



How many weight can a cyclicc ode have?

Minjia Shi, Xiaoxiao Li, Alessandro Neri, Patrick Sole

► To cite this version:

Minjia Shi, Xiaoxiao Li, Alessandro Neri, Patrick Sole. How many weight can a cyclicc ode have?. IEEE Transactions on Information Theory, 2019. hal-02411137

HAL Id: hal-02411137

<https://hal.science/hal-02411137>

Submitted on 14 Dec 2019

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

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

How many weights can a cyclic code have

? *

Minjia Shi¹, Xiaoxiao Li¹, Alessandro Neri^{2†} and Patrick Solé³

¹School of Mathematical Sciences, Anhui University, Hefei, 230601, China

²Institute of Mathematics, University of Zürich, Switzerland

³CNRS/LAGA, University of Paris 8, 2 rue de la Liberté, 93 526 Saint-Denis, France

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.

Keywords: cyclic codes, irreducible cyclic codes, Hamming codes, Reed-Muller codes

*This research is supported by National Natural Science Foundation of China (61672036), Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20), Technology Foundation for Selected Overseas Chinese Scholar, Ministry of Personnel of China (05015133).

[†]The author was supported by the Swiss National Science Foundation through grant no. 169510.

1 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 kq . 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 $q \geq 3$.

2 Definitions and Notation

2.1 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 $\mathbf{x} \in \mathbb{F}_q^n$ is the number of indices i where $x_i \neq 0$, and it is denoted by $w_H(\mathbf{x})$. 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** [16, Th 11, Chap. 1] on its parameters

$$d \leq n - k + 1.$$

A code meeting that bound is called **maximum distance separable (MDS)**. See [16, Chap. 11] for general knowledge on this family of codes.

2.2 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 \mathbf{c} can be continued by repetition into a bi-infinite periodic sequence $\hat{\mathbf{c}}$ which is periodic of least period a divisor of n . The **period** of a codeword \mathbf{c} is understood to be the smallest integer T_0 such $\hat{\mathbf{c}}_{i+T_0} = \hat{\mathbf{c}}_i$ 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 .

2.3 Combinatorial functions

Here we introduce the combinatorial functions we are going to study in this work. Let q be a prime power, $0 \leq k \leq n$ be non negative integers. 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 that a linear code of dimension k over \mathbb{F}_q , and the maximum number of nonzero weights for linear codes 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].

3 Upper bounds

3.1 Cycle structure

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

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

$$\alpha \mathbf{c} = \rho^i(\mathbf{c}).$$

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 $\gcd(t, q - 1)$.*

Proof. Let \mathbf{c} be a codeword of period t and suppose $\alpha \mathbf{c} = \rho^i(\mathbf{c})$. Then $\mathbf{c} = \rho^{ri}(\mathbf{c}) = \alpha^r \mathbf{c}$, and this implies $\alpha^r = 1$. Let now H be the unique subgroup of \mathbb{F}_q^* of order

$\gcd(t, q-1)$. Since by definition $r|t$ and also $\alpha^{q-1} = 1$, we get $\alpha^{\gcd(t, q-1)} = 1$, i.e. $\alpha \in H$. \square

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*

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

Proof. The number of cyclic classes of codewords of period t is at most $\frac{B_t}{t}$. All codewords in the same class share the same weight. Then, we use the Lemma above. Let \mathbf{c} be a codeword and H be the unique subgroup of \mathbb{F}_q^* of order $\gcd(t, q-1)$. Now, for every representative α of \mathbb{F}_q^*/H , the codeword $\alpha\mathbf{c}$ gives a different class that obviously shares the same weight of the one of \mathbf{c} . Hence, there are at most $\frac{B_t \gcd(t, q-1)}{t(q-1)} = \frac{B_t}{\text{lcm}(t, q-1)}$ 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 $B_1 \in \{0, q-1\}$. \square

Example. Consider the code of dimension 2 over \mathbb{F}_5 , 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.

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 $\frac{n}{q-1}$ for some large class of cyclic codes, up to a factor n for another subclass.

Theorem 1. *If C is a $[n, k]_q$ strongly cyclic code with s nonzero weights, then*

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

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

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

One can observe that the function $\Gamma^0(n, k, q)$ has an intrisecly 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 1). This also implies that $\lim_{n \rightarrow \infty} \Gamma^0(n, k, q) = 0$, and this is in contrast to the behaviour of the function $L(n, k, q)$ that is non decreasing in n and $\lim_{n \rightarrow \infty} L(n, k, q) = L(k, q)$. As a second implication of Lemma 2, in the general case when many of the B_t 's are nonzero, we can prove the following result.

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

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

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

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

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

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

By definition of the B_t 's note that $\sum_{t | n} B_t = q^k - 1$, implying $\sum_{t | n} B_t^2 \leq (q^k - 1)^2$. The result follows by taking the square root of both sides. \square

3.2 Character sums

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

Theorem 3. *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

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

The result follows by computing the length of that interval. \square

3.3 Irreducible cyclic codes

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

Theorem 4. *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 1. The result follows. \square

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 5. *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 . \square

This shows that Theorem 4 can only be tight when $N = N_k$, or, equivalently, N divides $\frac{q^k-1}{q-1}$. Using Theorem 3, another bound can be derived.

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

Proof. As explained in the proof of Theorem 4 we know that all nonzero codewords have period n . Thus the code C is strongly cyclic, and we can apply Theorem 3. We get rid of k in Theorem 3 by writing $q^k = 1 + nN$. \square

Remark. Depending on the relative values of n and N , either Theorem 6, or Theorem 5 is sharper than the other.

A slight improvement on Theorem 6 can be derived for irreducible cyclic codes.

