IRREDUCIBLE POLYNOMIALS WITH PRESCRIBED TRACE AND RESTRICTED NORM

K. KONONEN, M. MOISIO, M. RINTA-AHO, AND K. VÄÄNÄNEN

ABSTRACT. Let $\mathbb{F}_q$, $q = p^r$, be a finite field with a primitive element g. In this paper we use exponential sums and Jacobi sums to compute the number of the irreducible polynomials of degree m over $\mathbb{F}_q$ with trace fixed and norm restricted to a coset of a subgroup $\langle g^s \rangle$, $s \mid (q-1)$. We give the number explicitly for $s = 2$, 3, 4 when $q = p$, and for $s \mid (p^e + 1)$ when $r = 2en$. Finally, we give explicit formulae for the number when both trace and norm are fixed, $p = 2$ and $m \leq 30$.

1. INTRODUCTION

Let p be a prime number, $\mathbb{F}_q$ a finite field with $q = p^r$ elements, and g a primitive element of $\mathbb{F}_q$. The explicit enumeration of irreducible polynomials

$$f(x) = x^m - ax^{m-1} + \cdots + (-1)^m b \in \mathbb{F}_q[x]$$

with some preassigned coefficients fixed is quite hard problem in general and it has been tackled only in certain special cases. For example, Carlitz [4] and Yucas [18] obtained explicit formulae for the number of $f(x)$ with a or b fixed. Carlitz also obtained explicit formulae for the number of $f(x)$ with a fixed and b in a fixed coset of the group of squares in $\mathbb{F}_q^*$. Moisio [10] considered the enumeration problem when both a and b are fixed, and gave the number of $f(x)$ in terms of exponential sums and in terms of the number of rational points on certain algebraic varieties defined over $\mathbb{F}_q$. Especially, the number of irreducible cubic polynomials with a and b fixed was given in terms of cubic Gauss sums (case $a = 0$) and in terms of the number of rational points on the elliptic curves over $\mathbb{F}_q$ defined by $\mathcal{E} : y^2 + ba^{-3}y + xy = x^3$, which, in a way, indicates the hardness of the explicit enumeration problem. For results on the enumeration problem when some other coefficients than a and b are fixed we refer to the survey by Cohen [5], and to a recent work by Moisio and Ranto [11].

The aim of this paper is to generalize results of [4] by giving explicit formulae for the number of $f(x)$ with a fixed and b in a fixed coset of a subgroup $\langle g^s \rangle$. Actually, we shall do this in the following three special cases:

Key words and phrases. Irreducible polynomials; Monomial exponential sums; Gauss sums; Jacobi sums.

- $s = 2$ (Carlitz's case),
- $s = 3$,
- $s = 4$,
- $r = 2en$ and $s\,(>1)$ is any factor of $p^e + 1$.

Moreover, we shall give explicit formulae for the number of $f(x)$ with both a and b fixed under the assumptions $q = 2^r$ and $m \leq 30$.

The method used in this paper is essentially the one used in [10] but here explicit evaluation of Jacobi sums and certain exponential sums are used instead of the theory of algebraic varieties. We also note that our method is more elementary than the method used in [4] in the sense that the use of L-functions is avoided.

2. Notations and basic formulae

We fix the following notations.

p, q, r, s, h, m, t	positive integers, p prime, $q = p^r$, $s \mid (q-1)$, $h \in \{0, 1, \ldots, s-1\}$, $m \geq 2$, $t \mid m$
d, l	$d = \gcd(\frac{m}{t}, s)$, $l = \gcd(t, \frac{s}{d})$
Tr_t, Norm_t	the trace and norm from $\mathbb{F}_{q^t}$ onto $\mathbb{F}_q$
$\gamma = \gamma_m$	a fixed primitive element of $\mathbb{F}_{q^m}$
γ_t	the primitive element of $\mathbb{F}_{q^t}$ that is the norm of γ onto $\mathbb{F}_{q^t}$
g	$\mathrm{Norm}_m(\gamma_m)$, a primitive elment of $\mathbb{F}_q$; also $g = \gamma_1 = \mathrm{Norm}_t(\gamma_t)$
$P_m(a, s, h)$	the number of the irreducible polynomials $f(x) = x^m - ax^{m-1} + \cdots + (-1)^m b \in \mathbb{F}_q[x]$, where a is fixed and $b \in g^h\langle g^s\rangle \subseteq \mathbb{F}_q^*$
$S_t = S_t(a, s, h)$	the set of x in $\mathbb{F}_{q^t}$ with $\mathrm{Tr}_m(x) = a$ and $\mathrm{Norm}_m(x) \in g^h\langle g^s\rangle$
$T_t = T_t(a, s, h)$	the set of x in S_t with $x \notin \mathbb{F}_{q^k}$ for any $k < t$
N_t	the number of elements in S_t
e_t	the canonical additive character $e_t(x) = \mathsf{e}^{2\pi \mathrm{i}\,\mathrm{tr}_t(x)/p}$ of $\mathbb{F}_{q^t}$, where tr_t is the absolute trace $\mathbb{F}_{q^t} \to \mathbb{F}_p$

Note that $N_m = \sum_{t|m} |T_t|$ and the Möbius inversion gives, see [10, Lemma 1],

$$P_m(a, s, h) = \frac{1}{m} \sum_{t|m} \mu(\tfrac{m}{t}) N_t. \tag{1}$$

Thus the knowledge of N_t for $t \mid m$ gives $P_m(a, s, h)$, and therefore we consider N_t.

From the definition of S_t it follows that

$$x \in S_t \iff \tfrac{m}{t}\,\mathrm{Tr}_t(x) = a \text{ and } \mathrm{Norm}_t(x^{\frac{m}{t}}) \in g^h\langle g^s\rangle.$$

By denoting $x = \gamma_t^i$, $i \in \{0, 1, \dots, q^t - 2\}$, we see that the condition $\mathrm{Norm}_t(x^{m/t}) \in g^h\langle g^s\rangle$ is satisfied if and only if the congruence

$$\frac{m}{t} i \equiv h \pmod{s} \tag{2}$$

holds. If $d \nmid h$ then (2) has no solution, and if $d \mid h$ then (2) has solutions

$$i = i_0 + j\frac{s}{d}, \qquad j = 0,\, 1, \dots,\, \frac{d}{s}(q^t - 1) - 1, \tag{3}$$

where i_0 is the solution of

$$\frac{m}{dt} i_0 \equiv \frac{h}{d} \pmod{\frac{s}{d}}, \qquad 0 \le i_0 < \frac{s}{d}. \tag{4}$$

Thus we obtain

Lemma 1. *(i)* $N_t = 0$ *if* $d \nmid h$.
(ii) $N_t = 0$ *if* $p \mid \frac{m}{t}$ *and* $a \neq 0$.
(iii) $N_t = \frac{d}{s}(q^t - 1)$ *if* $p \mid \frac{m}{t}$, $d \mid h$ *and* $a = 0$.

In the remaining cases

$$p \nmid \tfrac{m}{t} \text{ and } d \mid h. \tag{5}$$

To state a formula for N_t in this case we use the canonical additive character e_t.

Lemma 2. *If (5) holds then*

$$N_t = \frac{d}{sq}(q^t - 1 + M_t),$$

where

$$M_t = \sum_{c \in \mathbb{F}_q^*} e_1(-\tfrac{t}{m} ca) \sum_{x \in \mathbb{F}_{q^t}^*} e_t(c\gamma_t^{i_0} x^{\frac{s}{d}}). \tag{6}$$

Proof. By the definition of S_t, equation (3) and the orthogonality of characters we obtain

$$\begin{aligned} qN_t &= \sum_{j=0}^{\frac{d}{s}(q^t-1)-1} \sum_{c \in \mathbb{F}_q} e_1\big(c(\mathrm{Tr}_t(\gamma_t^{i_0 + j\frac{s}{d}}) - \tfrac{t}{m} a)\big) \\ &= \sum_{c \in \mathbb{F}_q} e_1(-\tfrac{t}{m} ca) \sum_{j=0}^{\frac{d}{s}(q^t-1)-1} e_1\big(\mathrm{Tr}_t(c\gamma_t^{i_0 + j\frac{s}{d}})\big) \\ &= \sum_{c \in \mathbb{F}_q} e_1(-\tfrac{t}{m} ca) \sum_{j=0}^{\frac{d}{s}(q^t-1)-1} e_t(c\gamma_t^{i_0 + j\frac{s}{d}}) \\ &= \frac{d}{s} \sum_{c \in \mathbb{F}_q} e_1(-\tfrac{t}{m} ca) \sum_{x \in \mathbb{F}_{q^t}^*} e_t(c\gamma_t^{i_0} x^{\frac{s}{d}}). \end{aligned}$$

This proves Lemma 2. □

We shall now consider separately the cases $a = 0$ and $a \neq 0$. For this consideration let $n \mid (q-1)$ and let H_n denote the subgroup of order n of the multiplicative character group of $\mathbb{F}_q$ and $H_n^* = H_n \setminus \{\lambda_0\}$, where λ_0 is the trivial multiplicative character of $\mathbb{F}_q$. If λ is a multiplicative character of $\mathbb{F}_q$, then $\lambda \circ \mathrm{Norm}_t$ is a multiplicative character of $\mathbb{F}_{q^t}$. We define the Gauss sum $G_t(\lambda)$ over $\mathbb{F}_{q^t}$ as follows:

$$G_t(\lambda) = \sum_{x \in \mathbb{F}_{q^t}^*} e_t(x)(\lambda \circ \mathrm{Norm}_t)(x).$$

The following Lemma 4 of [10] gives a connection of these sums with monomial exponential sums.

Lemma 3. *Let n be a positive factor of $q-1$ and let $\alpha \in \mathbb{F}_{q^t}^*$. Then*

$$\sum_{x \in \mathbb{F}_{q^t}^*} e_t(\alpha x^n) = \sum_{\lambda \in H_n} G_t(\bar{\lambda})(\lambda \circ \mathrm{Norm}_t)(\alpha),$$

where $\bar{\lambda} = \lambda^{-1}$.

3. Case $a = 0$

Assume in this section that $a = 0$. Then M_t in (6) has the following expressions.

Lemma 4. *Assume that (5) holds and $a = 0$. Then*

$$M_t = (q-1) \sum_{x \in \mathbb{F}_{q^t}^*} e_t(\gamma_t^{i_0} x^l) = (q-1) \sum_{\lambda \in H_l} G_t(\bar{\lambda}) \lambda(g^{i_0}),$$

where $l = \gcd(t, \frac{s}{d})$ is defined at the beginning of Section 2.

Proof. The claimed formulae for M_t are equal by Lemma 3 (recall that $\mathrm{Norm}_t(\gamma_t) = g$). Substituting $a = 0$ into (6) we get by Lemma 3

$$\begin{aligned} M_t &= \sum_{c \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_{q^t}^*} e_t(c\gamma_t^{i_0} x^{\frac{s}{d}}) = \sum_{c \in \mathbb{F}_q^*} \sum_{\lambda \in H_{s/d}} G_t(\bar{\lambda}) \lambda(\mathrm{Norm}_t(c\gamma_t^{i_0})) \\ &= \sum_{\lambda \in H_{s/d}} G_t(\bar{\lambda}) \lambda(g^{i_0}) \sum_{c \in \mathbb{F}_q^*} \lambda(c^t). \end{aligned} \tag{7}$$

Setting $n = \gcd(q-1, t)$ we have

$$\sum_{c \in \mathbb{F}_q^*} \lambda(c^t) = \sum_{c \in \mathbb{F}_q^*} \lambda^n(c) = \begin{cases} 0 & \text{if } \lambda^n \neq \lambda_0, \\ q-1 & \text{if } \lambda^n = \lambda_0. \end{cases}$$

Since $\lambda \in H_{s/d}$ in (7), the condition $\lambda^n = \lambda_0$ is equivalent to $\lambda \in H_n \cap H_{s/d} = H_l$, and the lemma follows. □

Furthermore, we present M_t in terms of (a special class of) Jacobi sums

$$J_t(\lambda) = \sum_{\substack{x_1,\dots,x_t\in\mathbb{F}_q\\ x_1+\cdots+x_t=1}} \lambda(x_1\cdots x_t),$$

where λ is a multiplicative character of $\mathbb{F}_q$ and, as usual, we define $\lambda(0)=0$, if $\lambda\neq\lambda_0$, and $\lambda_0(0)=1$.

