The Weight Distribution of a Family of Reducible Cyclic Codes

WAIFI 2012

Bochum

Gerardo Vega

UNAM

Itinerary

1. *Notations, definitions and main assumption*
2. *The evaluation of a specific exponential sum*
3. *Three preliminary results*
4. *The weight distribution of a family of reducible cyclic codes*
5. *An example of this family of reducible cyclic codes*
6. *An explicit formula for the number of cyclic codes in a family when length and dimension are given*
7. *Some examples of such formula*

Definitions, notations and main assumption

- By using p, q and k, we denote three positive integers such that p is a prime number and q is a positive power of p.

Definitions, notations and main assumption

- By using p, q and k, we denote three positive integers such that p is a prime number and q is a positive power of p.
- From now on, we set $\Delta = (q^k - 1)/(q - 1)$.

Definitions, notations and main assumption

- By using p, q and k, we denote three positive integers such that p is a prime number and q is a positive power of p.
- From now on, we set $\Delta = (q^k - 1)/(q - 1)$.
- By using γ we will denote a fixed primitive element of $\mathbb{F}_{q^k}$.

Definitions, notations and main assumption

- By using p, q and k, we denote three positive integers such that p is a prime number and q is a positive power of p.
- From now on, we set $\Delta = (q^k - 1)/(q - 1)$.
- By using γ we will denote a fixed primitive element of $\mathbb{F}_{q^k}$.
- For any integer a, the polynomial $h_a(x) \in \mathbb{F}_q[x]$ will denote the minimal polynomial of γ^{-a}.

Definitions, notations and main assumption

- By using p, q and k, we denote three positive integers such that p is a prime number and q is a positive power of p.
- From now on, we set $\Delta = (q^k - 1)/(q - 1)$.
- By using γ we will denote a fixed primitive element of $\mathbb{F}_{q^k}$.
- For any integer a, the polynomial $h_a(x) \in \mathbb{F}_q[x]$ will denote the minimal polynomial of γ^{-a}.
- Finally, for any two integers i and j, we will denote by $\mathcal{D}_i^{(j)}$ the i-th cyclotomic class of order $\gcd(q^k - 1, j)$ in $\mathbb{F}_{q^k}$.

Definitions, notations and main assumption

- By using p, q and k, we denote three positive integers such that p is a prime number and q is a positive power of p.
- From now on, we set $\Delta = (q^k - 1)/(q - 1)$.
- By using γ we will denote a fixed primitive element of $\mathbb{F}_{q^k}$.
- For any integer a, the polynomial $h_a(x) \in \mathbb{F}_q[x]$ will denote the minimal polynomial of γ^{-a}.
- Finally, for any two integers i and j, we will denote by $\mathcal{D}_i^{(j)}$ the i-th cyclotomic class of order $\gcd(q^k - 1, j)$ in $\mathbb{F}_{q^k}$. That is, $\mathcal{D}_i^{(j)}$ will be the coset

$$\mathcal{D}_i^{(j)} = \gamma^i \langle \gamma^j \rangle \ ,$$

where, as usual, $\langle \gamma^j \rangle$ denotes the subgroup of $\mathbb{F}_{q^k}^*$, which is generated by γ^j.

Some Definitions

- *The canonical additive character* χ, **of** $\mathbb{F}_{q^k}$, **is defined as**

$$\chi(y) = \exp(\frac{2\pi\sqrt{-1}\,\mathsf{Tr}(y)}{p}) \ , \qquad \text{for all } y \in \mathbb{F}_{q^k} \ ,$$

where "Tr" will denote the absolute trace mapping from $\mathbb{F}_{q^k}$ **to** $\mathbb{F}_p$**.**

Some Definitions

- *The canonical additive character* χ, **of** $\mathbb{F}_{q^k}$, **is defined as**

$$\chi(y) = \exp(\frac{2\pi\sqrt{-1}\,\mathsf{Tr}(y)}{p}) \ , \qquad \text{for all } y \in \mathbb{F}_{q^k} \ ,$$

  where "Tr" will denote the absolute trace mapping from $\mathbb{F}_{q^k}$ **to** $\mathbb{F}_p$**.**

- *An* N*-weight code* **is a code such that the cardinality of the set of its nonzero weights is** N**.**

Some Definitions

- *The canonical additive character* χ, **of** $\mathbb{F}_{q^k}$, **is defined as**

$$\chi(y) = \exp(\frac{2\pi\sqrt{-1}\,\mathsf{Tr}(y)}{p}) \ , \qquad \text{for all } y \in \mathbb{F}_{q^k} \ ,$$

  where "Tr" will denote the absolute trace mapping from $\mathbb{F}_{q^k}$ **to** $\mathbb{F}_p$**.**

- *An* N*-weight code* **is a code such that the cardinality of the set of its nonzero weights is** N**.**

- *A projective code* **is a linear code such that the minimum weight of its dual code is at least three.**

Some Definitions

- *The canonical additive character* χ, **of** $\mathbb{F}_{q^k}$, **is defined as**

$$\chi(y) = \exp(\frac{2\pi\sqrt{-1}\,\mathsf{Tr}(y)}{p}) \ , \qquad \text{for all } y \in \mathbb{F}_{q^k} \ ,$$

  where "Tr" will denote the absolute trace mapping from $\mathbb{F}_{q^k}$ **to** $\mathbb{F}_p$**.**

- *An* N*-weight code* **is a code such that the cardinality of the set of its nonzero weights is** N**.**

- *A projective code* **is a linear code such that the minimum weight of its dual code is at least three.**

- **A cyclic code is** *irreducible* **if its parity-check polynomial is irreducible (that is, if its polynomial representation is a minimal ideal).**

Some Definitions

- *The canonical additive character* χ, of $\mathbb{F}_{q^k}$, is defined as

$$\chi(y) = \exp(\frac{2\pi\sqrt{-1}\,\mathsf{Tr}(y)}{p}) \ , \qquad \text{for all } y \in \mathbb{F}_{q^k} \ ,$$

  where "Tr" will denote the absolute trace mapping from $\mathbb{F}_{q^k}$ to $\mathbb{F}_p$.

- *An N-weight code* is a code such that the cardinality of the set of its nonzero weights is N.

- *A projective code* is a linear code such that the minimum weight of its dual code is at least three.

- A cyclic code is *irreducible* if its parity-check polynomial is irreducible (that is, if its polynomial representation is a minimal ideal).

For this work, we are particularly interested in non-irreducible cyclic codes, whose parity-check polynomials are factorizable in exactly two different irreducible factors of the same degree.

Main assumption

We now establish our main assumption, which is done by saying that from now on, we are going to suppose that q is an odd integer greater than 3 such that the integer 4 divides $q+1$. In addition, we will always assume that k is an even integer.

Main assumption

We now establish our main assumption, which is done by saying that from now on, we are going to suppose that q is an odd integer greater than 3 such that the integer 4 divides $q+1$. In addition, we will always assume that k is an even integer.

Remark 1. As a consequence of our main assumption, observe that $\frac{q-1}{2}$ is an odd integer. Furthermore, observe that 4 must divide Δ (see Lemma 1).

