NUMBER OF MINIMAL CYCLIC CODES WITH GIVEN LENGTH AND DIMENSION

F. E. BROCHERO MARTÍNEZ

Abstract. In this article, we count the quantity of minimal cyclic codes of length n and dimension k over a finite field $\mathbb{F}_q$, in the case when the prime factors of n satisfy a special condition. This problem is equivalent to count the quantity of irreducible factors of $x^n - 1 \in \mathbb{F}_q[x]$ of degree k.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements. A linear $[n, k; q]$ code $\mathcal{C}$ is a linear subspace of $\mathbb{F}_q^n$ of dimension k. $\mathcal{C}$ is called a *cyclic code* if $\mathcal{C}$ is invariant by a shift permutation, i.e., if $(a_0, a_1, \dots, a_{n-1}) \in \mathcal{C}$ then $(a_{n-1}, a_0, a_1, \dots, a_{n-2}) \in \mathcal{C}$. It is known that every cyclic code can be seen as an ideal of the ring $\frac{\mathbb{F}_q[x]}{(x^n-1)}$. In addition, since $\frac{\mathbb{F}_q[x]}{(x^n-1)}$ is a principal ring, every ideal is generated by a polynomial $g(x)$ such that g is a divisor of $x^n - 1$. Thus, the polynomial g is called *generator* of the code and the polynomial $h(x) = \frac{x^n-1}{g(x)}$ is called the *parity-check* polynomial of $\mathcal{C}$. Observe that $\{g, xg, \dots x^{k-1}g\}$, where $k = \deg(h)$, is a basis of the linear space $(g) \in \frac{\mathbb{F}_q[x]}{(x^n-1)}$, then the dimension of the code is the degree of the parity-check polynomial. A cyclic code C is called *minimal cyclic code* if h is an irreducible polynomial in $\mathbb{F}_q[x]$. Thus, the number of irreducible factors of $x^n - 1 \in \mathbb{F}_q[x]$ corresponds to the number of minimal cyclic codes of length n in $\mathbb{F}_q$. Specifically, there exists a bijection between the minimal cyclic codes of dimension k and length n over $\mathbb{F}_q$, that we denote by $[n, k; q]$, and the irreducible factors of $x^n - 1 \in \mathbb{F}_q[x]$ of degree k.

Irreducible cyclic codes are very interesting by its applications in communication, storage systems like compact disc players, DVDs, disk drives, two-dimensional bar codes, etc. (see [5, Section 5.8 and 5.9]). The advantage of the cyclic codes, with respect to other linear codes, is that they have efficient encoding and decoding algorithms (see [5, Section 3.7]). For these facts, cyclic codes have been studied for the last decades and many progress has been found (see [8]).

A natural question is how many minimal cyclic codes of length n and dimension k over $\mathbb{F}_q$ does there exist? In other words, the quations is: given n, k and $\mathbb{F}_q$, find an explicit formula for the number of minimal cyclic $[n, k; q]$-codes. This question is in general unknown, and how to construct all of them too.

In this article, we determine the number of minimal cyclic $[n, k; q]$-codes assuming that the order of q modulo each prime factor of n satisfies some special relation.

Date: September 16, 2021.
2010 *Mathematics Subject Classification.* 20C05 (primary) and 16S34(secondary).
Key words and phrases. minimal cyclic codes, cyclotomic classes.

2. Preliminaries

Throughout this article, $\mathbb{F}_q$ denotes a finite field of order q, where q is a power of a prime. For each $a \in \mathbb{F}_l^*$, $\mathrm{ord}(a)$ denotes the order of a in a multiplicative group $\mathbb{F}_l^*$, i.e. $\mathrm{ord}(a)$ is the least positive integer k such that $a^k = 1$. In the same way, we denote by $\mathrm{ord}_n b$, the order of b in a multiplicative group $\mathbb{Z}_n^*$ and $\nu_p(m)$ is the maximal power of p that divides m. In addition, for each irreducible polynomial $P(x) \in \mathbb{F}_q[x]$, $\mathrm{ord}(P(x))$ denotes the order of some root of $P(x)$ in some extension of $\mathbb{F}_q$.

