How Many Weights Can a Cyclic Code Have?

Minjia Shi, Xiaoxiao Li, Alessandro Neri, and Patrick Solé

Abstract—Upper and lower bounds on the largest number of weights in a cyclic code of given length, dimension and alphabet are given. An application to irreducible cyclic codes is considered. Sharper upper bounds are given for the special cyclic codes (called here strongly cyclic), whose nonzero codewords have period equal to the length of the code. Asymptotics are derived on the function \( \Gamma(k, q) \), that is defined as the largest number of nonzero weights a cyclic code of dimension \( k \) over \( \mathbb{F}_q \) can have, and an algorithm to compute it is sketched. The nonzero weights in some infinite families of Reed-Muller codes, either binary or \( q \)-ary, as well as in the \( q \)-ary Hamming code are determined, two difficult results of independent interest.

Index Terms—Cyclic codes, irreducible cyclic codes, Hamming codes, Reed–Muller codes.

I. INTRODUCTION

RECENTLY, a series of works has been released on the study of the weight set of a code. In [21] Shi et al. conjectured that the maximum number of nonzero weights that a \( k \)-dimensional block code over \( \mathbb{F}_q \) can have is \( \frac{q^k - 1}{q - 1} \), giving an answer only for the case \( q = 2 \) or \( k = 2 \). The complete proof of this conjecture was given in [2] where the two authors provided two different constructions, and independently in [18]. Shorter codes with the maximum number of weights for a given dimension were then discussed in [1], [7]. In the present paper we address the same type of questions for cyclic codes. Thus, we study the function \( \Gamma(k, q) \), defined as the largest number of nonzero weights a cyclic code of dimension \( k \) over \( \mathbb{F}_q \) can have. We derive upper bounds on that quantity by simple counting arguments bearing on the cycle structure of the code. An alternative approach is to use weight concentration theorems, derived first in [15] in the language of linear recurrences. In the case of cyclic codes whose nonzero codewords have period equal to the length (called strongly cyclic codes in the sequel) we obtain smaller upper bounds than the ones derived for the class of all cyclic codes. This suggests to study \( \Gamma^0(k, q) \), that is the largest number of nonzero weights a strongly cyclic code of dimension \( k \) over \( \mathbb{F}_q \) can have. This discrepancy in behaviour between \( \Gamma(k, q) \), and \( \Gamma^0(k, q) \), is particularly evident in the asymptotic upper bounds. We also derive lower bounds on these two functions, using special codes, or the covering radius of the dual code. An algorithm is given to compute \( \Gamma(k, q) \), for small values of \( k \). A first appendix derives the number of weights in several infinite families of \( q \)-ary Reed-Muller codes, including the extended Hamming code and some binary, ternary and quinary Reed-Muller codes. A second appendix derives the number of weights in the \( q \)-ary Hamming code when \( q > 2 \). These last two technical results are of interest in their own right. While generating functions or recursions [12] are known in these cases, they are insufficient to determine the explicit weights in general. Exact enumeration of cyclic codes can require some deep techniques of Number Theory [11]. In particular, the codes of Melas and Zetterberg give interesting lower bounds for a wide range of parameters. The use of the celebrated Delsarte bound on the covering radius of codes [6], leads us to define a new combinatorial function \( (T[n, k]) \) of independent interest.

The material is organized as follows. The next section collects some background material on linear codes and cyclic codes. Section 3 is dedicated to upper bounds and Section 4 to lower bounds. Section 5 derives the asymptotic version of some of the preceding bounds. Section 6 gives an algorithm to compute \( \Gamma(k, q) \). Section 7 concludes the paper and mentions some challenging open problems. Appendix I derives the weight spectrum of some families of \( q \)-ary Reed-Muller codes. Appendix II determines the weights in the \( q \)-ary Hamming code for \( q \geq 3 \).

II. DEFINITIONS AND NOTATION

A. Linear Codes

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

The dual \( C^\perp \) of a code \( C \) is understood with respect to the standard inner product.

The (Hamming) weight of \( x \in \mathbb{F}_q^n \) is the number of indices \( i \) where \( x_i \neq 0 \), and it is denoted by \( w_H(x) \). The minimum nonzero weight \( d \) of a linear code is called the minimum distance. The dual distance of a code is the minimum distance of its dual. Every linear code satisfies the Singleton bound.
A code meeting that bound is called maximum distance separable (MDS). See [16, Chap. 11] for general knowledge on this family of codes.

B. Cyclic Codes

A cyclic code of length $n$ over a finite field $\mathbb{F}_q$ is a $\mathbb{F}_q$ linear code of length $n$ invariant under the coordinate shift. Under the polynomial correspondence such a code can be regarded as an ideal in the ring $\mathbb{F}_q[x]/(x^n - 1)$. It can be shown that this ideal is principal, with a unique monic generator $g(x)$, called the generator polynomial of the code. The check polynomial $h(x)$ is then defined as the quotient $(x^n - 1)/g(x)$. A well-known fact is that the codewords satisfy a linear recurrence of characteristic polynomial the reciprocal polynomial of $h(x)$ [16, p. 195]. Thus any codeword $c$ can be continued by repetition into a bi-infinite periodic sequence $\overline{c}$ which is periodic of least period a divisor of $n$. The period of a codeword $c$ is understood to be the smallest integer $T_0$ such $\overline{c}_{i + T_0} = \overline{c}_i$ for all integers $i$. Thus, the period is always a divisor of $n$. A cyclic code is irreducible over $\mathbb{F}_q$ if its check polynomial $h(x)$ is irreducible over $\mathbb{F}_q[x]$. The period of a polynomial $h(x) \in \mathbb{F}_q[x]$, such that $h(0) \neq 0$ is the smallest integer $t$ such that $h(x)$ divides $x^t - 1$ over $\mathbb{F}_q[x]$. If $C$ is a cyclic code, its codewords are partitioned into orbits under the action of the shift. We call these orbits the cyclic classes of $C$.

C. Combinatorial Functions

Here we introduce the combinatorial functions we are going to study in this work. Let $q$ be a prime power and let $k, n$ be non negative integers such that $0 \leq k \leq n$. We define $\Gamma(k, q)$ as the largest number of nonzero weights of a cyclic code of dimension $k$ over $\mathbb{F}_q$. Moreover, we define $\Gamma(n, k, q)$ 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. The same functions for strongly cyclic codes (to be defined below) are denoted by $\Gamma^0(k, q)$, and $\Gamma^0(n, k, q)$, respectively. Recall also the functions $L(k, q)$ and $L(n, k, q)$ introduced in [21], that represent respectively 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 a fixed length $n$. The function $L(k, q)$ was completely determined and shown to be equal to $\frac{q^k - 1}{q - 1}$ in [2], while for $L(n, k, q)$ some partial answers were given in [1], [21].

III. Upper Bounds

A. Cycle Structure

Let $\rho : \mathbb{F}_q^n \to \mathbb{F}_q^n$ denote the cyclic shift operator.

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

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

Proof. Let $c$ be a codeword of period $t$ and suppose $ac = \rho^i(c)$. Then $c = \rho^t(c) = \alpha^t c$, and this implies $\alpha^t = 1$. Let now $H$ be the unique subgroup of $\mathbb{F}_q^*$ of order $\gcd(t, q - 1)$. Since by definition $r|t$ and also $\alpha^{q^t - 1} = 1$, we get $\alpha^{\gcd(t, q - 1)} = 1$, i.e. $\alpha \in H$.