Lemma 5. *Assume that (5) holds and $a=0$. Then*

$$M_t = (q-1)\Big(-1+(-1)^t q\sum_{\lambda\in H_l^*} J_t(\lambda)\bar{\lambda}(g^{i_0})\Big),$$

where $l=\gcd(t,\frac{s}{d})$.

Proof. In Lemma 4 $G_t(\overline{\lambda_0})\lambda_0(g^{i_0})=-1$. For $\lambda\neq\lambda_0$, the Davenport-Hasse identity (see e.g. [7, Theorem 5.14]) gives $G_t(\lambda)=(-1)^{t-1}G_1(\lambda)^t$ and [3, Theorem 10.3.1] gives $G_1(\lambda)^t=-qJ_t(\lambda)$ since $l\mid t$. □

As we shall see, Lemmas 4 and 5 give M_t explicitly in many cases.

4. Case $a\neq 0$

The result corresponding to Lemmas 4 and 5 is for $a\neq 0$ the following lemma.

Lemma 6. *Assume that (5) holds and $a\neq 0$. Then*

$$\begin{aligned} M_t &= \sum_{\lambda\in H_{s/d}} G_t(\bar{\lambda})G_1(\lambda^t)\lambda(a_0^t g^{i_0})\\ &= 1+(-1)^{t-1}q\sum_{\lambda\in H_{s/d}^*} J_t(\bar{\lambda})\lambda((-a_0)^t g^{i_0}), \end{aligned}$$

where $a_0=-\frac{m}{ta}$.

Proof. Substituting $c\mapsto -\frac{mc}{ta}=a_0c$ into (6) we get by Lemma 3 and the Davenport-Hasse identity

$$\begin{aligned} M_t &= \sum_{c\in\mathbb{F}_q^*} e_1(c)\sum_{\lambda\in H_{s/d}} G_t(\bar{\lambda})\lambda(\mathrm{Norm}_t(a_0c\gamma_t^{i_0}))\\ &= \sum_{c\in\mathbb{F}_q^*} e_1(c)\sum_{\lambda\in H_{s/d}} G_t(\bar{\lambda})\lambda(a_0^t c^t g^{i_0})\\ &= \sum_{\lambda\in H_{s/d}} G_t(\bar{\lambda})\lambda(a_0^t g^{i_0})\sum_{c\in\mathbb{F}_q^*} e_1(c)\lambda^t(c)\\ &= (-1)^{t-1}\sum_{\lambda\in H_{s/d}} G_1(\bar{\lambda})^t G_1(\lambda^t)\lambda(a_0^t g^{i_0})\\ &= 1+(-1)^{t-1}\sum_{\lambda\in H_{s/d}^*} G_1(\bar{\lambda})^t G_1(\lambda^t)\lambda(a_0^t g^{i_0}). \end{aligned}$$

Thus

$$(-1)^{t-1}(M_t-1)=\sum_{\lambda\in H_l^*}G_1(\bar{\lambda})^tG_1(\lambda^t)\lambda(a_0^tg^{i_0})\\ +\sum_{\lambda\in H_{s/d}^*\setminus H_l^*}G_1(\bar{\lambda})^tG_1(\lambda^t)\lambda(a_0^tg^{i_0}). \tag{8}$$

By Theorems 10.3.1 and 1.1.4 (b) of [3],

$$G_1(\bar{\lambda})^t=\begin{cases}-qJ_t(\bar{\lambda}) & \text{if } \lambda^t=\lambda_0,\\ \lambda((-1)^t)J_t(\bar{\lambda})\overline{G_1(\lambda^t)} & \text{if } \lambda^t\neq\lambda_0.\end{cases}$$

For $\lambda\in H_l\subseteq H_t$, $G_1(\lambda^t)=-1$ and $\lambda((-1)^t)=1$. Hence in (8)

$$\sum_{\lambda\in H_l^*}G_1(\bar{\lambda})^tG_1(\lambda^t)\lambda(a_0^tg^{i_0})=q\sum_{\lambda\in H_l^*}J_t(\bar{\lambda})\lambda((-a_0)^tg^{i_0}). \tag{9}$$

For $\lambda\in H_{s/d}^*\setminus H_l^*$, $\overline{G_1(\lambda^t)}G_1(\lambda^t)=|G_1(\lambda^t)|^2=q$ and in (8)

$$\sum_{\lambda\in H_{s/d}^*\setminus H_l^*}G_1(\bar{\lambda})^tG_1(\lambda^t)\lambda(a_0^tg^{i_0})=q\sum_{\lambda\in H_{s/d}^*\setminus H_l^*}J_t(\bar{\lambda})\lambda((-a_0)^tg^{i_0})\\ =q\Big(\sum_{\lambda\in H_{s/d}^*}J_t(\bar{\lambda})\lambda((-a_0)^tg^{i_0})-\sum_{\lambda\in H_l^*}J_t(\bar{\lambda})\lambda((-a_0)^tg^{i_0})\Big).$$

Combining this with (8) and (9) we obtain the lemma. □

In some cases we are able to compute monomial sums $\sum_{x\in\mathbb{F}_{q^t}^*}e_t(\alpha x^n)$ explicitly. In such cases Lemma 4 is useful for $a=0$. The following lemma gives similar formula for $a\neq 0$.

Lemma 7. *Assume that (5) holds and $a\neq 0$. Then*

$$M_t=\frac{1}{u}\sum_{j=0}^{u-1}\Big(\sum_{x\in\mathbb{F}_{q^t}^*}e_t\big(a_0\gamma_t^{t_0j+i_0}x^{\frac{s}{d}}\big)\Big)\Big(\sum_{c\in\mathbb{F}_q^*}e_1(g^jc^u)\Big),$$

where $a_0=-\frac{m}{ta}$, $t_0=\frac{q^t-1}{q-1}$, and $u=\frac{s}{dl}$ with $l=\gcd(t,\frac{s}{d})=\gcd(t_0,\frac{s}{d})$.

Proof. First we observe that $t_0=(q-1)(q^{t-2}+2q^{t-3}+\cdots+(t-2)q+t-1)+t$ and therefore $l=\gcd(t_0,\frac{s}{d})$.

Substituting $c\mapsto a_0c$ and noting that $g=\gamma_t^{t_0}$, (6) transforms into

$$M_t=\sum_{c\in\mathbb{F}_q^*}e_1(c)\sum_{x\in\mathbb{F}_{q^t}^*}e_t(a_0c\gamma_t^{i_0}x^{\frac{s}{d}})=\sum_{i=0}^{q-2}e_1(\gamma_t^{t_0i})\sum_{x\in\mathbb{F}_{q^t}^*}e_t(a_0\gamma_t^{t_0i+i_0}x^{\frac{s}{d}}).$$

By the partitition $\langle\gamma_t^{t_0}\rangle=\bigcup_{j=0}^{u-1}\gamma_t^{t_0j}\langle\gamma_t^{t_0u}\rangle$ each element in $\langle\gamma_t^{t_0}\rangle$ can be written in the form $\gamma_t^{t_0j}\gamma_t^{t_0uk}$ with $j\in\{0,\dots,u-1\}$ and $k\in$

$\{0,\dots,\frac{q-1}{u}-1\}$. Thus,

$$\begin{aligned}\sum_{x\in\mathbb{F}_{q^t}^*} e_t(a_0\gamma_t^{t_0 i+i_0}x^{\frac{s}{d}}) &= \sum_{x\in\mathbb{F}_{q^t}^*} e_t(a_0\gamma_t^{t_0 j+i_0}(\gamma_t^{kt_0/l}x)^{\frac{s}{d}})\\ &= \sum_{x\in\mathbb{F}_{q^t}^*} e_t(a_0\gamma_t^{t_0 j+i_0}x^{\frac{s}{d}}),\end{aligned}$$

and consequently

$$M_t = \sum_{j=0}^{u-1}\sum_{x\in\mathbb{F}_{q^t}^*} e_t(a_0\gamma_t^{t_0 j+i_0}x^{\frac{s}{d}}) \sum_{k=0}^{\frac{q-1}{u}-1} e_1(\gamma_t^{t_0 j}\gamma_t^{t_0 uk}).$$

Here the inner sum equals

$$\frac{1}{u}\sum_{k=0}^{q-2} e_1(g^j g^{ku}) = \frac{1}{u}\sum_{c\in\mathbb{F}_q^*} e_1(g^j c^u),$$

and the proof is complete. □

5. Number of polynomials in certain special cases

In this section we consider some special cases when M_t, and hence $P_m(a,s,h)$, can be given expicitly. One case is that s is small. Then λ in the summations of Lemmas 5 and 6 has small order. The Jacobi sums for characters of several small orders have been computed explicitly in [3].

Another classes when M_t can be computed explicitly (or up to two choices) are the semiprimitive and index 2 cases for $p=2$ (see Subsection 5.5, p. 16, for definitions). In these cases the monomial sums, or at least their value distribution, in Lemmas 4 and 7 can be evaluated.

We shall consider several small s and semiprimitive and index 2 cases in the following subsections.

5.1. Case $s=2$ (Carlitz's case).

The case $s=2$ was studied already by Carlitz in [4]. Now $b\in g^h\langle g^2\rangle$ and $h=0$ or 1 according to whether b is a square or a non-square in $\mathbb{F}_q^*$. In addition, p must be odd since $2\mid(q-1)$. We have now three possibilities for d and l:

$$(d,l) = \begin{cases}(1,1) & \text{if } 2\nmid\frac{m}{t},\ 2\nmid t,\\ (1,2) & \text{if } 2\nmid\frac{m}{t},\ 2\mid t,\\ (2,1) & \text{if } 2\mid\frac{m}{t}.\end{cases}$$

Let us now compute M_t and N_t assuming (5). For other cases, N_t can be computed with Lemma 1. After computing M_t the N_t is obtained from Lemma 2, see Theorem 1 below.

If $(d,l)=(1,1)$ then $i_0=h$ in (4). For $a=0$ we have by Lemma 4

$$M_t=(q-1)\sum_{x\in\mathbb{F}_{q^t}^*}e_t(\gamma_t^h x)=1-q.$$

For $a\neq 0$, let ρ be the multiplicative character of order 2 of $\mathbb{F}_q$. Then $\bar{\rho}=\rho$ and $\rho(g^h)=(-1)^h$. Further,

$$J_t(\rho)=\begin{cases}-\rho((-1)^{\frac{t}{2}})q^{\frac{t-2}{2}} & \text{if } t \text{ is even},\\ \rho((-1)^{\frac{t-1}{2}})q^{\frac{t-1}{2}} & \text{if } t \text{ is odd},\end{cases} \tag{10}$$

by [3, Theorem 10.2.2]. As now t is odd, Lemma 6 and (10) give

$$\begin{aligned}M_t&=1+qJ_t(\rho)\rho((-a_0)^t g^h)=1+q\rho((-1)^{\frac{t-1}{2}})q^{\frac{t-1}{2}}\rho((\tfrac{m}{ta})^t g^h)\\&=1+(-1)^h q^{\frac{t+1}{2}}\rho\big((-1)^{\frac{t-1}{2}}\tfrac{m}{ta}\big).\end{aligned}$$

If $(d,l)=(1,2)$ then again $i_0=h$ in (4). Now t is even, so Lemma 5 and (10) give for $a=0$

$$\begin{aligned}M_t&=(q-1)(-1+qJ_t(\rho)\rho(g^h))\\&=(q-1)\big(-1-q\rho((-1)^{\frac{t}{2}})q^{\frac{t-2}{2}}(-1)^h\big)\\&=(q-1)\big(-1-(-1)^h q^{\frac{t}{2}}\rho((-1)^{\frac{t}{2}})\big).\end{aligned}$$

For $a\neq 0$ we get by Lemma 6 and (10)

$$\begin{aligned}M_t&=1-qJ_t(\rho)\rho((-a_0)^t g^h)=1+q\rho((-1)^{\frac{t}{2}})q^{\frac{t-2}{2}}(-1)^h\\&=1+(-1)^h\rho((-1)^{\frac{t}{2}})q^{\frac{t}{2}}.\end{aligned}$$

If $(d,l)=(2,1)$ then (5) can hold only if $h=0$ ($N_t=0$ for $h=1$ by Lemma 1). By Lemmas 4 and 6, $M_t=1-q$ for $a=0$ and $M_t=1$ for $a\neq 0$. Lemma 2 now gives the following theorem.

