EXPLICIT EVALUATION OF SOME EXPONENTIAL SUMS

MARKO MOISIO

ABSTRACT. Let m be a positive integer, let r be a prime such that 2 is a primitive root modulo r^m, and let $q = 2^{(r-1)r^{m-1}}$. In this note a binomial exponential sum over $\mathbb{F}_q$ which assumes $\frac{3}{2}\log_2 q + 2$ distinct values is explicitly evaluated and its value distribution is determined.

1. INTRODUCTION

Let m be a positive integer, and let r be a prime such that 2 is a primitive root modulo r^m. Let $q = 2^{\phi(r^m)}$, where ϕ is the Euler function. Let $a, b \in \mathbb{F}_q$, and let γ be a primitive element of $\mathbb{F}_q$. Let χ be the canonical additive character of $\mathbb{F}_q$. In this note we shall explicitly evaluate sum

$$S(a,b) := \sum_{x \in \mathbb{F}^*} \chi(ax^{\frac{q-1}{r^m}} + bx)$$

(see Theorems 1 and 7), and moreover, determine its value distribution (see Theorems 3 and 8, and Examples 4 and 9). As an application, the weight distribution of the dual of a cyclic code of length $q-1$ with defining zeros γ and $\gamma^{(q-1)/r^m}$ is given (see Corollary 10 and Example 11).

The evaluation of an exponential sum over a finite field is a very hard problem in general, and it has been achieved only in certain special cases (see e.g. [1, 2, 3, 4, 10, 8, 6]). A common feature for the sums for which the evaluation has been succeeded seems to be that they attain only a few distinct values. Here we shall see that $S(a,b)$ assumes $3\phi(r^m)/2 + 2$ distinct values.

2. EVALUATION OF $S(a,0)$

Let r,m, $q = 2^{\phi(r^m)}$, χ and γ be as in the introduction. Let Tr be the trace function from $\mathbb{F}_q$ onto $\mathbb{F}_2$, and let $\alpha = \gamma^{\frac{q-1}{r^m}}$.

Date: December 19, 2008.

Key words and phrases. Cyclotomic polynomial; Cyclic code; Exponential sum; Weight distribution.

Let $a \in \mathbb{F}_q$ and consider sum

$$S(a,0) = \tfrac{q-1}{r^m} S(a),$$

where

$$S(a) = \sum_{i=0}^{r^m-1} \chi(a\alpha^i).$$

We observe that $\mathbb{F}_q = \mathbb{F}_2(\alpha)$ since 2 is a primitive root modulo r^m, and express a in basis $\{\alpha, \alpha^2, \ldots, \alpha^{\phi(r^m)}\}$, say

$$a = \sum_{j=1}^{(r-1)r^{m-1}} a_j \alpha^j,$$

where $a_j \in \mathbb{F}_2$ for all $j = 1, \ldots, (r-1)r^{m-1}$.

For $i = 0, \ldots, r^{m-1}-1$ we denote by $\mathbf{a}^{(i)}$ the following subvector of length $r-1$ of the coordinate vector $\mathbf{a} = (a_1, \ldots, a_{\phi(r^m)})$ of a:

$$\mathbf{a}^{(i)} = (a_{r^{m-1}-i}, a_{2r^{m-1}-i}, \ldots, a_{(r-1)r^{m-1}-i}).$$

Let $\mathrm{wt}(\mathbf{x})$ denote the Hamming weight of a binary vector $\mathbf{x}$.

Theorem 1. *Let $a \in \mathbb{F}_q$. Then,*

$$S(a) = \sum_{i=0}^{r^{m-1}-1} (-1)^{\mathrm{wt}(\mathbf{a}^{(i)})} \big(r - 2\mathrm{wt}(\mathbf{a}^{(i)})\big).$$

Moreover, there exists $b \in \mathbb{F}_q$ such that each subvector $\mathbf{b}^{(i)}$ is of even weight and $S(a) = r^m - 2\mathrm{wt}(\mathbf{b})$.

The following simple lemma is key in proving Theorem 1.

