Available online at www.sciencedirect.com

ScienceDirect

Finite Fields and Their Applications 14 (2008) 798–815

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

Elliptic curves and explicit enumeration of irreducible polynomials with two coefficients prescribed ☆

Marko Moisio [a], Kalle Ranto [b,*,1]

[a] *Department of Mathematics and Statistics, University of Vaasa, PO Box 700, FIN-65101 Vaasa, Finland*
[b] *Department of Mathematics, University of Turku, FIN-20014 Turku, Finland*

Received 3 August 2007; revised 13 December 2007

Available online 13 February 2008

Communicated by Gary L. Mullen

Abstract

Let $\mathbf{F}_q$ be a finite field of characteristic $p = 2, 3$. We give the number of irreducible polynomials $x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in \mathbf{F}_q[x]$ with a_{m-1} and a_{m-3} prescribed for any given m if $p = 2$, and with a_{m-1} and a_1 prescribed for $m = 1, \ldots, 10$ if $p = 2, 3$. In the latter case an enumeration formula, applicable also if $m > 10$, is given, but it is explicit only up to the evaluation of certain Kronecker class numbers.

Keywords: Kloosterman sum; Exponential sum; Function field; Rational place; Dickson polynomial; BCH code; Melas code

1. Introduction

Let p be a prime, let r and m be positive integers, and let $\mathbf{F}_q$ denote the finite field with $q = p^r$ elements. The determination of the number N of irreducible polynomials

$$x^m + a_{m-1}x^m + \cdots + a_1x + a_0 \in \mathbf{F}_q[x],$$

☆ Part of the results have been presented in *Polynomials over Finite Fields and Applications*, November 18–23, 2006, BIRS, Canada, and in *8th International Conference on Finite Fields and Applications*, July 6–13, 2007, Melbourne, Australia.

* Corresponding author.
E-mail addresses: mamo@uwasa.fi (M. Moisio), kara@utu.fi (K. Ranto).

1 Research supported by the Academy of Finland, grant 108238.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2008.01.003

with some of the coefficients $a_0, \ldots, a_{m-1}$ prescribed, is a difficult problem in general and has been a subject of study for a long time, see e.g. [4, p. 340], where a short survey on recent results on this topic is given. For example, in [16,5] Yucas et al. considered the case of fixed a_{m-1}, a_{m-2}, and a_{m-3} over $\mathbf{F}_2$ and asked how these results could be generalized to $\mathbf{F}_{2^r}$. Our results on case (i) below can be seen as a partial, although not completely satisfactory, answer to this question.

Let $c \in \mathbf{F}_q$. In this paper the following special cases are considered:

(i) $p = 2$, $a_{m-1} = 0$, $a_{m-3} = c$,
(ii) $p = 2$ or $p = 3$, $a_{m-1} = c$, $a_1 = 0$.

In these cases the problem of determining N is closely related to the problem of counting the number of rational points on the fibre products of certain super-singular elliptic curves and of certain Kloosterman curves over $\mathbf{F}_{q^m}$. This problem can be tackled by using some properties of Kloosterman sums and cubic exponential sums, properties of Dickson polynomials, and the well-known (see e.g. [12,13,15]) weight distributions of the dual of the binary two-error-correcting BCH code of length $q-1$ and of the binary and ternary Melas codes of length $q-1$. This approach enables us to give N explicitly for any m in case (i) and for $m = 1, \ldots, 10$ in case (ii). In the latter case we have an enumeration formula which works for $m > 10$ as well, but it is explicit only up to the evaluation of certain Kronecker class numbers.

The rest of this note is organized as follows. In Section 2 we first recall some basic properties of Dickson polynomials and then a formula expressing the number of rational points on certain Artin–Schreier curves in terms of exponential sums is derived. That formula is used in Section 3 to get explicitly the number of rational points on the fibre product of certain super-singular elliptic curves, and finally, in Section 4, the number N of irreducible polynomials is determined by connecting it to the number of rational points on the curves studied in Sections 2 and 3.

2. Preliminaries

In this section some notations are fixed, a result concerning the point counting on fibre products of certain Artin–Schreier curves is established, and some results from [7,9,10] are recalled.

Let Tr and tr denote the trace functions from $\mathbf{F}_{q^m}$ onto $\mathbf{F}_p$ and $\mathbf{F}_q$, respectively, and let e and χ be the canonical additive characters of $\mathbf{F}_{q^m}$ and $\mathbf{F}_q$.

Let ω be a complex number, and let

$$D_m(T,\omega) := \sum_{j=0}^{\lfloor m/2 \rfloor} \frac{m}{m-j}\binom{m-j}{j}(-\omega)^j T^{m-2j} \in \mathbf{C}[T]$$

denote the Dickson polynomial of the first kind of degree m with parameter ω. We shall need the following two fundamental properties of Dickson polynomials:

$$D_m(t,\omega) = \left(\frac{t+\sqrt{t^2-4\omega}}{2}\right)^m + \left(\frac{t-\sqrt{t^2-4\omega}}{2}\right)^m \quad \forall t \in \mathbf{C}, \tag{1}$$

$$D_m\left(t+\frac{\omega}{t},\omega\right) = t^m + \frac{\omega^m}{t^m} \quad \forall t \in \mathbf{C}^*. \tag{2}$$

Next we consider point counting on fibre products of Artin–Schreier curves. Let L be a $\mathbf{F}_p$-subspace of the rational function field $\mathbf{F}_{q^m}(x)$ with a basis $\{f_1, \ldots, f_n\} \subset \mathbf{F}_{q^m}(x) \setminus \mathbf{F}_q$, and assume that the multiplicities of the poles of the non-zero elements of L are not divisible by p.

Let $f(x) \in L \setminus \{\mathbf{0}\}$, let $F_{f,m} = \mathbf{F}_{q^m}(x, y_f)$ with $y_f^p - y_f = f(x)$, and let

$$F_m = \mathbf{F}_{q^m}(x, y_{f_1}, \ldots, y_{f_n}).$$

Proposition 1. *(See [10, Theorem 18].) The number N_m of rational places of F_m is given by*

$$N_m = q^m + 1 - \frac{p^n - 1}{p - 1} + \sum_{f \in L \setminus \{0\}/\mathbf{F}_p^*} |S_f| + \sum_{f \in L \setminus \{0\}} \sum_{z \in \mathbf{F}_{q^m} \setminus P_f} e\big(f(z)\big),$$

where S_f is the set of rational places of $F_{f,m}$ lying above P_∞, and P_f is the set of poles of $f(x)$ in $\mathbf{F}_{q^m}$.

In [10] Proposition 1 was applied to the fibre product L_m of Kloosterman curves defined by

$$L_m = \mathbf{F}_{q^m}(x, y_a, y_b), \qquad y_a^q - y_a = x + ax^{-1}, \qquad y_b^q - y_b = x + bx^{-1},$$

for fixed $a, b \in \mathbf{F}_q$ with $a \neq b$.

Theorem 2 below will cover a more general situation. To state the result we fix some notations: let $a, b \in \mathbf{F}_q$, $a \neq b$, let $\beta \in \mathbf{F}_{q^m}$, and let $d = -1$ or $d = 3$. In addition, if $d = 3$ we assume $p \neq 3$.

Let

$$L_{m,d,\beta} := \mathbf{F}_{q^m}(x, y_a, y_b), \qquad y_a^q - y_a = x + a\big(\beta + x^d\big), \qquad y_b^q - y_b = x + b\big(\beta + x^d\big),$$

and for $u, v \neq 0$ in the subfield $\mathbf{F}_q$ denote

$$S_d^{(m)}(u, v) = \sum_z e\big(uz + vz^d\big),$$

where z runs over $\mathbf{F}_{q^m}^*$ or $\mathbf{F}_{q^m}$ according as d equals -1 or 3, respectively. Moreover, we denote $S_d(u, v) := S_d^{(1)}(u, v)$.

