of [27, Theorem 5] based on results of [21]. As the preceding section shows, it seems there is still room for improvement in Theorem 7. The monotonicity of all combinatorial functions considered is hard to guess. The conjecture in Section §VI is only an example.

References

[1] T. L. Alderson, A note on full weight spectrum codes, Transactions in Combinatorics, **8**(3), 15–22, 2019.

[2] T. L. Alderson, On the weights of general MDS codes, arXiv preprint arXiv:1910.05634, 2019.

[3] T. L. Alderson and A. Neri, Maximum weight spectrum codes, Advances in Mathematics of Communications, **13**(1), 101–119, 2019.

[4] E. Assmus and J. Key, Polynomial codes and finite geometries, in *Handbook of Coding Theory*, **2**:1269–1343, C. Huffman, V. Pless, eds, North-Holland, Amsterdam, 1998.

[5] E. Assmus and E. Mattson, New 5-designs, Journal of Combinatorial Theory, **6**(2):122–151,1969.

[6] T. Berger and P. Charpin. The automorphism group of generalized Reed-Muller codes. Discrete Mathematics, **117**(1-3): 1–17, 1993.

[7] T. Blackmore and G. Norton, Matrix product codes over $\mathbb{F}_q$, Applicable Algebra in Engineering, Communication and Computing, **12**(6): 477–500, 2001.

[8] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., **24**, 235-265, 1997, `http://magma.maths.usyd.edu.au/magma/`

[9] G. D. Cohen and L. Tolhuizen. Maximum weight spectrum codes with reduced length, arXiv preprint arXiv:1806.05427, 2018.

[10] P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, Information and Control, **23**(5) 407–438, 1973.

[11] S. T. Dougherty, P Gaborit, M. Harada, P. Solé, Type II Codes Over $\mathbb{F}_2+u\mathbb{F}_2$. IEEE Trans. Information Theory, **45**(1), 32–45, 1999.

[12] F. Ezerman, M. Grassl, and P. Solé, The weights in MDS codes, IEEE Transactions on Information Theory, **57**(1): 392–396, 2011.

[13] M. Grassl, T. Beth and M. Roetteler, On optimal quantum codes, International Journal of Quantum Information, **2**(1):55–64, 2004

[14] A. Granville, An introduction to additive combinatorics, CRM Proceedings and Lecture Notes, **43**: 1–27, 2007.

[15] A. Haily and D. Harzalla, On the automorphism group of Distinct Weight codes, Intelligent Information Management, **7**:80–92, 2015.

[16] R. Hill, An extension theorem for linear codes, Designs, Codes and Cryptography, **17**(1-3): 151–157, 1999.

[17] R. Hill and P. Lizak, Extensions of linear codes, In International Symposium on Information Theory, ISIT 1995, pp. 345–345, 1995.

[18] W. C. Huffman and V. Pless, *Fundamentals of error correcting codes*, Cambridge University Press, 2003.

[19] F.R. Kschischang and S. Pasupathy, Some ternary and quaternary codes and associated sphere packings, IEEE Transactions on Information Theory, **38**(2): 227–246, 1992.

[20] S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes I: finite fields, IEEE Transactions on Information Theory, **47**(7): 2751–2760, 2001.

[21] R. Lidl and H. Niederreiter, *Finite fields*, volume **20**, Cambridge University Press, 1997.

[22] J. MacWilliams, A theorem on the distribution of weights in a systematic code, The Bell System Technical Journal, **42**(1): 79–94, 1963.

[23] F.J. MacWilliams and N.J.A. Sloane, *The theory of error correcting codes*, North Holland, Amsterdam, 1977.

[24] A. Meneghetti, On linear codes and distinct weights. arXiv preprint arXiv:1804.04373, 2018.

[25] E. M. Rains, Nonbinary quantum codes IEEE Transactions on Information Theory, **45**(6): 1827–1832, 1999.

[26] M. Rotteler, M. Grassl, and T. Beth, On quantum MDS codes, In International Symposium onInformation Theory, ISIT 2004, pp. 356–356, 2004.

[27] M. Shi, X. Li, A. Neri, and P. Solé, How many weights can a cyclic code have?, IEEE Transactions on Information Theory, **66**(6): 1449–1459, 2020.

[28] M. Shi, H. Zhu, P. Solé, and G.D. Cohen, How many weights can a linear code have?, Des. Codes Cryptogr. **87**(1): 87–95, 2019.

PLACE PHOTO HERE

Minjia Shi

PLACE PHOTO HERE

Alessandro Neri was born in Campobasso, Italy, in 1988. He got the B.Sc. and M.Sc. degrees in mathematics from University of Pisa, Italy, in 2010 and 2014, respectively, and he received the Ph.D. degree in mathematics from University of Zurich, Switzerland, in 2019. He is currently recipient of a Swiss National Science Foundation Postdoctoral Fellowship, which he is spending at Technical University of Munich.

His research interests include, but are not limited to, applied algebra, algebraic coding theory, finite geometry and finite fields theory.

PLACE PHOTO HERE

Patrick Solé received the Ingénieur and Docteur-Ingénieur degrees both from Ecole Nationale Supérieure des Télécommunications, Paris, France, in 1984 and 1987, respectively, and the habilitation diriger des recherches from Université de Nice-Sophia Antipolis, Sophia Antipolis, France, in 1993.

He has held visiting positions in Syracuse University, Syracuse, NY, from 1987 to 1989, Macquarie University, Sydney, 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 Directeur de Recherche in 1996. He is currently member of the CNRS lab I2M in Marseilles, France.

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 is the author of more than 180 journal articles and of four books. He is the co-recipient of the best paper award for Information Theory in 1995, given by the Information Theory chapter of the IEEE.

He was associate editor of the IEEE Information Theory Transactions from 1996 till 1999.