It is a classical result (see, for instance, [4]) to determine the number of factors of $x^n - 1$ and its degree, when the order is given.

Theorem 2.1. *Let n be a positive integer such that $\gcd(n, q) = 1$, then each factor of $x^n - 1 \in \mathbb{F}_q[x]$ has order m, where m is a divisor of n. In addition, for each $m|n$, there exist $\frac{\varphi(m)}{\mathrm{ord}_m q}$ irreducible factors and each of these factors has degree $\mathrm{ord}_m q$.*

As a consequence of this theorem (see proposition 2.1 in [1]), the number of factors of degree k of $x^n - 1$ is $\sum\limits_{\substack{m|n \\ \mathrm{ord}_m q = k}} \frac{\varphi(m)}{k}$ and then the total number of irreducible factors is $\sum\limits_{m|n} \frac{\varphi(m)}{\mathrm{ord}_m q}$. So, the number of irreducible factors of degree k is zero if any m divisor of n satisfies $\mathrm{ord}_m q = k$. Clearly, this formula is not really explicit, because it depends on the calculation of the orders $\mathrm{ord}_m q$ for every divisor of n.

An equivalent approach is to use the technique of q-cyclotomic classes (see [11] page 157 or [9] Chapter 8). In fact, the q-cyclotomic class of j modulo n is the set $\{j, jq, jq^2, \dots, jq^{k-1}\}$ whose elements are distinct modulo n and $jq^k \equiv j \pmod{n}$. This q-cyclotomic class determines one irreducible factor of $x^n - 1$ of degree k.

If we denote by $\mathcal{C}_k$ the set of numbers j, with $1 \le j \le n$ that have q-cyclotomic class with k elements, then

$$\begin{aligned}
\mathcal{C}_k &= \{j \le n;\ k \text{ is the minimum positive integer such that } jq^k \equiv j \pmod{n}\} \\
&= \left\{j \le n;\ k \text{ is the minimum positive integer such that } q^k \equiv 1 \pmod{\frac{n}{\gcd(n,j)}}\right\} \\
&= \left\{j \le n;\ k = \mathrm{ord}_{\frac{n}{\gcd(n,j)}} q\right\}.
\end{aligned}$$

Since each q-cyclotomic class determines a minimal cyclic code, then the number of minimal cyclic $[n, k; q]$-codes is $\dfrac{|\mathcal{C}_k|}{k}$.

Using this technique, in [10] and [6] are shown explicit formulas for the total of minimal cyclic codes for some special cases.

Theorem 2.2 ([10])**.** *Suppose that $n = p_1^{\alpha_1} p_2$ satisfies that $d = \gcd(\varphi(p_1^{\alpha_1}), \varphi(p_2))$, $p_1 \nmid (p_2 - 1)$ and q is a primitive root $\bmod p_1^{\alpha_1}$ as well as $\bmod p_2$. Then the number of minimal cyclic codes of length n over $\mathbb{F}_q$ is $\alpha_1(d + 1) + 2$.*

Theorem 2.3 ([6, Theorem 2.6])**.** *Suppose that $n = p_1^{\alpha_1} \cdots p_l^{\alpha_l}$ satisfies that $\mathrm{ord}_{p_j^{\alpha_j}} q = \varphi(p_j^{\alpha_j})$ for every j, and $\gcd(p_j - 1, p_i - 1) = 2$ for every $i \neq j$. Then the number of minimal cyclic codes of length n over $\mathbb{F}_q$ is*

$$\frac{(2\alpha_1 + 1)(2\alpha_2 + 1) \cdots (2\alpha_k + 1) + 1}{2}.$$

Besides, some explicit formulas for the number of $[n,k;q]$-codes for some particular values of n and q are known

Theorem 2.4 ([3, Corollary 3.3 and 3.6])**.** *Suppose that n and q are numbers such that every prime factor of n divides $q-1$. Then*

(1) *If $8 \nmid n$ or $q \not\equiv 3 \pmod 4$ then the number of minimal cyclic $[n,d;q]$-codes is*
$$\begin{cases} \frac{\varphi(d)}{d}\cdot \gcd(n,q-1) & \text{if } d \mid \frac{n}{\gcd(n,q-1)} \\ 0 & \text{otherwise} \end{cases}$$
The total number of minimal cyclic codes of length n is
$$\gcd(n,q-1)\cdot \prod_{\substack{p\mid m \\ p \text{ prime}}} \left(1+\nu_p(m)\frac{p-1}{p}\right),$$
where φ is the Euler Totient function.