Lemma 2. *Let i be an integer. Then,*

$$\mathrm{Tr}(\alpha^i) = \begin{cases} 1 & \text{if } r^{m-1} \mid i \text{ and } r^m \nmid i, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If $r^m \mid i$, then $\alpha^i = 1$ and $\mathrm{Tr}(1) = \phi(r^m) \cdot 1 = 0$. Let $i = r^s i'$ where $0 \le s \le m-1$ and $r \nmid i'$. Obviously, α^i is a primitive r^{m-s}th root of unity. Moreover, since 2 is a primitive root modulo r^{m-s} for all $s = 0, \ldots, m-1$, the degree of α^i over $\mathbb{F}_2$ is $\phi(r^{m-s})$, and therefore the minimal polynomial of α^i over $\mathbb{F}_2$ is the r^{m-s}th cyclotomic polynomial $Q_{r^{m-s}}(x) = 1 + x^{r^{m-s-1}} + \cdots + x^{(r-2)r^{m-s-1}} + x^{(r-1)r^{m-s-1}}$ (see e.g. [9, p.65]).

Hence, the coefficient c of the monomial of second highest degree in $Q_{r^{m-s}}(x)$ equals 1, if $s = m-1$, and otherwise $c = 0$. By the transitivity of traces we now get $\mathrm{Tr}(\alpha^i) = \frac{\phi(r^m)}{\phi(r^{m-s})} \cdot c = r^s \cdot c = c$, which completes the proof. □

Proof of Theorem 1. By using the partition $\langle\alpha\rangle = \bigcup_{i=0}^{r^{m-1}-1} \alpha^i \langle \alpha^{r^{m-1}} \rangle$ we can write $S(a)$ in the form

$$S(a) = \sum_{t=0}^{r-1} \sum_{i=0}^{r^{m-1}-1} \chi(a\alpha^{i+tr^{m-1}}) = \sum_{t=0}^{r-1} \sum_{i=0}^{r^{m-1}-1} (-1)^{\mathrm{Tr}(a\alpha^{i+tr^{m-1}})}.$$

Here

$$\mathrm{Tr}(a\alpha^{i+tr^{m-1}}) = \sum_{j=1}^{r^m - r^{m-1}} a_j \,\mathrm{Tr}(\alpha^{j+i+tr^{m-1}}),$$

and $r^{m-1} \mid (j+i+tr^{m-1})$ if and only if $j = kr^{m-1} - i$, where $1 \le k \le r-1$. Moreover, since $1 \le j+i+tr^{m-1} < 2r^m$, we see that $r^m \mid (j+i+tr^{m-1})$ if and only if $j+i+tr^{m-1} = r^m$ if and only if $j = (r-t)r^{m-1} - i$. Hence, $r^m \mid (j+i+tr^{m-1})$ if and only if $1 \le r-t \le r-1$ if and only if $1 \le t \le r-1$. It now follows from Lemma 2, that

$$\mathrm{Tr}(a\alpha^{i+tr^{m-1}}) = \sum_{k=1}^{r-1} a_{kr^{m-1}-i} - \epsilon,$$

where $\epsilon = 0$ if $t = 0$, and otherwise $\epsilon = a_{(r-t)r^{m-1}-i}$.

Let $F(x) = (-1)^x$. Now,

$$\begin{aligned} S(a) &= \sum_{i=0}^{r^{m-1}-1} F\left(\sum_{k=1}^{r-1} a_{kr^{m-1}-i}\right) + \sum_{t=1}^{r-1} \sum_{i=0}^{r^{m-1}-1} F\left(\sum_{k=1}^{r-1} a_{kr^{m-1}-i} + a_{(r-t)r^{m-1}-i}\right) \\ &= \sum_{i=0}^{r^{m-1}-1} F\left(\sum_{k=1}^{r-1} a_{kr^{m-1}-i}\right) + \sum_{i=0}^{r^{m-1}-1} F\left(\sum_{k=1}^{r-1} a_{kr^{m-1}-i}\right) \sum_{t=1}^{r-1} F(a_{(r-t)r^{m-1}-i}). \end{aligned}$$

Here

$$F\left(\sum_{k=1}^{r-1} a_{kr^{m-1}-i}\right) = (-1)^{\mathrm{wt}(\mathbf{a}^{(i)})}$$

and

$$\sum_{t=1}^{r-1} F(a_{(r-t)r^{m-1}-i}) = r - 1 - 2\mathrm{wt}(\mathbf{a}^{(i)}),$$

and therefore

$$S(a) = r\sum_{i=0}^{r^{m-1}-1}(-1)^{\mathrm{wt}(\mathbf{a}^{(i)})} - 2\sum_{i=0}^{r^{m-1}-1}(-1)^{\mathrm{wt}(\mathbf{a}^{(i)})}\mathrm{wt}(\mathbf{a}^{(i)})$$
$$= \sum_{i=0}^{r^{m-1}-1}(-1)^{\mathrm{wt}(\mathbf{a}^{(i)})}(r - 2\mathrm{wt}(\mathbf{a}^{(i)})).$$

This proves the first assertion in Theorem 1.