Theorem 1. *The values of N_t for $s=2$ and assuming (5) are those listed in Table 1.*

TABLE 1: Values of N_t for $s=2$ assuming (5).

a	N_t	(d,l)
$a=0$	$\frac{1}{2}(q^{t-1}-1)$	$(1,1)$
	$\frac{1}{2}\big(q^{t-1}-1-(q-1)(-1)^h q^{\frac{t-2}{2}}\rho((-1)^{\frac{t}{2}})\big)$	$(1,2)$
	$q^{t-1}-1$	$(2,1)$
$a\neq 0$	$\frac{1}{2}\big(q^{t-1}+(-1)^h q^{\frac{t-1}{2}}\rho\big((-1)^{\frac{t-1}{2}}\frac{m}{ta}\big)\big)$	$(1,1)$
	$\frac{1}{2}\big(q^{t-1}+(-1)^h q^{\frac{t-2}{2}}\rho((-1)^{\frac{t}{2}})\big)$	$(1,2)$
	q^{t-1}	$(2,1)$

Equation (1) now gives $P_m(a,2,h)$ explicitly when the structure of the factorization of m is known. In particular, if $m>2$ is prime then

$P_m(a,2,h) = \frac{1}{m}(N_m - N_1)$, and $d = l = 1$ for both $t = 1$, m. First, from Table 1, $N_m = \frac{1}{2}(q^{m-1} - 1)$ for $a = 0$ and

$$N_m = \tfrac{1}{2}\big(q^{m-1} + (-1)^h q^{\frac{m-1}{2}} \rho((-1)^{\frac{m-1}{2}} a)\big)$$

for $a \neq 0$. If $m = p$ then by Lemma 1 $N_1 = \frac{q-1}{2}$ for $a = 0$ and $N_1 = 0$ for $a \neq 0$. If $m \neq p$ then Table 1 yields $N_1 = 0$ for $a = 0$ and $N_1 = \frac{1}{2}\big(1 + (-1)^h \rho(ma)\big)$ for $a \neq 0$. Combining these we obtain

$$P_m(0,2,h) = \begin{cases} \frac{1}{2p}(q^{p-1} - q) & \text{if } m = p, \\ \frac{1}{2m}(q^{m-1} - 1) & \text{if } m \neq p, \end{cases}$$

and, for $a \neq 0$,

$$P_m(a,2,h) = \begin{cases} \frac{1}{2p}(q^{p-1} + S) & \text{if } m = p. \\ \frac{1}{2m}(q^{m-1} + S - (-1)^h \rho(ma) - 1) & \text{if } m \neq p, \end{cases}$$

where $S = (-1)^h q^{\frac{m-1}{2}} \rho((-1)^{\frac{m-1}{2}} a)$. These results are in accordance with [4, eqs. (5.8) and (5.9)].

5.2. **Case $s = 4 = 2^2$.** For $s = 4$ we assume that $q = p$, i.e. $r = 1$. Then [3, Theorem 10.2.5] applies directly. The more general q will be considered in a future work. Since $4 \mid (q-1)$, $p = 4f + 1$ for some $f \in \mathbb{Z}$. This time we have six possibilities for d and l:

$$(d,l) = \begin{cases} (1,1) & \text{if } \frac{m}{t} \text{ and } t \text{ are odd}, \\ (1,2) & \text{if } \frac{m}{t} \text{ odd and } t \equiv 2 \pmod 4, \\ (1,4) & \text{if } \frac{m}{t} \text{ odd and } 4 \mid t, \\ (2,1) & \text{if } \frac{m}{t} \equiv 2 \pmod 4 \text{ and } t \text{ odd}, \\ (2,2) & \text{if } \frac{m}{t} \equiv 2 \pmod 4 \text{ and } t \text{ even}, \\ (4,1) & \text{if } 4 \mid \frac{m}{t}. \end{cases}$$

Let χ_4 be the multiplicative character of order 4 of $\mathbb{F}_q = \mathbb{F}_p$ satisfying $\chi_4(g) = \mathsf{i}$. Furthermore, let a_4 and b_4 be integers satisfying (see Theorems 3.2.1 and 3.2.2 in [3])

$$a_4^2 + b_4^2 = p, \quad a_4 \equiv -\left(\tfrac{2}{p}\right) \pmod 4, \quad b_4 \equiv a_4 g^{\frac{p-1}{4}} \pmod p,$$

where $\left(\frac{2}{p}\right)$ denotes the Legendre symbol. Set

$$\pi_4 = (-1)^f (a_4 + \mathsf{i} b_4) \in \mathbb{Z}[\mathsf{i}]. \tag{11}$$

Then $\pi_4 \overline{\pi_4} = p$ and, since $q = p$,

$$J_t(\chi_4) = \begin{cases} -p^{\frac{t-4}{4}} \pi_4^{\frac{t}{2}} & \text{if } t \equiv 0 \pmod 4, \\ p^{\frac{t-1}{4}} \pi_4^{\frac{t-1}{2}} & \text{if } t \equiv 1 \pmod 4, \\ p^{\frac{t-2}{4}} \pi_4^{\frac{t}{2}} & \text{if } t \equiv 2 \pmod 4, \\ (-1)^f p^{\frac{t-3}{4}} \pi_4^{\frac{t+1}{2}} & \text{if } t \equiv 3 \pmod 4 \end{cases} \tag{12}$$

by [3, Therem 10.2.5]. Note also that $\chi_4^2 = \rho$ (see $s = 2$), $\chi_4^3 = \overline{\chi_4}$, and consequently $J_t(\chi_4^3) = \overline{J_t(\chi_4)}$. Further, $\rho(-1) = \chi_4^2(-1) = 1$ and $q = p$, so (10) simplifies into

$$J_t(\chi_4^2) = J_t(\rho) = \begin{cases} -p^{\frac{t-2}{2}} & \text{if } t \text{ is even,} \\ p^{\frac{t-1}{2}} & \text{if } t \text{ is odd.} \end{cases} \tag{13}$$

Let us now assume (5) and compute the numbers M_t and N_t. As in the previous subsection, N_t is obtained in the other cases from Lemma 1. We use the above results on Jacobi sums, and Lemmas 5 and 6 in the cases $a = 0$ and $a \neq 0$, respectively. Let first $a = 0$. If $l = 1$, Lemma 5 gives $M_t = 1 - p$. In the case $l = 2$ we have

$$M_t = (p-1)\big(-1 + (-1)^t p J_t(\rho)\bar{\rho}(g^{i_0})\big)$$

by Lemma 5. Here $\bar{\rho}(g^{i_0}) = \rho(g^{i_0}) = (-1)^{i_0}$. As now t is even, (13) gives M_t. Finally, if $l = 4$,

$$\begin{aligned} \frac{M_t}{p-1} &= -1 + (-1)^t p \sum_{\lambda \in H_4^*} J_t(\lambda)\bar{\lambda}(g^{i_0}) \\ &= -1 + (-1)^t p\big(J_t(\chi_4)\chi_4^3(g^{i_0}) + J_t(\rho)\bar{\rho}(g^{i_0}) + J_t(\chi_4^3)\chi_4(g^{i_0})\big) \\ &= -1 + (-1)^t p\big((-1)^{i_0} J_t(\rho) + 2\,\mathrm{Re}(J_t(\chi_4)\mathrm{i}^{3i_0})\big). \end{aligned}$$

The formula for M_t is obtained from this by using (12) and (13) and by remembering that $4 \mid t$ in the case $l = 4$.

Let us next consider the case $a \neq 0$. If $\frac{s}{d} = 1$, $M_t = 1$ by Lemma 6. This corresponds to $(d, l) = (4, 1)$. If $\frac{s}{d} = 2$ then $(d, l) = (2, 1)$ and t is odd or $(d, l) = (2, 2)$ and t is even. Again by Lemma 6

$$M_t = 1 + (-1)^{t-1} p J_t(\rho)\rho((-a_0)^t g^{i_0}).$$

Here $\rho((-a_0)^t g^{i_0}) = (-1)^{i_0}\rho((-1)^t)\rho(a_0^t) = (-1)^{i_0}\rho(a_0)$ when t is odd and $\rho((-a_0)^t g^{i_0}) = (-1)^{i_0}$ when t is even. The equation (13) now gives M_t. If $\frac{s}{d} = 4$ we have three possibilities for (d, l). In the cases $(d, l) = (1, 2)$, $(1, 4)$ we know t modulo 4 but in the case $(d, l) = (1, 1)$ there are two possibilities: $t \equiv 1 \pmod 4$ or $t \equiv 3 \pmod 4$. Lemma 6 now gives

$$M_t = 1 + (-1)^{t-1} p\big(2\,\mathrm{Re}(J_t(\chi_4)\chi_4((-a_0)^{3t})\mathrm{i}^{3i_0}) + (-1)^{i_0} J_t(\rho)\rho(a_0^t)\big).$$

Again numbers M_t can be obtained from this by using the knowledge on t modulo 4 and the equations (12) and (13).

We summarize these results in the following theorem.

Theorem 2. *Assume $q = p$ and (5), and let*

$$Q_{t,4} = \begin{cases} p^{\frac{t-1}{4}} \pi_4^{\frac{t-1}{2}} \overline{\chi_4}(-a_0)\mathrm{i}^{i_0} & \text{if } t \equiv 1 \pmod 4, \\ (-1)^f p^{\frac{t-3}{4}} \pi_4^{\frac{t+1}{2}} \chi_4(-a_0)\mathrm{i}^{i_0} & \text{if } t \equiv 3 \pmod 4. \end{cases}$$

In addition, let π_4 be as in (11), i_0 as in (4) and let $a_0 = -\frac{m}{ta}$. Then the values of N_t for $s = 4$ are those listed in Table 2.

TABLE 2: Values of N_t for $s = 4$ assuming (5) and $q = p$.

a	N_t	(d, l)
$a = 0$	$\frac{1}{4}(p^{t-1} - 1)$	$(1, 1)$
	$\frac{1}{4}\big(p^{t-1} - 1 - (-1)^{i_0} p^{\frac{t-2}{2}}(p-1)\big)$	$(1, 2)$
	$\frac{1}{4}\big(p^{t-1} - 1 - (-1)^{i_0} p^{\frac{t-4}{4}}(p-1)\big(p^{\frac{t}{4}} + 2\,\mathrm{Re}(\pi_4^{\frac{t}{2}} \mathrm{i}^{i_0})\big)\big)$	$(1, 4)$
	$\frac{1}{2}(p^{t-1} - 1)$	$(2, 1)$
	$\frac{1}{2}\big(p^{t-1} - 1 - (-1)^{i_0} p^{\frac{t-2}{2}}(p-1)\big)$	$(2, 2)$
	$p^{t-1} - 1$	$(4, 1)$
$a \neq 0$	$\frac{1}{4}\big(p^{t-1} + (-1)^{i_0}(p^{\frac{t-1}{2}}\rho(a_0) + 2\,\mathrm{Re}\,Q_{t,4})\big)$	$(1, 1)$
	$\frac{1}{4}\big(p^{t-1} + (-1)^{i_0} p^{\frac{t-2}{4}}\big(p^{\frac{t-2}{4}} - 2\rho(a_0)\,\mathrm{Re}(\pi_4^{\frac{t}{2}} \mathrm{i}^{i_0})\big)\big)$	$(1, 2)$
	$\frac{1}{4}\big(p^{t-1} + (-1)^{i_0} p^{\frac{t-4}{4}}\big(p^{\frac{t}{4}} + 2\,\mathrm{Re}(\pi_4^{\frac{t}{2}} \mathrm{i}^{i_0})\big)\big)$	$(1, 4)$
	$\frac{1}{2}\big(p^{t-1} + (-1)^{i_0} p^{\frac{t-1}{2}}\rho(a_0)\big)$	$(2, 1)$
	$\frac{1}{2}\big(p^{t-1} + (-1)^{i_0} p^{\frac{t-2}{2}}\big)$	$(2, 2)$
	p^{t-1}	$(4, 1)$

If $m > 2$ is prime then we can use Theorem 2 to obtain $P_m(a, 4, h)$. As with $s = 2$, $P_m(a, 4, h) = \frac{1}{m}(N_m - N_1)$ and it is enough to consider N_t for $t = 1, m$.