The evaluation of a specific exponential sum

Theorem 1 (see Moisio [8]). By considering our main assumption, let i and w be two integers in such a way that w is given by

$$w = \begin{cases} 0 & \text{if } (2 \mid \frac{k}{2}) \text{ or } (2 \nmid \frac{k}{2} \text{ and } 2 \mid \frac{q+1}{4}), \\ 2 & \text{otherwise} \end{cases}.$$

The evaluation of a specific exponential sum

Theorem 1 (see Moisio [8]). By considering our main assumption, let i and w be two integers in such a way that w is given by

$$w = \begin{cases} 0 & \text{if } \ (2 \mid \frac{k}{2}) \quad \text{or} \quad (2 \nmid \frac{k}{2} \text{ and } 2 \mid \frac{q+1}{4}) \ , \\ 2 & \text{otherwise} \end{cases} .$$

Also let η_0 and η_1 be the two integers whose values are given by

$$\eta_0 = \frac{(-1)^{\frac{k}{2}-1} 3 q^{\frac{k}{2}}-1}{4} \ , \qquad \eta_1 = \frac{(-1)^{\frac{k}{2}} q^{\frac{k}{2}}-1}{4} \ .$$

The evaluation of a specific exponential sum

Theorem 1 (see Moisio [8]). By considering our main assumption, let i and w be two integers in such a way that w is given by

$$w = \begin{cases} 0 & \text{if } \ (2 \mid \frac{k}{2}) \quad \text{or} \quad (2 \nmid \frac{k}{2} \text{ and } 2 \mid \frac{q+1}{4}) \ , \\ 2 & \text{otherwise} \end{cases} .$$

Also let η_0 and η_1 be the two integers whose values are given by

$$\eta_0 = \frac{(-1)^{\frac{k}{2}-1} 3 q^{\frac{k}{2}} - 1}{4} \ , \qquad \eta_1 = \frac{(-1)^{\frac{k}{2}} q^{\frac{k}{2}} - 1}{4} \ .$$

Now, if χ is the canonical additive character of $\mathbb{F}_{q^k}$, and if $\mathcal{D}_i^{(4)}$ is the i-th cyclotomic class of order 4, then we have

$$\sum_{z \in \mathcal{D}_i^{(4)}} \chi(z) = \begin{cases} \eta_0 & \text{if } i \equiv w \pmod 4 \ , \\ \eta_1 & \text{otherwise} \end{cases} .$$

Three preliminary results

Result 1 Let q, k, Δ and γ be as before.

Three preliminary results

Result 1 Let q, k, Δ and γ be as before. Considering our main assumption, we also take λ to be a divisor of $q-1$, and define $n = \lambda\Delta$.

Three preliminary results

Result 1 Let q, k, Δ and γ be as before. Considering our main assumption, we also take λ to be a divisor of $q-1$, and define $n = \lambda\Delta$. Let a_2 be an integer such that $a_2 n \equiv 0 \pmod{q^k - 1}$.

Three preliminary results

Result 1 Let q, k, Δ and γ be as before. Considering our main assumption, we also take λ to be a divisor of $q-1$, and define $n = \lambda\Delta$. Let a_2 be an integer such that $a_2 n \equiv 0 \pmod{q^k - 1}$. If $\gcd(\frac{\Delta}{2}, a_2) = 2$, then there exist integers d and λ', such that $d = 0$ or 1, and λ' is the divisor of $q-1$, satisfying $\gcd(q-1, a_2) = \frac{q-1}{\lambda'}$

Three preliminary results

Result 1 Let q, k, Δ and γ be as before. Considering our main assumption, we also take λ to be a divisor of $q-1$, and define $n = \lambda\Delta$. Let a_2 be an integer such that $a_2 n \equiv 0 \pmod{q^k - 1}$. If $\gcd(\frac{\Delta}{2}, a_2) = 2$, then there exist integers d and λ', such that $d = 0$ or 1, and λ' is the divisor of $q-1$, satisfying $\gcd(q-1, a_2) = \frac{q-1}{\lambda'}$ (observe that $\lambda' | \lambda$).

Three preliminary results

Result 1 Let q, k, Δ and γ be as before. Considering our main assumption, we also take λ to be a divisor of $q-1$, and define $n = \lambda\Delta$. Let a_2 be an integer such that $a_2 n \equiv 0 \pmod{q^k - 1}$. If $\gcd(\frac{\Delta}{2}, a_2) = 2$, then there exist integers d and λ', such that $d = 0$ or 1, and λ' is the divisor of $q-1$, satisfying $\gcd(q-1, a_2) = \frac{q-1}{\lambda'}$ (observe that $\lambda' | \lambda$). Then, by defining now $n' = \lambda' \frac{\Delta}{2^d}$, we have

$$\{(\gamma^{a_2 m}, (-1)^m) \mid 0 \leq m < n\} = \frac{2^d \lambda}{\lambda'} * \{(\gamma^{2^d \frac{q-1}{\lambda'} m}, (-1)^m) \mid 0 \leq m < n'\}, \qquad (1)$$

where $\frac{2^d \lambda}{\lambda'} * \{(\gamma^{2^d \frac{q-1}{\lambda'} m}, (-1)^m) \mid 0 \leq m < n'\}$ is the multiset in which each element of $\{(\gamma^{2^d \frac{q-1}{\lambda'} m}, (-1)^m) \mid 0 \leq m < n'\}$ appears with multiplicity $\frac{2^d \lambda}{\lambda'}$.

Three preliminary results

Result 1 Let q, k, Δ and γ be as before. Considering our main assumption, we also take λ to be a divisor of $q-1$, and define $n = \lambda\Delta$. Let a_2 be an integer such that $a_2 n \equiv 0 \pmod{q^k - 1}$. If $\gcd(\frac{\Delta}{2}, a_2) = 2$, then there exist integers d and λ', such that $d = 0$ or 1, and λ' is the divisor of $q-1$, satisfying $\gcd(q-1, a_2) = \frac{q-1}{\lambda'}$ (observe that $\lambda' | \lambda$). Then, by defining now $n' = \lambda' \frac{\Delta}{2^d}$, we have

$$\{(\gamma^{a_2 m}, (-1)^m) \mid 0 \leq m < n\} = \frac{2^d \lambda}{\lambda'} * \{(\gamma^{2^d \frac{q-1}{\lambda'} m}, (-1)^m) \mid 0 \leq m < n'\}, \qquad (1)$$

where $\frac{2^d \lambda}{\lambda'} * \{(\gamma^{2^d \frac{q-1}{\lambda'} m}, (-1)^m) \mid 0 \leq m < n'\}$ is the multiset in which each element of $\{(\gamma^{2^d \frac{q-1}{\lambda'} m}, (-1)^m) \mid 0 \leq m < n'\}$ appears with multiplicity $\frac{2^d \lambda}{\lambda'}$.

What is really important for **Result 1** is the reordering suggested by (1).

Result 2 Consider the same notation and main assumption. In addition, let λ' and d be two integers such that λ' is any divisor of $q-1$ and d is equal to zero or one.

Result 2 Consider the same notation and main assumption. In addition, let λ' and d be two integers such that λ' is any divisor of $q-1$ and d is equal to zero or one. If $\gcd(\frac{\Delta}{2}, \frac{2^d(q-1)}{\lambda'}) = 2$, then, for any integer i, we have

$$\{xy \mid x \in \mathcal{D}_i^{(\frac{2^{d+1}(q-1)}{\lambda'})} \text{ and } y \in \mathbb{F}_q^*\} = \frac{2\lambda'}{2^d} * \mathcal{D}_i^{(4)}, \qquad (2)$$

where $\frac{2\lambda'}{2^d} * \mathcal{D}_i^{(4)}$ is the multiset in which each element of $\mathcal{D}_i^{(4)}$ appears with multiplicity $\frac{2\lambda'}{2^d}$.