For a proof of the second assertion we observe, that we may choose for each odd weight subvector $\mathbf{a}^{(i)}$ of $\mathbf{a}$ an element $\mathbf{b}^{(i)} \in \mathbb{F}_2^{r-1}$ such that $\mathrm{wt}(\mathbf{b}^{(i)}) = r - \mathrm{wt}(\mathbf{a}^{(i)})$. Now,

$$(-1)^{\mathrm{wt}(\mathbf{a}^{(i)})}\big(r - 2\mathrm{wt}(\mathbf{a}^{(i)})\big) = r - 2\mathrm{wt}(\mathbf{b}^{(i)}),$$

and therefore there exists $b \in \mathbb{F}_q$ such that

$$S(a) = \sum_{i=0}^{r^{m-1}-1}(r - 2\mathrm{wt}(\mathbf{b}^{(i)})) = r^m - 2\sum_{i=0}^{r^{m-1}-1}\mathrm{wt}(\mathbf{b}^{(i)}) = r^m - 2\mathrm{wt}(\mathbf{b}),$$

and the proof is complete. □

The method of replacing the odd weight subvectors with even weight subvectors, used in the proof of Theorem 1, can also be used in opposite direction to construct all the vectors $\mathbf{a}$ for which $S(a) = r^m - 4j$ for a fixed integer j, and this enables us to determine the value distribution of $S(a)$.

Theorem 3. *Let $t = r^{m-1}$. The value set of $S(a)$, as a runs over $\mathbb{F}_q^*$, is*

$$\{r^m - 4j \mid j = 1, \ldots, t(r-1)/2\}.$$

Moreover, for $j \in \{1, \ldots, t(r-1)/2\}$ the number of elements $a \in \mathbb{F}_q$ such that $S(a) = r^m - 4j$ is

$$\sum_{\substack{0\le i_1,\ldots,i_t\le\frac{r-1}{2}\\ i_1+\cdots+i_t=j}}\ \sum_{k=0}^{t}\ \sum_{\substack{1\le n_1<\cdots<n_k\le t\\ 1\le m_1<\cdots<m_{t-k}\le t}}\ \prod_{s=1}^{k}\binom{r-1}{r-2i_{n_s}}\prod_{v=1}^{t-k}\binom{r-1}{2i_{m_v}}, \tag{1}$$

where $n_s \neq m_v$ for all s, v. In particular, if $m = 1$, then each value $r - 4j$ is attained exactly $\binom{r}{2j}$ times.

If $k = 0$ or $k = t$, the most inner sum is defined to be $\prod_{v=1}^{t}\binom{r-1}{2i_{m_v}}$ or $\prod_{s=1}^{t}\binom{r-1}{r-2i_{n_s}}$, respectively.

Proof. Let $a \in \mathbb{F}_q^*$, and let $A := \{1, \ldots, r^{m-1}(r-1)/2\}$. By Theorem 1, $S(a) = r^m - 2\mathrm{wt}(\mathbf{b})$ for some $b \in \mathbb{F}_q$ consisting of even weight subvectors $\mathbf{b}^{(i)}$. It follows that $-r^m + 2r^{m-1} \leq S(a) \leq r^m - 4$, and therefore $S(a) = r^m - 4j$ for some $j \in A$.

On the other hand, for $j \in A$ we may write $2j = (r-1)s + k$, where s and k are non-negative integers with k even and $0 \leq k \leq r-3$. Therefore, for each number $2j$ with $j \in A$ there exists an element $b \in \mathbb{F}_q$ such that all its subvectors $\mathbf{b}^{(i)}$ are of even weight and $\mathrm{wt}(\mathbf{b}) = 2j$. Hence, the assertion concerning the value set is true.

