# The largest number of weights in cyclic codes *

Minjia Shi[1,2], and Patrick Solé[3]

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

[2]Key Laboratory of Intelligent Computing & Signal Processing,

Ministry of Education, Anhui University No. 3 Feixi Road,

Hefei Anhui Province 230039, P. R. China;

[3]CNRS/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 cyclic codes (called here strongly cyclic), all codewords of which have period the length. Asymptotics are derived on the function $\Gamma(k, q)$, 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.

**Keywords:** cyclic codes, irreducible cyclic codes, Hamming codes

## 1 Introduction

In a companion paper, we have studied the largest number of nonzero weights a linear code of given length and dimension can have [12]. In the present paper we

*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) and Key projects of support program for outstanding young talents in Colleges and Universities (gxyqZD2016008).

address the same type of questions for cyclic codes. Thus, we study the function $\Gamma(k, q)$, 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 [7] in the language of linear recurrences. In the case of cyclic codes the nonzero codewords of which have period the length (called strongly cyclic codes in the sequel) we obtain smaller upper bounds as for the class of all cyclic codes. This suggests to study $\Gamma^0(k, q)$, 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. Showing that the Hamming code is optimal for the number of nonzero weights requires so-called deficient numbers (integers that are larger than the sum of their proper divisors) and the computations of the Appendix. Exact enumeration of cyclic codes can require some deep techniques of Number Theory [4]. 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 [1], 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 contains some numerical values for the main combinatorial function of interest. Section 7 concludes the paper and mentions some open problems. An appendix derives a difficult property of the Hamming code.

# 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 w.r.t. the standard inner product.

The **(Hamming) weight** of $x \in \mathbb{F}_q^N$ is the number of indices $i$ where $x_i \neq 0$. 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** [8, Th 11, Chap. 1] on its parameters

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

A code meeting that bound is called MDS. See [8, 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 are the periods of the linear recurrence of characteristic polynomial the reciprocal polynomial of $h(x)$ [8, p. 195]. Thus any codeword $c$ can be continued into an infinite periodic sequence $\widehat{c}$ which is periodic of period $n$. The **period** of a codeword $c$ is understood to be the smallest integer $T$ such $\widehat{c}_{i+T} = \widehat{c}_i$ 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 $h(x) \in \mathbb{F}_q[x]$ 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

Define $\Gamma(k, q)$ as the largest number of nonzero weights of a cyclic code of dimension $k$ over $\mathbb{F}_q$. Define $\Gamma(n, k, q)$ as the largest number of nonzero weights of a cyclic code of 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.

# 3 Upper bounds

## 3.1 Cycle structure

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

$$s \leq \sum_{t|n} \frac{B_t}{t}.$$

*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. □

**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 [9, 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. Thus, it is a two-weight code satisfying $\frac{B_4}{4} = \frac{B_{20}}{20} = 1$. The bound of Lemma 1 is met with equality.

This simple counting lemma has two important applications. First, we improve the upper bound on $L(k,q)$ of [12, Prop. 2] by a factor $\frac{n}{q-1}$ for some large class of cyclic codes.

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

$$s \leq \frac{q^k - 1}{n}.$$

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

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

Next, in the general case several nonzero $B_t$s we can prove the following.

**Theorem 2.** *If $C$ is an $[n,k]_q$ cyclic code with $s$ nonzero weights, not containing the all-one codeword, then*

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

*Proof.* Note that, by hypothesis, $B_1 = 0$. Squaring the bound in the lemma, and applying Cauchy-Schwarz inequality we obtain

$$s^2 \leq \sum_{1<t|n} B_t^2 \sum_{1<t|n} \frac{1}{t^2}.$$

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. $\square$

**Remark:** Trivially, $s \leq q^k - 1$ for all linear codes, so we avoid $B_1 > 0$ and the summand on $t$ to be $\geq 1$.

## 3.2 Character sums

The following result can be derived by using the character sums techniques of [7, Chapt. 8].

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

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

*Thus*

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

*Proof.* By [7, Cor. 8.83] we know that the weights $w$ of $C$ lie in the range

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

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 [7, 5, 2] 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. □

**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 [5].

A slightly sharper bound can be derived using the results in [2].

**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 $s \leq N_k = GCD(N, \frac{q^k-1}{q-1})$.*

*Proof.* Follows by [2, (9)] which involves Gaussian periods of order $N_k$. □

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 5 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 $q^k = 1 + nN$. □

**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*

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

*where $h = LCM(n, q - 1)$.*

*Proof.* The proof follows the lines of Theorem 6 with [7, Th. 8.84, (8.37)] replacing [7, Cor. 8.83]. We get rid of $k$ by writing $q^k = 1 + nN$. □

# 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 zero polynomial, has $k$ nonzero weights. This shows that $\Gamma(k,k,q) \geq k$. The result follows by $\Gamma(k,k,q) \leq \Gamma(k,q)$. □

The following result is immediate by [11]. 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 **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 $m$ [8, 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 $2^m - 5$ ([8, Chap. 6, Ex. (E2)], see Appendix for a proof), and the fact that $S_m$ is a one-weight code [8, Chap.1 §9 , Ex]. □

The next two theorems rely on some deep algebraic geometric enumeration of cyclic codes [6, 10, 13]. See [4] for a survey.