Result 2 Consider the same notation and main assumption. In addition, let λ' and d be two integers such that λ' is any divisor of $q-1$ and d is equal to zero or one. If $\gcd(\frac{\Delta}{2}, \frac{2^d(q-1)}{\lambda'}) = 2$, then, for any integer i, we have

$$\{xy \mid x \in \mathcal{D}_i^{(\frac{2^{d+1}(q-1)}{\lambda'})} \text{ and } y \in \mathbb{F}_q^*\} = \frac{2\lambda'}{2^d} * \mathcal{D}_i^{(4)} , \qquad (2)$$

where $\frac{2\lambda'}{2^d} * \mathcal{D}_i^{(4)}$ is the multiset in which each element of $\mathcal{D}_i^{(4)}$ appears with multiplicity $\frac{2\lambda'}{2^d}$.

Similar to the previous result, what is really important for **Result 2** is the reordering suggested now by (2).

Result 3 Let r be any even integer and let χ be the canonical additive character of $\mathbb{F}_{q^k}$.

Result 3 Let r be any even integer and let χ be the canonical additive character of $\mathbb{F}_{q^k}$. Also let η_0 and η_1 be the two integers that are given in **Theorem 1**.

Result 3 Let r be any even integer and let χ be the canonical additive character of $\mathbb{F}_{q^k}$. Also let η_0 and η_1 be the two integers that are given in **Theorem 1**. Thus, by considering all possible values of α and β in $\mathbb{F}_{q^k}$, we have that

$$\text{Value distribution of } \sum_{m=0}^{1} \sum_{z \in \mathcal{D}_{rm}^{(4)}} \chi(z(\beta + (-1)^m \alpha)),$$

where r must be an even integer.

Value	Frequency
$\frac{q^k-1}{2}$	1
$\frac{q^k-1}{4} + \eta_0$	$\frac{q^k-1}{2}$
$\frac{q^k-1}{4} + \eta_1$	$\frac{3(q^k-1)}{2}$
$\eta_0 + \eta_1$	$\frac{6(q^k-1)^2}{16}$
$2\eta_0$	$\frac{(q^k-1)^2}{16}$
$2\eta_1$	$\frac{9(q^k-1)^2}{16}$

Result 3 Let r be any even integer and let χ be the canonical additive character of $\mathbb{F}_{q^k}$. Also let η_0 and η_1 be the two integers that are given in **Theorem 1**. Thus, by considering all possible values of α and β in $\mathbb{F}_{q^k}$, we have that

$$\text{Value distribution of } \sum_{m=0}^{1} \sum_{z \in \mathcal{D}_{rm}^{(4)}} \chi(z(\beta + (-1)^m \alpha)),$$

where r must be an even integer.

Value	Frequency
$\frac{q^k-1}{2}$	1
$\frac{q^k-1}{4} + \eta_0$	$\frac{q^k-1}{2}$
$\frac{q^k-1}{4} + \eta_1$	$\frac{3(q^k-1)}{2}$
$\eta_0 + \eta_1$	$\frac{6(q^k-1)^2}{16}$
$2\eta_0$	$\frac{(q^k-1)^2}{16}$
$2\eta_1$	$\frac{9(q^k-1)^2}{16}$

In addition, we need to say here that **Theorem 1** was quite important in order to obtain the proof for this result.

The weight distribution of a family of reducible cyclic codes

Theorem 2 With our main assumption in mind, take λ being a divisor of $q-1$ and define $n = \lambda\Delta$.

The weight distribution of a family of reducible cyclic codes

Theorem 2 With our main assumption in mind, take λ being a divisor of $q-1$ and define $n = \lambda\Delta$. Let a_1 and a_2 be two integers such that $a_2 n \equiv 0 \pmod{q^k - 1}$ and $a_2 - a_1 \equiv \frac{q^k-1}{2} \pmod{q^k - 1}$.

The weight distribution of a family of reducible cyclic codes

Theorem 2 With our main assumption in mind, take λ being a divisor of $q-1$ and define $n = \lambda\Delta$. Let a_1 and a_2 be two integers such that $a_2 n \equiv 0 \pmod{q^k - 1}$ and $a_2 - a_1 \equiv \frac{q^k-1}{2} \pmod{q^k - 1}$. Let $\mathcal{C}_{(a_1,a_2)}$ be the cyclic code with parity-check polynomial $h_{a_1}(x)h_{a_2}(x)$.

The weight distribution of a family of reducible cyclic codes

Theorem 2 With our main assumption in mind, take λ being a divisor of $q-1$ and define $n = \lambda\Delta$. Let a_1 and a_2 be two integers such that $a_2 n \equiv 0 \pmod{q^k - 1}$ and $a_2 - a_1 \equiv \frac{q^k-1}{2} \pmod{q^k - 1}$. Let $\mathcal{C}_{(a_1,a_2)}$ be the cyclic code with parity-check polynomial $h_{a_1}(x)h_{a_2}(x)$. If $\gcd(\frac{\Delta}{2}, a_2) = 2$, then $\mathcal{C}_{(a_1,a_2)}$ is a non-projective $[n, 2k]$ cyclic code with the weight distribution given by

Weight distribution of $\mathcal{C}_{(a_1,a_2)}$.

Weight	Frequency
0	1
$\frac{\lambda}{2}(q^{k-1} - 3(-q)^{(k-2)/2})$	$\frac{q^k-1}{2}$
$\frac{\lambda}{2}(q^{k-1} + (-q)^{(k-2)/2})$	$\frac{3(q^k-1)}{2}$
$\lambda(q^{k-1} - (-q)^{(k-2)/2})$	$\frac{6(q^k-1)^2}{16}$
$\lambda(q^{k-1} - 3(-q)^{(k-2)/2})$	$\frac{(q^k-1)^2}{16}$
$\lambda(q^{k-1} + (-q)^{(k-2)/2})$	$\frac{9(q^k-1)^2}{16}$

Sketch of proof It is not difficult to prove that $h_{a_1}(x) \neq h_{a_2}(x)$ and $\deg(h_{a_1}(x)) = \deg(h_{a_2}(x)) = k$.

Sketch of proof It is not difficult to prove that $h_{a_1}(x) \neq h_{a_2}(x)$ and $\deg(h_{a_1}(x)) = \deg(h_{a_2}(x)) = k$. In addition, since n is even (recall $4|\Delta$ and $n = \lambda\Delta$) we also have $a_1 n \equiv 0 \pmod{q^k - 1}$.

Sketch of proof It is not difficult to prove that $h_{a_1}(x) \neq h_{a_2}(x)$ and $\deg(h_{a_1}(x)) = \deg(h_{a_2}(x)) = k$. In addition, since n is even (recall $4|\Delta$ and $n = \lambda\Delta$) we also have $a_1 n \equiv 0 \pmod{q^k - 1}$. Therefore $\mathcal{C}_{(a_1,a_2)}$ is a cyclic code of length n and dimension $2k$.

Sketch of proof It is not difficult to prove that $h_{a_1}(x) \neq h_{a_2}(x)$ and $\deg(h_{a_1}(x)) = \deg(h_{a_2}(x)) = k$. In addition, since n is even (recall $4|\Delta$ and $n = \lambda\Delta$) we also have $a_1 n \equiv 0 \pmod{q^k - 1}$. Therefore $\mathcal{C}_{(a_1,a_2)}$ is a cyclic code of length n and dimension $2k$.

We will now prove the assertion about the W.D. of $\mathcal{C}_{(a_1,a_2)}$.