Let $j \in A$, and let $(2i_1, 2i_2, \ldots, 2i_t)$ be a non-negative solution of $x_1 + x_2 + \cdots + x_t = 2j$. Let $a \in \mathbb{F}_q$ such that $\mathrm{wt}(\mathbf{a}^{(i_n)}) = 2i_n$ for $n = 1, \ldots, t$. Now, by replacing the subvectors $\mathbf{a}^{(i_{n_1})}, \ldots, \mathbf{a}^{(i_{n_k})}$ with vectors $\mathbf{b}_1, \ldots, \mathbf{b}_k \in \mathbb{F}_2^{r-1}$ satisfying $\mathrm{wt}(\mathbf{b}_s) = r - 2i_{n_s}$ for $s = 1, \ldots, k$, and by replacing $\mathbf{a}^{(i_{m_1})}, \ldots, \mathbf{a}^{(i_{m_{t-k}})}$ with vectors $\mathbf{b}'_1, \ldots, \mathbf{b}'_{t-k} \in \mathbb{F}_2^{r-1}$ satisfying $\mathrm{wt}(\mathbf{b}'_v) = 2i_{m_v}$ for $v = 1, \ldots, t-k$, we get exactly

$$\sum_{\substack{1 \leq n_1 < \cdots < n_k \leq t \\ 1 \leq m_1 < \cdots < m_{t-k} \leq t}} \prod_{s=1}^{k} \binom{r-1}{r-2i_{n_s}} \prod_{v=1}^{t-k} \binom{r-1}{2i_{m_v}}$$

vectors $\mathbf{a}$ such that exactly k of its subvectors $\mathbf{a}^{(i)}$ are of odd weight and $S(a) = r^m - 4j$. Here we note that there does not exist $\mathbf{b}_s \in \mathbb{F}_2^{r-1}$ with $\mathrm{wt}(\mathbf{b}_s) = r - 2i_{n_s}$ if and only if $i_{n_s} = 0$. But in this case $\binom{r-1}{r-2i_{n_s}} = 0$. Finally we observe that if $t = 1$, then (1) equals $\binom{r-1}{2j} + \binom{r-1}{r-2j} = \binom{r-1}{2j} + \binom{r-1}{2j-1} = \binom{r}{2j}$, which completes the proof. □

Example 4. Let $r = 3$. Now $t = 3^{m-1}$, and $i_1 + \cdots + i_t = j$ has exactly $\binom{t}{j}$ solutions with $0 \leq i_1, \ldots, i_t \leq 1$. For each such solution

$$\sum_{k=0}^{t} \sum_{\substack{1 \leq n_1 < \cdots < n_k \leq t \\ 1 \leq m_1 < \cdots < m_{t-k} \leq t}} \prod_{s=1}^{k} \binom{2}{3-2i_{n_s}} \prod_{v=1}^{t-k} \binom{2}{2i_{m_v}} = 1 + \sum_{k=1}^{j} \binom{j}{k} 2^k = 3^j,$$

and therefore the value set value set of $S(a)$ is $\{3^m - 4j \mid j = 1, \ldots, t\}$, and each value $3^m - 4j$ is attained exactly $\binom{t}{j} 3^j$ times.

Remark 5. Assume 2 is a primitive root modulo r. Then, 2 is a primitive root modulo r^m for all positive integers m, if $2^{r-1} \not\equiv 1 \ (r^2)$ (see e.g. [5, Thm. 2, p.43]). Moreover, the only primes p which are less than $3 \cdot 10^7$ and for which $2^{p-1} \equiv 1 \ (p^2)$ are $p = 1093, 3511$ (see [7, p.73]).

3. Evaluation of $S(a,b)$

Consider next $S(a,b)$ with $ab \neq 0$. Since 2 is a primitive root modulo r^m, r^m is a factor of $2^{\phi(r^m)/2}+1$. By choosing $s=1$, $d=\phi(r^m)/2$ and $n=r^m$ in [11, Thm.1], we get

Lemma 6. *Let $b \in \mathbb{F}_q^*$. Then*

$$\sum_{x\in\mathbb{F}_q^*} \chi(bx^{r^m}) = \begin{cases} (r^m-1)\sqrt{q}-1 & \text{if } b \in H, \\ -\sqrt{q}-1 & \text{if } b \notin H, \end{cases}$$

where H is the subgroup of $\mathbb{F}_q^*$ generated by γ^{r^m}.