Theorem 2. *The number $N_{m,d}(\beta)$ of rational places of $L_{m,d,\beta}$ is given by*

$$N_{m,d}(\beta) = q^m + 1 + \sum_{v \in \mathbf{F}_q^*} e(\beta v) \sum_u S_d^{(m)}(u, v),$$

where u runs over $\mathbf{F}_q^*$ or $\mathbf{F}_q$ according as d equals -1 or 3, respectively.

Proof. Let $\{u_1, \ldots, u_r\}$ be a basis of $\mathbf{F}_q$ over $\mathbf{F}_p$. It follows by Proposition 1.2 and by the proof of Proposition 1.1 in [6] that

$$L_{m,d,\beta} = \mathbf{F}_{q^m}(x, y_{u_1}, \ldots, y_{u_r}, z_{u_1}, \ldots, z_{u_r})$$

with

$$y_{u_i}^p - y_{u_i} = u_i\big(x + a\big(\beta + x^d\big)\big) =: f_i(x),$$
$$z_{u_i}^p - z_{u_i} = u_i\big(x + b\big(\beta + x^d\big)\big) =: g_i(x)$$

for $i = 1, \dots, r$. Let L be the $\mathbf{F}_p$-subspace of $\mathbf{F}_{q^m}(x)$ spanned by the elements $f_1(x), \dots, f_r(x)$, $g_1(x), \dots, g_r(x)$. Now, each element $f(x)$ of L is of the form

$$f(x) = (au + bv)\beta + (u + v)x + (au + bv)x^d, \tag{3}$$

for some $u, v \in \mathbf{F}_q$.

If $f(x) = 0$, then $u = v = 0$ as $a \neq b$. It follows that the elements $f_1(x), \dots, g_r(x)$ are linearly independent over $\mathbf{F}_p$ and, moreover, the representation (3) is unique.

Since the mapping $(u, v) \mapsto (u + v, au + bv)$ is linear and invertible, it is a permutation of $\mathbf{F}_q^2 \setminus \{\mathbf{0}\}$, and therefore each non-zero $f(x) \in L$ is of the form $f(x) = v\beta + ux + vx^d$ for unique $(u, v) \in \mathbf{F}_q^2 \setminus \{\mathbf{0}\}$.

If $d = 3$, $|S_f| = 1$ for every $f \in L$ by [14, Proposition VI.4.1(c)] and Proposition 1 implies

$$N_{m,d}(\beta) = q^m + 1 + \sum_{(u,v)\in\mathbf{F}_q^2\setminus\{\mathbf{0}\}} \sum_{z\in\mathbf{F}_{q^m}} e\big(v\beta + uz + vz^d\big),$$

and the claim follows now by noting that the inner sum equals zero if $v = 0$.

Assume next that $d = -1$. Proposition 1 now implies that

$$\begin{aligned} N_{m,d}(\beta) = q^m + 1 &+ \frac{1}{p-1}\Bigg(-\big(q^2 - 1\big) + \sum_{(u,v)\in\mathbf{F}_q^2\setminus\{\mathbf{0}\}} |S_{u,v,\beta}|\Bigg) \\ &+ \sum_{(u,v)\in\mathbf{F}_q^2\setminus\{\mathbf{0}\}} e(v\beta) \sum_{z\in\mathbf{F}_{q^m}\setminus P_{u,v}} e\big(uz + vz^{-1}\big), \end{aligned} \tag{4}$$

where $S_{u,v,\beta}$ is the set of rational places of

$$\mathbf{F}_{q^m}(x, y),\ y^p - y = ux + v\big(\beta + x^{-1}\big)$$

lying above P_∞, and $P_{u,v}$ is the set of poles of $f(x) = ux + v(\beta + x^{-1})$ in $\mathbf{F}_{q^m}$. By [14, Proposition III.7.8(c), Corollary III.3.8] we know that

$$|S_{u,v,\beta}| = \begin{cases} 0 & \text{if } u = 0 \text{ and } \operatorname{Tr}(v\beta) \neq 0, \\ p & \text{if } u = 0 \text{ and } \operatorname{Tr}(v\beta) = 0, \\ 1 & \text{if } u \neq 0. \end{cases} \tag{5}$$

Assume $\operatorname{tr}(\beta) = 0$. Now, by (4) and (5), we get

$$\begin{aligned}N_{m,d}(\beta) &= q^m + 1 + \frac{1}{p-1}\left(-\left(q^2-1\right) + (q-1)p + q^2 - 1 - (q-1)\right)\\ &\quad + \sum_{v\in\mathbf{F}_q^*}\sum_{u\in\mathbf{F}_q^*} S_d^{(m)}(u,v) + \sum_{v\in\mathbf{F}_q^*}\sum_{z\in\mathbf{F}_{q^m}^*} e\left(vz^{-1}\right)\\ &= q^m + 1 + \sum_{v\in\mathbf{F}_q^*}\sum_{u\in\mathbf{F}_q^*} S_d^{(m)}(u,v).\end{aligned}$$

Assume finally that $\operatorname{tr}(\beta) \neq 0$. By (4) and (5) we now have

$$\begin{aligned}N_{m,d}(\beta) &= q^m + 1 + \frac{1}{p-1}\left(-\left(q^2-1\right) + (q/p-1)p + q^2 - 1 - (q-1)\right)\\ &\quad + \sum_{v\in\mathbf{F}_q^*} e(v\beta)\sum_{u\in\mathbf{F}_q^*} S_d^{(m)}(u,v) + \sum_{v\in\mathbf{F}_q^*} e(v\beta)\sum_{z\in\mathbf{F}_{q^m}^*} e\left(vz^{-1}\right)\\ &= q^m + 1 - 1 + \sum_{v\in\mathbf{F}_q^*} e(v\beta)\sum_{u\in\mathbf{F}_q^*} S_d^{(m)}(u,v) - \sum_{v\in\mathbf{F}_q^*}\chi\left(v\operatorname{tr}(\beta)\right)\end{aligned}$$

and the claim follows. □

By the following result we see that in order to count $N_{m,d}(\beta)$ it is enough to count $N_{m,d}(0)$ unless $\operatorname{tr}(\beta) \neq 0$, $d = 3$, and r is even. That case will be considered in the next section. From now on we use the abbreviated notation $N_{m,d} := N_{m,d}(0)$.

Corollary 3. *Let $\beta_1, \beta_2 \in \mathbf{F}_{q^m}$, and assume $\operatorname{tr}(\beta_1) = 0$, $\operatorname{tr}(\beta_2) \neq 0$. Then $N_{m,d}(\beta_1) = N_{m,d}$. Moreover, if $d = -1$, or $d = 3$ and r is odd, then*

$$N_{m,d}(\beta_2) = q^m + 1 - \frac{N_{m,d} - q^m - 1}{q-1}.$$

Proof. By Theorem 2 it is clear that $N_{m,d}(\beta_1) = N_{m,d}$. Let $\beta \in \mathbf{F}_{q^m}$. When $d = 3$, we have

$$N_{m,3}(\beta) = q^m + 1 + \sum_{v\in\mathbf{F}_q^*} e(v\beta)\sum_{u\in\mathbf{F}_q^*} S_3^{(m)}(u,v) + \sum_{v\in\mathbf{F}_q^*} e(v\beta)S_3^{(m)}(0,v),$$

where the last sum equals $\sum_{v,z} e(v(\beta + z^3)) = \sum_{v,z} e(vz) = 0$ since $z \mapsto z^3$ is a permutation by the assumptions. Therefore, in all cases

$$N_{m,d}(\beta) = q^m + 1 + \sum_{v\in\mathbf{F}_q^*} e(v\beta)\sum_{u\in\mathbf{F}_q^*}\sum_{z} e\left(uz + vz^d\right).$$