If $C$ is a cyclic code, denote by $B_t$ the number of nonzero codewords of period $t$ it contains. A cyclic code such that $B_t = 0$ for $1 \leq t < n$ shall be called strongly cyclic.

Lemma 2. If $C$ is an $[n, k]_q$ cyclic code with $s$ nonzero weights, then

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

Proof. The number of cyclic classes of codewords of period $t$ is at most $B_t$. All codewords in the same class share the same weight. Then, we use the Lemma above. Let $c$ be a codeword and $H$ be the unique subgroup of $\mathbb{F}_q^*$ of order $\gcd(t, q - 1)$. Now, for every representative $\alpha$ of $\mathbb{F}_q^*/H$, the codeword $\alpha c$ gives a different class that obviously shares the same weight of the one of $c$. Hence, there are at most $\frac{B_t}{\gcd(t, q - 1)} = \frac{B_t}{\gcd(t, q - 1)}$ distinct weights among these codewords, and this shows the first inequality. The second directly follows from the fact that if a codeword has period 1 then it is necessarily a multiple of the vector of all ones, and therefore $B_1 \in \{0, q - 1\}$.

Example. Consider the code of dimension 2 over $\mathbb{F}_3$, with length 20 and check polynomial $x^2 + x - 1$. This code contains the Fibonacci numbers read mod 5 [22, A082116]. It can be checked to contain 4 codewords of period 4 (namely 1, 3, 4, 2, repeated five times) and 20 codewords of period 20. By Lemma 2, we see that $s \leq 3$.

This simple counting lemma has two important applications. First, we improve the upper bound on $L(k, q)$ of [21, Prop. 2] by a factor of at least $\frac{n}{q^k - 1}$ for some large class of cyclic codes, up to a factor $n$ for another subclass.

Theorem 3. If $C$ is a $[n, k]_q$ strongly cyclic code with $s$ nonzero weights, then

$$s \leq \frac{q^k - 1}{\gcd(q^k - 1, n)}.$$ 

Thus $\Gamma^0(n, k, q) \leq \frac{q^k - 1}{\gcd(q^k - 1, n)}$.

Proof. We apply Lemma 2 when $B_t = 0$ for $t < n$, so that the sum in the right handside contains only one summand.

One can observe that the function $\Gamma^0(n, k, q)$ has an intrinsically different behaviour than the one of $L(n, k, q)$. Indeed, it was proved in [1] $L(n, k, q) = \frac{q^{k} - 1}{q - 1}$ for $n \geq q^{3k} - 4$, while it is easy to see that a strongly cyclic code with that restriction on $n$ can not exist, i.e. $\Gamma^0(n, k, q) = 0$ for $n \geq q^{3k} - 4$ (it is actually already true for $n \geq q^k$ by Theorem 3). This also implies that $\lim_{n \to \infty} \Gamma^0(n, k, q) = 0$, and this is in contrast to the behaviour of the function $L(n, k, q)$ that is non decreasing in $n$ and $\lim_{n \to \infty} L(n, k, q) = L(k, q)$. 

[16, Th 11, Chap. 1] on its parameters $d \leq n - k + 1$. 

[1450 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 66, NO. 3, MARCH 2020]
As a second implication of Lemma 2, in the general case when many of the $B_i$’s are nonzero, we can prove the following result.

**Theorem 4.** If $C$ is an $[n, k]_q$ cyclic code with $s$ nonzero weights, then

$$s \leq 1 + (q^k - 1) \left( \frac{1}{\text{lcm}(t, q - 1)^2} \right)^{1/2}.$$ 

**Proof.** From the second inequality in Lemma 2, we get

$$s - 1 \leq \sum_{1 < i \leq n} B_i \frac{1}{\text{lcm}(t, q - 1)}.$$ 

Squaring both sides of this inequality and applying Cauchy-Schwarz inequality we obtain

$$(s - 1)^2 \leq \left( \sum_{1 < i \leq n} B_i^2 \right) \left( \sum_{1 < i \leq n} \frac{1}{\text{lcm}(t, q - 1)^2} \right).$$

By definition of the $B_i$’s note that $\sum_{i | n} B_i = q^k - 1$, implying

$$\sum_{i | n} B_i^2 \leq (q^k - 1)^2.$$

The result follows by taking the square root of both sides.

**B. Character Sums**

The following result can be derived by using the character sums techniques of [15, Chapt. 8].

**Theorem 5.** If $C$ is an $[n, k]_q$ strongly cyclic code with $s$ nonzero weights, then

$$s \leq 2 \left( 1 - \frac{1}{q} \right) q^{k/2}.$$

Thus

$$\Gamma^0(n, k, q) \leq 2 \left( 1 - \frac{1}{q} \right) q^{k/2}.$$ 

**Proof.** By [15, Cor. 8.83] we know that the weights $w$ of $C$ lie in the range

$$n \left( 1 - \frac{1}{q} \right) - w \leq \left( 1 - \frac{1}{q} \right) q^{k/2}.$$ 

The result follows by computing the length of that interval.

**C. Irreducible Cyclic Codes**

The weight structure of irreducible cyclic codes has been a research topic since the first works of McEliece and others [8], [15], [17] due to their connection to Gauss sums and $L$-functions, and its intrinsic complexity.

**Theorem 6.** If $C$ is an $[n = \frac{q^k - 1}{N}, k]_q$ irreducible cyclic code with a check polynomial of period $n$, and $s$ nonzero weights, then $s \leq N$.

**Proof.** Since the check polynomial $h(x)$ is irreducible, it generates the annihilating ideal of each sequence attached to a codeword. If the period of such a sequence were $T < n$, then $h(x)$ would divide $x^T - 1$, contradicting the hypothesis on the period of $h(x)$. Hence $C$ is strongly cyclic, and we can apply Theorem 3. The result follows.

**Example.** Consider the case of $N = 2$, and $q = p$ an odd prime. Such a code is well-known to be a two-weight code [17].

A slightly sharper bound can be derived using the results in [8].

**Theorem 7.** If $C$ is an $[n = \frac{q^k - 1}{N}, k]_q$ irreducible cyclic code with a check polynomial of period $n$, and $s$ nonzero weights then

$$s \leq N_k = \gcd \left( N, \frac{q^k - 1}{q - 1} \right).$$

**Proof.** Follows by [8, (12)] which involves Gaussian periods of order $N_k$.

This shows that Theorem 6 can only be tight when $N = N_k$, or, equivalently, $N$ divides $\frac{q^k - 1}{q - 1}$. Using Theorem 5, another bound can be derived.

**Theorem 8.** If $C$ is an $[n = \frac{q^k - 1}{N}, k]_q$ irreducible cyclic code with a check polynomial of period $n$, and $s$ nonzero weights then

$$s \leq 2 \left( 1 - \frac{1}{q} \right) \sqrt{1 + nN}.$$ 

**Proof.** As explained in the proof of Theorem 6 we know that all nonzero codewords have period $n$. Thus the code $C$ is strongly cyclic, and we can apply Theorem 5. We get rid of $k$ in Theorem 5 by writing $q^k = 1 + nN$.

**Remark.** Depending on the relative values of $n$ and $N$, either Theorem 8, or Theorem 7 is sharper than the other.

A slight improvement on Theorem 8 can be derived for irreducible cyclic codes.