(2) *If $8|n$ and $q \equiv 3 \pmod 4$ then the number of minimal cyclic $[n,d;q]$-codes is*
$$\begin{cases} \frac{\varphi(d)}{d}\cdot \gcd(n,q-1) & \text{if } d \text{ is odd and } d \mid \frac{n}{\gcd(n,q^2-1)} \\ \frac{\varphi(k)}{2k}\cdot (2^r-1)\gcd(n,q-1) & \text{if } d=2k,\ k \text{ is odd and } k \mid \frac{n}{\gcd(n,q^2-1)} \\ \frac{\varphi(k)}{k}\cdot 2^{r-1}\gcd(n,q-1) & \text{if } d=2k,\ k \text{ is even and } k \mid \frac{n}{\gcd(n,q^2-1)} \\ 0 & \text{otherwise} \end{cases}$$
where $r=\min\{\nu_2(n/2),\nu_2(q+1)\}$. The total number of minimal cyclic codes of length n is
$$\gcd(n,q-1)\cdot\left(\frac{1}{2}+2^{r-2}(2+\nu_2(m))\right)\cdot \prod_{\substack{p\mid m \\ p \text{ odd prime}}} \left(1+\nu_p(m)\frac{p-1}{p}\right).$$

3. Codes with power of a prime length

In this section, we are going to suppose that n is a power of a prime. In order to determine the number of irreducible codes of length n, we need the following lemma, that it is pretty well-known in the Mathematical Olympiads folklore and it is attributed to E. Lucas and R. D. Carmichael (see [7]).

Lemma 3.1 (Lifting-the-exponent Lemma)**.** *Let p be a prime. For all $a,b\in\mathbb{Z}$ and $n\in\mathbb{N}$, such that $p\nmid ab$ and $p|(a-b)$, the following proprieties are satisfied*

(i) *If $p\geq 3$, then $\nu_p(a^n-b^n)=\nu_p(a-b)+\nu_p(n)$.*
(ii) *If $p=2$ and n is odd then $\nu_2(a^n-b^n)=\nu_2(a-b)$.*
(iii) *If $p=2$ and n is even then $\nu_2(a^n-b^n)=\nu_2(a^2-b^2)+\nu_2(n)-1$.*

As a consequence of the previous lemma we obtain

Corollary 3.2. *Let p be a prime and $\rho=\operatorname{ord}_p q$.*

(1) *If $q\not\equiv 3 \pmod 4$ or $p\neq 2$ then*
$$\operatorname{ord}_{p^\theta} q = \begin{cases} 1 & \text{if } \theta=0 \\ \rho & \text{if } \theta\leq\beta \\ \rho p^{\theta-\beta} & \text{if } \theta>\beta. \end{cases}$$
where $\beta=\nu_p(q^\rho-1)$.

(2) If $q \equiv 3 \pmod 4$ *and* $p = 2$, *then*

$$\operatorname{ord}_{2^\theta} q = \begin{cases} 1 & \text{if } \theta = 0 \text{ or } 1. \\ 2 & \text{if } \theta \le \beta \\ 2^{\theta-\beta+1} & \text{if } \theta > \beta. \end{cases}$$

where $\beta = \nu_2(q^2 - 1)$.