**Theorem 9.** *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 [6, 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 [6, 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. □

A ternary analogue is as follows.

**Theorem 10.** *For all integers $m \geq 2$ we have* $\Gamma(3^m - 1, 2m, 3) \geq \lceil 4 \times 3^{\frac{m-2}{2}} \rceil$.

*Proof.* The dual of the ternary Melas code is cyclic of parameters $[3^m - 1, 3m]$. It is proved in [13] 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. □

It is remarkable that the last two theorems imply lower bounds on $\Gamma(k, 2)$ and $\Gamma(k, 3)$ 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 $k$ [1]. Trivially $t[n, k] \leq T[n, k, 2]$. The Delsarte bound [8], stated for the dual of a linear code $C$, is $\rho(C^\perp) \leq s(C)$ [8, 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 $\Gamma(n, k, q) \geq T[n, n-k, q]$. □

**Remark:** This bound is tight when $n = q - 1$. By the Singleton bound $\Gamma(q-1, k, q) \leq k$. It is well-known that MDS codes of dimension $k$ have exactly $k$ weights [3]. Thus, considering cyclic MDS codes shows that $\Gamma(q-1, k, q) = k$. Further, $T[q-1, k, q] \leq q-1-k$ by the so-called redundancy bound [1, Cor. 8.1.4], which is known to be met by the Reed-Solomon codes by a nesting argument [1, Th. 10.5.7]. Thus $T[q-1, k, q] = q-1-k$ for all $q \geq k+1$. This shows that $\Gamma(q-1, k, q) = T[q-1, q-1-k, q]$.

## 5 Asymptotics

Recall that the $q$-ary **entropy function** $H_q(\cdot)$ is defined for $0 < y < \frac{q-1}{q}$ by

$$H_q(y) = y \log_q(q-1) - y \log_q(y) - (1-y) \log_q(1-y).$$

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

$$\gamma_q(R) = \limsup_{n \to \infty} \Gamma(n, \lfloor Rn \rfloor, q).$$

**Theorem 11.** *For all rates $R \in (0, 1)$ we have*

$$H_q^{-1}(R) \leq \gamma_q(R) \leq R.$$

*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 upper bound comes from the immediate inequalities $\Gamma(n, k, q) \leq \Gamma(k, q) \leq q^k - 1$. The lower bound follows by combining the sphere-covering bound [1, 8] with Proposition 3. □

Similarly for strongly cyclic codes we define

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

We obtain a different upper bound.

**Theorem 12.** *For all rates $R \in (0,1)$ we have*

$$H_q^{-1}(R) \leq \gamma_q^0(R) \leq \frac{R}{2}.$$

*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 upper bound comes from the immediate inequalities $\Gamma^0(n, k, q) \leq \Gamma^0(k, q)$ and Theorem 3. The lower bound follows by combining the sphere-covering bound [1, 8] with Delsarte bound on the dual code. □

# 6 Numerics

We conjecture, but cannot prove, based on the figures of Table 1, that the local maxima of $n \mapsto \Gamma(n, k, 2)$, for fixed $k$ 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 $\Gamma(k, q)$

| $\Gamma(k,q) \geq$ | $q$ | $k$ | $n$ | $h(x)$ |
|---|---|---|---|---|
| 7 | 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 $\mathbb{F}_q[x]$

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

(i) $x^2 + x + 1$ when $T = 3$ and $s_h = 1$ (Simplex code)

(ii) $x^2 + 1$ when $T = 2$ and $s_h = 2$ (Universe code)

(iii) $x^2 GCD(x^T + 1, x^2) = 1$ for any $T \geq 1$ yielding $T = 2$ and $s_h = 0$ (Null code)

(iv) $x^2 + x$ when $GCD(x^T + 1, x^2 + x) = x + 1$ for any $T \geq 1$ yielding $s_h = 1$ (Repetition code)

We conclude that $\Gamma(2, 2) = 2$.

# 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 linear in $k$, when the upper bounds are exponential. Even showing that the Hamming code is optimal for $\Gamma(n, k)$ required to assume $n = 2^m - 1$ with $m$ prime and the heavy claculations of the Appendix. Extending this result to BCH codes either double-error correcting or triple-error correcting seems possible at the price of calculations similar to, but more complicated than, those in the Appendix.