Now, by the substitution $z \mapsto u^{-1}z$ we get

$$N_{m,d}(\beta) = q^m + 1 + \sum_{v\in\mathbf{F}_q^*} e(v\beta)\sum_{u\in\mathbf{F}_q^*}\sum_{z} e\left(z + vu^{-d}z^d\right),$$

and since the map $u \mapsto vu^{-d}$ is a permutation of $\mathbf{F}_q^*$ we obtain

$$N_{m,d}(\beta) = q^m + 1 + \underbrace{\left(\sum_{v\in\mathbf{F}_q^*} e(v\beta)\right)}_{=:S}\left(\sum_{u\in\mathbf{F}_q^*} S_d^{(m)}(1,u)\right),$$

where S equals $q-1$ or -1 according as $\mathrm{tr}(\beta)=0$ or $\mathrm{tr}(\beta)\neq 0$, respectively, and the claim follows now easily. □

Corollary 4. *If $q=2$, then*

$$N_{m,-1} - \left(2^m+1\right) = (-1)^{m-1} D_m(1,2) = -\left(\frac{-1+\sqrt{-7}}{2}\right)^m - \left(\frac{-1-\sqrt{-7}}{2}\right)^m.$$

If $q=3$, then

$$\begin{aligned} N_{m,-1} - \left(3^m+1\right) &= 2(-1)^{m-1}\left(D_m(-1,3)+D_m(2,3)\right) \\ &= -2\left(\left(\frac{1+\sqrt{-11}}{2}\right)^m + \left(\frac{1-\sqrt{-11}}{2}\right)^m + \left(-1+\sqrt{-2}\right)^m \right. \\ &\quad \left. + \left(-1-\sqrt{-2}\right)^m\right). \end{aligned}$$

Proof. Since $S_{-1}^{(m)}(u,v) = (-1)^{m-1} D_m(S_{-1}(u,v),q)$ for $uv\neq 0$ by [8, Theorem 5.46], the claim follows now by Theorem 2, Eq. (1), and the fact $D_m(-t,\omega) = (-1)^m D_m(t,\omega)$. □

If q is a power of two or three, we can count $N_{m,-1}$ up to the evaluation of Kronecker class numbers:

Proposition 5. *(See [10, Lemma 35].) Let $p=2$ or $p=3$, and let $q=p^r$ with $r\geqslant 2$. Then*

$$N_{m,-1} = q^m + 1 + (-1)^{m-1}(q-1)\sum_{t\in S_p} H\left(t^2-4q\right) D_m(t,q),$$

where $H(d)$ is the Kronecker class number defined for any negative integer d, $d\equiv 0,1 \pmod 4$, as

$$\left|\left\{(u,v,w)\in\mathbf{Z}^3\colon\ v^2-4uw=d,\ |v|\leqslant u\leqslant w,\ \text{and } v\geqslant 0 \text{ if } |v|=u \text{ or } u=w\right\}\right|$$

and

$$S_p = \left\{t\in\mathbf{Z}\colon\ |t|<2\sqrt{q}, t\equiv -1(e)\right\} \quad \text{with } e = \begin{cases} 4, & \text{if } p=2, \\ 3, & \text{if } p=3. \end{cases}$$

In the case where q is unbounded power of two or three we are still able to give the $N_{m,-1}$ provided that m is relatively small:

Proposition 6. *(See [10, Theorem 32, Remark 33].) Let $q = p^r$ with $p = 2$ or $p = 3$ and $r \geqslant 2$. The number $N_{m,-1}$ of rational places of $L_{m,-1,0}$ is given by*

m	N'_m when $q = 2^r$	N'_m when $q = 3^r$
1	q	q
2	q^2	q^2
3	$\pm q^2$	0
4	0	q^2
5	$(t_7 \mp 1)q^3$	$\pm q^3$
6	$\pm q^3$	$(-1 \pm 1)q^3$
7	$(t_9 - t_7 + 1)q^4$	$(u_9 \mp 1)q^4$
8	$(1 \mp 1)q^4$	$q^4 - q + 1$
9	$(t_{11} - t_9 - 1)q^5$	$(u_{11} - u_9)q^5$
10	$\tau_2 q^2 - q^5$	$\tau_3 q^2 - q^5$

where $N'_m = (N_{m,-1} - q^m - 1)/(q-1) + q - 1$, $\pm = (-1)^r$, and

$w^r + \overline{w}^r$	w
t_7	$(1 + \sqrt{-15})/4$
t_9	$(-5 + \sqrt{-39})/8$
u_9	$(5 + 2\sqrt{-14})/9$
u_{11}	$(-1 + 4\sqrt{-5})/9$
τ_2	$-3 + \sqrt{-119}$
τ_3	$14 + \sqrt{-1991}$
t_{11}	$w_+^r + \overline{w_+}^r + w_-^r + \overline{w_-}^r$
$w_\pm$	$(-3 \pm \sqrt{505} + \sqrt{-510 \mp 6\sqrt{505}})/32$

3. The number of rational places of $L_{m,3,\beta}$

In order to count $N_{m,3}(\beta)$ we need the following three results.

Lemma 7. *Assume $p \neq 3$. Then*

$$S_3^{(m)}(u,v) = (-1)^{m-1} D_m\big(S_3(u,v), q\big) \quad \forall u, v \in \mathbf{F}_q,\ u \neq 0.$$

Proof. By Weil's theorem (see e.g. [8, Theorem 5.36]) we know that there exist complex numbers ω and ν satisfying $|\omega| = |\nu| = \sqrt{q}$ and

$$S_3^{(m)}(u,v) = -\big(\omega^m + \nu^m\big).$$

Clearly, $\overline{S_3^{(m)}(u,v)} = \sum_z e(-uz - vz^3) = S_3^{(m)}(u,v)$ so $S_3^{(m)}(u,v)$ is real and $\nu = \bar{\omega}$. Now, by (2)

$$D_m(\omega + q/\omega, q) = \omega^m + q^m/\omega^m = \omega^m + \bar{\omega}^m$$

and therefore

$$S_3^{(m)}(u,v) = -D_m(\omega + \bar{\omega}, q) = -D_m\big(-S_3(u,v), q\big). \qquad \square$$

Proposition 8. *Let $q = 2^r$. The value distribution of $S_3(u, v)$ is given by*

$S_3(u,v)$	# in case $2 \mid r$	# in case $2 \nmid r$
q	1	1
$-2\sqrt{q}$	$\frac{q-1}{24}(q-2\sqrt{q})$	0
$-\sqrt{2q}$	0	$\frac{q-1}{4}(q-\sqrt{2q})$
$-\sqrt{q}$	$\frac{q-1}{3}(q-\sqrt{q})$	0
0	$\frac{q-1}{4}q+(q-1)$	$\frac{q-1}{2}q+(q-1)$
$\sqrt{q}$	$\frac{q-1}{3}(q+\sqrt{q})$	0
$\sqrt{2q}$	0	$\frac{q-1}{4}(q+\sqrt{2q})$
$2\sqrt{q}$	$\frac{q-1}{24}(q+2\sqrt{q})$	0

where $S_3(u, v)$ is attained # times as (u, v) varies over $\mathbf{F}_q^2$.