Proof: (1) Clearly, $\operatorname{ord}_{p^\theta} q = \rho$ if $1 \le \theta \le \beta$. In the case $\theta > \beta$, since $\operatorname{ord}_p q$ divides $\operatorname{ord}_{p^\theta}$ then, by Lemma 3.1 item *(i)*, we have

$$\theta = \nu_p(q^k - 1) = \nu_p(q^\rho - 1) + \nu_p\left(\frac{k}{\rho}\right) = \beta + \nu_p\left(\frac{k}{\rho}\right).$$

In addition to the minimality of k, we obtain that $\frac{k}{\rho} = p^{\theta-\beta}$.

The proof of part *(2)* is similar by using items *(ii)* and *(iii)* of Lemma 3.1 . □

Theorem 3.3. *Suppose that* $n = p^\alpha$, *where* p *is a prime and* ρ *and* β *as in the previous lemma. Then*

(1) If $p \ne 2$ *or* $q \not\equiv 3 \pmod 4$ *then the number of minimal cyclic* $[n, d; q]$*-codes is*

$$\begin{cases} \gcd(n, q-1) & \text{if } d = 1 \\ \frac{p^{\min\{\alpha,\beta\}}-1}{\rho} & \text{if } d = \rho \ne 1 \\ \frac{p^\beta - p^{\beta-1}}{\rho} & \text{if } d = \rho \cdot p^j \text{ and } 1 \le j \le \alpha - \beta \\ 0 & \text{otherwise} \end{cases}$$

(2) If $n = 2^\alpha$ *and* $q \equiv 3 \pmod 4$ *then the number of minimal cyclic* $[n, d; q]$*-codes is*

$$\begin{cases} 2 & \text{if } d = 1 \\ 1 & \text{if } d = 2 \text{ and } \alpha = 2 \\ 3 & \text{if } d = 2 \text{ and } \alpha \ge 3 \\ 2 & \text{if } d = 2^j \text{ and } 2 \le j \le \alpha - 2 \\ 0 & \text{otherwise} \end{cases}$$

Proof: (1) In the case when $k = 1$, the number of $[n, 1 : q]$-codes is equivalent to the number of roots of the polynomial $x^n - 1$ in $\mathbb{F}_q^*$. Since every element of $\mathbb{F}_q^*$ is root of $x^{q-1} - 1$, and $\gcd(x^n - 1, x^{q-1} - 1) = x^{\gcd(n,q-1)} - 1$, we conclude that the number of minimal $[n, 1; q]$-codes is $\gcd(n, q - 1)$.

Now, suppose that $d \ne 1$. Since ρ divides $\operatorname{ord}_{p^s} q$ for every $s \ge 1$ and $\frac{\operatorname{ord}_{p^s} q}{\rho}$ is a power of p, it follows that if $\frac{k}{\rho}$ is not a power of p, then there not exist $[n, k; q]$-codes.

In the case when $d = \rho$, by Corollary 3.2, we know that $\operatorname{ord}_{p^s} q = \rho$ if and only if $1 \le s \le \beta$ and then the number of $[n, \rho; q]$-codes is

$$\sum_{s=1}^{\min\{\alpha,\beta\}} \frac{\varphi(p^s)}{\rho} = \sum_{s=1}^{\min\{\alpha,\beta\}} \frac{p^s - p^{s-1}}{\rho} = \frac{p^{\min\{\alpha,\beta\}} - 1}{\rho}$$

Finally, in the case $d = \rho p^j$, since $\operatorname{ord}_{p^s} q = \rho p^j$ if and only if $s = j + \beta$, and $s \le \alpha$, we conclude that $j \le \alpha - \beta$ and the number of $[n, \rho p^j; q]$-codes is

$$\frac{\varphi(p^s}{\operatorname{ord}_{p^s} q} = \frac{\varphi(p^{j+\beta})}{\rho p^j} = \frac{p^\beta - p^{\beta-1}}{\rho}.$$

So, this identity concludes the proof of (1).