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*

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

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

Proof. The proof follows the lines of Theorem 6 with [15, Th. 8.84, (8.37)] replacing [15, Cor. 8.83]. We get rid of k by writing $q^k = 1 + nN$. \square

4 Lower bounds

4.1 Special values

We begin with an easy bound.

Proposition 1. *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 $\Gamma(k, k, q) \leq \Gamma(k, q)$. \square

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

Proposition 2. *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 $\frac{x^n - 1}{x - 1}$. Its dual is $P(n, q) = \langle (x - 1) \rangle$. The **binary Hamming code** \mathcal{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 8. 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 are easy to compute. To prove the second statement, observe that $x^{2^m} - x$ is the product of all monic irreducible polynomials whose degree divides m [16, Chap. 4, Th. 11]. If m is a prime number, any divisor of $x^{2^m-1} - 1$ of degree m will have then to be irreducible. Thus, cyclic codes of dimension (resp. codimension) m will have to be S_m (resp. \mathcal{H}_m) or replicated versions of $S_{m'}$ (resp. $\mathcal{H}_{m'}$) for m a proper divisor of m' . The result follows on observing that the number of nonzero weights of \mathcal{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]. \square

Remark. The fact that the number of nonzero weights of \mathcal{H}_m is $2^m - 5$ can also be derived applying part (1) of Theorem 16 of the Appendix if we notice that H_m is a punctured $R(m-2, m)$.

Theorem 9. Let $q > 2$ be a prime power and $r \geq 2$ such that $\gcd(r, q-1) = 1$. 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 $\gcd(r, q-1) = 1$ [10]. The result follows then by Theorem 19 of Appendix II. \square

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

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

Theorem 10. *With the notations above, we have the following results.*

$$\begin{aligned}
\Gamma\left(2^m - 1, \sum_{i=0}^{m-3} \binom{m}{i}, 2\right) &\geq 2^{m-1} - 9 \quad \text{for } m \geq 6, \\
\Gamma\left(3^m - 1, \sum_{i=0}^{2m-2} B(3, m, i), 3\right) &\geq 3^m - 3 \quad \text{for } m \geq 1, \\
\Gamma\left(3^m - 1, \sum_{i=0}^{2m-3} B(3, m, i), 3\right) &\geq 3^m - 7 \quad \text{for } m \geq 3, \\
\Gamma\left(5^m - 1, \sum_{i=0}^{4m-3} B(5, m, i), 5\right) &\geq 5^m - 4 \quad \text{for } m \geq 1. \\
\Gamma\left(q^m - 1, \sum_{i=0}^{(q-1)m-r-1} B(q, m, i), q\right) &\geq q^m - r - 2 \quad \text{for } 0 \leq r \leq \frac{q-3}{2}.
\end{aligned}$$

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. \square

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

Theorem 11. *For all integers $m \geq 3$, we have*

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

and

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

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

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

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

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

The result follows after elementary calculations. \square

A ternary analogue is as follows.

Theorem 12. *For all integers $m \geq 2$ we have $\Gamma(3^m - 1, 2m, 3) \geq \lceil 2 \times 3^{\frac{m-2}{2}} \rceil$.*

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 $\frac{3^m - 1 + t}{3}$ with $t \in \mathbb{Z}$, satisfying $t \equiv 1 \pmod{3}$, and $t^2 < 3^m$. The result follows after elementary calculations. \square

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 .

4.2 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 3. *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

5 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

$$\gamma_q(R) = \limsup_{n \rightarrow \infty} \frac{1}{n} \log_q(\Gamma(n, \lfloor Rn \rfloor, q)).$$

Theorem 13. 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 $(0, \frac{q-1}{q})$ of the equation $H_q(x) = x$.

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

Similarly for strongly cyclic codes we define

$$\gamma_q^0(R) = \limsup_{n \rightarrow \infty} \frac{1}{n} \log_q(\Gamma^0(n, \lfloor Rn \rfloor, q)).$$

We obtain a different upper bound.

Theorem 14. For all rates $R \in (0, 1)$ we have

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

In particular, $\gamma_q(R) \leq t^0(q)$, the unique solution in $(0, \frac{q-1}{q})$ 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 3. \square

6 Numerics

We conjecture, but cannot prove, based on the figures of Table 1, that some local maxima of $n \mapsto \Gamma(n, k, 2)$, for fixed k of the form $k = \frac{s(s+1)}{2}$ are met for codes with check polynomials of the form $\prod_{i=1}^s h_i(x)$, 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.

Table 1: lower bounds on $\Gamma(k, q)$

$\Gamma(k, q) \geq$	q	k	n	$h(x)$
8	2	6	21	$(1+x)(1+x+x^2)(1+x+x^3)$
15	2	10	105	$(1+x)(1+x+x^2)(1+x+x^3)(1+x+x^4)$
11	3	6	104	$(x+1)(x^2+1)(x^3+2x+1)$
20	3	10	1040	$(x+1)(x^2+1)(x^3+2x+1)(x^4+x+2)$
11	4	6	315	$(x+1)(x^2+x+w)(x^3+x+1)$
18	4	8	315	$(x+1)(x^2+x+w)(x^2+x+w^2)(x^3+x+1)$

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. \square

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 $1 + x^3$.

Table 2: exact values of $\Gamma(k, 2)$

	$k = 3$	$k = 4$	$k = 5$	$k = 6$	$k = 7$	$k = 8$	$k = 9$
$q = 2$	3	4	5	8	9	12	16
$h(x)$	(1001)	(11011) (10001)	(100001)	(1110011)	(11100111)	(111101111)	(1100100001) (1000010011)

Table 3: exact values of $\Gamma(k, 3)$

	$k = 3$	$k = 4$	$k = 5$	$k = 6$
$q = 3$	3	5	8	12
$h(x)$	(2211)			
	(2121)	(20221)	(222021)	
	(2101)	(22011)	(211101)	
	(2021)	(21021)	(210111)	(1201101)
	(2001)	(21011)	(202221)	(1102101)
	(1221)	(12111)	(121011)	(1012011)
	(1111)	(11121)	(112101)	(1011021)
	(1101)	(10201)	(110121)	
	(1011)	(10101)	(101211)	
	(1001)			

7 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.