Proof. Let γ be a primitive element of $\mathbf{F}_q$, and let

$$c(u,v) = \big(\mathrm{Tr}(u+v), \mathrm{Tr}\big(u\gamma + v\gamma^3\big), \ldots, \mathrm{Tr}\big(u\gamma^{q-2} + v\gamma^{3(q-2)}\big)\big),$$

be a codeword in the dual $B^\perp$ of the binary two-error-correcting BCH code of length $q-1$, and let $w(c(u, v))$ denote the Hamming weight of $c(u, v)$.

The claim follows now by the weight distribution of $B^\perp$ (see e.g. [12]) and by the following two facts which are easy to verify:

(1) Map $\psi : (\mathbf{F}_q^2, +) \to B^\perp$, $(u, v) \mapsto c(u, v)$ is a group isomorphism.
(2) $S_3(u, v) = q - 2w(c(u, v))$. □

In our results we need to separate the cases where some trace is a cube or not. Therefore, we let γ be a primitive element of $\mathbf{F}_q$ and then the non-zero cubes of $\mathbf{F}_q$ are denoted by $\langle\gamma^3\rangle$.

We rephrase a result by Carlitz [1] in the following form.

Proposition 9. *Let $q = 2^r$ and $v \in \mathbf{F}_q^*$. If r is even, then*

$$S_3(u,v) \in \begin{cases} \{0, \pm 2\sqrt{q}\} & \text{if } v \in \langle\gamma^3\rangle, \\ \{\pm\sqrt{q}\} & \text{if } v \notin \langle\gamma^3\rangle, \end{cases}$$

and each value is attained at least once as u varies over $\mathbf{F}_q$. Moreover,

$$S_3(0,v) = \begin{cases} (-1)^{r/2+1}2\sqrt{q} & \text{if } v \in \langle\gamma^3\rangle, \\ (-1)^{r/2}\sqrt{q} & \text{if } v \notin \langle\gamma^3\rangle. \end{cases}$$

Now we have all the tools in order to establish the main result of this section:

Theorem 10. *Let $q = 2^r$. The number $N_{m,3}$ of rational places of $L_{m,3,0}$ is given by*

r is odd		*r is even*	
m mod 8	$N_{m,3} - (q^m + 1)$	m mod 12	$N_{m,3} - (q^m + 1)$
0	$-2(q-1)q^{\frac{m+2}{2}}$	0	$-2(q-1)q^{\frac{m+2}{2}}$
± 1	$(q-1)q^{\frac{m+1}{2}}$	$\pm 1, \pm 5$	$(q-1)q^{\frac{m+1}{2}}$
± 2	$(q-1)q^{\frac{m+2}{2}}$	± 2	$(q-1)q^{\frac{m+2}{2}}$
± 3	$-(q-1)q^{\frac{m+1}{2}}$	± 3	$-(q-1)q^{\frac{m+1}{2}}$
4	0	± 4	0
		6	$-(q-1)q^{\frac{m+2}{2}}$

Let $\beta \in \mathbf{F}_{q^m}$ and $\mathrm{tr}(\beta) = c \neq 0$. If $r = 2s$, the number $N_{m,3}(\beta)$ of rational places of $L_{m,3,\beta}$ is given by

m mod 12	$N_{m,3}(\beta) - (q^m + 1)$, $c \in \langle \gamma^3 \rangle$	$N_{m,3}(\beta) - (q^m + 1)$, $c \notin \langle \gamma^3 \rangle$
0	$2q^{\frac{m+2}{2}}$	$2q^{\frac{m+2}{2}}$
$\pm 1, \pm 5$	$-q^{\frac{m+1}{2}}$	$-q^{\frac{m+1}{2}}$
± 2	$-q^{\frac{m+2}{2}}$	$-q^{\frac{m+2}{2}}$
± 3	$(1-(-1)^s 2\sqrt{q})q^{\frac{m+1}{2}}$	$(1+(-1)^s\sqrt{q})q^{\frac{m+1}{2}}$
± 4	$(-1)^s 2q^{\frac{m+3}{2}}$	$(-1)^{s+1}q^{\frac{m+3}{2}}$
6	$(1-(-1)^s 2\sqrt{q})q^{\frac{m+2}{2}}$	$(1+(-1)^s\sqrt{q})q^{\frac{m+2}{2}}$

Proof. Assume first that r is odd. Now, by Theorem 2, Lemma 7, and Proposition 8 we obtain

$$\begin{aligned} N_{m,3} - \left(q^m + 1\right) &= \sum_{v \in \mathbf{F}_q^*} \sum_{u \in \mathbf{F}_q} S_3^{(m)}(u, v) \\ &= (-1)^{m-1}\left(\frac{q-1}{4}(q - \sqrt{2q})D_m(-\sqrt{2q}, q)\right. \\ &\quad \left. + \frac{q-1}{4}(q + \sqrt{2q})D_m(\sqrt{2q}, q) + \frac{q-1}{2}qD_m(0, q)\right). \end{aligned}$$

We note that above the $q-1$ zeros of $S_3(u, v)$ corresponding to the pairs $(u, 0)$, $u \neq 0$, are excluded. By (1) we see that $D_m(\pm\sqrt{2q}, q) = 2(\pm\sqrt{q})^m \cos(\frac{m\pi}{4})$, $D_m(0, q) = 0$ if m is odd, and $D_m(0, q) = 2(-q)^{m/2}$ if m is even. Thus

$$N_{m,3} - \left(q^m + 1\right) = \begin{cases} \sqrt{2}(q-1)q^{\frac{m+1}{2}}\cos(\frac{m\pi}{4}) & \text{if } 2 \nmid m, \\ -(q-1)q^{\frac{m+2}{2}}(\cos(\frac{m\pi}{4}) + (-1)^{\frac{m}{2}}) & \text{if } 2 \mid m, \end{cases}$$

and the claim follows.

Assume next that r is even. By Theorem 2

$$S := N_{m,3}(\beta) - \left(q^m + 1\right) = \sum_{v \in \mathbf{F}_q^*} \chi(cv) \sum_{u \in \mathbf{F}_q} S_3^{(m)}(u, v)$$

$$= \sum_{i=0}^{2} \sum_{v \in \gamma^i \langle \gamma^3 \rangle} \chi(cv) \sum_{u \in \mathbf{F}_q} S_3^{(m)}(u, v)$$

$$= \sum_{i=0}^{2} \sum_{j=0}^{(q-4)/3} \chi\left(c\gamma^{i+3j}\right) \underbrace{\sum_{u \in \mathbf{F}_q} \sum_{x \in \mathbf{F}_{q^m}} e\left(ux + \gamma^i \left(\gamma^j x\right)^3\right)}_{=:S^*}.$$

By the substitution $x \mapsto \gamma^{-j} x$ we have

$$S^* = \sum_{u \in \mathbf{F}_q} \sum_{x \in \mathbf{F}_{q^m}} e\left(u\gamma^{-j} x + \gamma^i x^3\right) \overset{u \mapsto \gamma^j u}{=} \sum_{u \in \mathbf{F}_q} S_3^{(m)}\left(u, \gamma^i\right),$$

and therefore

$$S = \sum_{j=0}^{(q-4)/3} \chi\left(c\gamma^{3j}\right) \sum_{u \in \mathbf{F}_q} S_3^{(m)}(u, 1) + \sum_{i=1}^{2} \sum_{j=0}^{(q-4)/3} \chi\left(c\gamma^{i+3j}\right) \sum_{u \in \mathbf{F}_q} S_3^{(m)}\left(u, \gamma^i\right).$$