We note that the proof of (2) is essencially the same of (1) and we omit. □

Remark 3.4. *In [2], we show one way to construct the primitive idempotents of the ring* $\frac{\mathbb{F}_q[x]}{(x^n-1)}$ *where* $n = p^\alpha$ *and it is known that each primitive idempotent is a generator of one minimal cyclic code of length* n*.*

4. The number of cyclic codes given an special condition

Throughout this section, $n = p_1^{\alpha_1} \cdots p_l^{\alpha_l}$ is the factorization in primes of n, where n is odd or $q \not\equiv 3 \pmod 4$. Moreover, we put $\rho_i = \operatorname{ord}_{p_i} q$ and $\beta_i = \nu_{p_i}(q^{\rho_i} - 1)$.

Definition 4.1. *The pair* (n, q) *satisfies the* homogeneous order condition *(H.O.C.) if* $\gcd(\rho_i, n) = 1$*, for every* i*, and there exists* $\rho \in \mathbb{N}$ *such that* $\rho = \gcd(\rho_i, \rho_j)$*, for every* $i \neq j$*.*

Observe that every pair (n, q) considered in Theorems 2.2, 2.3, 2.4 and 3.3 satisfies H.O.C.. Furthermore, if (n, q) satisfies H.O.C then

$$R := \operatorname{lcm}(\rho_1, \rho_2, \ldots, \rho_k) = \frac{\rho_1 \rho_2 \cdots \rho_k}{\rho^{k-1}}$$

and, by Lemma 3.1, we have

$$\nu_{p_i}(q^R - 1) = \nu_{p_i}(q^{\rho_i} - 1) + \sum_{\substack{1 \le j \le k \\ j \neq i}} \nu_{p_i}\left(\frac{\rho_j}{\rho}\right) = \beta_i.$$

Lemma 4.2. *Let* (n, q) *be a pair which satisfies H.O.C. and* $d = p_1^{\theta_1} \cdots p_l^{\theta_l}$ *be a divisor of* n *other than* 1*. Then*

$$\operatorname{ord}_d q = \frac{\rho d}{\gcd(d, q^R - 1)} \prod_{\substack{1 \le i \le l \\ \theta_i \neq 0}} \frac{\rho_i}{\rho}.$$

Proof: Observe that if $\theta_i \neq 0$ then

$$\operatorname{ord}_{p_i^{\theta_i}} q = \rho_i \frac{p_i^{\theta_i}}{\gcd(p_i^{\theta_i}, q^{\rho_i} - 1)} = \rho_i \frac{p_i^{\theta_i}}{\gcd(p_i^{\theta_i}, q^R - 1)}.$$

Thus, in the case when $d = p_{i_1}^{\theta_{i_1}} \cdots p_{i_s}^{\theta_{i_s}}$, where $\theta_{i_j} \neq 0$, we have

$$\begin{aligned} \operatorname{ord}_d q &= \operatorname{lcm}(\operatorname{ord}_{p_{i_1}^{\theta_{i_1}}} q, \ldots \operatorname{ord}_{p_{i_s}^{\theta_{i_s}}} q) \\ &= \rho \cdot \operatorname{lcm}\left(\frac{\operatorname{ord}_{p_{i_1}^{\theta_{i_1}}} q}{\rho}, \ldots, \frac{\operatorname{ord}_{p_{i_s}^{\theta_{i_s}}} q}{\rho}\right) \\ &= \rho \prod_{j=1}^{s} \frac{\rho_{i_j}}{\rho} \frac{p_{i_j}^{\theta_{i_j}}}{\gcd(p_{i_j}^{\theta_{i_j}}, q^R - 1)} \\ &= \rho \frac{d}{\gcd(d, q^R - 1)} \prod_{p_i \mid d} \frac{\rho_i}{\rho}. \end{aligned}$$

□

Corollary 4.3. *Let* (n, q) *be a pair which satisfies H.O.C.. If there exist minimal cyclic* $[n, k; q]$*-codes then*

(1) $\gcd(k,\rho_i)=1$ *or* ρ_i*, for every* i*.*
(2) If p_i *divides* $\gcd(n,k)$*, then* ρ_i *divides* k*.*
(3) $\gcd(n,k)$ *divides* $\dfrac{\cdot n}{\gcd(n,q^R-1)}$.