We are now able to evaluate $S(a,b)$ in the case $ab \neq 0$.

Theorem 7. *Let $a,b \in \mathbb{F}_q^*$, and let $c = ab^{-\frac{q-1}{r^m}}$. Then,*

$$\sum_{x\in\mathbb{F}_q^*} \chi(ax^{\frac{q-1}{r^m}}+bx) = (-1)^{\mathrm{wt}(\mathbf{c}^{(0)})}\sqrt{q} - \tfrac{\sqrt{q}+1}{r^m}S(c),$$

where $S(c)$ is given in Theorem 1. In particular, if $m=1$, then

$$\sum_{x\in\mathbb{F}_q^*} \chi(ax^{\frac{q-1}{r}}+bx) = (-1)^{\mathrm{wt}(\mathbf{c})}\big(\sqrt{q} - \tfrac{\sqrt{q}+1}{r}(r-2\mathrm{wt}(\mathbf{c}))\big).$$

Proof. By using the partition $\mathbb{F}_q^* = \bigcup_{i=0}^{r^m-1}\gamma^i H$, we get

$$\begin{aligned} S(a,b) &= \sum_{x\in\mathbb{F}_q^*} \chi(cx^{\frac{q-1}{r^m}}+x) = \sum_{i=0}^{r^m-1}\chi(c\alpha^i)\sum_{x\in H}\chi(\gamma^i x) \\ &= \frac{1}{r^m}\sum_{i=0}^{r^m-1}\chi(c\alpha^i)\sum_{x\in\mathbb{F}_q^*}\chi(\gamma^i x^{r^m}), \end{aligned}$$

and now, by Lemma 6, we get

$$\begin{aligned} S(a,b) &= \frac{1}{r^m}\big(((r^m-1)\sqrt{q}-1)\chi(c) - (\sqrt{q}+1)\sum_{i=1}^{r^m-1}\chi(c\alpha^i)\big) \\ &= \frac{1}{r^m}\big(((r^m-1)\sqrt{q}-1)\chi(c) - (\sqrt{q}+1)(S(c)-\chi(c))\big) \\ &= (\sqrt{q}-\tfrac{\sqrt{q}+1}{r^m})\chi(c) - \tfrac{\sqrt{q}+1}{r^m}(S(c)-\chi(c)) \\ &= \chi(c)\sqrt{q} - \tfrac{\sqrt{q}+1}{r^m}S(c). \end{aligned}$$

By Lemma 2, $\mathrm{Tr}(c) = \sum_{i=1}^{r-1} c_{ir^{m-1}} = \mathrm{wt}(\mathbf{c}^{(0)})$, and the proof is complete. □

Theorem 8. *Let $t = r^{m-1}$. The value set of $S(a,b)$, as (a,b) runs over $(\mathbb{F}_q^*)^2$, is*

$$\{\pm\sqrt{q} - \tfrac{\sqrt{q}+1}{r^m}(r^m - 4j) \mid j = 1, \dots, t(r-1)/2\}.$$

Moreover, for $j \in \{1, \dots, t(r-1)/2\}$ the number of pairs $(a,b) \in (\mathbb{F}_q^*)^2$ such that $S(a,b) = \epsilon\sqrt{q} - \frac{\sqrt{q}+1}{r^m}(r^m - 4j)$ is

$$(q-1) \sum_{\substack{0 \le i_1, \dots, i_t \le \frac{r-1}{2} \\ i_1 + \cdots + i_t = j}} h_{i_1} \sum_{k=0}^{t-1} \sum_{\substack{2 \le n_1 < \cdots < n_k \le t \\ 2 \le m_1 < \cdots < m_{t-k-1} \le t}} \prod_{s=1}^{k} \binom{r-1}{r-2i_{n_s}} \prod_{v=1}^{t-k-1} \binom{r-1}{2i_{m_v}}, \tag{2}$$

where $n_s \neq m_v$ for all s, v, and $h_{i_1} = \binom{r-1}{2i_1}$ if $\epsilon = 1$, and $h_{i_1} = \binom{r-1}{r-2i_1}$ if $\epsilon = -1$.