If $t = 1$, we have $d = 1$ by the assumption $m > 2$, and $l = 1$. In the case $p = m$ we have by Lemma 1

$$N_1 = \begin{cases} \frac{1}{4}(p-1) & \text{if } a = 0, \\ 0 & \text{if } a \neq 0. \end{cases}$$

If $p \neq m$, (5) holds and from Table 2 $N_1 = 0$ for $a = 0$ and

$$N_1 = \tfrac{1}{4}\big(1 + (-1)^{i_0}\big(\rho(a_0) + 2\,\mathrm{Re}(\overline{\chi_4}(-a_0)\mathrm{i}^{i_0})\big)\big)$$

for $a \neq 0$. Here $a_0 = -\frac{m}{ta} = -ma^{-1}$ and, modulo 4,

$$i_0 \equiv \begin{cases} h & \text{if } m \equiv 1 \pmod 4, \\ 3h & \text{if } m \equiv 3 \pmod 4. \end{cases}$$

Thus $\rho(a_0) = \rho(-1)\rho(m)\bar{\rho}(a) = \rho(ma)$ and $\overline{\chi_4}(-a_0) = \overline{\chi_4}(ma^{-1}) = \overline{\chi_4}(ma^3) = \chi_4(m^3 a)$.

If $t = m$, we have $d = 1$ and, by the assumption $m > 2$, $l = 1$. Clearly, (5) holds in this case. So for $a = 0$ we have $N_m = \frac{1}{4}(p^{m-1} - 1)$. For $a \neq 0$ we have $i_0 \equiv h \pmod 4$ by (4) and $a_0 = -\frac{m}{ta} = -a^{-1}$. Thus $\rho(a_0) = \rho(-1)\bar{\rho}(a) = \rho(a)$ and $\chi_4(-a_0) = \chi_4(a^{-1}) = \overline{\chi_4}(a) = \chi_4(a^3)$. Table 2 now yields N_m for both $m \equiv 1 \pmod 4$ and $m \equiv 3 \pmod 4$. Note that if $m = p$ then $m = q \equiv 1 \pmod 4$.

Combining the above we have

$$P_m(0,4,h) = \begin{cases} \frac{1}{4}(p^{p-2}-1) & \text{if } m = p, \\ \frac{1}{4m}(p^{m-1}-1) & \text{if } m \neq p \end{cases}$$

for $a = 0$. If $a \neq 0$ then

$$P_p(a,4,h) = \tfrac{1}{4p}\big(p^{p-1} + (-1)^h\big(p^{\frac{p-1}{2}}\rho(a) + 2p^{\frac{p-1}{4}}\operatorname{Re}(\pi_4^{\frac{p-1}{2}}\chi_4(a)\mathsf{i}^h)\big)\big)$$

for $m = p$ and

$$P_m(a,4,h) = \tfrac{1}{4m}\big(p^{m-1} - 1 + (-1)^h\big(\rho(a)\big(p^{\frac{m-1}{2}} - \rho(m)\big) + 2\operatorname{Re} R_m\big)\big)$$

for $m \neq p$, where

$$R_m = \begin{cases} p^{\frac{m-1}{4}}\pi_4^{\frac{m-1}{2}}\chi_4(a)\mathsf{i}^h - \chi_4(m^3a)\mathsf{i}^h & \text{if } m \equiv 1 \pmod 4, \\ (-1)^f p^{\frac{m-3}{4}}\pi_4^{\frac{m+1}{2}}\overline{\chi_4}(a)\mathsf{i}^h - \chi_4(m^3a)\mathsf{i}^{3h} & \text{if } m \equiv 3 \pmod 4. \end{cases}$$

5.3. **Case $s = 3$.** For $s = 3$ we again assume that $q = p$, i.e. $r = 1$. Since $3 \mid (p-1)$, $p \equiv 1 \pmod 3$. As for $s = 2$, we have three possibilities for d and l:

$$(d,l) = \begin{cases} (1,1) & \text{if } 3 \nmid \frac{m}{t},\ 3 \nmid t, \\ (1,3) & \text{if } 3 \nmid \frac{m}{t},\ 3 \mid t, \\ (3,1) & \text{if } 3 \mid \frac{m}{t}. \end{cases}$$

Let χ_3 be the multiplicative character of order 3 of $\mathbb{F}_q$ satisfying $\chi_3(g) = \zeta := \mathsf{e}^{2\pi\mathsf{i}/3}$. Obviously $\overline{\chi_3} = \chi_3^{-1} = \chi_3^2$ and consequently $\overline{J_t(\chi_3)} = J_t(\chi_3^2)$. We also note the useful properties $\chi_3^2(-1) = \chi_3((-1)^2) = 1$ and $\chi_3(-1) = \overline{\chi_3^2(-1)} = 1$. Let a_3 and b_3 be integers satisfying (see Theorems 3.1.1 and 3.1.2 in [3])

$$a_3^2 + 3b_3^2 = p, \quad a_3 \equiv -1 \pmod 3, \quad 3b_3 \equiv (2g^{\frac{p-1}{3}} + 1)a_3 \pmod p,$$

and denote

$$\pi_3 = \chi_3(2)(a_3 + \mathsf{i}b_3\sqrt{3}) \in \mathbb{Z}[\zeta]. \tag{14}$$

Since we assume $q = p$, [3, Theorem 10.2.4] is applicable and it yields together with $\pi_3\overline{\pi_3} = p$ that

$$J_t(\chi_3) = \begin{cases} -p^{\frac{t-3}{3}}\pi_3^{\frac{t}{3}} & \text{if } t \equiv 0 \pmod 3, \\ p^{\frac{t-1}{3}}\pi_3^{\frac{t-1}{3}} & \text{if } t \equiv 1 \pmod 3, \\ p^{\frac{t-2}{3}}\pi_3^{\frac{t+1}{3}} & \text{if } t \equiv 2 \pmod 3. \end{cases} \tag{15}$$

Let us now assume (5) and compute the numbers M_t and N_t. Again, in the other cases N_t is obtained from Lemma 1.

If $(d,l)=(1,1)$ then $t\equiv 1 \pmod 3$ or $t\equiv 2 \pmod 3$. In the case $a=0$ we again obtain $M_t = 1-q$ by Lemma 4. For $a\neq 0$ Lemma 6 gives

$$\begin{aligned}\tfrac{(-1)^{t-1}}{q}(M_t-1) &= \sum_{\lambda\in H_3^*} J_t(\lambda)\overline{\lambda}((-a_0)^t g^{i_0}) \\ &= J_t(\chi_3)\chi_3^2((-a_0)^t g^{i_0}) + \overline{J_t(\chi_3)\chi_3^2((-a_0)^t g^{i_0})} \\ &= 2\operatorname{Re}(J_t(\chi_3)\chi_3(a_0^{2t})\zeta^{2i_0}).\end{aligned}$$

As (15) tells the value of the Jacobi sum in the above equation, M_t and N_t are easily obtained from this.

If $(d,l)=(1,3)$ then $t\equiv 0 \pmod 3$. The numbers N_t can again be obtained as above using Jacobi sums and Lemmas 5 and 6 for $a=0$ and $a\neq 0$, respectively. Finally, for $(d,l)=(3,1)$ Lemmas 5 and 6 give $M_t = 1-q$ if $a=0$, and $M_t = 1$ if $a\neq 0$.

Again, Lemma 2 completes the following theorem.

Theorem 3. *Assume $q=p$ and (5), and let*

$$Q_{t,3} = \begin{cases} p^{\frac{t-1}{3}}\pi_3^{\frac{t-1}{3}}\overline{\chi_3}(a_0)\zeta^{2i_0}, & \text{if } t\equiv 1 \pmod 3, \\ p^{\frac{t-2}{3}}\pi_3^{\frac{t+1}{3}}\chi_3(a_0)\zeta^{2i_0}, & \text{if } t\equiv 2 \pmod 3. \end{cases}$$

Further, let π_3 be as in (14), i_0 as in (4), and let $a_0 = -\frac{m}{ta}$. Then the values of N_t for $s=3$ are those listed in Table 3.

TABLE 3: Values of N_t for $s=3$ assuming (5) and $q=p$.

a	N_t	(d,l)
$a=0$	$\frac{1}{3}(p^{t-1}-1)$	$(1,1)$
	$\frac{1}{3}\big(p^{t-1}-1-2(-1)^t p^{\frac{t-3}{3}}(p-1)\operatorname{Re}(\pi_3^{\frac{t}{3}}\zeta^{2i_0})\big)$	$(1,3)$
	$p^{t-1}-1$	$(3,1)$
$a\neq 0$	$\frac{1}{3}\big(p^{t-1}-2(-1)^t\operatorname{Re}Q_{t,3}\big)$	$(1,1)$
	$\frac{1}{3}\big(p^{t-1}+2(-1)^t p^{\frac{t-3}{3}}\operatorname{Re}(\pi_3^{\frac{t}{3}}\zeta^{2i_0})\big)$	$(1,3)$
	p^{t-1}	$(3,1)$

Again, we shall finally consider the situation when $m>3$ is prime. The computations are straightforward and similar as in the case $s=4$ so we just state the results:

$$P_m(0,3,h) = \begin{cases} \frac{1}{3}(p^{p-2}-1) & \text{if } m=p, \\ \frac{1}{3m}(p^{m-1}-1) & \text{if } m\neq p, \end{cases}$$

for $a=0$ and

$$P_m(a,3,h) = \begin{cases} \frac{1}{3p}\big(p^{p-1}+2p^{\frac{p-1}{3}}\operatorname{Re}(\pi_3^{\frac{p-1}{3}}\chi_3(a)\zeta^{2h})\big) & \text{if } m=p, \\ \frac{1}{3m}(p^{m-1}-1+2\operatorname{Re}L_m) & \text{if } m\neq p, \end{cases}$$

for $a \neq 0$, where

$$L_m = \begin{cases} \big((p\pi_3)^{\frac{m-1}{3}} - \overline{\chi_3}(m)\big)\chi_3(a)\zeta^{2h} & \text{if } m \equiv 1 \pmod 3, \\ \big(p^{\frac{m-2}{3}}\pi_3^{\frac{m+1}{3}}\chi_3(a)\zeta^h - \overline{\chi_3}(m)\big)\chi_3(a)\zeta^h & \text{if } m \equiv 2 \pmod 3. \end{cases}$$

5.4. **Case** $s \mid (p^e+1)$**.** Assume $r = 2en$ and let $s > 1$ be a factor of p^e+1. Then -1 is a power of p in $\mathbb{Z}_s$, and s is called *semiprimitive*. The semiprimitive numbers N appear also in [1, 17] in connection to semiprimitive cyclic codes. We recall Theorem 1 in [9], which we shall use in the following form:

Proposition 1. *If $s \mid (p^e+1)$ and $r = 2en$ then*

$$\sum_{x\in\mathbb{F}_{q^t}^*} e_t(\gamma_t^i x^s) = \begin{cases} (-1)^{nt}\sqrt{q^t} - 1 & \text{if } i \not\equiv k_s \pmod s, \\ (-1)^{nt-1}(s-1)\sqrt{q^t} - 1 & \text{if } i \equiv k_s \pmod s, \end{cases}$$

where $k_s = s/2$ if $p > 2$, $2 \nmid nt$ and $2 \nmid (p^e+1)/s$, and $k_s = 0$ otherwise.