**Theorem 9.** If $C$ is an $[n = \frac{q^k - 1}{N}, k]_q$ irreducible cyclic code with a check polynomial of period $n$, and $s$ nonzero weights then

$$s \leq 2 \left( 1 - \frac{1}{q} \right) \left( \frac{n}{h} - \frac{1}{N} \right) \sqrt{1 + nN},$$

where $h = \text{lcm}(n, q - 1)$.

**Proof.** The proof follows the lines of Theorem 8 with [15, Th. 8.84, (8.37)] replacing [15, Cor. 8.83]. We get rid of $k$ by writing $q^k = 1 + nN$.

**IV. LOWER BOUNDS**

**A. Special Values**

We begin with an easy bound.

**Proposition 10.** For all prime powers $q$, we have $\Gamma(k, q) \geq k$.

**Proof.** The universe code, the cyclic $[k, k]_q$ code with generator the constant polynomial $g(x) = 1$, has $k$ nonzero
weights. This shows that $\Gamma(k, k, q) \geq k$. The result follows by $\Gamma(k, k, q) \leq \Gamma(k, q)$. \hfill \square

The following result is immediate by [20]. The proof is omitted.

**Proposition 11.** For all prime powers $q$, we have $\Gamma(2, q) = 2$.

We recall now some classical cyclic codes. The repetition code $R(n, q)$ is the ideal of $\mathbb{F}_q[x]/(x^n - 1)$ with generator $x - 1$. Its dual is $P(n, q) = ((x - 1))$. The binary Hamming code $H_m$ is the binary cyclic code of length $n = 2^m - 1$ with generator any primitive irreducible polynomial of $\mathbb{F}_2[x]$ of degree $m$. Its dual the simplex code $S_m$ is a one-weight code.

**Theorem 12.** For all integers $n \geq 1$ and all prime powers $q$ with $(n, q) = 1$, we have that $\Gamma(n, 1, q) = 1$, and that $\Gamma(n, n - 1, q)$ is the number of nonzero weights in $P(n, q)$. For all primes $m \geq 2$, we have $\Gamma(n, n - m, 2) = n - 4$, and $\Gamma(n, m, 2) = 1$, where $n = 2^m - 1$.

**Proof.** The first statement follows by the unicity of cyclic codes with dimension (resp. codimension) one. These are the repetition codes (resp. their duals). Their number of weights is equivalent to a cyclic code iff $\text{gcd}(q - 1, q - 1) = 1$. Thus, cyclic codes of dimension (resp. codimension) $m$ will have to be irreducible. We have the bound on the number of nonzero weights of $H_m$ is $2^m - 5$ ([16, Chap. 6, Ex. (E2)]), and the fact that $S_m$ is a one-weight code [16, Chap.1 §9 , Ex]. \hfill \square

**Remark.** The fact that the number of nonzero weights of $H_m$ is $2^m - 5$ can also be derived applying part (1) of Theorem 27 of the Appendix if we notice that $H_m$ is a punctured $R(m - 2, m)$.

**Theorem 13.** Let $q > 2$ be a prime power and $r > 2$ such that $\text{gcd}(r, q - 1) = 1$. We have the bound

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

**Proof.** Note that the $q$-ary Hamming code of length $\frac{q^r - 1}{q - 1}$ is equivalent to a cyclic code iff $\text{gcd}(r, q - 1) = 1$ [10]. The result follows then by Theorem 38 of Appendix II. \hfill \square

The next result also uses Reed-Muller codes. We will need some generalization of the binomial coefficients given by the following generating function

$$(1 + z + \ldots + z^{q - 1})^m = \sum_{\ell=0}^{m(q-1)} B(q, m, \ell) z^{\ell}.$$  

**Theorem 14.** With the notations above, we have the following results.

$\Gamma\left(\frac{2^m - 1}{2}, \frac{m-3}{2}, 2\right) \geq 2^{m-4} - 9$ for $m \geq 6,$

$\Gamma\left(\frac{3^m - 1}{3}, \frac{2m-2}{3}, 3\right) \geq 3^{m-3} - 3$ for $m \geq 1,$

$\Gamma\left(\frac{3^m - 1}{3}, \frac{2m-3}{3}, 3\right) \geq 3^{m-3} - 7$ for $m \geq 3,$

$\Gamma\left(\frac{5^m - 1}{5}, \frac{4m-3}{5}, 5\right) \geq 5^{m-4} - 4$ for $m \geq 1,$

$\Gamma\left(q^m - 1, \sum_{r=0}^{(q-1)m-1}(q^r - 1), q\right) \geq q^m - r - 2$ for $0 \leq r \leq \frac{q-3}{2}.$

**Proof.** The result combines Appendix I with the fact that punctured Reed Muller codes are cyclic [3, p.1312]. Note that the dimensions are not affected by puncturing due to the large minimum weights. The number of weights can decrease by at most 1 by transitivity of the automorphism group. \hfill \square

The next two theorems rely on some deep algebraic geometric enumeration of cyclic codes [14], [19], [24]. See [11] for a survey.

**Theorem 15.** For all integers $m \geq 3$, we have

$$\Gamma(2^m - 1, 2m, 2) \geq \frac{2^{m/2}}{2},$$

and

$$\Gamma(2^m + 1, 2m, 2) \geq \frac{2^{m/2}}{2}.$$  

**Proof.** The dual of the binary Melas code is cyclic of parameters $[2^m - 1, 2m]$. It is proved in [14, Th. 6.3] that its nonzero weights are all the even integers $w$ in the range

$$|w - \frac{2^m - 1}{2}| \leq 2^{m/2}.$$  

Similarly, the dual of the Zetterberg code is an irreducible cyclic code of parameters $[2^m + 1, 2m]$. It is proved in [14, Th. 6.6] that its nonzero weights are all the even integers $w$ in the range

$$|w - \frac{2^m + 1}{2}| \leq 2^{m/2}.$$  

The result follows after elementary calculations. \hfill \square

A ternary analogue is as follows.

**Theorem 16.** For all integers $m \geq 2$ we have $\Gamma(3^m - 1, 2m, 3) \geq [2 \times 3^{m/3}]$. 

**Proof.** We have the bound on the number of nonzero weights of $H_m$ is $2^m - 5$ ([16, Chap. 6, Ex. (E2)]), and the fact that $S_m$ is a one-weight code [16, Chap.1 §9 , Ex]. \hfill \square
Proof. The dual of the ternary Melas code is cyclic of parameters \([3^m - 1, 3m]\). It is proved in [24] that its nonzero weights are of the form \(3^m + t\) with \(t \in \mathbb{Z}\), satisfying \(t \equiv 1 \pmod{3}\), and \(t^2 < 3^m\). The result follows after elementary calculations.

It is remarkable that the last two theorems imply lower bounds on \(\Gamma(k, q)\), that are exponential in the dimension. It would be desirable to extend these results to \(\Gamma(k, q)\) with \(q\) a prime power \(> 3\).

B. Covering Radius

Recall that the covering radius \(\rho(C)\) of a code \(C\) is the smallest integer \(t\) such that every point in \(\mathbb{F}_q^n\) is at distance at most \(t\) from some codeword of \(C\). A combinatorial function that is, as far as we know, new, is \(T[n, k, q]\), the largest covering radius of a cyclic code of length \(n\) and dimension \(k\) over \(\mathbb{F}_q\). Note that the closest classical function in that context is, for \(q = 2\), the quantity \(t[n, k]\), the smallest covering radius of a binary linear code of length \(n\) and dimension \(k\) [6]. Trivially \(t[n, k] \leq T[n, k, 2]\). The Delsarte bound [16], stated for the dual of a linear code \(C\), is \(\rho(C^\perp) \leq s(C)\) [16, Chap. 6, Th. 21]. With the above definitions, we can state the following result.