Sketch of proof It is not difficult to prove that $h_{a_1}(x) \neq h_{a_2}(x)$ and $\deg(h_{a_1}(x)) = \deg(h_{a_2}(x)) = k$. In addition, since n is even (recall $4|\Delta$ and $n = \lambda\Delta$) we also have $a_1 n \equiv 0 \pmod{q^k - 1}$. Therefore $\mathcal{C}_{(a_1,a_2)}$ is a cyclic code of length n and dimension $2k$.

We will now prove the assertion about the W.D. of $\mathcal{C}_{(a_1,a_2)}$. Thus, for each two elements $\alpha, \beta \in \mathbb{F}_{q^k}$, we define $c(n, a_1, a_2, \alpha, \beta)$ as the vector of length n over $\mathbb{F}_q$, which is given by:

$$(\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha(\gamma^{a_1})^0 + \beta(\gamma^{a_2})^0), \cdots, \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha(\gamma^{a_1})^{n-1} + \beta(\gamma^{a_2})^{n-1})),$$

where "$\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$" is the trace mapping from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$.

Sketch of proof It is not difficult to prove that $h_{a_1}(x) \neq h_{a_2}(x)$ and $\deg(h_{a_1}(x)) = \deg(h_{a_2}(x)) = k$. In addition, since n is even (recall $4|\Delta$ and $n = \lambda\Delta$) we also have $a_1 n \equiv 0 \pmod{q^k - 1}$. Therefore $\mathcal{C}_{(a_1,a_2)}$ is a cyclic code of length n and dimension $2k$.

We will now prove the assertion about the W.D. of $\mathcal{C}_{(a_1,a_2)}$. Thus, for each two elements $\alpha, \beta \in \mathbb{F}_{q^k}$, we define $c(n, a_1, a_2, \alpha, \beta)$ as the vector of length n over $\mathbb{F}_q$, which is given by:

$$(\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha(\gamma^{a_1})^0 + \beta(\gamma^{a_2})^0), \cdots, \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha(\gamma^{a_1})^{n-1} + \beta(\gamma^{a_2})^{n-1})),$$

where "$\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$" is the trace mapping from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$. Thanks to Delsarte's Theorem, it is well known that

$$\mathcal{C}_{(a_1,a_2)} = \{c(n, a_1, a_2, \alpha, \beta) \mid \alpha, \beta \in \mathbb{F}_{q^k}\} .$$

Sketch of proof It is not difficult to prove that $h_{a_1}(x) \neq h_{a_2}(x)$ and $\deg(h_{a_1}(x)) = \deg(h_{a_2}(x)) = k$. In addition, since n is even (recall $4|\Delta$ and $n = \lambda\Delta$) we also have $a_1 n \equiv 0 \pmod{q^k - 1}$. Therefore $\mathcal{C}_{(a_1,a_2)}$ is a cyclic code of length n and dimension $2k$.

We will now prove the assertion about the W.D. of $\mathcal{C}_{(a_1,a_2)}$. Thus, for each two elements $\alpha, \beta \in \mathbb{F}_{q^k}$, we define $c(n, a_1, a_2, \alpha, \beta)$ as the vector of length n over $\mathbb{F}_q$, which is given by:

$$(\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha(\gamma^{a_1})^0 + \beta(\gamma^{a_2})^0), \cdots, \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha(\gamma^{a_1})^{n-1} + \beta(\gamma^{a_2})^{n-1})),$$

where "$\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$" is the trace mapping from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$. Thanks to Delsarte's Theorem, it is well known that

$$\mathcal{C}_{(a_1,a_2)} = \{c(n, a_1, a_2, \alpha, \beta) \mid \alpha, \beta \in \mathbb{F}_{q^k}\} .$$

Thus, considering this fact, the Hamming weight of any codeword $c(n, a_1, a_2, \alpha, \beta) \in \mathcal{C}_{(a_1,a_2)}$ will be equal to $n - Z(\alpha, \beta)$, where

$$Z(\alpha, \beta) = \sharp\{m | 0 \leq m < n, \text{ and } \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha\gamma^{a_1 m} + \beta\gamma^{a_2 m}) = 0\}.$$

If χ denotes the canonical additive character of $\mathbb{F}_{q^k}$, then it is not difficult to prove that number of zeros, $Z(\alpha, \beta)$ can be computed by means of the following exponential sum

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{1}{q} \sum_{m=0}^{n-1} \sum_{y \in \mathbb{F}_q^*} \chi(\gamma^{a_2 m} y((-1)^m \alpha + \beta)) \; .$$

If χ denotes the canonical additive character of $\mathbb{F}_{q^k}$, then it is not difficult to prove that number of zeros, $Z(\alpha, \beta)$ can be computed by means of the following exponential sum

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{1}{q}\sum_{m=0}^{n-1}\sum_{y\in\mathbb{F}_q^*}\chi(\gamma^{a_2 m}y((-1)^m\alpha+\beta)) \ .$$

Now, thanks to Result 1, we know that there exist integers d, λ' and n', such that $d = 0$ or 1, λ' is the divisor of $q-1$ satisfying $\gcd(q-1, a_2) = \frac{q-1}{\lambda'}$ and $n' = \lambda'\frac{\Delta}{2^d}$.

If χ denotes the canonical additive character of $\mathbb{F}_{q^k}$, then it is not difficult to prove that number of zeros, $Z(\alpha, \beta)$ can be computed by means of the following exponential sum

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{1}{q}\sum_{m=0}^{n-1}\sum_{y\in\mathbb{F}_q^*}\chi(\gamma^{a_2 m}y((-1)^m\alpha+\beta)) \ .$$

Now, thanks to Result 1, we know that there exist integers d, λ' and n', such that $d = 0$ or 1, λ' is the divisor of $q-1$ satisfying $\gcd(q-1, a_2) = \frac{q-1}{\lambda'}$ and $n' = \lambda'\frac{\Delta}{2^d}$. In addition, we also know

$$\{(\gamma^{a_2 m}, (-1)^m) \mid 0 \le m < n\} = \frac{2^d\lambda}{\lambda'} * \{(\gamma^{2^d\frac{q-1}{\lambda'}m}, (-1)^m) \mid 0 \le m < n'\}.$$

If χ denotes the canonical additive character of $\mathbb{F}_{q^k}$, then it is not difficult to prove that number of zeros, $Z(\alpha, \beta)$ can be computed by means of the following exponential sum

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{1}{q}\sum_{m=0}^{n-1}\sum_{y\in\mathbb{F}_q^*}\chi(\gamma^{a_2 m}y((-1)^m\alpha+\beta)) \ .$$

Now, thanks to Result 1, we know that there exist integers d, λ' and n', such that $d = 0$ or 1, λ' is the divisor of $q-1$ satisfying $\gcd(q-1, a_2) = \frac{q-1}{\lambda'}$ and $n' = \lambda'\frac{\Delta}{2^d}$. In addition, we also know

$$\{(\gamma^{a_2 m}, (-1)^m) \mid 0 \le m < n\} = \frac{2^d\lambda}{\lambda'} * \{(\gamma^{2^d\frac{q-1}{\lambda'}m}, (-1)^m) \mid 0 \le m < n'\}.$$

Thus, after applying the reordering suggested by Result 1 to number of zeros $Z(\alpha, \beta)$, we have

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{2^d\lambda}{q\lambda'}\sum_{m=0}^{n'-1}\sum_{y\in\mathbb{F}_q^*}\chi(\gamma^{2^d\frac{q-1}{\lambda'}m}y((-1)^m\alpha+\beta)).$$

For clarity we rewrite the previous equality:

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{2^d\lambda}{q\lambda'} \sum_{m=0}^{n'-1} \sum_{y\in\mathbb{F}_q^*} \chi(\gamma^{2^d \frac{q-1}{\lambda'} m} y((-1)^m\alpha+\beta)).$$

For clarity we rewrite the previous equality:

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{2^d\lambda}{q\lambda'}\sum_{m=0}^{n'-1}\sum_{y\in\mathbb{F}_q^*}\chi(\gamma^{2^d\frac{q-1}{\lambda'}m}y((-1)^m\alpha+\beta)).$$

Now, we know that $d = 0$ or 1, and since $4|\Delta$, then $n' = \lambda'\frac{\Delta}{2^d}$ must be an even integer. But $n' = |\mathcal{D}_0^{(\frac{2^d(q-1)}{\lambda'})}|$, therefore,

$$\mathcal{D}_0^{(\frac{2^d(q-1)}{\lambda'})} = \mathcal{D}_0^{(\frac{2^{d+1}(q-1)}{\lambda'})} \cup \mathcal{D}_{2^d\frac{q-1}{\lambda'}}^{(\frac{2^{d+1}(q-1)}{\lambda'})}. \qquad (3)$$

For clarity we rewrite the previous equality:

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{2^d\lambda}{q\lambda'}\sum_{m=0}^{n'-1}\sum_{y\in\mathbb{F}_q^*}\chi(\gamma^{2^d\frac{q-1}{\lambda'}m}y((-1)^m\alpha+\beta)).$$

Now, we know that $d = 0$ or 1, and since $4|\Delta$, then $n' = \lambda'\frac{\Delta}{2^d}$ must be an even integer. But $n' = |\mathcal{D}_0^{(\frac{2^d(q-1)}{\lambda'})}|$, therefore,

$$\mathcal{D}_0^{(\frac{2^d(q-1)}{\lambda'})} = \mathcal{D}_0^{(\frac{2^{d+1}(q-1)}{\lambda'})} \cup \mathcal{D}_{2^d\frac{q-1}{\lambda'}}^{(\frac{2^{d+1}(q-1)}{\lambda'})}. \qquad (3)$$

On the other hand, $\mathcal{D}_0^{(\frac{2^d(q-1)}{\lambda'})} = \{\gamma^{2^d\frac{q-1}{\lambda'}m} \mid 0 \le m < n'\}$, thus (3) suggests a reordering for the summations in $Z(\alpha,\beta)$.

For clarity we rewrite the previous equality:

$$Z(\alpha,\beta)=\frac{n}{q}+\frac{2^d\lambda}{q\lambda'}\sum_{m=0}^{n'-1}\sum_{y\in\mathbb{F}_q^*}\chi(\gamma^{2^d\frac{q-1}{\lambda'}m}y((-1)^m\alpha+\beta)).$$

Now, we know that $d=0$ or 1, and since $4|\Delta$, then $n'=\lambda'\frac{\Delta}{2^d}$ must be an even integer. But $n'=|\mathcal{D}_0^{(\frac{2^d(q-1)}{\lambda'})}|$, therefore,

$$\mathcal{D}_0^{(\frac{2^d(q-1)}{\lambda'})}=\mathcal{D}_0^{(\frac{2^{d+1}(q-1)}{\lambda'})}\cup\mathcal{D}_{2^d\frac{q-1}{\lambda'}}^{(\frac{2^{d+1}(q-1)}{\lambda'})}. \qquad (3)$$

On the other hand, $\mathcal{D}_0^{(\frac{2^d(q-1)}{\lambda'})}=\{\gamma^{2^d\frac{q-1}{\lambda'}m}\mid 0\le m<n'\}$, thus (3) suggests a reordering for the summations in $Z(\alpha,\beta)$. Therefore

$$Z(\alpha,\beta)=\frac{n}{q}+\frac{2^d\lambda}{q\lambda'}\sum_{m=0}^{1}\sum_{x\in\mathcal{D}_{2^d\frac{q-1}{\lambda'}m}^{(\frac{2^{d+1}(q-1)}{\lambda'})}}\sum_{y\in\mathbb{F}_q^*}\chi(xy((-1)^m\alpha+\beta)).$$

Again, for clarity we rewrite the previous equality:

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{2^d\lambda}{q\lambda'}\sum_{m=0}^{1}\sum_{x\in\mathcal{D}_{2^d\frac{q-1}{\lambda'}m}^{(\frac{2^{d+1}(q-1)}{\lambda'})}}\sum_{y\in\mathbb{F}_q^*}\chi(xy((-1)^m\alpha+\beta)).$$

Again, for clarity we rewrite the previous equality:

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{2^d\lambda}{q\lambda'} \sum_{m=0}^{1} \sum_{x\in\mathcal{D}_{2^d\frac{q-1}{\lambda'}m}^{(\frac{2^{d+1}(q-1)}{\lambda'})}} \sum_{y\in\mathbb{F}_q^*} \chi(xy((-1)^m\alpha+\beta)).$$

Now, since we are supposing that $\gcd(\frac{\Delta}{2}, a_2) = 2$, then it is easy prove that $\gcd(\frac{\Delta}{2}, 2^d\frac{q-1}{\lambda'}) = 2$. Therefore, thanks to Result 2, we know that, for any integer i, we have

$$\{xy \mid x \in \mathcal{D}_i^{(\frac{2^{d+1}(q-1)}{\lambda'})} \text{ and } y \in \mathbb{F}_q^*\} = \frac{2\lambda'}{2^d} * \mathcal{D}_i^{(4)} \ ,$$

Again, for clarity we rewrite the previous equality:

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{2^d\lambda}{q\lambda'}\sum_{m=0}^{1}\sum_{x\in\mathcal{D}_{2^d\frac{q-1}{\lambda'}m}^{(\frac{2^{d+1}(q-1)}{\lambda'})}}\sum_{y\in\mathbb{F}_q^*}\chi(xy((-1)^m\alpha+\beta)).$$

Now, since we are supposing that $\gcd(\frac{\Delta}{2}, a_2) = 2$, then it is easy prove that $\gcd(\frac{\Delta}{2}, 2^d\frac{q-1}{\lambda'}) = 2$. Therefore, thanks to Result 2, we know that, for any integer i, we have

$$\{xy \mid x \in \mathcal{D}_i^{(\frac{2^{d+1}(q-1)}{\lambda'})} \text{ and } y \in \mathbb{F}_q^*\} = \frac{2\lambda'}{2^d} * \mathcal{D}_i^{(4)} \ ,$$

Thus, after applying the reordering suggested, now, by Result 2 to number of zeros $Z(\alpha,\beta)$, we have

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{2\lambda}{q}\sum_{m=0}^{1}\sum_{z\in\mathcal{D}^{(4)}_{2^d\frac{q-1}{\lambda'}m}}\chi(z(\beta+(-1)^m\alpha)).$$

Once again, we rewrite the previous equality:

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{2\lambda}{q} \sum_{m=0}^{1} \sum_{z \in \mathcal{D}^{(4)}_{2^d \frac{q-1}{\lambda'} m}} \chi(z(\beta + (-1)^m \alpha)).$$

Once again, we rewrite the previous equality:

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{2\lambda}{q}\sum_{m=0}^{1}\sum_{z\in\mathcal{D}^{(4)}_{2^d\frac{q-1}{\lambda'}m}} \chi(z(\beta+(-1)^m\alpha)).$$

Now, since $\gcd(\frac{\Delta}{2}, a_2) = 2$, then it is possible to prove that $2^d\frac{q-1}{\lambda'} = \gcd(q^k-1, a_2)$.