Note that Proposition 1 holds for $s = 1$, too.

If $a = 0$, Lemma 4 and Proposition 1 immediately give

$$\frac{M_t}{q-1} + 1 = \begin{cases} (-1)^{nt}\sqrt{q^t} & \text{if (17) holds,} \\ (-1)^{nt-1}(l-1)\sqrt{q^t} & \text{if (18) holds,} \end{cases} \tag{16}$$

where the conditions are

$$l > 1 \text{ and } i_0 \not\equiv k_l \pmod l, \tag{17}$$

$$l = 1; \quad \text{or} \quad l > 1 \text{ and } i_0 \equiv k_l \pmod l. \tag{18}$$

Assume next that $a \neq 0$. We combine Proposition 1 with Lemma 7 and observe first that the congruence $\operatorname{ind}_{\gamma_t} a_0 + t_0 j + i_0 \equiv k_{s/d} \pmod{\frac{s}{d}}$ is solvable in j if and only if

$$l \mid (k_{s/d} - i_0 - \operatorname{ind}_{\gamma_t} a_0) \quad \text{and} \quad \tfrac{t_0}{l} j \equiv \tfrac{k_{s/d} - i_0 - \operatorname{ind}_{\gamma_t} a_0}{l} \pmod u. \tag{19}$$

Assume first that $l \nmid (k_{s/d} - i_0 - \operatorname{ind}_{\gamma_t} a_0)$. Now, by Lemma 7 and Proposition 1, we get

$$\begin{aligned} uM_t &= \big((-1)^{nt}\sqrt{q^t} - 1\big) \sum_{c\in\mathbb{F}_q^*} \sum_{j=0}^{u-1} e_1(g^j c^u) \\ &= \big((-1)^{nt-1}\sqrt{q^t} + 1\big)u. \end{aligned} \tag{20}$$

Assume next that $l \mid (k_{s/d} - i_0 - \operatorname{ind}_{\gamma_t} a_0)$. Since the congruence in (19) has unique solution $j_0 \in \{0, \ldots, u-1\}$, Lemma 7 and Proposition 1 imply

$$\begin{aligned} uM_t = \big((-1)^{nt-1}(\tfrac{s}{d} - 1)\sqrt{q^t} - 1\big) \sum_{c\in\mathbb{F}_q^*} e_1(g^{j_0} c^u) \\ + \big((-1)^{nt}\sqrt{q^t} - 1\big) \sum_{j\neq j_0} \sum_{c\in\mathbb{F}_q^*} e_1(g^j c^u). \end{aligned}$$

Here

$$\sum_{j\neq j_0}\sum_{c\in\mathbb{F}_q^*} e_1(g^jc^u) = \sum_{j=0}^{u-1}\sum_{c\in\mathbb{F}_q^*} e_1(g^jc^u) - \sum_{c\in\mathbb{F}_q^*} e_1(g^{j_0}c^u),$$

and therefore

$$uM_t = (-1)^{nt-1}\frac{s}{d}\sqrt{q^t}\sum_{c\in\mathbb{F}_q^*} e_1(g^{j_0}c^u) + \big((-1)^{nt-1}\sqrt{q^t}+1\big)u.$$

Finally, by applying Proposition 1 with $t=1$, we get

$$\sum_{c\in\mathbb{F}_q^*} e_1(g^{j_0}c^u) = \begin{cases}(-1)^n\sqrt{q}-1 & \text{if (21) holds,}\\ (-1)^{n-1}(u-1)\sqrt{q}-1 & \text{if (22) holds.}\end{cases}$$

where the conditions are

$$u>1 \text{ and } j_0 \not\equiv k_u \pmod u, \tag{21}$$

$$u=1; \quad \text{or} \quad u>1 \text{ and } j_0 \equiv k_u \pmod u. \tag{22}$$

Altogether, if $l \mid (k_{s/d} - i_0 - \operatorname{ind}_{\gamma_t} a_0)$, then

$$M_t - 1 = \tag{23}$$
$$\begin{cases}(-1)^{nt-1}\big(((-1)^n\sqrt{q}-1)l+1\big)\sqrt{q^t} & \text{if (21) holds,}\\ (-1)^{nt-1}\big(((-1)^{n-1}(u-1)\sqrt{q}-1)l+1\big)\sqrt{q^t} & \text{if (22) holds.}\end{cases}$$

Combining (16), (20) and (23) with Lemma 2 we get the values of N_t which we gather in the following theorem.

Theorem 4. *Assume $s \mid (p^e+1)$ and $r=2en$. Then the N_t are those listed in Table 4. Especially, if $a=0$ and $l=1$ then $N_t = \frac{d}{s}(q^{t-1}-1)$, and if $a\neq 0$ and $d=s$ then $N_t = q^{t-1}$.*

TABLE 4: Values of N_t for $s \mid (p^e+1)$ and $r=2en$ with "$\mid$" and "$\nmid$" telling whether l divides $k_{s/d} - i_0 - \operatorname{ind}_{\gamma_t} a_0$ or not.

a	N_t	with
$a=0$	$\frac{d}{s}\big(q^{t-1}-1+(-1)^{nt}(q-1)\sqrt{q^{t-2}}\big)$	(17)
	$\frac{d}{s}\big(q^{t-1}-1-(-1)^{nt}(q-1)(l-1)\sqrt{q^{t-2}}\big)$	(18)
$a\neq 0$	$\frac{d}{s}\big(q^{t-1}-(-1)^{nt}\sqrt{q^{t-2}}\big)$	$\nmid$
	$\frac{d}{s}\big(q^{t-1}-(-1)^{nt}\big(((-1)^n\sqrt{q}-1)l+1\big)\sqrt{q^{t-2}}\big)$	$\mid$, (21)
	$\frac{d}{s}\big(q^{t-1}-(-1)^{nt}\big(((-1)^{n-1}(u-1)\sqrt{q}-1)l+1\big)\sqrt{q^{t-2}}\big)$	$\mid$, (22)

5.5. **The semiprimitive and index 2 cases for $p = 2$.** In this subsection we assume that $p = 2$ and show how to calculate $P_m(a, q-1, h)$ in semiprimitive or index 2 cases by applying the results from [8, II] and [14]. In particular, we give $P_m(0, q-1, h)$ explicitly for all $m \leq 30$. We also give a table of these numbers for $q = 2$, 4, 8, and small values of m to cross-check our formulae against the results given by the irreducible polynomial generator in [15].

As $p = 2$, the semiprimitive case holds for an odd integer $N > 1$ if -1 is a power of 2 in $\mathbb{Z}_N$. Correspondingly, the *index 2 case* is said to hold for N if $-1 \notin \langle 2 \rangle \subseteq \mathbb{Z}_N$ and $\operatorname{ord}_N 2 = \phi(N)/2$ where ϕ is the Euler function.

If s is semiprimitive then clearly its factors, especially l, s/d and u in Lemmas 4 and 7, are too. Proposition 1 can be written for characteristic $p = 2$ in the following form, see also [8, II Theorem 1].

Proposition 2. *Assume that $rt = N' \operatorname{ord}_N 2$, $N > 1$ and -1 is a power of 2 modulo N. Then*

$$\sum_{x \in \mathbb{F}_{q^t}} e_t(\gamma_t^a x^N) = \begin{cases} (-1)^{N'} \sqrt{q^t} & \text{if } N \nmid a, \\ (-1)^{N'-1} (N-1) \sqrt{q^t} & \text{if } N \mid a. \end{cases}$$

Similarly, if the index 2 case holds for N then its factors satisfy either the index 2 or the semiprimitive case, see [8, II Lemmas 2 and 5]. In what follows we consider only square-free N in the index 2 cases. From the general classification result [8, II Lemmas 3 and 6] it follows that the following three cases are then possible, where p_1 and p_2 are primes:

1. $N = p_2 \equiv 7 \pmod 8$;
2. $N = p_1 p_2$, $p_1 \equiv 5 \pmod 8$, $p_2 \equiv 3 \pmod 8$, 2 is a primitive root modulo p_1 and modulo p_2;
3. $N = p_1 p_2$, $p_1 \equiv 3, 5 \pmod 8$, $p_2 \equiv 7 \pmod 8$, $\operatorname{ord}_{p_1} 2 = p_1 - 1$, and $\operatorname{ord}_{p_2} 2 = (p_2 - 1)/2$ with $-1 \notin \langle 2 \rangle \subseteq \mathbb{Z}_{p_2}$.

The value distribution of the monomial sums in the above square-free cases were studied in [2] (case 1) and [16] (cases 2 and 3). The general (characteristic 2) index 2 cases has been studied in [8] (cases 1 and 2) and in [14] (case 3). We are able to compute the value distribution except for few case 3 parameters. Knowing only the value distribution and not the exact values is not enough to compute the $P_m(a, s, h)$ exactly but with the methods from [8] and [14] we get (except for some cases 3) at most two possibilities for the values of each $P_m(a, s, h)$ when the index 2 case holds for m.

Let us next recall how the index 2 sums $\sum_{x \in \mathbb{F}_{q^t}} e_t(\gamma_t^i x^N)$ can be computed in our three cases. For the results and methods we refer to [13, 8] for cases 1 and 2 and to [14], especially Theorems 4, 6 and 7, for case 3. Also [2, 16] can be used. Let $rt = r't'$ with $r' = \phi(N)/2 = \operatorname{ord}_N 2$ and denote by $\delta = \operatorname{Norm}(\gamma_t)$ a primitive element of $\mathbb{F}_{2^{r'}}$, where Norm is the norm from $\mathbb{F}_{q^t}$ onto $\mathbb{F}_{2^{r'}}$. Further, since $N \mid (2^{r'} - 1)$, there

exists a multiplicative character χ of $\mathbb{F}_{2^{r'}}$ for which $\chi(\delta) = \mathsf{e}^{2\pi\mathrm{i}/N}$. The character χ has order N and $\chi' = \chi \circ \mathrm{Norm}$ is a multiplicative character of order N of $\mathbb{F}_{q^t}$.

The value of the monomial index 2 sum $\sum_{x\in\mathbb{F}_{q^t}} e_t(\gamma_t^i x^N)$ can now be computed in terms of $G_t(\chi) = \sum_{x\in\mathbb{F}_{q^t}^*} e_t(x)\chi'(x)$ by using [8, Theorem 2] in the case 1, [8, Theorem 3] in the case 2 and [14, eq. (16), Theorem 4] in the case 3. By the Davenport-Hasse identity

$$G_t(\chi) = -(-F_{r'}(\chi))^{t'}, \qquad F_{r'}(\chi) = \sum_{x\in\mathbb{F}_{2^{r'}}} \chi(x)e(x), \tag{24}$$

where in the last Gauss sum over $\mathbb{F}_{2^{r'}}$ e is the canonical additive character of $\mathbb{F}_{2^{r'}}$. These latter Gauss sums can be computed up to the sign of the imaginary part, see [13, p. 1245] and [14, p. 9 and Theorem 7].