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

8 Appendix I: Reed-Muller codes

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

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

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

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

Let m be a positive integer and \mathbb{F}_q be a finite field. Consider $R_m := \mathbb{F}_q[x_1, \dots, x_m]$ the ring of polynomials in m variables over \mathbb{F}_q . Moreover, list all the points of \mathbb{F}_q^m as $\mathbf{P}_1, \dots, \mathbf{P}_n$, where $n = q^m$, and consider the evaluation map

$$\begin{aligned} \text{ev}_m : R_m &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(\mathbf{P}_1), \dots, f(\mathbf{P}_n)). \end{aligned}$$

Definition 1. 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

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

Observe that the choice of the order of the points \mathbf{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 γ be a primitive element of \mathbb{F}_q . For $m = 1$ we consider $P_1 = 0$ and $P_i = \gamma^{i-1}$ for $i = 2, \dots, q$. Inductively, if $\{\mathbf{P}_1, \dots, \mathbf{P}_n\}$ is the set of points chosen for $n = q^m$, then for $m + 1$ we choose $\{\mathbf{P}'_1, \dots, \mathbf{P}'_N\}$, where $N = q^{m+1}$, as follows.

$$\begin{aligned} \mathbf{P}'_i &= (\mathbf{P}_i, 0) && \text{for } 1 \leq i \leq n. \\ \mathbf{P}'_{nj+i} &= (\mathbf{P}_i, \gamma^j) && \text{for } 1 \leq i \leq n, 1 \leq j \leq q-1. \end{aligned}$$

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 4. *There exist $\lambda_{i,j} \in \mathbb{F}_q$ for $1 \leq i < j \leq q$ such that*

$$G_q(r, m+1) = \begin{pmatrix} G_q(r, m) & \lambda_{1,2}G_q(r, m) & \dots & \lambda_{1,q}G_q(r, m) \\ 0 & \ddots & & \vdots \\ \vdots & & G_q(r-q+2, m) & \lambda_{q-1,q}G_q(r-q+2, m) \\ 0 & & 0 & G_q(r-q+1, m) \end{pmatrix}.$$

Remark 1. Observe that, in the case $m = 1$, the Reed-Muller code $\mathcal{RM}_q(r, 1)$ is simply the extended Reed-Solomon code of length q and dimension $r + 1$. It is well-known that in this case $wt(\mathcal{RM}_q(r, 1)) = \{q - r, q - r + 1, \dots, q\}$ (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 $\mathcal{RM}_q(r, m)$. The following result can be found in [4], and explains more about the structure of this family of codes.

Proposition 5. *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 $(1 + z + \dots + z^{q-1})^m$.
- (3) $d(r, m) = (q - S)q^{m-1-Q}$, where $r = Q(q - 1) + S$ with $0 \leq S \leq q - 2$.
- (4) $\mathcal{RM}_q(r, m)^\perp = \mathcal{RM}_q(m(q - 1) - r - 1, m)$, and therefore $G_q(r, m)$ is a parity check matrix for the code $\mathcal{RM}_q(m(q - 1) - r - 1, m)$.

Corollary 1. *Let r, m be integers such that $m \geq 1$ and $0 \leq r \leq m(q - 1)$. Let $\mathbf{u}_1, \dots, \mathbf{u}_q \in \mathcal{RM}_q((m - 1)(q - 1) - r - 1, m - 1)$. Then $(\mathbf{u}_1 \mid \dots \mid \mathbf{u}_q) \in \mathcal{RM}_q(m(q - 1) - r - 1, m)$.*

Proof. Let $\mathbf{u}_1, \dots, \mathbf{u}_q \in \mathcal{RM}_q((m - 1)(q - 1) - r - 1, m - 1)$. By Proposition 5 we know that $\mathcal{RM}_q((m - 1)(q - 1) - r - 1, m - 1)^\perp = \mathcal{RM}_q(r, m - 1)$, and therefore, $G_q(r, m - 1)\mathbf{u}_i^T = 0$ for $i = 1, \dots, q$. Moreover, for every $s \leq r$ we have $\mathcal{RM}_q(r, m - 1) \supseteq \mathcal{RM}_q(s, m - 1)$. This implies, by part (4) of Proposition 5, that $\mathcal{RM}_q((m - 1)(q - 1) - r - 1, m - 1) \subseteq \mathcal{RM}_q((m - 1)(q - 1) - s - 1, m - 1)$. Hence, we also have that $G_q(s, m - 1)\mathbf{u}_i^T = 0$. Using the characterization given in Proposition 4, we get that $G_q(r, m)(\mathbf{u}_1 \mid \dots \mid \mathbf{u}_q)^T = 0$ and this completes the proof. \square

As a direct consequence of Corollary 1, we get the following result.

Corollary 2. *Let r, m be integers such that $m \geq 1$ and $0 \leq r \leq m(q-1)$. Then*

$$wt(\mathcal{RM}_q(m(q-1) - r - 1, m)) \supseteq \bigoplus_{i=1}^q wt(\mathcal{RM}_q((m-1)(q-1) - r - 1, m-1)).$$

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

Theorem 15. *For every positive integer m and every integer r such that $0 \leq r \leq \frac{q-3}{2}$, it holds that*

$$wt(\mathcal{RM}_q(m(q-1) - r - 1, m)) = \{0, r+2, r+3, \dots, q^m\}.$$

Proof. We proceed by induction on m . For $m = 1$ we get that $\mathcal{RM}_q(q - r - 2, 1)$ is the Reed-Solomon code of length q and dimension $q - r - 1$. Therefore, $wt(\mathcal{RM}_q(q - r - 2, 1)) = \{r+2, r+3, \dots, q\}$ by [9, Theorem 6].