Once again, we rewrite the previous equality:

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{2\lambda}{q}\sum_{m=0}^{1}\sum_{z\in\mathcal{D}^{(4)}_{2^{d}\frac{q-1}{\lambda'}m}} \chi(z(\beta+(-1)^{m}\alpha)).$$

Now, since $\gcd(\frac{\Delta}{2}, a_2) = 2$, then it is possible to prove that $2^{d}\frac{q-1}{\lambda'} = \gcd(q^k - 1, a_2)$. But, clearly, $q^k - 1$ and a_2 are even integers, thus $2^{d}\frac{q-1}{\lambda'}$ must be an even integer too.

Once again, we rewrite the previous equality:

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{2\lambda}{q}\sum_{m=0}^{1}\sum_{z\in\mathcal{D}^{(4)}_{2^{d}\frac{q-1}{\lambda'}m}} \chi(z(\beta+(-1)^{m}\alpha)).$$

Now, since $\gcd(\frac{\Delta}{2}, a_2) = 2$, then it is possible to prove that $2^{d}\frac{q-1}{\lambda'} = \gcd(q^{k}-1, a_2)$. But, clearly, $q^{k}-1$ and a_2 are even integers, thus $2^{d}\frac{q-1}{\lambda'}$ must be an even integer too. Therefore, we can now apply Result 3 in order to find, exactly, the value distribution of the exponential sum

$$\sum_{m=0}^{1}\sum_{z\in\mathcal{D}^{(4)}_{2^{d}\frac{q-1}{\lambda'}m}} \chi(z(\beta+(-1)^{m}\alpha)),$$

which, clearly, is the same exponential sum that appears in the number of zeros $Z(\alpha,\beta)$.

Once again, we rewrite the previous equality:

$$Z(\alpha,\beta) = \frac{n}{q} + \frac{2\lambda}{q}\sum_{m=0}^{1}\sum_{z\in\mathcal{D}^{(4)}_{2^d\frac{q-1}{\lambda'}m}} \chi(z(\beta+(-1)^m\alpha)).$$

Now, since $\gcd(\frac{\Delta}{2}, a_2) = 2$, then it is possible to prove that $2^d\frac{q-1}{\lambda'} = \gcd(q^k-1, a_2)$. But, clearly, q^k-1 and a_2 are even integers, thus $2^d\frac{q-1}{\lambda'}$ must be an even integer too. Therefore, we can now apply Result 3 in order to find, exactly, the value distribution of the exponential sum

$$\sum_{m=0}^{1}\sum_{z\in\mathcal{D}^{(4)}_{2^d\frac{q-1}{\lambda'}m}} \chi(z(\beta+(-1)^m\alpha)),$$

which, clearly, is the same exponential sum that appears in the number of zeros $Z(\alpha,\beta)$. But we already said that the Hamming weight of any codeword $c(n,a_1,a_2,\alpha,\beta) \in \mathcal{C}_{(a_1,a_2)}$ is equal to $n - Z(\alpha,\beta)$, consequently, the assertion about the weight distribution for the cyclic code $\mathcal{C}_{(a_1,a_2)}$ comes now directly from Result 3.

It remains to prove that $\mathcal{C}_{(a_1,a_2)}$ is a non-projective cyclic code.

It remains to prove that $\mathcal{C}_{(a_1,a_2)}$ is a non-projective cyclic code. Thus, suppose that, for some positive integer N, $w_1,w_2,\cdots,w_N$ are the nonzero weights of $\mathcal{C}_{(a_1,a_2)}$, and for $1 \leq i \leq N$, let A_i be the number of words of weight w_i in $\mathcal{C}_{(a_1,a_2)}$.

It remains to prove that $\mathcal{C}_{(a_1,a_2)}$ is a non-projective cyclic code. Thus, suppose that, for some positive integer N, $w_1,w_2,\cdots,w_N$ are the nonzero weights of $\mathcal{C}_{(a_1,a_2)}$, and for $1 \leq i \leq N$, let A_i be the number of words of weight w_i in $\mathcal{C}_{(a_1,a_2)}$. In addition, let B_j be the number of words of weight j in the dual code of $\mathcal{C}_{(a_1,a_2)}$.

It remains to prove that $\mathcal{C}_{(a_1,a_2)}$ is a non-projective cyclic code. Thus, suppose that, for some positive integer N, $w_1, w_2, \cdots, w_N$ are the nonzero weights of $\mathcal{C}_{(a_1,a_2)}$, and for $1 \leq i \leq N$, let A_i be the number of words of weight w_i in $\mathcal{C}_{(a_1,a_2)}$. In addition, let B_j be the number of words of weight j in the dual code of $\mathcal{C}_{(a_1,a_2)}$. Then, by the third identity of Pless, applied to $\mathcal{C}_{(a_1,a_2)}$, we have

$$\sum_{i=1}^{N} w_i^2 A_i = [n(q-1)(n(q-1)+1) - B_1(q+2(n-1)(q-1)) + 2B_2]q^{2k-2}.$$

It remains to prove that $\mathcal{C}_{(a_1,a_2)}$ is a non-projective cyclic code. Thus, suppose that, for some positive integer N, $w_1,w_2,\cdots,w_N$ are the nonzero weights of $\mathcal{C}_{(a_1,a_2)}$, and for $1 \leq i \leq N$, let A_i be the number of words of weight w_i in $\mathcal{C}_{(a_1,a_2)}$. In addition, let B_j be the number of words of weight j in the dual code of $\mathcal{C}_{(a_1,a_2)}$. Then, by the third identity of Pless, applied to $\mathcal{C}_{(a_1,a_2)}$, we have

$$\sum_{i=1}^{N} w_i^2 A_i = [n(q-1)(n(q-1)+1) - B_1(q+2(n-1)(q-1)) + 2B_2]q^{2k-2}.$$

Observe that, in the context of the previous identity, a linear code is a projective one if and only if B_1 and B_2 are zero.

It remains to prove that $\mathcal{C}_{(a_1,a_2)}$ is a non-projective cyclic code. Thus, suppose that, for some positive integer N, $w_1,w_2,\cdots,w_N$ are the nonzero weights of $\mathcal{C}_{(a_1,a_2)}$, and for $1 \leq i \leq N$, let A_i be the number of words of weight w_i in $\mathcal{C}_{(a_1,a_2)}$. In addition, let B_j be the number of words of weight j in the dual code of $\mathcal{C}_{(a_1,a_2)}$. Then, by the third identity of Pless, applied to $\mathcal{C}_{(a_1,a_2)}$, we have

$$\sum_{i=1}^{N} w_i^2 A_i = [n(q-1)(n(q-1)+1) - B_1(q+2(n-1)(q-1)) + 2B_2]q^{2k-2}.$$

Observe that, in the context of the previous identity, a linear code is a projective one if and only if B_1 and B_2 are zero. But it is well known that there are no 1-weight words in the dual code of any cyclic code, therefore $B_1 = 0$.

It remains to prove that $\mathcal{C}_{(a_1,a_2)}$ is a non-projective cyclic code. Thus, suppose that, for some positive integer N, $w_1,w_2,\cdots,w_N$ are the nonzero weights of $\mathcal{C}_{(a_1,a_2)}$, and for $1 \leq i \leq N$, let A_i be the number of words of weight w_i in $\mathcal{C}_{(a_1,a_2)}$. In addition, let B_j be the number of words of weight j in the dual code of $\mathcal{C}_{(a_1,a_2)}$. Then, by the third identity of Pless, applied to $\mathcal{C}_{(a_1,a_2)}$, we have

$$\sum_{i=1}^{N} w_i^2 A_i = [n(q-1)(n(q-1)+1) - B_1(q+2(n-1)(q-1)) + 2B_2]q^{2k-2}.$$

Observe that, in the context of the previous identity, a linear code is a projective one if and only if B_1 and B_2 are zero. But it is well known that there are no 1-weight words in the dual code of any cyclic code, therefore $B_1 = 0$. On the other hand, we already found the weight distribution for $\mathcal{C}_{(a_1,a_2)}$.