Theorem 4.4. *Let* $\mathbb{F}_q$ *be a finite field and* n *be a positive integer such that the pair* (n,q) *satisfies H.O.C. and suppose that* n *is odd or* $q\not\equiv 3 \pmod 4$*. Let* k *be a positive integer satisfying the conditions of the corollary 4.3. Then the number of minimal cyclic* $[n,k;q]$*-codes is*

$$\begin{cases}\gcd(n,q-1) & \text{if } k=1\\ \gcd(n,q^R-1)\frac{\varphi(\gcd(k,n))}{k} & \text{if } k\neq 1.\end{cases}$$

The total number of minimal cyclic codes of length n *is*

$$\frac{\rho-1+\prod_{i=1}^{l}\left(\frac{\rho}{\rho_i}\left(\varphi(p_i^{\beta_i})\max\{\alpha_i-\beta_i,0\}+p^{\min\{\alpha_i,\beta_i\}}-1\right)+1\right)}{\rho}$$

Proof: We are going to suppose that $k\neq 1$, because the case $k=1$ has been proved in Theorem 3.3. Let $\mathcal{I}$ be the set of indices i such that $\frac{\rho_i}{\rho}$ divides k, $\mathcal{J}=\{i\in\mathcal{I}|p_i \text{ divides } k\}$ and $\mathcal{I}_0=\mathcal{I}\setminus\mathcal{J}$.

Let d be a divisor of n such that $\operatorname{ord}_d q=k$. By Lemma 4.2, it follows that $d|n_{\mathcal{I}}$ and $k=tR_{\mathcal{I}}$ where

$$t=\gcd(k,n)=\frac{d}{\gcd(d,q^R-1)}\qquad\text{and}\qquad R_{\mathcal{I}}=\rho\prod_{i\in\mathcal{I}}\frac{\rho_i}{\rho}.$$

Since $t=\prod_{i\in\mathcal{I}}p_i^{\theta_i}$, then

$$\theta_i=\nu_{p_i}(d)-\min\{\nu_{p_i}(d),\beta_i\}=\max\{0,\nu_{p_i}(d)-\beta_i\}\qquad\text{for all } i\in\mathcal{I}.$$

Observe that $\theta_i\le\max\{0,\alpha_i-\beta_i\}$ for all $i\in\mathcal{I}$ and then t divides $\dfrac{n_{\mathcal{I}}}{\gcd(n_{\mathcal{I}},q^R-1)}$. Furthermore, if $\theta_i\neq 0$, then $\nu_{p_i}(d)=\theta_i+\beta_i\le\alpha_i$, and in the case $\theta_i=0$, we have $\nu_{p_i}(d)\le\alpha_i\le\beta_i$. If follows that $d=d_0d_1$, where

$$d_1=\prod_{i\in J}p_i^{\theta_i+\beta_j}=\gcd(k,n)\cdot\gcd(n_1,q^R-1),\quad\text{with}\quad n_1=\prod_{i\in\mathcal{J}}p_i^{\alpha_i}$$

and d_0 is a divisor of $n_0=\prod_{i\in\mathcal{I}_0}p_i^{\alpha_i}$. Therefore, the number of $[n,k;q]$-codes is

$$\begin{aligned}\frac{1}{k}\sum_{\substack{d|n\\ \operatorname{ord}_d n=k}}\varphi(d)&=\frac{1}{k}\sum_{d_0|n_0}\varphi(d_0d_1)=\frac{n_0\cdot\varphi(d_1)}{k}\\ &=\frac{n_0\cdot\gcd(k,n)\cdot\gcd(n_1,q^R-1)}{k}\prod_{i\in\mathcal{J}}\left(1-\frac{1}{p_i}\right).\end{aligned}$$

By using the fact that $n_0=\gcd(n_0,q^R-1)$ and $\prod_{i\in\mathcal{J}}\left(1-\frac{1}{p_i}\right)=\frac{\varphi(\gcd(k,n))}{\gcd(k,n)}$, we conclude that the number of irreducible cyclic $[n,k;q]$-codes is