Suppose now it is true for $m-1$ and we want to prove the statement for m . Let $n = q^{m-1}$ and $N = q^m = qn$. We already know by part (3) of Proposition 5, that the minimum distance is equal to $r+2$. Moreover, by Corollary 2 and inductive hypothesis, we have that

$$wt(\mathcal{RM}_q(m(q-1) - r - 1, m)) \supseteq \bigoplus_{i=1}^q \{0, r+2, \dots, n\}.$$

Let $x \in \{0, r+2, \dots, qn\}$, we need to prove that we can write $x = x_0 + x_1 + \dots + x_{q-1}$ with $x_i \in \{0, r+2, \dots, n\}$. 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: If $b \in \{0, r+2, \dots, n-1\}$, then we choose $x_0 = b$, $x_1 = \dots = x_a = n$ and $x_{a+1} = \dots = x_{q-1} = 0$.

Case 2: If $b \in \{1, \dots, r+1\}$, then, necessarily $a \geq 1$. By hypothesis we have $n \geq q \geq 2r+3$. Therefore, $n - r - 2 + b \in \{0, r+2, \dots, n\}$ and we choose $x_0 = r+2$, $x_1 = n - r - 2 + b$, $x_2 = \dots = x_a = n$ and $x_{a+1} = \dots = x_{q-1} = 0$. This concludes the proof. \square

8.1 Binary Reed-Muller codes

Here we provide an additional result not covered by Theorem 15 for binary Reed-Muller codes.

Theorem 16. *Let m be a positive integer, then we have*

- (1) *If $m \geq 3$, then $wt(\mathcal{RM}_2(m-2, m)) = \{0, 2, 4, \dots, 2^m\} \setminus \{2, 2^m - 2\}$.*
- (2) *If $m \geq 6$, then $wt(\mathcal{RM}_2(m-3, m)) \supseteq \{0, 2, 4, \dots, 2^m\} \setminus \{2, 4, 6, 10, 2^m - 2, 2^m - 4, 2^m - 6, 2^m - 10\}$.*

Proof. (1) We prove it by induction on m . In the case $m = 3$, a Magma [5] computation shows that $wt(\mathcal{RM}_2(1, 3)) = \{0, 2, 4, 6, 8\} \setminus \{2, 6\}$, $wt(\mathcal{RM}_2(2, 4)) = \{0, 2, 4, 6, 8, 10, 12, 14, 16\} \setminus \{2, 14\}$ and $wt(\mathcal{RM}_2(3, 5)) = \{0, 2, 4, 6, \dots, 32\} \setminus \{2, 30\}$. Now, suppose that the claim is true for $m \geq 3$, by Corollary 2, we have $wt(\mathcal{RM}_2(m-1, m+1)) \supseteq A$, where $A = \{i + j|i, j \in wt(\mathcal{RM}_2(m-2, m))\}$. It is easy to check that $A = \{0, 2, 4, \dots, 2^{m+1}\} \setminus \{2, 2^{m+1} - 2\}$. We know, by minimum distance arguments in Proposition 5, that the integer 2 is not in $wt(\mathcal{RM}_2(m-1, m+1))$. Moreover, since the all ones vector is a codeword, also $2^m - 2$ can not be a weight. This completes the proof.

- (2) We also prove it by induction on m . In the case $m = 6$, a Magma [5] computation shows that $wt(\mathcal{RM}_2(3, 6)) = \{0, 2, 4, 6, 8, \dots, 64\} \setminus \{2, 4, 6, 10, 54, 58, 60, 62\}$. Now, suppose that the claim is true for $m \geq 6$, then $B = \{i + j|i, j \in wt(\mathcal{RM}_2(m-3, m))\}$. It is also easy to check that $B = \{0, 2, 4, \dots, 2^{m+1}\} \setminus \{2, 4, 6, 10, 2^m - 2, 2^m - 4, 2^m - 6, 2^m - 10\}$. We know, by minimum distance arguments in Proposition 5, that the integers 2, 4 and 6 are not in $wt(\mathcal{RM}_2(m-1, m+1))$. However, we don't know whether 10 belongs to $wt(\mathcal{RM}_2(m-1, m+1))$. Thus from Corollary 2, we have $wt(\mathcal{RM}_2(m-1, m+1)) \supseteq B$.

This completes the proof. □

8.2 Ternary Reed-Muller codes

In this subsection we give an additional result not covered by Theorem 15 for ternary Reed-Muller codes.

Theorem 17. *Let m be a positive integer, then we have*

- (1) *If $m \geq 1$, then $wt(\mathcal{RM}_3(2m-2, m)) = \{0, 3, 4, 5, \dots, 3^m\}$.*
- (2) *If $m \geq 3$, then $wt(\mathcal{RM}_3(2m-3, m)) \supseteq \{0, 6, 8, 9, \dots, 3^m\}$.*

Proof. (1) We prove it by induction on m . The cases $m = 1, 2, 3$ can be checked in Magma [5] to be $wt(\mathcal{RM}_3(0, 1)) = \{0, 3\}$, $wt(\mathcal{RM}_3(2, 2)) = \{0, 3, 4, 5, 6, 7, 8, 9\}$ and $wt(\mathcal{RM}_3(4, 3)) = \{0, 3, 4, \dots, 27\}$. Now, suppose that the claim is true for $m \geq 4$, from Corollary 2, we have $wt(\mathcal{RM}_3(2m, m+1)) \supseteq A = \{i+j+l | i, j, l \in wt(\mathcal{RM}_3(2m-2, m))\}$. It is easy to check $A = \{i+j+l | i, j, l \in wt(\mathcal{RM}_3(2m-2, m))\} = \{0, 3, 4, 5, \dots, 3^{m+1}\}$. According to part (3) of Proposition 5, $d(2m-2, m) = 3$. This completes the proof.