We observe that

$$\sum_{u \in \mathbf{F}_q} S_3^{(m)}\left(u, \gamma^2\right) \overset{x \mapsto x^2}{=} \sum_{u \in \mathbf{F}_q} \sum_{x \in \mathbf{F}_{q^m}} e\left(ux^2 + \gamma^2 \left(x^3\right)^2\right)$$

$$\overset{u \mapsto u^2}{=} \sum_{u \in \mathbf{F}_q} \sum_{x \in \mathbf{F}_{q^m}} e\left(\left(ux + \gamma x^3\right)^2\right) = \sum_{u \in \mathbf{F}_q} S_3^{(m)}(u, \gamma), \tag{6}$$

and we now get

$$S = \underbrace{\sum_{j=0}^{(q-4)/3} \chi\left(c\gamma^{3j}\right)}_{S_1} \underbrace{\sum_{u \in \mathbf{F}_q} S_3^{(m)}(u, 1)}_{S_2} + \underbrace{\sum_{i=1}^{2} \sum_{j=0}^{(q-4)/3} \chi\left(c\gamma^{i+3j}\right)}_{S_3} \underbrace{\sum_{u \in \mathbf{F}_q} S_3^{(m)}(u, \gamma)}_{S_4}.$$

Let us consider each sum S_i separately. Clearly, $S_1 = (S_3(0, c) - 1)/3$, and by Proposition 9

$$S_3 = \frac{1}{3}\left(S_3(0, c\gamma) - 1 + S_3\left(0, c\gamma^2\right) - 1\right)$$

$$= \begin{cases} \frac{2}{3}(q-1) & \text{if } c = 0, \\ \frac{2}{3}((-1)^s q^{1/2} - 1) & \text{if } c \in \langle \gamma^3 \rangle, \\ \frac{1}{3}((-1)^{s+1} 2q^{1/2} + (-1)^s q^{1/2} - 2) & \text{if } c \notin \langle \gamma^3 \rangle. \end{cases}$$

We apply the argument used with the sum S^* above to the opposite direction to get

$$S_2 = \frac{3}{q-1} \sum_{j=0}^{(q-4)/3} \sum_{u \in \mathbf{F}_q} S_3^{(m)}\left(u, \gamma^{3j}\right) = \frac{3}{q-1} \sum_{v \in \langle \gamma^3 \rangle} \sum_{u \in \mathbf{F}_q} S_3^{(m)}(u, v).$$

By Proposition 9 we know that the sum $S_3(u, v)$ gets exactly the values $0, \pm 2\sqrt{q}$ when $v \in \langle \gamma^3 \rangle$. By Lemma 7 and Proposition 8 we obtain

$$\begin{aligned} \frac{q-1}{3} S_2 = (-1)^{m-1} \Bigg(& \frac{q-1}{24}(q - 2\sqrt{q}) D_m(-2\sqrt{q}, q) \\ & + \frac{q-1}{24}(q + 2\sqrt{q}) D_m(2\sqrt{q}, q) + \frac{q-1}{4} q D_m(0, q) \Bigg), \end{aligned}$$

where in the last term we exclude $q-1$ zeros for $S_3(u, v)$ as they correspond to sums with $v = 0$.

By (1) we see that $D_m(\pm 2\sqrt{q}, q) = 2(\pm\sqrt{q})^m$, $D_m(0, q) = 0$ if m is odd, and $D_m(0, q) = 2(-q)^{m/2}$ if m is even. All in all,

$$S_2 = \begin{cases} -\frac{1}{2} q^{\frac{m}{2}+1} - \frac{3}{2} q (-q)^{\frac{m}{2}} & \text{if } 2 \mid m, \\ q^{\frac{m+1}{2}} & \text{if } 2 \nmid m. \end{cases}$$

Consider finally S_4. Now

$$S_4 = \frac{1}{2} \sum_{i=1}^{2} \sum_{u \in \mathbf{F}_q} S_3^{(m)}\left(u, \gamma^i\right) = \frac{3}{2(q-1)} \sum_{v \in \mathbf{F}_q^* \setminus \langle \gamma^3 \rangle} \sum_{u \in \mathbf{F}_q} S_3^{(m)}(u, v)$$

and by Proposition 9 the value set of $S_3(u, v)$ is $\{\pm\sqrt{q}\}$. Again, by Lemma 7 and Proposition 8 we get

$$\frac{2(q-1)}{3} S_4 = (-1)^{m-1} \left(\frac{q-1}{3}(q - \sqrt{q}) D_m(-\sqrt{q}, q) + \frac{q-1}{3}(q + \sqrt{q}) D_m(\sqrt{q}, q) \right).$$

By (1) $D_m(\pm\sqrt{q}, q)$ equals $2q^{m/2}$, $\pm q^{m/2}$, $-q^{m/2}$, and $\mp 2q^{m/2}$ when $m \equiv 0$, ± 1, ± 2, and 3 (mod 6), respectively. Hence, we get

$$S_4 = \begin{cases} -2q^{\frac{m}{2}+1} & \text{if } m \equiv 0 \pmod 6, \\ q^{\frac{m+1}{2}} & \text{if } m \equiv \pm 1 \pmod 6, \\ q^{\frac{m}{2}+1} & \text{if } m \equiv \pm 2 \pmod 6, \\ -2q^{\frac{m+1}{2}} & \text{if } m \equiv 3 \pmod 6. \end{cases}$$

By collecting all the calculations we obtain the claimed result. □

4. Enumeration of irreducible polynomials with prescribed coefficients

In this section we calculate the number of irreducible polynomials over $\mathbf{F}_q$ in the cases (i) and (ii) of the Introduction. The method we use here is a modification of the method introduced in [11] (see also [3,2]). Roughly speaking, this method involves two steps: first, count the number of all the elements of $\mathbf{F}_{q^m}$ with prescribed traces, and second, use Möbius inversion to count the number of elements of degree m with prescribed traces. From now on we assume that $p = 2$ or $p = 3$.

4.1. Elements of degree m with prescribed traces

Let $d = 3$ or $d = -1$ and employ the convention $0^{-1} = 0$.

Definition 11. For $c \in \mathbf{F}_q$ define

$$H_{c,d}(m) = \left|\left\{z \in \mathbf{F}_{q^m} \;\middle|\; \operatorname{tr}(z) = 0,\ \operatorname{tr}\left(z^d\right) = c\right\}\right|.$$

Lemma 12. *Let* $\alpha \in \mathbf{F}_{q^m}$ *satisfy* $\operatorname{tr}(\alpha) = 1$. *Then*

$$H_{c,d}(m) = \frac{1}{q^2}\left(N_{m,d}(-\alpha c) - 1 + \epsilon\right),$$

where

$$\epsilon = \begin{cases} 0 & \text{if } d = 3, \\ 1 - q & \text{if } d = -1 \text{ and } c \neq 0, \\ (q-1)^2 & \text{if } d = -1 \text{ and } c = 0. \end{cases}$$

Proof. With the standard techniques we get

$$\begin{aligned} H_{c,d}(m) &= \sum_{z \in \mathbf{F}_{q^m}} \left(\frac{1}{q} \sum_{u \in \mathbf{F}_q} \chi\left(\operatorname{tr}(z)u\right)\right)\left(\frac{1}{q} \sum_{v \in \mathbf{F}_q} \chi\left(\operatorname{tr}\left(z^d - \alpha c\right)v\right)\right) \\ &= \frac{1}{q^2} \sum_{u,v \in \mathbf{F}_q} \sum_{z \in \mathbf{F}_{q^m}} e\left(uz + vz^d - \alpha c v\right) \\ &= \frac{1}{q^2}\left(q^m + \sum_{v \in \mathbf{F}_q^*} e(-\alpha c v) \sum_{u \in \mathbf{F}_q} \sum_{z \in \mathbf{F}_{q^m}} e\left(uz + vz^d\right)\right) \\ &= \frac{1}{q^2}\left(q^m + \sum_{v \in \mathbf{F}_q^*} e(-\alpha c v) \sum_{u} S_d^{(m)}(u, v) + \epsilon\right), \end{aligned}$$

where the last equality follows by the definition of $S_d^{(m)}(u, v)$. The claim follows now by Theorem 2. □

Next we shall count the number of elements z in $\mathbf{F}_{q^m}$ of degree m satisfying $\operatorname{tr}(z) = 0$ and $\operatorname{tr}(z^d) = c$.