The above cases cover all values $m \le 30$, so we able to compute (possibly up to two choices) $P_m(0, s, h)$ for $m \le 30$ by Lemma 4 and $P_m(a, s, h)$ for $a \ne 0$, $m \le 30$, by Lemma 7. As an example we give $P_m := P_m(0, q-1, h)$ for $m \le 30$. Since $s = q-1$, we have b fixed and $h = \operatorname{ind} b = \operatorname{ind}_g b$. We consider the values $m \le 30$ in the following order: 2^k (2, 4, 8, 16), semiprimitive primes v (3, 5, 11, 13, 17, 19, 29) and the cases related to these: $2v$ (6, 10, 22, 26), $4v$ (12, 20), $8v$ (24), v^2 (9, 25), $2v^2$ (18), v^3 (27). Finally, we cover the index 2 cases: 7, 23 with related 14, 28 (case 1), 15 with related 30 (case 2), and 21 (case 3).

If $m = 2^k$ then (1) gives $P_m = \frac{1}{m}(N_m - N_{m/2})$. By Lemma 1 $N_{m/2} = \frac{q^{m/2}-1}{q-1}$. Lemma 4 gives $M_m = 1-q$ and then $N_m = \frac{q^{m-1}-1}{q-1}$ by Lemma 2. Thus, as in [10, Example 2],

$$P_m = \frac{q^{m-1} - q^{m/2}}{m(q-1)}.$$

In the case $m = v$ equation (1) implies $P_v = \frac{1}{v}(N_v - N_1)$. If $v \nmid (q-1)$ then $d = l = 1$ for both values $t = 1, v$. By Lemma 4, $M_1 = M_v = 1-q$ and therefore Lemma 2 gives $N_1 = 0$ and $N_v = \frac{q^{v-1}-1}{q-1}$. Thus

$$P_v = \frac{q^{v-1} - 1}{v(q-1)}.$$

Assume now that $v \mid (q-1)$. If $t = 1$ then $d = v$ and $l = 1$. By Lemma 1 $N_1 = 0$ if $v \nmid h$. If $v \mid h$ then $M_1 = 1-q$ by Lemma 4 and therefore Lemma 2 gives $N_1 = 0$ in this case, too. If $t = v$ then $d = 1$ and $l = v$. By Lemma 4 and Proposition 2 we now have

$$M_v = \begin{cases} (q-1)(-1 \pm \sqrt{q^v}) & \text{if } v \nmid h, \\ (q-1)(-1 \mp (v-1)\sqrt{q^v}) & \text{if } v \mid h, \end{cases}$$

where $\pm = (-1)^{v'}$ with $rv = v' \operatorname{ord}_v 2$. Since v is odd, $\pm = (-1)^{\frac{r}{\operatorname{ord}_v 2}}$. By using Lemma 2 and combining the above results we get

$$P_v - \frac{q^{v-1}-1}{v(q-1)} = \begin{cases} 0 & \text{if } \operatorname{ord}_v 2 \nmid r, \\ \pm\frac{1}{v}\sqrt{q^{v-2}} & \text{if } \operatorname{ord}_v 2 \mid r,\ v \nmid \operatorname{ind} b, \\ \mp\frac{v-1}{v}\sqrt{q^{v-2}} & \text{if } \operatorname{ord}_v 2 \mid r,\ v \mid \operatorname{ind} b. \end{cases} \tag{25}$$

To consider the case $m = 2v$ we note the following. If $\frac{m}{2}$ is odd we have $\mu(m)N_1 + \mu(\frac{m}{2})N_2 = 0$. Namely, for $t = 1$, $d = \gcd(m, q-1) = \gcd(\frac{m}{2}, q-1)$, and Lemma 1 gives $N_1 = 0$ or d if $d \nmid h$ or $d \mid h$, respectively. For $t = 2$ we have $d = \gcd(\frac{m}{2}, q-1)$ again and $l = \gcd(2, \frac{q-1}{d}) = 1$. If $d \nmid h$ then $N_2 = 0$ by Lemma 1. If $d \mid h$ then Lemma 4 gives $M_2 = 1 - q$ and therefore $N_2 = \frac{d}{(q-1)q}(q^2 - 1 + 1 - q) = d$. This proves the claim $\mu(m)N_1 + \mu(\frac{m}{2})N_2 = 0$ for odd $\frac{m}{2}$. Note that this claim holds true also if $8 \mid m$ or m is non-square-free. The use of (1) now gives $P_{2v} = \frac{1}{2v}(N_{2v} - N_v)$ by the above consideration.

For $t = v$, $d = \gcd(2, q-1) = 1$ and $2 \mid \frac{m}{t}$. By Lemma 1 $N_v = \frac{q^v-1}{q-1}$. For $t = 2v$, $d = 1$ again and $l = \gcd(2v, q-1) = \gcd(v, q-1)$. If $v \nmid (q-1)$ then $l = 1$ and Lemmas 2 and 4 yield

$$N_{2v} = \frac{1}{(q-1)q}(q^{2v} - 1 + 1 - q) = \frac{q^{2v-1}-1}{q-1}.$$

If $v \mid (q-1)$ then $l = v$ and Lemma 4 and Proposition 2 give

$$M_{2v} = \begin{cases} (q-1)(-1+q^v) & \text{if } v \nmid h, \\ (q-1)(-1-(v-1)q^v) & \text{if } v \mid h, \end{cases}$$

since now $\frac{2rv}{\operatorname{ord}_v 2}$ is even. The use of Lemma 2 together with these results gives

$$P_{2v} - \frac{q^{2v-1}-q^v}{2v(q-1)} = \begin{cases} 0 & \text{if } \operatorname{ord}_v 2 \nmid r, \\ \frac{1}{2v}q^{v-1} & \text{if } \operatorname{ord}_v 2 \mid r,\ v \nmid \operatorname{ind} b, \\ -\frac{v-1}{2v}q^{v-1} & \text{if } \operatorname{ord}_v 2 \mid r,\ v \mid \operatorname{ind} b. \end{cases}$$

For the remaining cases related to semiprimitive primes v the use of Lemmas 1, 2 and 4 and Proposition 2 gives the following results. The details of the calculations are given in [6].

If $m = 4v$ (12, 20) then

$$P_{4v} - \frac{q^{2v}(q^{2v-1}-1)}{4v(q-1)} = \begin{cases} -\frac{q^2}{4v} & \text{if } \operatorname{ord}_v 2 \nmid r, \\ \frac{q^{2v-1}}{4v} & \text{if } \operatorname{ord}_v 2 \mid r,\ v \nmid \operatorname{ind} b, \\ -\frac{v-1}{4v}q^{2v-1} - (\frac{q}{2})^2 & \text{if } \operatorname{ord}_v 2 \mid r,\ v \mid \operatorname{ind} b. \end{cases}$$

If $m = 24$ then

$$P_{24} - \frac{q^{12}(q^{11}-1)}{24(q-1)} = \begin{cases} -\frac{q^4(q^3-1)}{24(q-1)} & \text{if } 2 \nmid r, \\ \frac{q^{11}}{24} & \text{if } 2 \mid r,\ 3 \nmid \operatorname{ind} b, \\ -\frac{q^{11}}{12} - \frac{q^4(q^3-1)}{8(q-1)} & \text{if } 2 \mid r,\ 3 \mid \operatorname{ind} b. \end{cases}$$

If $m = v^2$ (9, 25, which are semiprimitive) then

$$P_{v^2} - \frac{q^{v^2-1}-1}{v^2(q-1)} = \frac{q^{v-1}-1}{v^2(q-1)}$$

for $\operatorname{ord}_v 2 \nmid r$,

$$P_{v^2} - \frac{q^{v^2-1}-1}{v^2(q-1)} = \begin{cases} \pm_1 \frac{1}{v^2}\sqrt{q^{v^2-2}} & \text{if } v \nmid \operatorname{ind} b, \\ -\frac{q^{v-1}-1}{v(q-1)} \mp_1 \frac{v-1}{v^2}\sqrt{q^{v^2-2}} & \text{if } v \mid \operatorname{ind} b \end{cases}$$

for $\operatorname{ord}_v 2 \mid r$, $\operatorname{ord}_{v^2} 2 \nmid r$, and

$$P_{v^2} - \frac{q^{v^2-1}-1}{v^2(q-1)} =$$

$$\begin{cases} \pm_2 \frac{1}{v^2}\sqrt{q^{v^2-2}} & \text{if } v \nmid \operatorname{ind} b, \\ \pm_2 \frac{1}{v^2}\sqrt{q^{v^2-2}} - \frac{1}{v}\left(\frac{q^{v-1}-1}{q-1} \pm_1 \sqrt{q^{v-2}}\right) & \text{if } v \mid \operatorname{ind} b,\ v^2 \nmid \operatorname{ind} b, \\ \mp_2 \frac{v^2-1}{v^2}\sqrt{q^{v^2-2}} - \frac{1}{v}\left(\frac{q^{v-1}-1}{q-1} \mp_1 (v-1)\sqrt{q^{v-2}}\right) & \text{if } v^2 \mid \operatorname{ind} b \end{cases}$$

for $\operatorname{ord}_{v^2} 2 \mid r$, where $\pm_i = (-1)^{\frac{r}{\operatorname{ord}_{v^i} 2}}$ for $i = 1, 2$.

If $m = 18$ then

$$P_{18} - \frac{q^9(q^8-1)}{18(q-1)} = -\frac{q^3(q+1)}{18}$$

for $2 \nmid r$,

$$P_{18} - \frac{q^9(q^8-1)}{18(q-1)} = \begin{cases} \frac{q^8}{18} & \text{if } 3 \nmid \operatorname{ind} b, \\ -\frac{q^3}{3}(\frac{q^5}{3} + \frac{q+1}{2}) & \text{if } 3 \mid \operatorname{ind} b \end{cases}$$

for $2 \mid r$ and $6 \nmid r$, and

$$P_{18} - \frac{q^9(q^8-1)}{18(q-1)} = \begin{cases} \frac{q^8}{18} & \text{if } 3 \nmid \operatorname{ind} b, \\ \frac{q^8}{18} - \frac{q^2(q^3-1)}{6(q-1)} & \text{if } 3 \mid \operatorname{ind} b,\ 9 \nmid \operatorname{ind} b, \\ -\frac{q^2(8q^6+3q(q+1)-6)}{18} & \text{if } 9 \mid \operatorname{ind} b \end{cases}$$

for $6 \mid r$.

If $m = 27$ then

$$P_{27} - \frac{q^{26}-1}{27(q-1)} = -\frac{q^8-1}{27(q-1)}$$

for $2 \nmid r$,

$$P_{27} - \frac{q^{26}-1}{27(q-1)} = \begin{cases} \pm\frac{1}{27}\sqrt{q^{25}} & \text{if } 3 \nmid \operatorname{ind} b, \\ -\frac{1}{27}\left(\frac{3(q^8-1)}{q-1} \pm 2\sqrt{q^{25}}\right) & \text{if } 3 \mid \operatorname{ind} b \end{cases}$$

for $2 \mid r$, $6 \nmid r$,

$$P_{27} - \frac{q^{26}-1}{27(q-1)} = \begin{cases} \pm\frac{1}{27}\sqrt{q^{25}} & \text{if } 3 \nmid \operatorname{ind} b, \\ -\frac{q^8-1}{9(q-1)} \pm \frac{1}{27}(\sqrt{q^{25}} - 3\sqrt{q^7}) & \text{if } 3 \mid \operatorname{ind} b,\ 9 \nmid \operatorname{ind} b, \\ -\frac{q^8-1}{9(q-1)} \mp \frac{2}{27}(4\sqrt{q^{25}} - 3\sqrt{q^7}) & \text{if } 9 \mid \operatorname{ind} b \end{cases}$$

for $6 \mid r$, $18 \nmid r$, and

$$P_{27} - \frac{q^{26}-1}{27(q-1)} = \begin{cases} \pm\frac{1}{27}\sqrt{q^{25}} & \text{if } 3 \nmid \operatorname{ind} b, \\ -\frac{q^8-1}{9(q-1)} \pm \frac{1}{27}(\sqrt{q^{25}} - 3\sqrt{q^7}) & \text{if } 3 \mid \operatorname{ind} b,\ 27 \nmid \operatorname{ind} b, \\ -\frac{q^8-1}{9(q-1)} \mp \frac{2}{27}(13\sqrt{q^{25}} - 12\sqrt{q^7}) & \text{if } 27 \mid \operatorname{ind} b \end{cases}$$

for $18 \mid r$, where $\pm = (-1)^{\frac{r}{2}}$.