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

**Theorem 13.** *The binary Hamming code $\mathcal{H}_m$ of length $n = 2^m - 1$ has exactly $s = n - 4$ nonzero weights.*

*Proof.* Let $(A_0, A_1, \cdots, A_n)$ denote the weight distribution of $\mathcal{H}_m$. Since the minimum distance is 3 we have $A_1 = A_2 = 0$ and, because $\mathcal{H}_m$ contains the all-ones vector, it follows that $A_{n-1} = A_{n-2} = 0$. Thus $s \leq n - 4$. To prove $s \geq n - 4$, we need an explicit formula for the weight distribution. According to the MacWilliams identity between the binary Hamming code and its dual code (the simplex code of parameters $[2^m - 1, m, 2^{m-1}]_2$), we can get the following generating function

$$2^m \sum_{j=0}^{n} A_j x^{n-j} y^j = (x + y)^n + n(x^2 - y^2)^{2^{m-1}-1}(x - y),$$

and, from there, the following equations for $A_j$, with $3 \leq j \leq n - 4$.

$$2^m A_{2i} = \binom{n}{2i} + (-1)^i \binom{2^{m-1} - 1}{i} n, \text{ where } 4 \leq 2i \leq n - 3, \quad (1)$$

$$2^m A_{2i+1} = \binom{n}{2i + 1} + (-1)^{i+1} \binom{2^{m-1} - 1}{i} n, \text{ where } 3 \leq 2i + 1 \leq n - 4 \quad (2)$$

Note that $A_{2i} > 0$ if and only if

$$\frac{\binom{n}{2i}}{\binom{2^{m-1}-1}{i} n} > 1 \text{ with } n = 2^m - 1 \text{ and } i = 2t + 1$$

if and only if

$$\frac{(2^m - 3)!!}{(4t + 2)!!(2^m - 1 - (4t + 2))!!} > 1,$$

where the **double factorial** $N!!$ of an integer $N$ is

$$N!! = \prod_{j=0}^{\lfloor N/2 \rfloor} (N - 2j).$$

The last inequality is equivalent to

$$\frac{(2^m - 4t - 1) \times (2^m - 4t + 1) \times \cdots \times (2^m - 3)}{4 \times 6 \times \cdots \times (4t + 2)} > 2.$$

The left handside is the product of $2t + 1$ ratios and showing the first one $> 2$ is enough, since then the remaining $2t$ will be $\geq 1$. Now $\frac{2^m - 4t - 1}{4} > 2$ is true when $m \geq 4$, (assuming $2i \leq \frac{n-1}{2}$ by symmetry), and can be checked numerically for $m = 2, 3$. We can prove $A_{2i+1} > 0$ similarly. $\square$

The formulas (1) and (2) for the weight distribution of $\mathcal{H}_m$ can be found in [10, p.176]. The proof given here solves Problem 1 of [8, Chap. 6] on the external distance of Hadamard codes.

# References


[1] G.D. Cohen, I. Honkala, S. Litsyn, A. Lobstein, *Covering codes*, North-Holland, Amsterdam (1997).

[2] C. Ding, J. Yang, Hamming weights of irreducible cyclic codes, Discr. Math., **313** (4), (2013), 434–446.

[3] F. Ezerman, M. Grassl, P. Solé, The weights in MDS codes, IEEE Trans. on Information Theory, **IT-57**, (2011), 392–396.

[4] N. Hurt, Exponential Sums and Coding Theory: A Review, Acta Applicandae Mathematicae **46**, (1997), 49–91.

[5] R.J. MacEliece, Irreducible Cyclic Codes and Gauss Sums, Combinatorica, **16**, (1975), 185–202.

[6] G. Lachaud,J. Wolfmann, The weights of the orthogonals of the extended quadratic binary Goppa codes, IEEE Trans. on Information Theory **36**, (1990) 686–692.

[7] R. Lidl, H. Niederreiter, *Finite fields*, Encycl. of Math and Appl., vol. 20, Cambridge (1997).

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

[9] Online Encyclopedia of Integer Sequences `www.oeis.org`

[10] R. Schoof, Families of curves and weight distributions of codes, Bull. of the AMS, **32**, (2), (1995) 171–183.

[11] M. Shi, Z. Zhang, P. Solé, Two-weight codes and second order recurrences, Chinese J. of Electronics, to appear (2018).

[12] M. Shi, H. Zhu, P. Solé, G.D.Cohen, How many weights can a linear code have ?, Des. Codes and Crypt. Doi.org/10.1007/s10623-018-0488-z(2018).

[13] G. Van der Geer, M. van der Vlugt, Artin?Schreier curves and codes, J. Algebra **139** (1991), 256–272.