**Proposition 17.** For all integers \(n, k\) with \(1 \leq k \leq n\), we have \(\Gamma(n, k, q) \geq T[n, n - k, q]\).

**Proof.** Upon using Delsarte bound for the dual of an \([n, k]_q\) code with \(\Gamma(n, k, q)\) nonzero weights, which is, in particular, an \([n, n - k]_q\) code we see that \(\Gamma(n, k, q) \geq T[n, n - k, q]\). \(\square\)

V. ASYMPTOTICS

To consider the number of weights of long codes of given rate, we study the behavior of \(\gamma_q(R)\) defined for \(0 < R < 1\) as

\[
\gamma_q(R) = \limsup_{n \to \infty} \frac{1}{n} \log_q (\Gamma(n, [Rn], q)).
\]

**Theorem 18.** For all rates \(R \in (0, 1)\) we have

\[
\gamma_q(R) \leq R.
\]

In particular, \(\gamma_q(R) \leq t(q)\), the unique solution in \((0, \frac{2^t - 1}{q})\) of the equation \(H_q(x) = x\).

**Proof.** The bound comes from the immediate inequalities \(\Gamma(n, k, q) \leq \Gamma(k, q) \leq q^k - 1\).

Similarly for strongly cyclic codes we define

\[
\gamma_q^0(R) = \limsup_{n \to \infty} \frac{1}{n} \log_q (\Gamma^0(n, [Rn], q)).
\]

We obtain a different upper bound.

**Theorem 19.** For all rates \(R \in (0, 1)\) we have

\[
\gamma_q^0(R) \leq \frac{R}{2}.
\]

In particular, \(\gamma_q(R) \leq l_0(q)\), the unique solution in \((0, \frac{2^t - 1}{q})\) of the equation \(H_q(x) = \frac{x}{2}\).

**Proof.** The bound comes from the immediate inequalities \(\Gamma^0(n, k, q) \leq \Gamma^0(k, q)\) and Theorem 5. \(\square\)

VI. NUMERICS

We conjecture, but cannot prove, based on the figures of Table 1, that some local maxima of \(n \mapsto \Gamma(n, k, q)\), for fixed \(k\) of the form \(k = \frac{d(n+1)}{2}\) are met for codes with check polynomials of the form \(\prod_{i=1}^{d} h_i(x)\), where \(h_i\) is irreducible of degree \(i\). Another motivation for the conjecture is that cyclic codes with irreducible check polynomials are one-weight codes in primitive length. (Note that 8 is not of the form \(\frac{d(n+1)}{2}\).)

What can be noted from Table 1 is that the bound \(\Gamma(k, q) \geq k\) of Proposition 1 is weak.

A systematic algorithm to compute \(\Gamma(k, q)\) can be sketched as follows.

(i) Find all polynomials \(h\) of degree \(k\) of \(\mathbb{F}_q[x]\), such that \(h(0) \neq 0\);

(ii) For each \(h\) compute its period \(T_h\);

(iii) Count the number \(s_h\) of nonzero weights of the cyclic code of length \(T_h\) and check polynomial \(h\);

(iv) Maximize \(s_h\) over all \(h\)’s in Step (i).

We justify this algorithm as follows.

**Proof.** View \(h\) as the check polynomial of an \([n, k]\) cyclic code \(C\). If \(h(x) = x^a H(x)\), with \(a \geq 1\), and \(H(0) \neq 0\), then \(\gcd(x^n - 1, h) = H(x)\) and \(C\) has for dimension the degree
of $H < k$. Contradiction. Since $h(0) \neq 0$, the period of $h$ is well-defined. All cyclic codes with check polynomial $h$ will have lengths a multiple of $T_h$, and will be repetitions of the code of length $T_h$, with the same number of weights. □

We illustrate this algorithm by the special case $k = 3, q = 2$. The polynomials $h$ can take the following values

(i) $x^3 + x + 1$, $x^3 + x^2 + 1$, when $T = 7$ and $s = 1$ (Simplex code)
(ii) $x^3 + 1$ when $T = 3$ and $s = 3$ (Universe code)
(iii) $x^3 + x^2 + x + 1 = \frac{x^4 - 1}{x + 1}$ when $T = 4$ and $s = 2$ (Even weight code)

We conclude that $\Gamma(3, 2) = 3$. More generally, we have the following results for $q = 2$ and $q = 3$. If the number $s_h$ of nonzero weight of the cyclic code of check polynomial $h(x)$ meets $\Gamma(k, q)$, we call $h(x)$ the optimal polynomial. We list some optimal polynomials $h(x)$ as follows. The coefficients of the polynomial $h(x)$ are written in increasing powers of $x$, for example for $k = 3$, the entry 1001 means $1 + x^3$.

### VII. Conclusion and Open Problems

In this paper, we have studied the largest number of distinct nonzero weights a cyclic code of given length and dimension could have. We have derived some upper bounds on that quantity that seem especially sharp for irreducible cyclic codes. Lower bounds appear weak so far, being mostly linear in $k$, when the upper bounds are exponential. The Melas and Zetterberg codes provided lower bounds exponential in the dimension and it is worth extending these bounds to other range of parameters. The results on the weights of $q$-ary Reed-Muller and Hamming codes, while of interest in their own right only provide lower bounds that are polynomial in the dimension.

So sharpening the lower bounds is the main open problem. Finding a pattern in the local maxima of $n \mapsto \Gamma(n, k, q)$ by running extensively the algorithm of the last section for large $n$’s might help. This programming effort could lead to a table of the function $\Gamma(k, q)$ for modest values of $kq$, let us say $kq \leq 100$ for instance.

### APPENDIX I

#### REED-MULLER CODES

In both the appendices, the symbol $wt(C)$ denotes the set of weights of the code $C$, i.e.

$$wt(C) = \{i \in \mathbb{N} \mid \exists c \in C \text{ s.t. } \omega_H(c) = i\}.$$ 

Moreover, let $t$ be a positive integer. Given $t$ sets of integers $A_1, \ldots, A_t$, we define the set of sums

$$\bigoplus_{i=1}^{t} A_i := \{a_1 + a_2 + \ldots + a_t \mid a_i \in A_i\}.$$

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

$$ev_m : R_m \longrightarrow \mathbb{F}_q^m$$

$$f \mapsto (f(P_1), \ldots, f(P_n)).$$

**Definition 20.** 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 defined by

$$RM_q(r, m) := \{ev_m(f) \mid f \in R_m, \deg(f) \leq r\}.$$ 

Observe that the choice of the order of the points $P_i$ of $\mathbb{F}_q^m$ does not matter. Indeed, different choices lead to equivalent codes. However, it is possible to define the order in a smart way, such that we have an inductive construction of the $q$-ary Reed-Muller codes. Let $\gamma$ be a primitive element of $\mathbb{F}_q$. For $m = 1$ we consider $P_1 = 0$ and $P_i = \gamma^{i-1}$ for $i = 2, \ldots, q$. Inductively, if $\{P_1, \ldots, P_n\}$ is the set of points chosen for $n = q^m$, then for $m + 1$ we choose $\{P_1', \ldots, P_N\}$, where $N = q^{m+1}$, as follows.

$$P_i' = (P_i, 0) \quad \text{for } 1 \leq i \leq n.$$ 

$$P_{nj+i}' = (P_i, \gamma^j) \quad \text{for } 1 \leq i \leq n, 1 \leq j \leq q - 1.$$
With this choice of the order of the points, one can prove the following result whose proof is omitted since it can be found in [4]. For the rest of this section, for any integers \(s, t\), we denote by \(G_q(s, t)\) a generator matrix for the \(q\)-ary-Reed Muller code of order \(s\) in \(t\) variables.