Definition 13. For $c \in \mathbf{F}_q$ define

$$G_{c,d}(m) = \left|\left\{z \in \mathbf{F}_{q^m} \;\middle|\; \operatorname{tr}(z) = 0,\ \operatorname{tr}\left(z^d\right) = c,\ z \notin \mathbf{F}_{q^n} \text{ if } n < m\right\}\right|.$$

We need the following well-known formula for the number of all irreducible polynomials (see e.g. [8, Theorem 3.25]):

Proposition 14. *The number of monic irreducible polynomials in $\mathbf{F}_q[x]$ of degree m is given by $I(m)/m$, where*

$$I(m) = \sum_{t|m} \mu(t) q^{\frac{m}{t}}.$$

Let n be a positive factor of m, and let $\operatorname{tr}_n : \mathbf{F}_{q^n} \to \mathbf{F}_q$ denote the relative trace function. Clearly, for every $z \in \mathbf{F}_{q^n}$ we have $\operatorname{tr}(z) = \frac{m}{n} \operatorname{tr}_n(z)$ and therefore

$$\operatorname{tr}(z) = \operatorname{tr}\left(z^d\right) = 0 \quad \text{iff} \quad \left[p \mid \frac{m}{n} \text{ or } \left(p \nmid \frac{m}{n} \text{ and } \operatorname{tr}_n(z) = \operatorname{tr}_n\left(z^d\right) = 0\right)\right].$$

Let $m = p^k s$ such that $p \nmid s$. Now

$$\begin{aligned} H_{0,d}(m) = H_{0,d}\left(p^k s\right) &= \sum_{n|m,\, p|\frac{m}{n}} I(n) + \sum_{n|m,\, p\nmid\frac{m}{n}} G_{0,d}(n) \\ &= \sum_{t|s} \sum_{i=0}^{k-1} I\left(p^i t\right) + \sum_{t|s} G_{0,d}\left(p^k t\right) = \sum_{t|s} \left(S\left(p^k t\right) + G_{0,d}\left(p^k t\right)\right), \end{aligned}$$

where $S(p^k t) = \sum_{i=0}^{k-1} I(p^i t)$. By Möbius inversion, see e.g. [8, Theorem 3.24], we get

$$S\left(p^k s\right) + G_{0,d}\left(p^k s\right) = \sum_{t|s} \mu\left(\frac{s}{t}\right) H_{0,d}\left(p^k t\right).$$

By Lemma 12 we now get the following theorem.

Theorem 15. *Let $m = p^k s$ with p and s coprime. Then*

$$G_{0,d}(m) = \sum_{t|s} \mu\left(\frac{s}{t}\right) H_{0,d}\left(p^k t\right) - S(m),$$

where

$$H_{0,d}(n) = \frac{1}{q^2}\left(N_{n,d}(0) - 1 + \epsilon\right) \quad \textit{and} \quad S(m) = \sum_{i=0}^{k-1} I\left(p^i s\right)$$

with

$$\epsilon = \begin{cases} 0 & \text{if } d = 3, \\ (q-1)^2 & \text{if } d = -1. \end{cases}$$

Assume next that $c \neq 0$, and let n be a positive factor of m. Now, for each $z \in \mathbf{F}_{q^n}$, we have that

$$\operatorname{tr}(z) = 0 \quad \text{and} \quad \operatorname{tr}\bigl(z^d\bigr) = c \quad \text{iff} \quad \operatorname{tr}_n(z) = 0 \quad \text{and} \quad \operatorname{tr}_n\bigl(z^d\bigr) = \frac{n}{m}c.$$

Since $n/m = 1$ or $n/m = \pm 1$ according as p equals 2 or 3, respectively, we see that

$$G_{\frac{nc}{m},d}(n) = G_{c,d}(n),$$

and therefore

$$H_{c,d}(m) = \sum_{t|s} G_{c,d}\bigl(p^k t\bigr).$$

Now, by Möbius inversion and Lemma 12 we get the following result.

Theorem 16. *Let $m = p^k s$ with p and s coprime, let $c \in \mathbf{F}_q^*$, and let $\alpha \in \mathbf{F}_{q^m}$ satisfy* $\operatorname{tr}(\alpha) = 1$. *Then*

$$G_{c,d}(m) = \sum_{t|s} \mu\left(\frac{s}{t}\right) H_{c,d}\bigl(p^k t\bigr),$$

where

$$H_{c,d}(n) = \frac{1}{q^2}\bigl(N_{n,d}(-\alpha c) - 1 + \epsilon\bigr) \quad \textit{and} \quad \epsilon = \begin{cases} 0 & \text{if } d = 3, \\ 1-q & \text{if } d = -1. \end{cases}$$

4.2. Irreducible polynomials of degree m with prescribed coefficients

Lemma 17. *Let $q = p^r$ with $p = 2$ or $p = 3$, and let $c \in \mathbf{F}_q$. The number of irreducible polynomials $p(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ in $\mathbf{F}_q[x]$ with $a_{m-1} = c$ and $a_1 = 0$ equals $G_{c,-1}(m)/m$.*

Proof. If $p(x)$ is irreducible, then $a_{m-1} = \operatorname{tr}(z)$, where z is any of the m distinct roots of $p(x)$ in $\mathbf{F}_{q^m}$. Moreover, since $a_0^{-1}x^m p(x^{-1})$ is monic and irreducible we get $\operatorname{tr}(z^{-1}) = a_1/a_0$. Hence, the number of irreducible $p(x)$ with $a_{m-1} = c$ and $a_1 = 0$ equals $G'_{c,-1}(m)/m$, where $G'_{c,-1}(m)$ is the number of elements z of degree m over $\mathbf{F}_q$ in $\mathbf{F}_{q^m}$ satisfying $\operatorname{tr}(z) = c$ and $\operatorname{tr}(z^{-1}) = 0$. But clearly $G'_{c,-1}(m) = G_{c,-1}(m)$. □

Remark 18. By the preceding proof it is clear that the number of irreducible polynomials $x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ in $\mathbf{F}_q[x]$ such that $a_{m-1} = 0$ and $a_1/a_0 = c$ also equals $G_{c,-1}(m)/m$.