In the index 2 case 1, $m = p_2$ (7, 23) and we have $P_m = \frac{1}{m}(N_m - N_1)$ by (1). In considering N_1 we have $d = \gcd(m, q-1)$ and $l = 1$. Thus Lemma 1 gives $N_1 = 0$ if $d \nmid h$. In the case $d \mid h$ the use of Lemmas 2 and 4 implies $N_1 = 0$, too.

If $t = m$ then $d = 1$ and $l = \gcd(m, q-1)$. If $m \nmid (q-1)$ then $l = 1$ and $M_m = 1 - q$ by Lemma 4. Thus Lemma 2 gives $N_m = \frac{q^{m-1}-1}{q-1}$. For $m \mid (q-1)$ we have

$$N_m = \frac{q^{m-1}-1}{q-1} + \frac{1}{q} \sum_{x \in \mathbb{F}_{q^m}} e_m(\gamma_m^{i_0} x^m)$$

by Lemmas 2 and 4.

To determine N_7 we note that $r' = \phi(7)/2 = 3 = \operatorname{ord}_7 2$ and $t' = 7r/3$ in (24). Further, as given on [12, p. 3],

$$F_3(\chi) = -1 + c\sqrt{-7}, \qquad c \in \{1, -1\},$$

in (24) and the use of [12, Lemma 3] togehter with the above consideration gives

$$P_7 - \frac{q^6-1}{7(q-1)} = \begin{cases} 0 & \text{if } 3 \nmid r, \\ -\frac{3}{7}(\omega_7^{\frac{7r}{3}} + \bar{\omega}_7^{\frac{7r}{3}})\sqrt{q^5} & \text{if } 3 \mid r,\ 7 \mid \operatorname{ind} b, \\ \frac{\sqrt{2}}{7}(\omega_7^{\frac{7r}{3}-1} + \bar{\omega}_7^{\frac{7r}{3}-1})\sqrt{q^5} & \text{if } 3 \mid r,\ \operatorname{ind} b \in C_c^7, \\ \frac{\sqrt{2}}{7}(\omega_7^{\frac{7r}{3}+1} + \bar{\omega}_7^{\frac{7r}{3}+1})\sqrt{q^5} & \text{if } 3 \mid r,\ \operatorname{ind} b \in C_{-c}^7, \end{cases}$$

where $\omega_7 = (1 + \sqrt{-7})/\sqrt{8}$, bar denotes the complex conjugation and C_i^N denotes the 2-cyclotomic coset modulo N containing i.

In the related case $m = 2 \cdot 7 = 14$ we see as above in the case $m = 2v$ that $\mu(14)N_1 + \mu(7)N_2 = 0$ in (1). Thus $P_{14} = \frac{1}{14}(N_{14} - N_7)$. If $t = 7$ then $d = \gcd(2, q-1) = 1$. Since $\frac{m}{t} = 2$, Lemma 1 can be applied to get $N_7 = \frac{q^7-1}{q-1}$. In the case $t = 14$, $d = 1$ and $l = \gcd(14, q-1) =$

$\gcd(7, q-1)$. If $7 \nmid (q-1)$ then $l = 1$ and Lemmas 2 and 4 give $N_{14} = \frac{q^{13}-1}{q-1}$. By using again Lemmas 2 and 4 we have

$$N_{14} = \frac{q^{13}-1}{q-1} + \frac{1}{q} \sum_{x \in \mathbb{F}_{q^m}} e_m(\gamma_m^{i_0} x^7)$$

if $7 \mid (q-1)$. Now $rm = m' \operatorname{ord}_7 2$ or $m' = 14r/3$, and therefore we get as above

$$P_{14} - \frac{q^7(q^6-1)}{14(q-1)} = \begin{cases} 0 & \text{if } 3 \nmid r, \\ -\frac{3}{14}(\omega_7^{\frac{14r}{3}} + \bar{\omega}_7^{\frac{14r}{3}})q^6 & \text{if } 3 \mid r,\ 7 \mid \operatorname{ind} b, \\ \frac{\sqrt{2}}{14}(\omega_7^{\frac{14r}{3}-1} + \bar{\omega}_7^{\frac{14r}{3}-1})q^6 & \text{if } 3 \mid r,\ \operatorname{ind} b \in C_c^7, \\ \frac{\sqrt{2}}{14}(\omega_7^{\frac{14r}{3}+1} + \bar{\omega}_7^{\frac{14r}{3}+1})q^6 & \text{if } 3 \mid r,\ \operatorname{ind} b \in C_{-c}^7 \end{cases}$$

with the same c and ω_7 as in P_7.

For the details of the cases $m = 4 \cdot 7 = 28$ and $m = 23$ we refer to [6] and state here the results:

$$P_{28} - \frac{q^{14}(q^{13}-1)}{28(q-1)} = \begin{cases} -\frac{q^2}{28} & \text{if } 3 \nmid r, \\ -\frac{3}{28}(\omega_7^{\frac{28r}{3}} + \bar{\omega}_7^{\frac{28r}{3}})q^{13} - (\frac{q}{2})^2 & \text{if } 3 \mid r,\ 7 \mid \operatorname{ind} b, \\ \frac{\sqrt{2}}{28}(\omega_7^{\frac{28r}{3}-1} + \bar{\omega}_7^{\frac{28r}{3}-1})q^{13} & \text{if } 3 \mid r,\ \operatorname{ind} b \in C_c^7, \\ \frac{\sqrt{2}}{28}(\omega_7^{\frac{28r}{3}+1} + \bar{\omega}_7^{\frac{28r}{3}+1})q^{13} & \text{if } 3 \mid r,\ \operatorname{ind} b \in C_{-c}^7 \end{cases}$$

with the same c and ω_7 as in P_7. For $m = 23$ the Gauss sum $F_{11}(\chi)$ can be calculated with the method described on [12, p. 3]. We obtain $F_{11}(\chi) = 2^3(-3 + c\sqrt{-23})$, where $c \in \{1, -1\}$. Then

$$P_{23} - \frac{q^{22}-1}{23(q-1)} = \begin{cases} 0 & \text{if } 11 \nmid r, \\ -\frac{11}{23}(\omega_{23}^{\frac{23r}{11}} + \bar{\omega}_{23}^{\frac{23r}{11}})q^{\frac{69}{11}} & \text{if } 11 \mid r,\ 23 \mid \operatorname{ind} b, \\ \frac{q^{\frac{69}{11}}}{23} \operatorname{Re}(\omega_{23}^{\frac{23r}{11}}(1 + \sqrt{-23})) & \text{if } 11 \mid r,\ \operatorname{ind} b \in C_c^{23}, \\ \frac{q^{\frac{69}{11}}}{23} \operatorname{Re}(\omega_{23}^{\frac{23r}{11}}(1 - \sqrt{-23})) & \text{if } 11 \mid r,\ \operatorname{ind} b \in C_{-c}^{23}, \end{cases}$$

where $\omega_{23} = 3 - \sqrt{-23}$.

The index 2 case 2 holds for $m = 15$. Now $F_4(\chi) = 1 + c\sqrt{-15}$ in (24) is given in [12, Lemma 5], where $c \in \{1, -1\}$. We again just state the results for $m = 15$ and the related $m = 30$, and refer to [6] for the details. If $m = 15$ then

$$P_{15} - \frac{q^{14}-1}{15(q-1)} = -\frac{q^4+q^2-2}{15(q-1)}$$

for $2 \nmid r$,

$$P_{15} - \frac{q^{14}-1}{15(q-1)} = \begin{cases} -\frac{1}{15}\big(q+1+\sqrt{q^{13}}-\sqrt{q}\big) & \text{if } 3 \nmid \operatorname{ind} b, \\ -\frac{1}{15}\big(\frac{3(q^4-1)}{q-1} - 2\sqrt{q^{13}} + (\sqrt{q}+1)^2\big) & \text{if } 3 \mid \operatorname{ind} b \end{cases}$$

for $2 \mid r$, $4 \nmid r$, and

$$P_{15} - \frac{q^{14}-1}{15(q-1)} =$$

$$\begin{cases} -\frac{2}{15}\big(2(\omega_{15}^{\frac{15r}{4}} + \bar{\omega}_{15}^{\frac{15r}{4}}) + 1 \pm 2\big)\sqrt{q^{13}} & \\ \qquad -\frac{1}{5}\big(\frac{q^4-1}{q-1} \mp 4\sqrt{q^3}\big) - \frac{1}{3}(\sqrt{q}-1)^2 & \text{if } 15 \mid \operatorname{ind} b, \\ \frac{1}{15}\big(\omega_{15}^{\frac{15r}{4}} + \bar{\omega}_{15}^{\frac{15r}{4}} - 2 \pm 1\big)\sqrt{q^{13}} - \frac{1}{5}\big(\frac{q^4-1}{q-1} \pm \sqrt{q^3}\big) & \text{if } \operatorname{ind} b \in C_3^{15}, \\ \frac{1}{15}\big(2(\omega_{15}^{\frac{15r}{4}} + \bar{\omega}_{15}^{\frac{15r}{4}}) + 1 \mp 4\big)\sqrt{q^{13}} - \frac{1}{3}(q+1+\sqrt{q}) & \text{if } \operatorname{ind} b \in C_5^{15}, \\ \frac{1}{15}\big(2(\omega_{15}^{\frac{15r}{4}+1} + \bar{\omega}_{15}^{\frac{15r}{4}+1}) + 1 \pm 1\big)\sqrt{q^{13}} & \text{if } \operatorname{ind} b \in C_c^{15}, \\ \frac{1}{15}\big(2(\omega_{15}^{\frac{15r}{4}-1} + \bar{\omega}_{15}^{\frac{15r}{4}-1}) + 1 \pm 1\big)\sqrt{q^{13}} & \text{if } \operatorname{ind} b \in C_{-c}^{15} \end{cases}$$

for $4 \mid r$, where $\pm = (-1)^{\frac{r}{4}}$ and $\omega_{15} = -(1+\sqrt{-15})/4$.

If $m = 30$ then

$$P_{30} - \frac{q^{15}(q^{14}-1)}{30(q-1)} = -\frac{q^3(q^6-1)}{30(q-1)}$$

for $2 \nmid r$,

$$P_{30} - \frac{q^{15}(q^{14}-1)}{30(q-1)} = \begin{cases} -\frac{q^3(q^2-1)}{30(q-1)} + \frac{q^2}{30}(q^{12}-1) & \text{if } 3 \nmid \operatorname{ind} b, \\ -\frac{q^3(3q^6-2q^2-1)}{30(q-1)} - \frac{q^2}{15}(q^{12}-1) & \text{if } 3 \mid \operatorname{ind} b \end{cases}$$

for $2 \mid r$, $4 \nmid r$, and

$$P_{30} - \frac{q^{15}(q^{14}-1)}{30(q-1)}$$

$$= \begin{cases} -\frac{1}{15}\big(2(\omega_{15}^{\frac{15r}{2}} + \bar{\omega}_{15}^{\frac{15r}{2}}) + 3\big)q^{14} & \\ \qquad -\frac{q^5(q^4-1)}{10(q-1)} - \frac{q^3}{6}(q+1) + \frac{q^2}{15}(6q^2+5) & \text{if } 15 \mid \operatorname{ind} b, \\ \frac{1}{30}\big(\omega_{15}^{\frac{15r}{2}} + \bar{\omega}_{15}^{\frac{15r}{2}} - 1\big)q^{14} - \frac{q^4(q^5-1)}{10(q-1)} & \text{if } \operatorname{ind} b \in C_3^{15}, \\ \frac{1}{30}\big(2(\omega_{15}^{\frac{15r}{2}} + \bar{\omega}_{15}^{\frac{15r}{2}}) - 3\big)q^{14} - \frac{q^2(q^3-1)}{6(q-1)} & \text{if } \operatorname{ind} b \in C_5^{15}, \\ \frac{1}{15}\big(\omega_{15}^{\frac{15r}{2}+1} + \bar{\omega}_{15}^{\frac{15r}{2}+1} + 1\big)q^{14} & \text{if } \operatorname{ind} b \in C_c^{15}, \\ \frac{1}{15}\big(\omega_{15}^{\frac{15r}{2}-1} + \bar{\omega}_{15}^{\frac{15r}{2}-1} + 1\big)q^{14} & \text{if } \operatorname{ind} b \in C_{-c}^{15}, \end{cases}$$

for $4 \mid r$, where $\omega_{15} = -(1+\sqrt{-15})/4$.