(2) We also prove it by induction on m . The cases $m = 3, 4$ can be checked in Magma [5] to be $wt(\mathcal{RM}_3(3, 3)) = \{0, 6, 8, 9, \dots, 27\}$, $wt(\mathcal{RM}_3(5, 4)) = \{0, 6, 8, 9, \dots, 81\}$. Now, suppose that the claim is true for $m \geq 5$, then $B = \{i+j+l | i, j, l \in wt(\mathcal{RM}_3(2m-3, m))\} = \{0, 6, 8, 9, \dots, 3^{m+1}\}$. However, we don't know whether 7 belongs to $wt(\mathcal{RM}_3(2m-1, m+1))$. Thus, from Corollary 2, we have $wt(\mathcal{RM}_3(2m-1, m+1)) \supseteq \{0, 6, 8, 9, \dots, 3^{m+1}\}$. According to part (3) of Proposition 5, $d(2m-3, m) = 6$. This completes the proof. \square

8.3 Reed-Muller codes over the field \mathbb{F}_5

Here we provide an additional result not covered by Theorem 15 for Reed-Muller codes over the field \mathbb{F}_5 .

Theorem 18. *Let m be a positive integer, then we have*

$$wt(\mathcal{RM}_5(4m-3, m)) = \{0, 4, 5, 6, \dots, 5^m\} \text{ for } m \geq 1.$$

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 $wt(\mathcal{RM}_5(1, 1)) = \{0, 4, 5\}$ and $wt(\mathcal{RM}_5(5, 2)) = \{0, 4, 5, 6, \dots, 25\}$. Now, suppose that the claim is true for $m \geq 3$, then $B = \{i+j+l+s+t | i, j, l, s, t \in wt(\mathcal{RM}_5(4m-3, m))\} = \{0, 4, 5, 6, \dots, 5^{m+1}\}$. From Corollary 2, we have $wt(\mathcal{RM}_5(4m+1, m+1)) \supseteq \{0, 4, 5, 6, \dots, 5^{m+1}\}$. Finally, from part (3) of Proposition 5, we have $d(4m-3, m) = 4$. This completes the proof. \square

9 Appendix II: q -ary Hamming codes

9.1 Block Codes and Hamming Codes

Let q be a prime power, and let \mathbb{F}_q denote the finite field with q elements. We denote by $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ the multiplicative group of \mathbb{F}_q . It is well-known that \mathbb{F}_q^* is a

cyclic group, i.e. there always exists a generator γ such that

$$\mathbb{F}_q = \{\gamma^i \mid 1 \leq i \leq q-1\} \cup \{0\}.$$

For $\mathbf{u} = (u_1, \dots, u_n), \mathbf{v} = (v_1, \dots, v_n) \in \mathbb{F}_q^n$ we denote by $\langle \mathbf{u}, \mathbf{v} \rangle$ the standard inner product between \mathbf{u} and \mathbf{v} , i.e.

$$\langle \mathbf{u}, \mathbf{v} \rangle := \sum_{i=1}^n u_i v_i.$$

Moreover, given two vectors $\mathbf{u} \in \mathbb{F}_q^{n_1}, \mathbf{v} \in \mathbb{F}_q^{n_2}$ we will use the notation $(\mathbf{u} \mid \mathbf{v})$ to indicate the vector in $\mathbb{F}_q^{n_1+n_2}$ obtained by concatenating u and v , i.e.

$$(\mathbf{u} \mid \mathbf{v}) = (u_1, \dots, u_{n_1}, v_1, \dots, v_{n_2}),$$

where $\mathbf{u} = (u_1, \dots, u_{n_1})$ and $\mathbf{v} = (v_1, \dots, v_{n_2})$. With this notation, given $\mathbf{u}_i, \mathbf{v}_i \in \mathbb{F}_q^{n_i}$ for $i = 1, \dots, m$, it trivially holds that

$$w_H(\mathbf{u}_1 \mid \dots \mid \mathbf{u}_m) = \sum_{i=1}^m w_H(\mathbf{u}_i), \quad \text{and} \quad (1)$$

$$\langle (\mathbf{u}_1 \mid \dots \mid \mathbf{u}_m), (\mathbf{v}_1 \mid \dots \mid \mathbf{v}_m) \rangle = \sum_{i=1}^m \langle \mathbf{u}_i, \mathbf{v}_i \rangle. \quad (2)$$

Suppose r is a positive integer. On the set $\mathbb{F}_q^r \setminus \{\mathbf{0}\}$ we can consider the following equivalence relation:

$$\mathbf{u} \sim \mathbf{v} \iff \exists \lambda \in \mathbb{F}_q^* \text{ such that } \mathbf{u} = \lambda \mathbf{v}.$$

The projective geometry of order q and dimension r is defined as

$$PG(r-1, q) = (\mathbb{F}_q^r \setminus \{\mathbf{0}\}) / \sim.$$

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 \mathbb{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 \mathbb{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

$$\theta_q(r-1) := \frac{q^r - 1}{q - 1} = |P_r(q)|.$$

Definition 2. Let q be a prime power, and let $r \geq 2$ be a positive integer. We define the q -ary **Hamming code** $\mathcal{H}_r(q)$ as the $[\theta_q(r-1), \theta_q(r-1) - r]$ linear code over \mathbb{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 2 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 by Definition 2.