**Proposition 21.** There exist \(\lambda_{i,j} \in \mathbb{F}_q\) for \(1 \leq i < j \leq q\) such that

\[
G_q(r, m + 1) = \begin{pmatrix}
G_q(r, m) & \lambda_{1,2}G_q(r, m) & \ldots & \lambda_{1,q}G_q(r, m) \\
0 & \ddots & \vdots & \vdots \\
\vdots & \ddots & \ddots & \vdots \\
0 & \ldots & G_q(r-q+2,m) & \lambda_{q-1,q}G_q(r-q+2,m) \\
0 & \ldots & \ldots & G_q(r-q+1,m)
\end{pmatrix},
\]

**Remark 22.** Observe that, in the case \(m = 1\), the Reed-Muller code \(\mathcal{R}_m(q, 1)\) is simply the extended Reed-Solomon code of length \(q\) and dimension \(r + 1\). It is well-known that in this case \(wt(\mathcal{R}_m(q, 1)) = \{q - r, q - r + 1, \ldots, q\}\) (see [9, Theorem 6]).

Let now denote by \(n_q(r, m), k_q(r, m)\) and \(d_q(r, m)\) respectively the length, dimension and minimum distance of the Reed-Muller code \(R_q(r, m)\). The following result can be found in [4], and explains more about the structure of this family of codes.

**Proposition 23.** Let \(r, m\) be integers such that \(0 \leq r \leq (q - 1)m\). Then

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. \(d(r, m) = (q - S)^{q-1-n}\), where \(S = Q(q - 1) + S\) with \(0 \leq S \leq q - 2\).
4. \(\mathcal{R}_m(q, m) = \mathcal{R}_m(q - 1 - r, 1, m)\), and therefore \(G_q(r, m)\) is a parity check matrix for the code \(\mathcal{R}_m(q - 1 - r, 1, m)\).

**Corollary 24.** Let \(r, m\) be integers such that \(m \geq 1\) and \(0 \leq r \leq m(q - 1)\). Let \(u_1, \ldots, u_q \in \mathcal{R}_m((m-1)(q-1)-r-1,m)\). Then \(u_1 \mid \ldots \mid u_q \in \mathcal{R}_m(m(q-1)-r-1,m)\).

**Corollary 25.** Let \(r, m\) be integers such that \(m \geq 1\) and \(0 \leq r \leq m(q - 1)\). Then

\[
wt(\mathcal{R}_m(q - 1 - r, 1, m)) \geq \bigoplus_{i=1}^q wt(\mathcal{R}_m((m-1)(q-1)-r-1, m-1)).
\]

We can finally give a general statement on the set of weights for some classes of \(q\)-ary Reed-Muller codes.

**Theorem 26.** For every positive integer \(m\) and every integer \(r\) such that \(0 \leq r \leq \frac{q^m}{2}\), it holds that

\[
wt(\mathcal{R}_m(q - 1 - r, 1, m)) = \{0, r + 2, r + 3, \ldots, q^m\}.
\]

**Proof.** We proceed by induction on \(m\). For \(m = 1\) we get that \(\mathcal{R}_m(q - r, 1)\) is the Reed-Solomon code of length \(q\) and dimension \(q - r - 1\). Therefore, \(wt(\mathcal{R}_m(q - r, 1)) = \{r + 2, r + 3, \ldots, \}\). By Euclidean division, we have \(x = an + b\), with \(0 \leq a < q\) and \(0 \leq b < n\). At this point we distinguish two cases.

1. **Case 1:** If \(a = 0, r + 2, r + 3, \ldots, \) then we choose \(x_0 = b, x_1 = \cdots = x_q = n\) and \(x_{a+1} = \cdots = x_{q-1} = 0\). This concludes the proof.

2. **Case 2:** If \(a = 1, r + 1, \) then, necessarily \(a \geq 1\) by hypothesis we have \(n \geq q \geq 2r + 3\). Therefore, \(r + 2 + b \in \{0, r + 2, \ldots, n\}\). We choose \(x_0 = r + 2, x_1 = \cdots = x_{q-2} = x_q = n\) and \(x_{a+1} = \cdots = x_{q-1} = 0\). This concludes the proof.

**A. Binary Reed-Muller Codes**

Here we provide an additional result not covered by Theorem 26 for binary Reed-Muller codes.

**Theorem 27.** Let \(m\) be a positive integer, then we have

1. If \(m \geq 3\), then \(wt(\mathcal{R}_m(2m-2,m)) = \{0, 2, 4, \ldots, 2^m\} \setminus\{2, 2^m\}\).
2. If \(m \geq 6\), then \(wt(\mathcal{R}_m(2m-3,m)) \supseteq \{0, 2, 4, \ldots, 2^m\} \setminus\{2, 4, 6, 10, 2^m-2, 2^m-4, 2^m-6, 2^m-10\}\).

**Proof.** (1) We prove it by induction on \(m\). In the case \(m = 3\), a Magma [5] computation shows that \(wt(\mathcal{R}_m(2m-1,m)) = \{0, 2, 4, 6, 8\} \setminus\{2, 6\}\). Now, suppose that the claim is true for \(m \geq 3\), by Corollary 25, we have \(wt(\mathcal{R}_m(2m-1,m+1)) \supseteq A\), where \(A = \{i \mid i + j, j \in wt(\mathcal{R}_m(2m-2,m))\}\). It is easy to check that \(A = \{0, 2, 4, \ldots, 2^{m+1}\} \setminus\{2, 2^{m+1} - 2\}\). We know, by minimum distance arguments in Proposition 23, that the integer 2 is not in
Theorem 28. Let \( m \) be a positive integer, then we have
\[
\text{wt}(R,M_2(4m - 3, m)) = \{0, 4, 5, 6, \ldots, 5^m\} \text{ for } m \geq 1.
\]

Proof. We also prove it by induction on \( m \). The cases \( m = 1, 2 \) can be checked with the aid of the software Magma [5] to be wt\((R,M_2(1, 1)) = \{0, 4, 5\} \) and wt\((R,M_2(5, 2)) = \{0, 4, 5, 6, \ldots, 25\} \). Now, suppose that the claim is true for \( m \geq 2 \), then \( B = \{i + j + l | i, j, l, t \in \text{wt}(R,M_2(4m - 3, m))\} = \{0, 4, 5, 6, \ldots, 5^m + 1\} \). From Corollary 25, we have \( \text{wt}(R,M_2(5m + 2, m + 1)) \supseteq \{0, 4, 5, 6, \ldots, 5^m + 1\} \). Finally, from part (3) of Proposition 23, we have \( d(4m - 3, m) = 4 \). This completes the proof.