Lemma 19. *Let $q = 2^r$ and $c \in \mathbf{F}_q$. The number of irreducible polynomials $p(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$ in $\mathbf{F}_q[x]$ with $a_{m-1} = 0$ and $a_{m-3} = c$ equals $G_{c,3}(m)/m$.*

Proof. Let $z = z_1, \ldots, z_m$ be the roots of an irreducible polynomial $p(x)$ in $\mathbf{F}_{q^m}$. If $m \geqslant 3$, we have, by Newton's formula (see [8, Theorem 1.75]), that

$$s_3 + s_2a_{m-1} + s_1a_{m-2} + a_{m-3} = 0,$$

where $s_k = \sum_{i=1}^m z_i^k = \mathrm{tr}(z^k)$. Since $s_1 = a_{m-1} = 0$, we get $a_{m-3} = \mathrm{tr}(z^3)$, and the claim follows. □

Lemma 17, Theorems 15 and 16, Corollary 3, and Proposition 6 give the following two corollaries:

Corollary 20. *Let $q = p^r$ with $p = 2$ or $p = 3$. The number of irreducible polynomials $x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$ in $\mathbf{F}_q[x]$ with $a_{m-1} = a_1 = 0$ equals $G_{0,-1}(m)/m$, where*

m	$G_{0,-1}(m)$ *with* $q = 2^r$	$G_{0,-1}(m)$ *with* $q = 3^r$
1	1	1
2	0	$q - 1$
3	$(1 \pm 1)(q - 1)$	0
4	0	$q^2 - 1$
5	$q^3 + (t_7 \mp 1)q(q - 1) - 1$	$q^3 \pm q(q - 1) - 1$
6	$(q - 1)(q^3 \pm q)$	$q(q - 1)(q^2 + q - 1 \pm 1)$
7	$q^5 + q^2(q - 1)(t_9 - t_7 + 1) - 1$	$q^5 + q^2(q - 1)(u_9 \mp 1) - 1$
8	$q^6 - q^4 + (1 \mp 1)q^2(q - 1)$	$q^6 + q^3 - 2q^2 - q + 1$
9	$q^7 + (q - 1)(q^3(t_{11} - t_9 - 1) - 1 \mp 1) - 1$	$q^7 + q^3(q - 1)(u_{11} - u_9) - q^3$
10	$q^8 - q^5 - q^4 + q^3 + (q - 1)\tau_2$	$q^8 - q^4 - (q - 1)(1 \pm q) + (q - 1)\tau_3$

Corollary 21. *Let $q = p^r$ with $p = 2$ or $p = 3$, and let $c \in \mathbf{F}_q^*$. The number of irreducible polynomials $x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$ in $\mathbf{F}_q[x]$ with $a_{m-1} = c$ and $a_1 = 0$ equals $G_{c,-1}(m)/m$, where*

m	$G_{c,-1}(m)$ *with* $q = 2^r$	$G_{c,-1}(m)$ *with* $q = 3^r$
1	0	0
2	0	0
3	$q \mp 1$	q
4	q^2	$q^2 - 1$
5	$q^3 - q(t_7 \mp 1)$	$q^3 \mp q$
6	$q^4 \mp q$	$q^4 \mp q$
7	$q^5 - q^2(t_9 - t_7 + 1)$	$q^5 - q^2(u_9 \mp 1)$
8	$q^6 + (-1 \pm 1)q^2$	$q^6 - 2q^2 + 1$
9	$q^7 - q^3(t_{11} - t_9 - 1) - q \pm 1$	$q^7 - q^3(u_{11} - u_9)$
10	$q^8 + q^3 - \tau_2$	$q^8 \pm q - \tau_3$

In principle, one could calculate the two tables above even further but the computations will become quite involved and the formulas will include more traces of Hecke operators, t_i, and values of Ramanujan's tau-function, τ_i.

Finally, we give some formulas for the number of irreducible polynomials in the case (i) in Introduction. This case differs essentially from the case (ii) above: we have all information needed in closed form and we just plug our formulas in e.g. *Mathematica* and count the formulas as far as we like. Unfortunately, we cannot give this result in any simple general formula due to the Möbius inversion and to the several cases in Theorem 10. Therefore, we illustrate our results by giving the number of the polynomials for every degree $m \leqslant 30$.

Lemma 19, Theorems 15 and 16, Corollary 3, and Theorem 10 give, with help of *Mathematica*, the following corollary.

Corollary 22. *Let $q = 2^r$ and $c \in \mathbf{F}_q$. The number of monic irreducible polynomials $x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$ in $\mathbf{F}_q[x]$ with $a_{m-1} = 0$ and $a_{m-3} = c$ equals $G_{c,3}(m)/m$, where*

m	$G_{0,3}(m)$, *if* $2 \mid r$	$G_{0,3}(m)$, *if* $2 \nmid r$	$G_{c,3}(m)$, *if* $2 \nmid r$ *and* $c \neq 0$
1	1	1	0
2	0	0	0
3	0	0	$q+1$
4	0	0	q^2
5	q^3+q^2-q-1	q^3-q^2+q-1	q^3+q
6	$q^4-2q^3+q^2$	q^4-q^2	q^4-q^2
7	$q^5+q^3-q^2-1$	$q^5+q^3-q^2-1$	q^5-q^2
8	q^6-q^4	$q^6-3q^4+2q^3$	q^6+2q^3
9	$q^7-q^4+q^3-1$	$q^7+q^4-q^3-1$	q^7-q^3-q-1
10	q^8-q^4	q^8-q^4	q^8-q^4
11	$q^9+q^5-q^4-1$	$q^9-q^5+q^4-1$	q^9+q^4
12	$q^{10}-3q^6+2q^5$	$q^{10}-q^6$	$q^{10}-q^2$
13	$q^{11}+q^6-q^5-1$	$q^{11}-q^6+q^5-1$	$q^{11}+q^5$
14	$q^{12}-q^6$	$q^{12}-q^6$	$q^{12}-q^6$
15	$q^{13}-q^7+q^6-q^3-q^2+q$	$q^{13}+q^7-q^6-q^3+q^2-q$	$q^{13}-q^6-q^3-2q-1$
16	$q^{14}-q^8$	$q^{14}-3q^8+2q^7$	$q^{14}+2q^7$
17	$q^{15}+q^8-q^7-1$	$q^{15}+q^8-q^7-1$	$q^{15}-q^7$
18	$q^{16}-2q^9+q^8-q^4+2q^3-q^2$	$q^{16}-q^8-q^4+q^2$	$q^{16}-q^8-q^4+q^2$
19	$q^{17}+q^9-q^8-1$	$q^{17}-q^9+q^8-1$	$q^{17}+q^8$
20	$q^{18}-q^{10}$	$q^{18}-q^{10}$	$q^{18}-q^2$
21	$q^{19}-q^{10}+q^9-q^5-q^3+q^2$	$q^{19}-q^{10}+q^9-q^5-q^3+q^2$	$q^{19}+q^9-q^5+q^2-q-1$
22	$q^{20}-q^{10}$	$q^{20}-q^{10}$	$q^{20}-q^{10}$
23	$q^{21}+q^{11}-q^{10}-1$	$q^{21}+q^{11}-q^{10}-1$	$q^{21}-q^{10}$
24	$q^{22}-3q^{12}+2q^{11}-q^6+q^4$	$q^{22}-3q^{12}+2q^{11}-q^6+3q^4-2q^3$	$q^{22}+2q^{11}-q^6-2q^3$
25	$q^{23}+q^{12}-q^{11}-q^3-q^2+q$	$q^{23}+q^{12}-q^{11}-q^3+q^2-q$	$q^{23}-q^{11}-q^3-q$
26	$q^{24}-q^{12}$	$q^{24}-q^{12}$	$q^{24}-q^{12}$
27	$q^{25}-q^{13}+q^{12}-q^7+q^4-q^3$	$q^{25}-q^{13}+q^{12}-q^7-q^4+q^3$	$q^{25}+q^{12}-q^7+q^3$
28	$q^{26}-q^{14}$	$q^{26}-q^{14}$	$q^{26}-q^2$
29	$q^{27}+q^{14}-q^{13}-1$	$q^{27}-q^{14}+q^{13}-1$	$q^{27}+q^{13}$
30	$q^{28}-2q^{15}+q^{14}-q^8+2q^3-q^2$	$q^{28}-q^{14}-q^8+q^2$	$q^{28}-q^{14}-q^8+q^2$