Lemma 3. Let H_{r-1} be the parity check matrix for the Hamming code $\mathcal{H}_{r-1}(q)$ as described in Definition 2. Then we can obtain a parity check matrix for $\mathcal{H}_r(q)$ as

$$H_r = \left(\begin{array}{ccc|ccc|ccc|c|ccc|c} 0 & \cdots & 0 & 1 & \cdots & 1 & 1 & \cdots & 1 & \cdots & 1 & \cdots & 1 & 1 \\ \hline & & H_{r-1} & & & \gamma H_{r-1} & & & \gamma^2 H_{r-1} & \cdots & & & \gamma^{q-1} H_{r-1} & \\ \hline & & & & & & & & & & & & & 0 \\ & & & & & & & & & & & & & \vdots \\ & & & & & & & & & & & & & 0 \end{array} \right),$$

where γ is a primitive element of \mathbb{F}_q and $H_1 = (1)$.

9.2 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 $\mathcal{H}_r(q)$ 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 $\mathcal{H}_r(q)$ is greater than zero or not. In the particular case that $r = 2$ we know more about the structure of $\mathcal{H}_2(q)$.

Lemma 4. For $r = 2$ the Hamming code $\mathcal{H}_2(q)$ is an MDS code of parameters $[q+1, q-1, 3]$. In particular, $wt(\mathcal{H}_2(3)) = \{0, 3\}$ and $wt(\mathcal{H}_2(q)) = \{0, 3, 4, \dots, q+1\}$ for every $q > 3$.

Proof. The parameters of $\mathcal{H}_2(q)$ 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]. \square

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 5. *Let $q > 2$ be a prime power, and let $r \geq 1$ be a positive integer. Then*

$$\sum_{\mathbf{v} \in \mathbb{F}_q^r} \mathbf{v} = \mathbf{0} \text{ and } \sum_{\mathbf{u} \in P_r(q)} \mathbf{u} = \mathbf{e}_r,$$

where $\mathbf{e}_r = (0, 0, \dots, 0, 1)^T$.

Proof. For the first equality, we prove it by induction. Let $r = 1$, $q \geq 3$, and γ be a primitive element of \mathbb{F}_q . Then

$$\sum_{v \in \mathbb{F}_q} v = \sum_{i=0}^{q-2} \gamma^i = \frac{\gamma^{q-1} - 1}{\gamma - 1},$$

since $\gamma \neq 1$. Moreover, $\gamma^{q-1} = 1$ and then we get the result.

For $r > 1$, we can write $\mathbb{F}_q^r = \bigcup_{\alpha \in \mathbb{F}_q} \mathcal{T}_\alpha$, where

$$\mathcal{T}_\alpha := \{(\alpha, \mathbf{v}') \mid \mathbf{v}' \in \mathbb{F}_q^{r-1}\},$$

and the union is clearly disjoint. Therefore,

$$\sum_{\mathbf{v} \in \mathbb{F}_q^r} \mathbf{v} = \sum_{\alpha \in \mathbb{F}_q} \sum_{\mathbf{v}' \in \mathbb{F}_q^{r-1}} (\alpha, \mathbf{v}') = \sum_{\alpha \in \mathbb{F}_q} (q^{r-1}\alpha, \mathbf{0}) = \mathbf{0},$$

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

$$\underbrace{\alpha + \dots + \alpha}_{q^{r-1} \text{ times}},$$

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

$$P_r(q) = \{(0, \mathbf{u}') \mid \mathbf{u}' \in P_{r-1}(q)\} \cup \{(1, \mathbf{v}') \mid \mathbf{v}' \in \mathbb{F}_q^{r-1}\}.$$

Therefore,

$$\sum_{\mathbf{u} \in P_r(q)} \mathbf{u} = \sum_{\mathbf{u}' \in P_{r-1}(q)} (0, \mathbf{u}') + \sum_{\mathbf{v}' \in \mathbb{F}_q^{r-1}} (1, \mathbf{v}') = \mathbf{e}_r + \mathbf{0} = \mathbf{e}_r,$$

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

Proposition 6. *For every $q > 2$, and every integer $r \geq 2$, there exists a codeword $\mathbf{c} \in \mathcal{H}_r(q)$ of full weight, i.e., such that $w_H(\mathbf{c}) = \theta_q(r-1)$, except for the case $(q, r) = (3, 2)$.*

Proof. For $r = 2$ the statement trivially follows from Lemma 4. Suppose now $r \geq 3$, and let γ be a primitive element of \mathbb{F}_q . Consider the set

$$\mathcal{D} = \{\mathbf{w}_0, \mathbf{w}_1, \dots, \mathbf{w}_{q-1}\},$$

where $\mathbf{w}_0 = \mathbf{e}_1 = (1, 0, \dots, 0)$ and $\mathbf{w}_i = (1, \gamma^i, \gamma^i, \dots, \gamma^i)$ for $i = 1, 2, \dots, q-2$ and $\mathbf{w}_{q-1} = (1, 1, \dots, 1, 0)$. It is easy to see that with this choice of \mathcal{D} , we have

$$\sum_{i=0}^{q-1} \mathbf{w}_i + \mathbf{e}_r = \mathbf{0}.$$

Let $\alpha \in \mathbb{F}_q$. We consider the sum

$$\begin{aligned} \sum_{\substack{\mathbf{u} \in P_r(q) \\ \mathbf{u} \notin \mathcal{D} \cup \{\mathbf{e}_r\}}} \mathbf{u} + (1 + \alpha) \sum_{i=0}^{q-1} \mathbf{w}_i + \alpha \mathbf{e}_r &= \sum_{\substack{\mathbf{u} \in P_r(q) \\ \mathbf{u} \neq \mathbf{e}_r}} \mathbf{u} + \alpha \sum_{i=0}^{q-1} \mathbf{w}_i + \alpha \mathbf{e}_r \\ &= \alpha \left(\sum_{i=0}^{q-1} \mathbf{w}_i + \mathbf{e}_r \right) = \mathbf{0}. \end{aligned}$$

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. \square

Proposition 6 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 6. *If $\mathbf{u}_i \in \mathcal{H}_{r-1}(q)$ for $i = 0, 1, \dots, q-1$, then*

$$(\mathbf{u}_0 \mid \mathbf{u}_1 \mid \dots \mid \mathbf{u}_{q-1} \mid \alpha) \in \mathcal{H}_r(q),$$

where

$$\alpha = - \sum_{i=1}^{q-1} \langle \mathbf{u}_i, \mathbf{e} \rangle,$$

and \mathbf{e} denotes the vector with all entries equal to 1.