It remains to prove that $\mathcal{C}_{(a_1,a_2)}$ is a non-projective cyclic code. Thus, suppose that, for some positive integer N, $w_1,w_2,\cdots,w_N$ are the nonzero weights of $\mathcal{C}_{(a_1,a_2)}$, and for $1 \leq i \leq N$, let A_i be the number of words of weight w_i in $\mathcal{C}_{(a_1,a_2)}$. In addition, let B_j be the number of words of weight j in the dual code of $\mathcal{C}_{(a_1,a_2)}$. Then, by the third identity of Pless, applied to $\mathcal{C}_{(a_1,a_2)}$, we have

$$\sum_{i=1}^{N} w_i^2 A_i = [n(q-1)(n(q-1)+1) - B_1(q+2(n-1)(q-1)) + 2B_2]q^{2k-2}.$$

Observe that, in the context of the previous identity, a linear code is a projective one if and only if B_1 and B_2 are zero. But it is well known that there are no 1-weight words in the dual code of any cyclic code, therefore $B_1 = 0$. On the other hand, we already found the weight distribution for $\mathcal{C}_{(a_1,a_2)}$. Therefore, the LHS of the previous identity is completely known.

It remains to prove that $\mathcal{C}_{(a_1,a_2)}$ is a non-projective cyclic code. Thus, suppose that, for some positive integer N, $w_1,w_2,\cdots,w_N$ are the nonzero weights of $\mathcal{C}_{(a_1,a_2)}$, and for $1 \leq i \leq N$, let A_i be the number of words of weight w_i in $\mathcal{C}_{(a_1,a_2)}$. In addition, let B_j be the number of words of weight j in the dual code of $\mathcal{C}_{(a_1,a_2)}$. Then, by the third identity of Pless, applied to $\mathcal{C}_{(a_1,a_2)}$, we have

$$\sum_{i=1}^{N} w_i^2 A_i = [n(q-1)(n(q-1)+1) - B_1(q+2(n-1)(q-1)) + 2B_2]q^{2k-2}.$$

Observe that, in the context of the previous identity, a linear code is a projective one if and only if B_1 and B_2 are zero. But it is well known that there are no 1-weight words in the dual code of any cyclic code, therefore $B_1 = 0$. On the other hand, we already found the weight distribution for $\mathcal{C}_{(a_1,a_2)}$. Therefore, the LHS of the previous identity is completely known. Thus, by obtaining B_2 directly from such identity we get

$$B_2 = \frac{n(q-1)(2\lambda-1)}{2}.$$

It remains to prove that $\mathcal{C}_{(a_1,a_2)}$ is a non-projective cyclic code. Thus, suppose that, for some positive integer N, $w_1,w_2,\cdots,w_N$ are the nonzero weights of $\mathcal{C}_{(a_1,a_2)}$, and for $1 \leq i \leq N$, let A_i be the number of words of weight w_i in $\mathcal{C}_{(a_1,a_2)}$. In addition, let B_j be the number of words of weight j in the dual code of $\mathcal{C}_{(a_1,a_2)}$. Then, by the third identity of Pless, applied to $\mathcal{C}_{(a_1,a_2)}$, we have

$$\sum_{i=1}^{N} w_i^2 A_i = [n(q-1)(n(q-1)+1) - B_1(q+2(n-1)(q-1)) + 2B_2]q^{2k-2}.$$

Observe that, in the context of the previous identity, a linear code is a projective one if and only if B_1 and B_2 are zero. But it is well known that there are no 1-weight words in the dual code of any cyclic code, therefore $B_1 = 0$. On the other hand, we already found the weight distribution for $\mathcal{C}_{(a_1,a_2)}$. Therefore, the LHS of the previous identity is completely known. Thus, by obtaining B_2 directly from such identity we get

$$B_2 = \frac{n(q-1)(2\lambda-1)}{2}.$$

Finally, since $n(q-1) \neq 0$ and $\lambda \neq \frac{1}{2}$, then $B_2 \neq 0$. Therefore $\mathcal{C}_{(a_1,a_2)}$ is a non-projective cyclic code. □

An example for this family of reducible cyclic codes

In order to illustrate the application of Theorem 2, we present the following

Example 1 If we take $q = 7$, $k = 2$, $\lambda = 1$ and $a_2 = 6$, then we have that $\Delta = 8$ and $a_1 = 30$.

An example for this family of reducible cyclic codes

In order to illustrate the application of Theorem 2, we present the following

Example 1 If we take $q = 7$, $k = 2$, $\lambda = 1$ and $a_2 = 6$, then we have that $\Delta = 8$ and $a_1 = 30$. In addition, observe that for this particular set of values we have that

$$\frac{\lambda}{2}(q^{k-1} + (-q)^{(k-2)/2}) = \lambda(q^{k-1} - 3(-q)^{(k-2)/2}) = 4.$$

An example for this family of reducible cyclic codes

In order to illustrate the application of Theorem 2, we present the following

Example 1 If we take $q = 7$, $k = 2$, $\lambda = 1$ and $a_2 = 6$, then we have that $\Delta = 8$ and $a_1 = 30$. In addition, observe that for this particular set of values we have that

$$\tfrac{\lambda}{2}(q^{k-1} + (-q)^{(k-2)/2}) = \lambda(q^{k-1} - 3(-q)^{(k-2)/2}) = 4.$$

Now, since $\frac{\Delta}{2} = 4$ and $a_2 = 6$ then, clearly, $\gcd(\frac{\Delta}{2}, a_2) = 2$. Therefore, by Theorem 2, we can be sure that $\mathcal{C}_{(30,6)}$ is a 4-weight non-projective cyclic code, over $\mathbb{F}_7$, of length 8, dimension 4 and weight enumerator polynomial

$$A(z) = 1 + 24z^2 + 216z^4 + 864z^6 + 1296z^8.$$

An explicit formula for the number of cyclic codes in a family when length and dimension are given

Now, observe that, for a divisor λ of $q-1$ and for any integer a_2, Theorem 2 basically states that if a_2 satisfies the easy-to-check condition

$$\gcd(\frac{\Delta}{2}, a_2) = 2 \ ,$$

then, for any integer j, the cyclic code

$$\mathcal{C}_{(a_2 q^j \pm \frac{q^k-1}{2}, a_2)} \ ,$$

could be described by means of such theorem.

An explicit formula for the number of cyclic codes in a family when length and dimension are given

Now, observe that, for a divisor λ of $q-1$ and for any integer a_2, Theorem 2 basically states that if a_2 satisfies the easy-to-check condition

$$\gcd(\frac{\Delta}{2}, a_2) = 2 \, ,$$

then, for any integer j, the cyclic code

$$\mathcal{C}_{(a_2 q^j \pm \frac{q^k-1}{2}, a_2)} \, ,$$

could be described by means of such theorem. Thanks to this easy-to-check condition we can now give the exact number of different cyclic codes $\mathcal{C}_{(a_1,a_2)}$ that satisfy the hypotheses in Theorem 2. We now present such a result by means of the following:

Theorem 3 Let q, k and Δ be as before.