If $k = 0$ or $k = t-1$, the most inner sum is defined to be $\prod_{v=1}^{t-1} \binom{r-1}{2i_{m_v}}$ or $\prod_{s=1}^{t-1} \binom{r-1}{r-2i_{n_s}}$, respectively.

Proof. By Theorems 3 and 1, for each number $r^m - 4j$ with $j \in A := \{1, \dots, r^{m-1}(r-1)/2\}$ there exists $c \in \mathbb{F}_q^*$ such that $S(c) = r^m - 4j$ and $\mathrm{wt}(\mathbf{c}^{(i)})$ is even for all $i = 0, \dots, t-1$. Since some of the subvectors of c is nonzero, we may assume that $\mathrm{wt}(\mathbf{c}^{(0)}) \neq 0$. Let $d \in \mathbb{F}_q$ satisfying $\mathrm{wt}(\mathbf{d}^{(0)}) = r - \mathrm{wt}(\mathbf{c}^{(0)})$ and $\mathrm{wt}(\mathbf{d}^{(i)}) = \mathrm{wt}(\mathbf{c}^{(i)})$ for all $1 \le i \le t-1$. Now, by Theorem 1, $S(c) = S(d)$ and therefore, by Theorem 7, $S(c,1) = \sqrt{q} - \frac{\sqrt{q}+1}{r^m}(r^m - 4j)$ and $S(d,1) = -\sqrt{q} - \frac{\sqrt{q}+1}{r^m}(r^m - 4j)$. This proves the assertion concerning the value set.

We observe that, for each $c \in \mathbb{F}_q^*$ there exist exactly $q-1$ pairs $(a,b) \in (\mathbb{F}_q^*)^2$ such that $ab^{-\frac{q-1}{r^m}} = c$. Let $j \in A$. For each non-negative solution $(2i_1, 2i_2, \dots, 2i_t)$ of $x_1 + x_2 + \cdots + x_t = 2j$ we can construct exactly

$$\binom{r-1}{2i_1} \sum_{k=0}^{t-1} \sum_{\substack{2 \le n_1 < \cdots < n_k \le t \\ 2 \le m_1 < \cdots < m_{t-k-1} \le t}} \prod_{s=1}^{k} \binom{r-1}{r-2i_{n_s}} \prod_{v=1}^{t-k-1} \binom{r-1}{2i_{m_v}}$$

vectors $\mathbf{c}$ such that $\mathrm{wt}(\mathbf{c}^{(0)})$ is even, exactly k of the subvectors $\mathbf{c}^{(i)}$, $i = 1, \dots, t-1$, are of odd weight, and $S(c) = r^m - 4j$. Hence the assertion concerning the number of pairs $(a,b) \in (\mathbb{F}_q^*)^2$ such that $S(a,b) = \sqrt{q} - \frac{\sqrt{q}+1}{r^m}(r^m - 4j)$ is true. The second case is proved similarly. □

Example 9. Let $r = 3$ and $m > 1$. Now $t = 3^{m-1}$, and $i_1 + \cdots + i_t = j$ has exactly $\binom{t-1}{j}$ or $\binom{t-1}{j-1}$ solutions with $0 \le i_1, \dots, i_t \le 1$, depending on whether $i_1 = 0$ or

$i_1 = 1$, respectively. For each such solution

$$\sum_{k=0}^{t-1} \sum_{\substack{2\le n_1<\cdots<n_k\le t \\ 2\le m_1<\cdots<m_{t-k-1}\le t}} \prod_{s=1}^{k} \binom{2}{3-2i_{n_s}} \prod_{v=1}^{t-k-1} \binom{2}{2i_{m_v}}$$

$$= \begin{cases} 1+\sum_{k=1}^{j}\binom{j}{k}2^k = 3^j & \text{if } i_1 = 0, \\ 1+\sum_{k=1}^{j-1}\binom{j-1}{k}2^k = 3^{j-1} & \text{if } i_1 = 1. \end{cases}$$

Hence, the value distribution of $S(a,b)$, as (a,b) runs over $(\mathbb{F}_q^*)^2$, is the following

value	frequency
$\sqrt{q} - \frac{\sqrt{q}+1}{3^m}(3^m - 4j)$	$(q-1)\left(\binom{t-1}{j}3^j + \binom{t-1}{j-1}3^{j-1}\right)$
$-\sqrt{q} - \frac{\sqrt{q}+1}{3^m}(3^m - 4j)$	$2(q-1)\binom{t-1}{j-1}3^{j-1}$

where j runs over the set $\{1,\dots,t\}$.