Proof. According to Lemma 3, it is straightforward to see that the vector $(\mathbf{u}_0 \mid \mathbf{u}_1 \mid \dots \mid \mathbf{u}_{q-1} \mid \alpha)$ satisfies the check equations given by the rows $i = 2, \dots, r$ of the parity check matrix. Moreover, the condition on α ensures that it also satisfies the first check equation. \square

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

$$(\mathbb{F}_q^n)^q = \underbrace{\mathbb{F}_q^n \times \dots \times \mathbb{F}_q^n}_{q \text{ times}}.$$

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

$$\begin{aligned} \varphi : ((\mathbb{F}_q^*)^q \rtimes S_q) \times (\mathbb{F}_q^n)^q &\longrightarrow (\mathbb{F}_q^n)^q \\ ((\boldsymbol{\beta}, \sigma), (\mathbf{u}_0 \mid \dots \mid \mathbf{u}_{q-1})) &\longmapsto (\beta_0 \mathbf{u}_{\sigma(0)} \mid \dots \mid \beta_{q-1} \mathbf{u}_{\sigma(q-1)}). \end{aligned}$$

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

$$(\boldsymbol{\beta}, \sigma) \cdot \mathbf{u} := \varphi((\boldsymbol{\beta}, \sigma), \mathbf{u}).$$

Proposition 7. *Let $q > 2$ be a prime power and let $(\mathbf{u}_0 \mid \dots \mid \mathbf{u}_{q-1}) \in (\mathcal{H}_{r-1}(q))^q$. Then there exists $(\boldsymbol{\beta}, \sigma) \in (\mathbb{F}_q^*)^q \rtimes S_q$ such that*

$$(\beta_0 \mathbf{u}_{\sigma(0)} \mid \dots \mid \beta_{q-1} \mathbf{u}_{\sigma(q-1)} \mid 0) \in \mathcal{H}_r(q).$$

Proof. Let $\mathbf{u}_0, \mathbf{u}_1, \dots, \mathbf{u}_{q-1} \in \mathcal{H}_{r-1}(q)$. By Lemma 6 we have that $(\mathbf{u}_0 \mid \mathbf{u}_1 \mid \dots \mid \mathbf{u}_{q-1} \mid \alpha) \in \mathcal{H}_r(q)$, where $\alpha = - \sum_{i=1}^{q-1} \langle \mathbf{u}_i, \mathbf{e} \rangle$. If $\alpha = 0$ we are done. Therefore, suppose $\alpha \neq 0$, and consider the set

$$\mathcal{T} := \{i \in \{1, \dots, q-1\} \mid \langle \mathbf{u}_i, \mathbf{e} \rangle \neq 0\}.$$

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

Case 1: $|\mathcal{T}| \geq 2$. Let $r, s \in \mathcal{T}$ be two distinct elements. Consider a generic vector $\boldsymbol{\beta} = (\beta_0, \dots, \beta_{q-1})$ whose entries are $\beta_i = 1$ for $i \neq r, s$, and consider the element $(\boldsymbol{\beta}, id) \cdot (\mathbf{u}_0 \mid \dots \mid \mathbf{u}_{q-1})$. By Lemma 6, the vector

$$((\boldsymbol{\beta}, id) \cdot (\mathbf{u}_0 \mid \dots \mid \mathbf{u}_{q-1}) \mid \tilde{\alpha}),$$

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

$$\begin{aligned} \tilde{\alpha} &= - \sum_{i=1}^{q-1} \langle \beta_i \mathbf{u}_i, \mathbf{e} \rangle \\ &= - \sum_{i=1}^{q-1} \langle \mathbf{u}_i, \mathbf{e} \rangle + (1 - \beta_r) \langle \mathbf{u}_r, \mathbf{e} \rangle + (1 - \beta_s) \langle \mathbf{u}_s, \mathbf{e} \rangle \\ &= \alpha + (1 - \beta_r) \langle \mathbf{u}_r, \mathbf{e} \rangle + (1 - \beta_s) \langle \mathbf{u}_s, \mathbf{e} \rangle. \end{aligned}$$

Imposing the condition $\tilde{\alpha} = 0$ we get

$$(1 - \beta_s) = - \frac{\alpha + (1 - \beta_r) \langle \mathbf{u}_r, \mathbf{e} \rangle}{\langle \mathbf{u}_s, \mathbf{e} \rangle}. \quad (3)$$

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

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

- (i) If $\langle \mathbf{u}_0, \mathbf{e} \rangle = 0$, then consider the transposition $\sigma = (0, r) \in \mathcal{S}_q$. Consider the element

$$(\mathbf{e}, \sigma) \cdot (\mathbf{u}_0 \mid \dots \mid \mathbf{u}_{q-1}) = (\mathbf{v}_0 \mid \dots \mid \mathbf{v}_{q-1}).$$

By Lemma 6, we have

$$(\mathbf{v}_0 \mid \dots \mid \mathbf{v}_{q-1} \mid \alpha) \in \mathcal{H}_r(q),$$

where

$$\alpha = - \sum_{i=1}^{q-1} \langle \mathbf{v}_i, \mathbf{e} \rangle = - \sum_{\substack{i=0 \\ i \neq r}}^{q-1} \langle \mathbf{u}_i, \mathbf{e} \rangle = - \sum_{\substack{i=0 \\ i \neq r}}^{q-1} 0 = 0,$$

and we are done.