Theorem 3 Let q, k and Δ be as before. Considering our main assumption, we also take λ to be a divisor of $q-1$ and define $n = \lambda\Delta$.

Theorem 3 Let q, k and Δ be as before. Considering our main assumption, we also take λ to be a divisor of $q-1$ and define $n = \lambda\Delta$. For any integers a_1 and a_2, let $\mathcal{C}_{(a_1,a_2)}$ be the cyclic code with parity-check polynomial given by $h_{a_1}(x)h_{a_2}(x)$.

Theorem 3 Let q, k and Δ be as before. Considering our main assumption, we also take λ to be a divisor of $q-1$ and define $n = \lambda\Delta$. For any integers a_1 and a_2, let $\mathcal{C}_{(a_1,a_2)}$ be the cyclic code with parity-check polynomial given by $h_{a_1}(x)h_{a_2}(x)$. Let $\mathcal{N}_{(q,k,\lambda)}$ be the number of cyclic codes, $\mathcal{C}_{(a_1,a_2)}$ of length n and dimension $2k$ that satisfy conditions in Theorem 2.

Theorem 3 Let q, k and Δ be as before. Considering our main assumption, we also take λ to be a divisor of $q-1$ and define $n = \lambda\Delta$. For any integers a_1 and a_2, let $\mathcal{C}_{(a_1,a_2)}$ be the cyclic code with parity-check polynomial given by $h_{a_1}(x)h_{a_2}(x)$. Let $\mathcal{N}_{(q,k,\lambda)}$ be the number of cyclic codes, $\mathcal{C}_{(a_1,a_2)}$ of length n and dimension $2k$ that satisfy conditions in **Theorem 2**. Then the number of such cyclic codes can be obtained by

$$\mathcal{N}_{(q,k,\lambda)} = \begin{cases} 0 & \text{if } \gcd(\frac{\Delta}{2}, \frac{q-1}{\lambda}) > 2 \\ \frac{2\lambda\phi(\frac{\Delta}{4})}{\gcd(\lambda,2)k} & \text{otherwise} \end{cases},$$

where ϕ denotes here the well-known Euler ϕ-function.

Some examples

The following examples are direct applications of Theorem 3.

Example 2 If $q = 7$, $k = 2$ and $\lambda = 3$, then $\Delta = 8$.

Some examples

The following examples are direct applications of Theorem 3.

Example 2 If $q = 7$, $k = 2$ and $\lambda = 3$, then $\Delta = 8$. Therefore, by Theorem 3, $\mathcal{N}_{(7,2,3)} = 3$.

Some examples

The following examples are direct applications of Theorem 3.

Example 2 If $q = 7$, $k = 2$ and $\lambda = 3$, then $\Delta = 8$. Therefore, by Theorem 3, $\mathcal{N}_{(7,2,3)} = 3$. In fact, if $q = 7$, $k = 2$ and $\lambda = 3$, then the family of cyclic codes $\mathcal{C}_{(a_1,a_2)}$ described by Theorem 2, are the 3 cyclic codes

$$\mathcal{C}_{(2,26)}, \ \mathcal{C}_{(6,30)} \text{ and } \mathcal{C}_{(10,34)}.$$

Some examples

The following examples are direct applications of Theorem 3.

Example 2 If $q = 7$, $k = 2$ and $\lambda = 3$, then $\Delta = 8$. Therefore, by Theorem 3, $\mathcal{N}_{(7,2,3)} = 3$. In fact, if $q = 7$, $k = 2$ and $\lambda = 3$, then the family of cyclic codes $\mathcal{C}_{(a_1,a_2)}$ described by Theorem 2, are the 3 cyclic codes

$$\mathcal{C}_{(2,26)}, \mathcal{C}_{(6,30)} \text{ and } \mathcal{C}_{(10,34)}.$$

Furthermore, these 3 codes are 4-weight non-projective cyclic codes, over $\mathbb{F}_7$, of length 24, dimension 4 and weight enumerator polynomial

$$A(z) = 1 + 24z^6 + 216z^{12} + 864z^{18} + 1296z^{24}.$$

Some examples

The following examples are direct applications of Theorem 3.

Example 2 If $q = 7$, $k = 2$ and $\lambda = 3$, then $\Delta = 8$. Therefore, by Theorem 3, $\mathcal{N}_{(7,2,3)} = 3$. In fact, if $q = 7$, $k = 2$ and $\lambda = 3$, then the family of cyclic codes $\mathcal{C}_{(a_1,a_2)}$ described by Theorem 2, are the 3 cyclic codes

$$\mathcal{C}_{(2,26)}, \mathcal{C}_{(6,30)} \text{ and } \mathcal{C}_{(10,34)}.$$

Furthermore, these 3 codes are 4-weight non-projective cyclic codes, over $\mathbb{F}_7$, of length 24, dimension 4 and weight enumerator polynomial

$$A(z) = 1 + 24z^6 + 216z^{12} + 864z^{18} + 1296z^{24}.$$

Example 3 If $q = 11$, $k = 2$ and $\lambda = 10$, then $\Delta = 12$.

Some examples

The following examples are direct applications of Theorem 3.

Example 2 If $q = 7$, $k = 2$ and $\lambda = 3$, then $\Delta = 8$. Therefore, by Theorem 3, $\mathcal{N}_{(7,2,3)} = 3$. In fact, if $q = 7$, $k = 2$ and $\lambda = 3$, then the family of cyclic codes $\mathcal{C}_{(a_1,a_2)}$ described by Theorem 2, are the 3 cyclic codes

$$\mathcal{C}_{(2,26)}, \mathcal{C}_{(6,30)} \text{ and } \mathcal{C}_{(10,34)}.$$

Furthermore, these 3 codes are 4-weight non-projective cyclic codes, over $\mathbb{F}_7$, of length 24, dimension 4 and weight enumerator polynomial

$$A(z) = 1 + 24z^6 + 216z^{12} + 864z^{18} + 1296z^{24}.$$

Example 3 If $q = 11$, $k = 2$ and $\lambda = 10$, then $\Delta = 12$. Therefore, by Theorem 3, $\mathcal{N}_{(11,2,10)} = 10$.

Some examples

The following examples are direct applications of Theorem 3.

Example 2 If $q = 7$, $k = 2$ and $\lambda = 3$, then $\Delta = 8$. Therefore, by Theorem 3, $\mathcal{N}_{(7,2,3)} = 3$. In fact, if $q = 7$, $k = 2$ and $\lambda = 3$, then the family of cyclic codes $\mathcal{C}_{(a_1,a_2)}$ described by Theorem 2, are the 3 cyclic codes

$$\mathcal{C}_{(2,26)},\ \mathcal{C}_{(6,30)} \text{ and } \mathcal{C}_{(10,34)}.$$

Furthermore, these 3 codes are 4-weight non-projective cyclic codes, over $\mathbb{F}_7$, of length 24, dimension 4 and weight enumerator polynomial

$$A(z) = 1 + 24z^6 + 216z^{12} + 864z^{18} + 1296z^{24}.$$

Example 3 If $q = 11$, $k = 2$ and $\lambda = 10$, then $\Delta = 12$. Therefore, by Theorem 3, $\mathcal{N}_{(11,2,10)} = 10$. In fact, these ten codes are 5-weight non-projective cyclic codes, over $\mathbb{F}_{11}$, of length 120, dimension 4 and weight enumerator polynomial

$$A(z) = 1 + 60z^{40} + 180z^{60} + 900z^{80} + 5400z^{100} + 8100z^{120}.$$

Thank you very much!