The index 2 case 3 holds for $m = 21$. The Gauss sums $F_6(\chi) = -2(3+c\sqrt{-7})$ and $F_6(\chi^3) = 2(3+c\sqrt{-7}) = -F_6(\chi)$, where $c \in \{1,-1\}$, are computed in [14, Example 11]. Then

$$P_{21} - \frac{q^{20}-1}{21(q-1)} = -\frac{q^6+q^2-2}{21(q-1)}$$

for $2 \nmid r$, $3 \nmid r$,

$$P_{21} - \frac{q^{20}-1}{21(q-1)} = \begin{cases} -\frac{1}{21}\big(q+1 \mp (q^9-1)\sqrt{q}\big) & \text{if } 3 \nmid \operatorname{ind} b, \\ -\frac{1}{21}\big(\frac{3q^6+q^2-4}{q-1} \pm 2(q^9-1)\sqrt{q}\big) & \text{if } 3 \mid \operatorname{ind} b \end{cases}$$

for $2 \mid r$, $3 \nmid r$,

$$P_{21} - \frac{q^{20}-1}{21(q-1)} =$$

$$\begin{cases} -\big(\frac{q^6+7q^2-8}{21(q-1)} + \frac{\sqrt{q^5}}{7}\big((\omega_7^{7r}+\bar{\omega}_7^{7r})q^7 + (\omega_7^{\frac{7r}{3}}+\bar{\omega}_7^{\frac{7r}{3}})\big)\big) & \text{if } 7 \mid \operatorname{ind} b, \\ -\frac{q^6-1}{21(q-1)} + \frac{\sqrt{2q^5}}{21}\big((\omega_7^{7r-1}+\bar{\omega}_7^{7r-1})q^7 - (\omega_7^{\frac{7r}{3}+1}+\bar{\omega}_7^{\frac{7r}{3}+1})\big) & \\ & \text{if } \operatorname{ind} b \in C_c^7, \\ -\frac{q^6-1}{21(q-1)} + \frac{\sqrt{2q^5}}{21}\big((\omega_7^{7r+1}+\bar{\omega}_7^{7r+1})q^7 - (\omega_7^{\frac{7r}{3}-1}+\bar{\omega}_7^{\frac{7r}{3}-1})\big) & \\ & \text{if } \operatorname{ind} b \in C_{-c}^7 \end{cases}$$

for $2 \nmid r$, $3 \mid r$, and

$$P_{21} - \frac{q^{20}-1}{21(q-1)} =$$

$$\begin{cases} -\big(\frac{1}{21}\big(3(2 \pm 1)(\omega_{21}^{\frac{7r}{2}}+\bar{\omega}_{21}^{\frac{7r}{2}}) \pm 2q^7\big)\sqrt{q^5} & \\ \quad + \frac{1}{7}\big(\frac{q^6-1}{q-1} - 3(\omega_7^{\frac{7r}{3}}+\bar{\omega}_7^{\frac{7r}{3}})\sqrt{q^5}\big) + \frac{1}{3}(1 \mp \sqrt{q})^2\big) & \text{if } 21 \mid \operatorname{ind} b, \\ \frac{1}{21}\big(3(1 \mp 1)(\omega_{21}^{\frac{7r}{2}}+\bar{\omega}_{21}^{\frac{7r}{2}}) \pm q^7\big)\sqrt{q^5} - \frac{1}{3}(q+1 \pm \sqrt{q}) & \text{for } C_7^{21}, \\ \frac{\sqrt{q^5}}{21}\big(2\operatorname{Re}(\omega_{21}^{\frac{7r}{2}}(1+\sqrt{-7})) \pm \operatorname{Re}(\omega_{21}^{\frac{7r}{2}}(1-\sqrt{-7})) \mp 2q^7\big) & \\ \quad - \frac{1}{7}\big(\frac{q^6-1}{q-1} + (\omega_7^{\frac{7r}{3}-1}+\bar{\omega}_7^{\frac{7r}{3}-1})\sqrt{2q^5}\big) & \text{for } C_{3c}^{21}, \\ \frac{\sqrt{q^5}}{21}\big(2\operatorname{Re}(\omega_{21}^{\frac{7r}{2}}(1-\sqrt{-7})) \pm \operatorname{Re}(\omega_{21}^{\frac{7r}{2}}(1+\sqrt{-7})) \mp 2q^7\big) & \\ \quad - \frac{1}{7}\big(\frac{q^6-1}{q-1} + (\omega_7^{\frac{7r}{3}+1}+\bar{\omega}_7^{\frac{7r}{3}+1})\sqrt{2q^5}\big) & \text{for } C_{-3c}^{21}, \\ \frac{\sqrt{q^5}}{21}\big(-\operatorname{Re}(\omega_{21}^{\frac{7r}{2}}(1-\sqrt{-7})) \pm \operatorname{Re}(\omega_{21}^{\frac{7r}{2}}(1+\sqrt{-7})) \pm q^7\big) & \text{for } C_c^{21}, \\ \frac{\sqrt{q^5}}{21}\big(-\operatorname{Re}(\omega_{21}^{\frac{7r}{2}}(1+\sqrt{-7})) \pm \operatorname{Re}(\omega_{21}^{\frac{7r}{2}}(1-\sqrt{-7})) \pm q^7\big) & \text{for } C_{-c}^{21} \end{cases}$$

for $6 \mid r$, where C_i^{21} indicates the cyclotomic coset that $\operatorname{ind} b$ belongs to and $\pm = (-1)^{\frac{r}{2}}$. In addition, $\omega_7 = (1+\sqrt{-7})/\sqrt{8}$ is as in P_7 and $\omega_{21} = 3+\sqrt{-7}$.

The irreducible polynomial generator in [15] can be used to cross-check our formulae for small values of q and m. It lists every irreducible polynomial over $\mathbb{F}_q$, $q \le 8$, of a given degree m if there are at most 1000 such polynomials. We can use [15] to list every irreducible polynomial of degree $m \le 13$, 6, 3 over $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_8$, respectively. One can then pick the polynomials with $a = 0$ from this list. On the other hand, the formulae of this subsection give the number of these polynomials. For example, let $m = 3$. If $q = 2$, 8, then (25) gives $P_3 = \frac{q^2-1}{3\cdot(q-1)}$ for every b. The P_3 equals to 1 if $q = 2$, and to 3 if $q = 8$. If $q = 4$ then

(25) gives $P_3 = \frac{q^2-1}{3\cdot(q-1)} - \frac{1}{3}\sqrt{q} = 1$ for $3 \nmid \operatorname{ind} b$ ($b \neq 1$; 2 values), and $P_3 = \frac{q^2-1}{3\cdot(q-1)} + \frac{2}{3}\sqrt{q} = 3$ for $3 \mid \operatorname{ind} b$ ($b = 1$; 1 value). The other values in Table 5 are obtained similarly. Our results agree with those obtained using [15].

TABLE 5: The number of the irreducible polynomials with $a = 0$ and b fixed for small q and m.

q	m											
	2	3	4	5	6	7	8	9	10	11	12	13
2	0	1	1	3	4	9	14	28	48	93	165	315
4, $b = 1$	0	3	4	17	48							
4, $b \neq 1$	0	1	4	17	56							
8	0	3										

REFERENCES

[1] L.D. Baymert, R.J. McEliece: Weights of irreducible cyclic codes, *Inform. and Control*, vol. 20 (1972), 158–175.

[2] L.D. Baumert, J. Mykkeltveit: Weight distributions of some irreducible cyclic codes, *JPL Tech. Rep. 32-1526* (1973), 128–131.

[3] B.C. Berndt, R.J. Evans, K.S. Williams: *Gauss and Jacobi sums*, John Wiley & Sons, Inc., 1998.

[4] L. Carlitz: A theorem of Dickson on irreducible polynomials, *Proc. Amer. Math. Soc.*, vol. 3 (1952), 693–700.

[5] S.D. Cohen: Explicit theorems on generator polynomials, *Finite Fields Appl.,* vol. 11 (2005), 337–357.

[6] K. Kononen, M. Rinta-aho: Some computations on the number of certain irreducible polynomials, *Math. Univ. Oulu, Preprint* (October 2007). Available: `http://math.oulu.fi/raporttisarja.html`

[7] R. Lidl, H. Niederreiter: *Introduction to finite fields and their applications*, revised ed., Cambridge Univ. Press, 1994.

[8] M. Moisio: Exponential sums, Gauss sums, and irreducible cyclic codes, *Acta Univ. Oulu A306* (1998). Available: `http://www.uwasa.fi/~mamo/`

[9] M. Moisio: A note on evaluations of some exponential sums, *Acta Arith.,* vol. 93 (2000), 117–119.

[10] M. Moisio: Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm, submitted. Available: `http://www.uwasa.fi/~mamo/`

[11] M. Moisio, K. Ranto: Elliptic curves and explicit enumeration of irreducible polynomials with two coefficients prescribed, submitted. Available: `http://arxiv.org/`

[12] M. Moisio, K. Ranto, M. Rinta-aho, K. Väänänen: On the weight distribution of the duals of irreducible cyclic codes, cyclic codes with two zeros and hyper-Kloosterman codes, submitted. Available: `http://www.uwasa.fi/~mamo/`

[13] M. Moisio, K. Väänänen: Two recursive algorithms for computing the weight distribution of certain irreducible cyclic codes, *IEEE Trans. Inform. Theory*, vol. 45 (1999), 1244–1249.

[14] M. Rinta-aho: On the monomial exponential sums in certain index 2 cases and their connections to coding theory, *Math. Univ. Oulu, Preprint* (May 2007). Available: `http://math.oulu.fi/raporttisarja.html`
[15] F. Ruskey: An irreducible polynomial generator working over small finite fields. [Online] Available: `http://theory.cs.uvic.ca/gen/poly.html`
[16] M. van der Vlugt: Hasse-Davenport curves, Gauss sums, and weight distributions of irreducible cyclic codes, *J. Number Theory*, vol. 55 (1995), 145–159.
[17] M. van der Vlugt: On the weight hierarcy of irreducible cyclic codes, *J. Combin. Theory Ser. A*, vol. 71 (1995), 159–167.
[18] J.L. Yucas: Irreducible polynomials over finite fields with prescribed trace/ prescribed constant term, *Finite Fields Appl.,* vol. 12 (2006), 211–221.

K. Kononen: Department of Mathematical Sciences, University of Oulu, P.O. Box 3000, FIN-90014 OULUN YLIOPISTO, Finland
E-mail address: `kkononen@paju.oulu.fi`

M. Moisio: Department of Mathematics and Statistics, University of Vaasa, P.O. Box 700, FIN-65101 VAASA, Finland
E-mail address: `mamo@uwasa.fi`

M. Rinta-aho: Department of Mathematical Sciences, University of Oulu, P.O. Box 3000, FIN-90014 OULUN YLIOPISTO, Finland
E-mail address: `marko.rinta-aho@oulu.fi`

K. Väänänen: Department of Mathematical Sciences, University of Oulu, P.O. Box 3000, FIN-90014 OULUN YLIOPISTO, Finland
E-mail address: `keijo.vaananen@oulu.fi`