Appendix II

\( q \)-ary Hamming Codes

Let \( q \) be a prime power, and let \( F_q^* = F_q \setminus \{0\} \) denote the multiplicative group of \( F_q \). It is well-known that \( F_q^* \) is a cyclic group, i.e. there always exists a generator \( \gamma \) such that
\[
F_q = \{\gamma^i | 1 \leq i \leq q - 1\} \cup \{0\}.
\]

For \( u = (u_1, \ldots, u_n) \), \( v = (v_1, \ldots, v_n) \in F_q^n \) we denote by \( (u, v) \) the standard inner product between \( u \) and \( v \), i.e.
\[
(u, v) := \sum_{i=1}^n u_i v_i.
\]

With this notation, given \( u_i, v_i \in F_q^* \) for \( i = 1, \ldots, m \), it trivially holds that
\[
|w_H (u_1 | \ldots | u_m)| = \sum_{i=1}^m |w_H (u_i)|, \quad \sum_{i=1}^m (u_1 | \ldots | u_m), (v_1 | \ldots | v_m) = \sum_{i=1}^m (u_i, v_i).
\]

Suppose \( r \) is a positive integer. On the set \( F_q^r \setminus \{0\} \) we can consider the following equivalence relation:
\[
u \sim v \iff \exists \lambda \in F_q^r \text{ such that } u = \lambda v.
\]

The projective geometry of order \( q \) and dimension \( r \) is defined as
\[
PG(r - 1, q) = (F_q^r \setminus \{0\})/\sim.
\]

A set of representatives for \( PG(r - 1, q) \) is given by the set of all nonzero vectors of length \( r \) whose first nonzero entries is equal to 1. For this reason, the space \( PG(r - 1, q) \) can be embedded in \( F_q^r \). The image of this embedding will be denoted by \( P_r(q) \). We will use this different notations in order not to confuse it with the space \( PG(r - 1, q) \), since we will often use the elements of \( P_r(q) \) as elements of \( F_q^r \), where the notion of sum is well-defined. Since the cardinality of \( P_r(q) \) is equal to the cardinality of \( PG(r - 1, q) \), we have that
\[
\theta_r(q - 1) := \frac{q^r - 1}{q - 1} = |P_r(q)|.
\]

Definition 30. Let \( q \) be a prime power, and let \( r \geq 2 \) be a positive integer. We define the \( q \)-ary Hamming code \( H_r(q) \)
as the \([\theta_0(r - 1), \theta_0(r - 1) - r]\) linear code over \(F_q\) whose parity check matrix \(H_r\) is obtained by choosing all the vectors of \(P_r(q)\) (without repetitions) as columns.

Observe that in Definition 30 the order of the choice of the columns does not really matter. Indeed, permuting the columns of the parity check matrix of a code gives rise to an equivalent code. All the parameters of a code, such that length, dimension and weight distribution are invariant under equivalence of codes. Therefore, for our purpose of studying the weight set of an Hamming code, we are free to choose the order of the columns of \(H_r\) in the way we prefer.

**Lemma 31.** Let \(H_{r-1}\) be the parity check matrix for the Hamming code \(H_{r-1}(q)\) as described in Definition 30. Then we can obtain a parity check matrix for \(H_r(q)\) as

\[
H_r = \begin{pmatrix}
0 & 0 & 0 & 1 & 1 & 1 & \cdots & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & \gamma H_{r-1} & \cdots & \gamma^{q-1} H_{r-1} & 0
\end{pmatrix},
\]

where \(\gamma\) is a primitive element of \(F_q\) and \(H_1 = (1)\).

**D. The Main Theorem**

Hamming codes have been deeply studied in the theory of error correcting codes, since they represent the only existing infinite family of perfect codes. Indeed, in addition to Hamming codes, the only perfect linear codes that are non-trivial, are the binary Golay code and the ternary Golay code [10, 16, 23].

It is a well-known fact that \(q\)-ary Hamming codes always have minimum distance equal to 3. Moreover, a recursive formula for the weight distribution of a \(q\)-ary Hamming code \(H_r(q)\) is known, and it can be found in [12]. Anyway, from that recursion, it is not immediate how to deduce whether the number of codewords of weight \(i\) in \(H_r(q)\) is greater than or not. In the particular case that \(r = 2\) we know more about the structure of \(H_2(q)\).

**Lemma 32.** For \(r = 2\) the Hamming code \(H_2(q)\) is an MDS code of parameters \([q + 1, q - 1, 3]\). In particular, \(\text{wt}(H_2(3)) = [0, 3]\) and \(\text{wt}(H_2(q)) = \{0, 3, 4, \ldots, q + 1\}\) for every \(q > 3\).

**Proof.** The parameters of \(H_2(q)\) are well-known to be \([q + 1, q - 1, 3]\). From there we see that this code is MDS. The explicit determination of the weights follows then by [9, Theorem 10].

The above result represents, except for the case \(q = 3\), the base step of our proof for induction. Now, we give some auxiliary tools that will enable us to prove our main results in this section.

**Lemma 33.** Let \(q > 2\) be a prime power, and let \(r \geq 1\) be a positive integer. Then

\[
\sum_{u \in P_r(q)} u = 0\quad \text{and} \quad \sum_{u \in P_r(q)} u = e_r,
\]

where \(e_r = (0, 0, \ldots, 0, 1)^T\).

**Proof.** For the first equality, we prove it by induction. Let \(r = 1\) and \(q \geq 3\), and \(\gamma\) be a primitive element of \(F_q\). Then

\[
\sum_{u \in P_r(q)} u = \sum_{i=0}^{q-2} \gamma^i = \frac{\gamma^{q-1} - 1}{\gamma - 1},
\]

since \(\gamma \neq 1\). Moreover, \(\gamma^{q-1} = 1\) and then we get the result. For \(r > 1\), we can write \(F_{qr} = \bigcup_{a \in F_q} T_a\), where

\[
T_a := \{(a, v') \mid v' \in F_{q-1}^{r-1}\},
\]

and the union is clearly disjoint. Therefore,

\[
\sum_{v \in F_r} \sum_{u \in F_{qr}} (a, v') = \sum_{a \in F_q} (q^{r-1} a, 0) = 0,
\]

where \(q^{r-1} a\) denotes (with a slight abuse of notation)

\[
\underbrace{a + \ldots + a}_{q^{r-1}\text{ times}},
\]

and the second equality holds for inductive hypothesis.

Concerning the second statement, we proceed again by induction. For \(r = 1\) the statement is clearly true, since \(P_1(q)\) is the set with the only element \(e_1 = (1)\). Suppose now \(r > 1\). Then we can write

\[
P_r(q) = \{ (0, u') \mid u' \in P_{r-1}(q) \} \cup \{ (1, v') \mid v' \in F_{q-1}^{r-1} \}.
\]

Therefore,

\[
\sum_{u \in P_r(q)} u = \sum_{u' \in P_{r-1}(q)} (0, u') + \sum_{v' \in F_q^{r-1}} (1, v') = e_r + 0 = e_r,
\]

where the second equality comes from inductive hypothesis and from the first part of this lemma.

**Proposition 34.** For every \(q > 2\), and every integer \(r \geq 2\), there exists a codeword \(c \in H_r(q)\) of full weight, i.e., such that \(\omega_H(c) = \theta_0(r - 1)\), except for the case \((q, r) = (3, 2)\).