- (ii) Suppose now that $\langle \mathbf{u}_0, \mathbf{e} \rangle \neq 0$. Then there exists $s \in \{1, 2, \dots, q-1\}$ such that $s \notin \mathcal{T}$. We now consider the transposition $\sigma = (0, s)$ and the corresponding vector

$$(\mathbf{e}, \sigma) \cdot (\mathbf{u}_0 \mid \dots \mid \mathbf{u}_{q-1}).$$

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

This completes the proof. \square

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

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

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

We are now ready to prove the main result.

Theorem 19. *Let $q > 2$ be a prime power, and let $r \geq 2$ be an integer. Then*

$$wt(\mathcal{H}_r(q)) = \{0, 3, \dots, N\},$$

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

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

Case 1: $(q, 2)$ with $q > 3$. It follows from Lemma 4.

Case 2: $(q, r) = (3, 3)$. 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

$$wt(\mathcal{H}_{r-1}(q)) = \{0, 3, \dots, n\}$$

where $n = \theta_q(r-2)$, and observe that $N = qn + 1$. By Corollary 3, we know that

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

Moreover, since $(q, r-1) \neq (3, 2)$, we have that $n \geq 5$. By Proposition 6 we already know that $N \in wt(\mathcal{H}_r(q))$. Therefore it is enough to show that

$$\bigoplus_{i=0}^{q-1} \{0, 3, \dots, n\} = \{0, 3, \dots, qn\}.$$

It is clear that $N - 1 = qn$ belongs to our set, since $n \in wt(\mathcal{H}_{r-1}(q))$. Let $x \in \{0, 3, \dots, qn - 1\}$, we need to prove that we can write $x = x_0 + x_1 + \dots + x_{q-1}$ with $x_i \in \{0, 3, \dots, n\}$. 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: $b \in \{0, 3, \dots, n - 1\}$. We choose $x_0 = b$, $x_1 = \dots = x_a = n$ and $x_{a+1} = \dots = x_{q-1} = 0$.

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

References

- [1] T. L. Alderson, A note on full weight spectrum codes, arXiv preprint arXiv:1807.11798, 2018.
- [2] T. L. Alderson and A. Neri, Maximum weight spectrum codes, *Advances in Mathematics of Communications*, to appear, 2018.
- [3] 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.
- [4] T. Blackmore and G. Norton, Matrix product codes over \mathbb{F}_q , *Applicable Algebra in Engineering, Communication and Computing*, **12**(6): 477–500, 2001.
- [5] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.*, **24** (1997), 235–265, 1997, <http://magma.maths.usyd.edu.au/magma/>
- [6] G.D. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering codes*, volume **54**, North-Holland, Amsterdam, 1997.
- [7] G. D. Cohen and L. Tolhuizen. Maximum weight spectrum codes with reduced length. arXiv preprint arXiv:1806.05427, 2018.
- [8] C. Ding and J. Yang, Hamming weights of irreducible cyclic codes, *Discrete Mathematics*, **313**(4): 434–446, 2013.

- [9] F. Ezerman, M. Grassl, and P. Solé, The weights in MDS codes, *IEEE Transactions on Information Theory*, **IT-57**(1): 392–396, 2011.
- [10] W. C. Huffman and V. Pless, *Fundamentals of error correcting codes*, Cambridge University Press, 2003.
- [11] N. Hurt, Exponential Sums and Coding Theory: A Review, *Acta Applicandae Mathematicae*, **46**(1): 49–91, 1997.
- [12] D. S. Kim, Weight distributions of Hamming codes, *arXiv preprint arXiv:0710.1467*, 2007.
- [13] 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.
- [14] G. Lachaud and J. Wolfmann, The weights of the orthogonals of the extended quadratic binary Goppa codes, *IEEE Transactions on Information Theory*, **36**(3): 686–692, 1990.
- [15] R. Lidl and H. Niederreiter, *Finite fields*, volume **20**, Cambridge University Press, 1997.
- [16] F.J. MacWilliams and N.J.A. Sloane, *The theory of error correcting codes*, North Holland, Amsterdam, 1977.
- [17] R.J. McEliece, Irreducible Cyclic Codes and Gauss Sums, in *Combinatorics*, 185–202, 1975.
- [18] A. Meneghetti. On linear codes and distinct weights. *arXiv preprint arXiv:1804.04373*, 2018.
- [19] R. Schoof, Families of curves and weight distributions of codes, *Bulletin of the American Mathematical Society*, **32**(2): 171–183, 1995.
- [20] M. Shi, Z. Zhang, and P. Solé, Two-weight codes and second order recurrences, *Chinese Journal of Electronics*, to appear, 2018.
- [21] M. Shi, H. Zhu, P. Solé, and G.D. Cohen, How many weights can a linear code have?, *Designs Codes and Cryptography*, 1–9. [Doi.org/10.1007/s10623-018-0488-z](https://doi.org/10.1007/s10623-018-0488-z), 2018.

- [22] N.J. Sloane, et al.: The on-line encyclopedia of integer sequences, 2003, <http://www.oeis.org>.
- [23] A. Tietäväinen. On the nonexistence of perfect codes over finite fields. SIAM Journal on Applied Mathematics, **24**(1): 88-96, 1973.
- [24] G. Van der Geer and M. van der Vlugt, Artin-Schreier curves and codes, Journal of Algebra, **139**(1): 256–272, 1991.