Corollary 10. *Let C be a binary cyclic $[2^{\phi(r^m)}-1, 2\phi(r^m)]$ code with defining zeros γ and $\gamma^{\frac{2^{\phi(r^m)}-1}{r^m}}$. The weight distribution of the dual of C is given in the following table, where $q = 2^{\phi(r^m)}$ and j runs over the set $\{1,2,\dots,\phi(r^m)/2\}$.*

weight	*frequency*
0	1
$q/2$	$q-1$
$\frac{1}{2}(q-1-\frac{q-1}{r^m}(r^m-4j))$	f_1
$\frac{1}{2}(q-1-\sqrt{q}+\frac{\sqrt{q}+1}{r^m}(r^m-4j))$	f_2
$\frac{1}{2}(q-1+\sqrt{q}+\frac{\sqrt{q}+1}{r^m}(r^m-4j))$	f_3

where f_1 is given by (1), f_2 is given by (2) with $h_{i_1} = \binom{r-1}{2i_1}$, and f_3 by (2) with $h_{i_1} = \binom{r-1}{r-2i_1}$.

Proof. The dual in question can be given as a trace code:

$$C^\perp = \{c(a,b) = (\mathrm{Tr}(a+b), \mathrm{Tr}(a\gamma^{\frac{q-1}{r^m}} + b\gamma), \dots, \mathrm{Tr}(a\gamma^{\frac{(q-1)(q-2)}{r^m}} + b\gamma^{q-2})) \mid a,b \in \mathbb{F}_q\}.$$

Hence, for $c(a,b) \in C^\perp$ we have

$$\mathrm{wt}(c(a,b)) = \tfrac{1}{2}\sum_{i=0}^{q-2}(1-(-1)^{\mathrm{Tr}(a\gamma^{\frac{q-1}{r^m}i}+b\gamma^i)}) = \tfrac{1}{2}(q-1-S(a,b)).$$

Since $S(0,0) = q-1$ and $S(0,b) = -1$ for all $b \in \mathbb{F}_q^*$, Theorems 3 and 8 now completes the proof. □

Example 11. If $m = 1$, the frequencies are

$$f_1 = \tbinom{r}{2j}, f_2 = (q-1)\tbinom{r-1}{2j}, \text{ and } f_3 = (q-1)\tbinom{r-1}{2j-1}.$$

If $r = 3$ and $m > 1$, then, by Examples 4 and 9, the frequencies are

$$f_1 = \binom{3^{m-1}}{j}3^j, f_2 = (q-1)\left(\binom{3^{m-1}-1}{j}3^j + \binom{3^{m-1}-1}{j-1}3^{j-1}\right),$$
$$f_3 = 2(q-1)\binom{3^{m-1}-1}{j-1}3^{j-1}.$$

References

[1] L. Carlitz, Explicit evaluation of certain exponential sums, Math. Scand. 44 (1979) 5–16.
[2] L. Carlitz, Evaluation of some exponential sums over a finite field, Math. Nachr. 96 (1980) 319–339.
[3] R.S. Coulter, Explicit evaluations of some Weil sums, Acta Arith. 83 (1998) 241–251.
[4] R.S. Coulter, On the evaluation of a class of Weil sums in characteristic 2, N.Z.J. Math. 28 (1999) 171–184.
[5] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, 1998.
[6] K. Feng, J. Luo, Weight distribution of some reducible cyclic codes, Finite Fields Appl. 14 (2008) 390–409
[7] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, 1995.
[8] X. Hou, Explicit evaluation of certain exponential sums of binary quadratic functions, Finite Fields Appl. 13 (2007) 843–868.
[9] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
[10] D. Mills, On the evaluation of Weil sums of Dembowski-Ostrom polynomials, J. Number Theory 92 (2002) 87–98.
[11] M. Moisio, A note on evaluations of some exponential sums, Acta Arith. 93 (2000) 117–119.

E-mail address: mamo@uwasa.fi

Department of Mathematics and Statistics, University of Vaasa, P.O. Box 700, FIN-65101 Vaasa, Finland