moreover, with $r = 2s$, $\pm = (-1)^s$, and $c \neq 0$ we have

m	$G_{c,3}(m)$, *if* $c \in \langle \gamma^3 \rangle$	$G_{c,3}(m)$, *if* $c \notin \langle \gamma^3 \rangle$
1	0	0
2	0	0
3	$q \mp 2q^{\frac{1}{2}} + 1$	$q \pm q^{\frac{1}{2}} + 1$
4	$q^2 \pm 2q^{\frac{3}{2}}$	$q^2 \mp q^{\frac{3}{2}}$
5	$q^3 - q$	$q^3 - q$
6	$q^4 \mp 2q^{\frac{5}{2}} + q^2$	$q^4 \pm q^{\frac{5}{2}} + q^2$
7	$q^5 - q^2$	$q^5 - q^2$
8	$q^6 \pm 2q^{\frac{7}{2}}$	$q^6 \mp q^{\frac{7}{2}}$
9	$q^7 \mp 2q^{\frac{7}{2}} + q^3 - q \pm 2q^{\frac{1}{2}} - 1$	$q^7 \pm q^{\frac{7}{2}} + q^3 - q \mp q^{\frac{1}{2}} - 1$
10	$q^8 - q^4$	$q^8 - q^4$
11	$q^9 - q^4$	$q^9 - q^4$
12	$q^{10} + 2q^5 - q^2 \mp 2q^{\frac{3}{2}}$	$q^{10} + 2q^5 - q^2 \pm q^{\frac{3}{2}}$
13	$q^{11} - q^5$	$q^{11} - q^5$
14	$q^{12} - q^6$	$q^{12} - q^6$
15	$q^{13} \mp 2q^{\frac{13}{2}} + q^6 - q^3 \pm 2q^{\frac{1}{2}} - 1$	$q^{13} \pm q^{\frac{13}{2}} + q^6 - q^3 \mp q^{\frac{1}{2}} - 1$
16	$q^{14} \pm 2q^{\frac{15}{2}}$	$q^{14} \mp q^{\frac{15}{2}}$
17	$q^{15} - q^7$	$q^{15} - q^7$
18	$q^{16} \mp 2q^{\frac{17}{2}} + q^8 - q^4 \pm 2q^{\frac{5}{2}} - q^2$	$q^{16} \pm q^{\frac{17}{2}} + q^8 - q^4 \mp q^{\frac{5}{2}} - q^2$
19	$q^{17} - q^8$	$q^{17} - q^8$
20	$q^{18} \pm 2q^{\frac{19}{2}} - q^2 \mp 2q^{\frac{3}{2}}$	$q^{18} \mp q^{\frac{19}{2}} - q^2 \pm q^{\frac{3}{2}}$
21	$q^{19} \mp 2q^{\frac{19}{2}} + q^9 - q^5 + q^2 - q \pm 2q^{\frac{1}{2}} - 1$	$q^{19} \pm q^{\frac{19}{2}} + q^9 - q^5 + q^2 - q \mp q^{\frac{1}{2}} - 1$
22	$q^{20} - q^{10}$	$q^{20} - q^{10}$
23	$q^{21} - q^{10}$	$q^{21} - q^{10}$
24	$q^{22} + 2q^{11} - q^6 \mp 2q^{\frac{7}{2}}$	$q^{22} + 2q^{11} - q^6 \pm q^{\frac{7}{2}}$
25	$q^{23} - q^{11} - q^3 + q$	$q^{23} - q^{11} - q^3 + q$
26	$q^{24} - q^{12}$	$q^{24} - q^{12}$
27	$q^{25} \mp 2q^{\frac{25}{2}} + q^{12} - q^7 \pm 2q^{\frac{7}{2}} - q^3$	$q^{25} \pm q^{\frac{25}{2}} + q^{12} - q^7 \mp q^{\frac{7}{2}} - q^3$
28	$q^{26} \pm 2q^{\frac{27}{2}} - q^2 \mp 2q^{\frac{3}{2}}$	$q^{26} \mp q^{\frac{27}{2}} - q^2 \pm q^{\frac{3}{2}}$
29	$q^{27} - q^{13}$	$q^{27} - q^{13}$
30	$q^{28} \mp 2q^{\frac{29}{2}} + q^{14} - q^8 \pm 2q^{\frac{5}{2}} - q^2$	$q^{28} \pm q^{\frac{29}{2}} + q^{14} - q^8 \mp q^{\frac{5}{2}} - q^2$

Remark 23. The expressions for $G_{c,d}(m)$ are approximately of the form $q^{m-2} + O(q^{\frac{m}{2}})$. In the case $2 \nmid r$ and $c \neq 0$ the formulas for $G_{c,3}(m)$ are quite close to q^{m-2} when $m = 4s$ and s is an odd prime. Indeed, if $m = 4s$ and $s = n^j$ for some odd prime n, we see by Corollary 3, Theorem 10, and Lemma 12 that $H_{c,3}(m) = q^{m-2}$, and then, by Theorem 16, we have $G_{c,3}(m) = q^{m-2} - q^{\frac{m}{n}-2}$. Especially, if $j = 1$, then $G_{c,3}(m) = q^{m-2} - q^2$.

Acknowledgments

This work was inspired by the *Polynomials over Finite Fields and Applications* workshop at Banff International Research Station, Canada. We thank the organizers for the invitation to the BIRS workshop. We also thank two anonymous referees for their comments which improved this article.

References

[1] L. Carlitz, Explicit evaluation of certain exponential sums, Math. Scand. 44 (1) (1979) 5–16.
[2] W.-S. Chou, S.D. Cohen, Primitive elements with zero traces, Finite Fields Appl. 7 (1) (2001) 125–141.
[3] S.D. Cohen, Kloosterman sums and primitive elements in Galois fields, Acta Arith. 94 (2) (2000) 173–201.
[4] S.D. Cohen, Explicit theorems on generator polynomials, Finite Fields Appl. 11 (3) (2005) 337–357.
[5] R.W. Fitzgerald, J.L. Yucas, Irreducible polynomials over GF(2) with three prescribed coefficients, Finite Fields Appl. 9 (3) (2003) 286–299.
[6] A. García, H. Stichtenoth, Elementary abelian p-extensions of algebraic function fields, Manuscripta Math. 72 (1) (1991) 67–79.
[7] R. Lidl, G.L. Mullen, G. Turnwald, Dickson Polynomials, Pitman Monogr. Surv. Pure Appl. Math., vol. 65, Longman Scientific & Technical, Harlow, 1993.
[8] R. Lidl, H. Niederreiter, Finite Fields, second ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, 1997.
[9] M. Moisio, The moments of a Kloosterman sum and the weight distribution of a Zetterberg-type binary cyclic code, IEEE Trans. Inform. Theory 53 (2) (2007) 843–847.
[10] M. Moisio, On the moments of Kloosterman sums and fibre products of Kloosterman curves, Finite Fields Appl. (2008), doi:10.1016/j.ffa.2007.06.001, in press.
[11] H. Niederreiter, An enumeration formula for certain irreducible polynomials with an application to the construction of irreducible polynomials over the binary field, Appl. Algebra Engrg. Comm. Comput. 1 (2) (1990) 119–124.
[12] R. Schoof, Families of curves and weight distributions of codes, Bull. Amer. Math. Soc. (N.S.) 32 (2) (1995) 171–183.
[13] R. Schoof, M. van der Vlugt, Hecke operators and the weight distributions of certain codes, J. Combin. Theory Ser. A 57 (2) (1991) 163–186.
[14] H. Stichtenoth, Algebraic Function Fields and Codes, Universitext, Springer-Verlag, Berlin, 1993.
[15] G. van der Geer, R. Schoof, M. van der Vlugt, Weight formulas for ternary Melas codes, Math. Comp. 58 (198) (1992) 781–792.
[16] J.L. Yucas, G.L. Mullen, Irreducible polynomials over GF(2) with prescribed coefficients, Discrete Math. 274 (2004) 265–279.