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

On the other hand, by Lemma 4.2, the function $f(d) = \begin{cases} 1 & \text{if } d = 1 \\ \frac{\rho\cdot\varphi(d)}{\mathrm{ord}_d\, q} & \text{if } d \neq 1 \end{cases}$ is multiplicative for every d divisor of n. So, the total number of minimal cyclic codes of length n is

$$\sum_{d|n} \frac{\varphi(d)}{\mathrm{ord}_d\, q} = 1 - \frac{1}{\rho} + \frac{1}{\rho}\sum_{d|n} f(d).$$

In order to calculate the sum, observe that

$$\begin{aligned}
\sum_{d|p_i^{\alpha_i}} f(d) &= 1 + \sum_{s=1}^{\alpha_i} \frac{\rho\cdot(p_i^s - p_i^{s-1})}{\rho_i \frac{p_i^s}{\gcd(p_i^s, q^R-1)}} \\
&= 1 + \frac{\rho}{\rho_i}\left(1 - \frac{1}{p_i}\right)\sum_{s=1}^{\alpha_i} \gcd(p_i^s, q^R - 1) \\
&= 1 + \frac{\rho}{\rho_i}\left(1 - \frac{1}{p_i}\right)\left[\sum_{s=1}^{\min\{\alpha_i,\beta_i\}} p_i^s + \max\{0, \alpha_i - \beta_i\} p_i^{\beta_i}\right] \\
&= 1 + \frac{\rho}{\rho_i}\left({p_i}^{\min\{\alpha_i,\beta_i\}} - 1 + \left(1 - \frac{1}{p_i}\right)\max\{0, \alpha_i - \beta_i\} p_i^{\beta_i}\right) \\
&= 1 + \frac{\rho}{\rho_i}\left({p_i}^{\min\{\alpha_i,\beta_i\}} - 1 + \max\{0, \alpha_i - \beta_i\}\varphi(p_i^{\beta_i})\right).
\end{aligned}$$

Then, by using the fact that $\sum_{d|n} f(d)$ is a multiplicative function, we conclude the proof. □

References

[1] Agou, S., *Factorisation sur un Corps Fini $\mathbb{F}_{p^n}$ des Polynômes Composés $f(x^s)$ lorque $f(x)$ est un Polynôme Irréductible de $\mathbb{F}_{p^n}[x]$*, L'Enseignement mathém. **22** (1976) 305-312

[2] Brochero Martínez, F.E., Giraldo Vergara, C.R., *Explicit Idempotents of Finite Group Algebra* Finite Fields Appl. **28** (2014) 123-131

[3] Brochero Martínez, F.E., Giraldo Vergara, C.R., Batista de Oliveira, L., *Explicit Factorization of $x^n - 1 \in \mathbb{F}_q[x]$*, submitted for publication in Designs, Codes and Cryptography.

[4] Butler, M.C.R., *The Irreducible factors of $f(x^m)$ over a finite field*, J. London Math. Soc, 2nd Ser. **30** (1955) 480-482.

[5] Farrell, P. G., Castieira Moreira, J., *Essentials of Error-Control Coding* John Wiley & Sons Ltd (2006).

[6] Kumar P, Arora, S.K. *λ-Mapping and Primitive Idempotents in semi simple ring $\mathcal{R}_m$.* Comm. Algebra **41** (2013) 3679-3694

[7] R. D. Carmichael, *On the Numerical Factors of Certain Arithmetic Forms*, Amer. Math. Monthly, **16**,10 (1909), 153-159.

[8] Huffman, W.C. , Pless, V. , *Fundamentals of Error-Correcting Codes*, Cambridge University Press, (2003).

[9] MacWilliams, F.J., Sloane,N.J.A. , *Theory of Error-Correcting Codes*, North-Holland (1977).

[10] Sahni, A., Sehgal, P. *Minimal cyclic codes of length $p^n q$*, Finite Fields Appl. **18** (2012), no. 5, 1017-1036.

[11] Xambo-Descamps, S. *Block Error-Correcting Codes* Universitext, Springer (2003)

Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte, MG, 30123-970, Brazil,

E-mail address: fbrocher@mat.ufmg.br