**Proof.** For \(r = 2\) the statement trivially follows from Lemma 32. Suppose now \(r \geq 3\), and let \(\gamma\) be a primitive element of \(F_q\). Consider the set

\[
D = \{w_0, w_1, \ldots, w_{q-1}\},
\]

where \(w_0 = e_1 = (1, 0, \ldots, 0)\) and \(w_i = (1, \gamma^i, \gamma^{2i}, \ldots, \gamma^{r-1})\) for \(i = 1, 2, \ldots, q - 2\) and \(w_{q-1} = (1, 1, \ldots, 1, 0)\). It is easy to see that with this choice of \(D\), we have

\[
\sum_{i=0}^{q-1} w_i + e_r = 0.
\]

Let \(\alpha \in F_q\). We consider the sum

\[
\sum_{u \in P_r(q)} u + (1 + \alpha) \sum_{i=0}^{q-1} w_i + \alpha e_r = \sum_{u \in P_r(q)} u + \alpha \sum_{i=0}^{q-1} w_i + \alpha e_r
\]

\[
= \alpha \left( \sum_{i=0}^{q-1} w_i + e_r \right) = 0.
\]
Choosing $\alpha \in \mathbb{F}_q \setminus \{0, -1\}$, we have a linear combination of the columns of $H_r$ that gives the zero vector, and in which every column is multiplied by a nonzero coefficient. This gives a codeword that has all nonzero entries.

Proposition 34 proves the existence of a codeword of maximum weight in every Hamming code, with the exception of $\mathcal{H}_2(3)$. For all the remaining weights we will use an induction argument based on the following two results.

Lemma 35. If $u_i \in \mathcal{H}_{r-1}(q)$ for $i = 0, 1, \ldots, q - 1$, then

$$(u_0 \mid u_1 \mid \ldots \mid u_{q-1} \mid \alpha) \in \mathcal{H}_r(q),$$

where

$$\alpha = -\sum_{i=1}^{q-1} (u_i, e),$$

and $e$ denotes the vector with all entries equal to 1.

Proof. According to Lemma 31, it is straightforward to see that the vector $(u_0 \mid u_1 \mid \ldots \mid u_{q-1} \mid \alpha)$ satisfies the check equations given by the rows $i = 2, \ldots, r$ of the parity check matrix. Moreover, the condition on $\alpha$ ensures that it also satisfies the first check equation. \Halmos

Let $q$ be a prime power, $n$ be a positive integer. Consider the space

$$((\mathbb{F}_q^n)^q)^q$$

Let $S_q$ denote the symmetric group on the set $\{0, 1, \ldots, q - 1\}$. $id$ denote identical permutation and consider the action of the group $((\mathbb{F}_q^n)^q)^q \times S_q$ on $(\mathbb{F}_q^n)^q$ defined as

$$\varphi : ((\mathbb{F}_q^n)^q \times S_q) \times ((\mathbb{F}_q^n)^q)^q$$

$$(\beta, \sigma, (u_0 \mid \ldots \mid u_{q-1})) \mapsto (\beta_0u_0(0) \mid \ldots \mid \beta_{q-1}u_{\sigma(q-1)}).$$

It is straightforward to see that the same group acts on $((\mathcal{H}_{r-1}(q))^q)^q$. In order to simplify the notation, for $(\beta, \sigma) \in ((\mathbb{F}_q^n)^q \times S_q)$, $u \in (\mathbb{F}_q^n)^q$, we will write

$$(\beta, \sigma) \cdot u := \varphi((\beta, \sigma), u).$$

Proposition 36. Let $q > 2$ be a prime power and let $(u_0 \mid \ldots \mid u_{q-1}) \in \mathcal{H}_{r-1}(q)^q$. Then there exists $(\beta, \sigma) \in ((\mathbb{F}_q^n)^q \times S_q)$ such that

$$(\beta_0u_0(0) \mid \ldots \mid \beta_{q-1}u_{\sigma(q-1)} \mid 0) \in \mathcal{H}_r(q).$$

Proof. Let $u_0, u_1, \ldots, u_{q-1} \in \mathcal{H}_{r-1}(q)$. By Lemma 35 we have that $(u_0 \mid u_1 \mid \ldots \mid u_{q-1} \mid \alpha) \in \mathcal{H}_r(q)$, where $\alpha = -\sum_{i=1}^{q-1} (u_i, e)$. If $\alpha = 0$ we are done. Therefore, suppose $\alpha \neq 0$, and consider the set

$$T := \{i \in \{1, \ldots, q - 1\} \mid (u_i, e) \neq 0\}.$$

Since $\alpha \neq 0$, then $|T| \geq 1$. We distinguish two cases.

Case 1 ($|T| \geq 2$): Let $r, s \in T$ be two distinct elements. Consider a generic vector $\beta = (\beta_0, \ldots, \beta_{q-1})$ whose entries are $\beta_i = 1$ for $i \neq r, s$, and consider the element $(\beta, id) \cdot (u_0 \mid \ldots \mid u_{q-1})$. By Lemma 35, the vector

$$((\beta, id) \cdot (u_0 \mid \ldots \mid u_{q-1}) \mid \alpha) \in \mathcal{H}_r(q),$$

belongs to $\mathcal{H}_r(q)$, where

$$\alpha = -\sum_{i=1}^{q-1} (\beta_iu_i, e)$$

$$= -\sum_{i=1}^{q-1} (u_i, e) + (1 - \beta_r)(u_r, e) + (1 - \beta_s)(u_s, e)$$

$$= \alpha + (1 - \beta_r)(u_r, e) + (1 - \beta_s)(u_s, e).$$

Imposing the condition $\alpha = 0$ we get

$$(1 - \beta_r) = -\alpha + (1 - \beta_s)(u_r, e).$$

Since $q > 2$, there exists $(\beta_r, \beta_s) \in \mathbb{F}_q^2 \times \mathbb{F}_q^2$ satisfying Equation (3), and we can conclude.

Case 2: $|T| = 1$: Let $r$ be the only element in $T$. We divide this case into two subcases:

(i) If $(u_0, e) = 0$, then consider the transposition $\sigma = (0, r) \in S_q$. Consider the element

$$(e, \sigma) \cdot (u_0 \mid \ldots \mid u_{q-1}) = (v_0 \mid \ldots \mid v_{q-1}).$$

By Lemma 35, we have

$$(v_0 \mid \ldots \mid v_{q-1} \mid \alpha) \in \mathcal{H}_r(q),$$

where

$$\alpha = -\sum_{i=1}^{q-1} (v_i, e) = -\sum_{i=0}^{q-1} (u_i, e) = -\sum_{i=0}^{q-1} 0 = 0,$$

and we are done.

(ii) Suppose now that $(u_0, e) \neq 0$. Then there exists $s \in \{1, 2, \ldots, q - 1\}$ such that $s \notin T$. We now consider the transposition $\sigma = (0, s)$ and the corresponding vector

$$(e, \sigma) \cdot (u_0 \mid \ldots \mid u_{q-1}).$$

For this new vector we have now $|T| = 2$ and we can conclude by Case 1.

This completes the proof. \Halmos

As a direct consequence, we immediately get the following result.

Corollary 37. Let $q > 2$ be a prime power, and let $r \geq 3$ be a positive integer. Then

$$\text{wt}(\mathcal{H}_r(q)) \geq \sum_{i=0}^{q-1} \text{wt}(\mathcal{H}_{r-1}(q)).$$

We are now ready to prove the main result.

Theorem 38. Let $q > 2$ be a prime power, and let $r \geq 2$ be an integer. Then

$$\text{wt}(\mathcal{H}_r(q)) = \{0, 3, \ldots, N\},$$
where \( N := \theta_q(r - 1) \), except when \((q, r) = (3, 2)\), in which case \( \text{wt}(\mathcal{H}_2(3)) = \{0, 3\} \).

**Proof.** We prove it by induction. The base step is divided in two cases.

**Case 1** \((q, 2) \text{ With } q > 3\): It follows from Lemma 32.

**Case 2** \((q, r) = (3, 2)\): We computed it with the aid of the software Magma [5].

Now, suppose that the claim is true for \((q, r - 1)\) and we want to prove it for \((q, r)\). By hypothesis we know that

\[
\text{wt}(\mathcal{H}_{r-1}(q)) = \{0, 3, \ldots, n\}
\]

where \( n = \theta_q(r - 2) \), and observe that \( N = qn + 1 \).

By Corollary 37, we know that

\[
\text{wt}(\mathcal{H}_r(q)) \supseteq \bigoplus_{i=0}^{q-1} \text{wt}(\mathcal{H}_{r-1}(q)) = \bigoplus_{i=0}^{q-1} \{0, 3, \ldots, n\}.
\]

Moreover, since \((q, r - 1) \neq (3, 2)\), we have that \( n \geq 5 \).

By Proposition 34 we already know that \( N \in \text{wt}(\mathcal{H}_r(q)) \).

Therefore it is enough to show that

\[
\bigoplus_{i=0}^{q-1} \{0, 3, \ldots, n\} = \{0, 3, \ldots, qn\}.
\]

It is clear that \( N - 1 = qn \) belongs to our set, since \( n \in \text{wt}(\mathcal{H}_{r-1}(q)) \). Let \( x \in \{0, 3, \ldots, qn - 1\} \), we need to prove that we can write \( x = x_0 + x_1 + \cdots + x_{q-1} \) with \( x_i \in \{0, 3, \ldots, n\} \). By Euclidean division, we have \( x = an + b \), with \( 0 \leq a < q \) and \( 0 \leq b < n \). At this point we distinguish two cases.

**Case 1** \((b \in \{0, 3, \ldots, n - 1\})\): We choose \( x_0 = b, x_1 = \cdots = x_a = n \) and \( x_{a+1} = \cdots = x_{q-1} = 0 \).

**Case 2** \((b \in \{1, 2\})\): Then, necessarily \( a \geq 1 \). Moreover, we already observed that \( n \geq 5 \). Therefore, \( n - 3 + b \in \{0, 3, \ldots, n\} \) and we choose \( x_0 = 3, x_1 = n - 3 + b, x_2 = \cdots = x_a = n \) and \( x_{a+1} = \cdots = x_{q-1} = 0 \). This concludes the proof.

**ACKNOWLEDGMENT**

The paper is dedicated to the memory of our friend and mentor G.D. Cohen (1951–2018). The authors would like to thank Prof. C. Ding for helpful discussions.

**REFERENCES**

[1] T. L. Alderson, “A note on full weight spectrum codes,” 2018, arXiv:1807.11798. [Online]. Available: https://arxiv.org/abs/1807.11798

[2] T. L. Alderson and A. Neri, “Maximum weight spectrum codes,” Adv. Math. Commun., vol. 13, no. 1, pp. 101–119, 2019.

[3] E. Assmus and J. Key, “Polynomial codes and finite geometries,” in Handbook of Coding Theory, W. C. Huffman and V. S. Pless, Eds. Amsterdam, The Netherlands: North Holland, 1998, pp. 1269–1343.

[4] T. Blackmore and G. Norton, “Matrix-product codes over \( F_q \),” Applicable Algebra Eng., Commun. Comput., vol. 12, no. 6, pp. 477–500, 2001.

[5] W. Bosma, J. Cannon, and C. Playoust, “The magma algebra system I: The user language,” J. Symbolic Comput., vol. 24, pp. 235–265, 1997. [Online]. Available: http://magma.maths.usyd.edu.au/magma/

[6] G. D. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, Covering Codes, vol. 54, Amsterdam, The Netherlands: North Holland, 1997.

[7] G. D. Cohen and L. Tolhuizen, “Maximum weight spectrum codes with reduced length,” 2018, arXiv:1806.05427. [Online]. Available: https://arxiv.org/abs/1806.05427

[8] C. Ding and J. Yang, “Hamming weights in irreducible cyclic codes,” Discrete Math., vol. 313, no. 4, pp. 434–446, 2013.

[9] M. F. Ezerman, M. Grassl, and P. Solé, “The weights in MDS codes,” IEEE Trans. Inf. Theory, vol. 57, no. 1, pp. 392–396, Jan. 2011.

[10] W. C. Huffman and V. Pless, Fundamentals Error Correcting Codes, Cambridge, U.K.: Cambridge Univ. Press, 2003.

[11] N. Hurt, “Exponential sums and coding theory: A review,” Acta Appl. Math., 46, no. 1, pp. 49–91, 1997.

[12] D. S. Kim, “Weight distributions of Hamming codes,” 2017, arXiv:0710.1407. [Online]. Available: https://arxiv.org/abs/0710.1407

[13] F. R. Kschischang and S. Pasupathy, “Some ternary and quaternary codes and associated sphere packings,” IEEE Trans. Inf. Theory, vol. 38, no. 2, pp. 227–246, Mar. 1992.

[14] G. Lachaud and J. Wolfmann, “The weights of the orthogonals of the extended quadratic binary Goppa codes,” IEEE Trans. Inf. Theory, vol. 36, no. 3, pp. 686–692, May 1990.

[15] R. Lidl and H. Niederreiter, Finite Fields, vol. 20. Cambridge, U.K.: Cambridge Univ. Press, 1997.

[16] F. J. MacWilliams and N. J. A. Sloane, The Theory Error Correcting Codes, Amsterdam, The Netherlands: North Holland, 1977.

[17] R. J. McEliece, “Irreducible cyclic codes and Gauss sums,” in Combinatorics. Dordrecht, The Netherlands: Springer, 1975, pp. 185–202.

[18] A. Meneghetti, “On linear codes and distinct weights,” 2018, arXiv:1804.04373. [Online]. Available: https://arxiv.org/abs/1804.04373

[19] R. Schoof, “Families of curves and weight distributions of codes,” Bull. Amer. Math. Soc., vol. 32, no. 2, pp. 171–183, 1995.

[20] M. Shi, Z. Zhang, and P. Solé, “Two-weight codes and second order recurrences,” Chin. J. Electron., to be published.

[21] M. Shi, H. Zhu, P. Solé, and G. D. Cohen, “How many weights can a linear code have?” Des., Codes Cryptogr., vol. 87, no. 1, pp. 87–95, 2019.

[22] N. J. Sloane, “The on-line encyclopedia of integer sequences,” Amer. Math. Soc., vol. 50, pp. 912–915, Dec. 2003. [Online]. Available: http://www.oeis.org

[23] A. Tietäväinen, “On the nonexistence of perfect codes over finite fields,” J. Algebra, vol. 24, no. 1, pp. 88–96, 1973.

[24] G. Van der Geer and M. van der Vlugt, “Artin-Schreier curves and codes,” J. Algebra, vol. 139, no. 1, pp. 256–272, 1991.