The Number of Irreducible Polynomials of Degree n over $\mathbb{F}_q$ with Given Trace and Constant Terms

B. Omidi Koma, D. Panario[1], Q. Wang[1]

School of Mathematics and Statistics, Carleton University
1125 Colonel By Drive, Ottawa, ON, K1S 5B6

Abstract

We study the number $N_\gamma(n, c, q)$ of irreducible polynomials of degree n over $\mathbb{F}_q$ where the trace γ and the constant term c are given. Under certain conditions on n and q, we obtain bounds on the maximum of $N_\gamma(n, c, q)$ varying c and γ. We show with concrete examples how our results improve previous known bounds. In addition, we improve upper and lower bounds of any $N_\gamma(n, c, q)$ when $n = a(q - 1)$ for nonzero constant term c and nonzero trace γ. As a byproduct, we give a simple and explicit formula for the number $N(n, c, q)$ of irreducible polynomials over $\mathbb{F}_q$ of degree $n = q - 1$ with prescribed primitive constant term c.

Key words: Finite fields, irreducible polynomials, trace and constant terms.
2008 MSC: 12E30

1. Introduction

Let $q = p^\omega$, where p is a prime. The problem of estimating the number of irreducible polynomials of degree n over the finite field $\mathbb{F}_q$ with some prescribed coefficients has been largely studied. Carlitz [1] and Kuz'min [8] give the number of irreducible polynomials with the first coefficient prescribed and the first two coefficients prescribed, respectively; see [2] for a similar result over $\mathbb{F}_2$, and [11] for more general results. Yucas and Mullen [13] and Fitzgerald and Yucas [6] consider the number of irreducible polynomials of degree n over $\mathbb{F}_2$ with the first three coefficients prescribed. Over any finite field $\mathbb{F}_q$, Yucas [12] gives the number of irreducible polynomials with prescribed first or last coefficient. More recently, Moisio et al. [7, 10] consider the number of irreducible polynomials with fixed trace and norm. Their approach is based on exponential sums and provide explicit results for some particular cases different from ours. Our approach here is completely elementary and it is based on Yucas [12]. For

Email addresses: `bomidi@math.carleton.ca` (B. Omidi Koma), `daniel@math.carleton.ca` (D. Panario), `wang@math.carleton.ca` (Q. Wang)

[1] The second and third authors are supported in part by NSERC of Canada.

an excellent survey paper (up to 2005) on polynomials (irreducible or primitive) with prescribed coefficients, see Cohen [4]. We do not treat here the case of primitive polynomials with prescribed coefficients; see [4, 5, 3].

We now give the format of the paper. In Section 2 we review the required background and fix the notation for this paper. The main results of this paper are given in Sections 3 and 4. Fix q and n; we study $N_\gamma(n,c,q)$, the number of irreducible polynomials of degree n over $\mathbb{F}_q$ where the trace γ and the constant term c are given. We obtain bounds on the maximum of $N_\gamma(n,c,q)$ under certain conditions on q and n (Theorem 6). We show with concrete examples how our results improve previous bounds. Our results are particularly better when the degree n is a multiple of $q-1$. We treat this case in Section 4. We give a simple and explicit formula for the number $N(n,c,q)$ of irreducible polynomials over $\mathbb{F}_q$ of degree $n=q-1$ with prescribed primitive constant term c, and a simple upper bound of it for $n=a(q-1)$ with $a>1$ (Theorem 9). Finally, we obtain improved upper and lower bounds of $N_\gamma(n,c,q)$ with $n=a(q-1)$ and nonzero trace γ and nonzero constant term c (Theorems 13 and 14, respectively).

2. Background and notation

The number of irreducible polynomials of degree n and trace γ over $\mathbb{F}_q$ is denoted by $N_\gamma(n,q)$. For given p and m, we say that m is *pfree*, if $p \nmid m$. For $n=p^\kappa\psi$ where ψ is *pfree*, Corollary 2.7 of [12] proves that the number $N_\gamma(n,q)$, for $\gamma \neq 0$, is given by

$$N_\gamma(n,q) = \frac{1}{nq}\sum_{d|\psi}\mu(d)q^{n/d}, \tag{1}$$

where μ represents the Mobius function defined by $\mu(1)=1$; $\mu(d)=0$, if $p^2|d$ for some prime p; and $\mu(d)=(-1)^r$ if d is the product of r distinct primes.

If $n=p^\kappa\psi$ then using κ we introduce a variable ε as $\varepsilon=1$ if $\kappa>0$ and $\varepsilon=0$ if $\kappa=0$. For trace zero, Corollary 2.8 of [12] gives $N_0(n,q)$ as

$$N_0(n,q) = \frac{1}{nq}\sum_{d|\psi}\mu(d)q^{n/d} - \frac{\varepsilon}{n}\sum_{d|\psi}\mu(d)q^{n/dp}.$$

We use $N(n,c,q)$ for the number of irreducible polynomials of degree n and constant term c over $\mathbb{F}_q$. Let

$$D_n = \{r\colon r \mid q^n-1, r \nmid q^m-1 \text{ for } m<n\}.$$

For each $r \in D_n$, let $r=m_r d_r$, where $d_r = \gcd\left(r, \frac{q^n-1}{q-1}\right)$. It is easy to see that $m_r \mid q-1$. Suppose that the order of the constant c is ρ. In [12] it is shown that the number $N(n,c,q)$ can be found as

$$N(n,c,q) = \frac{1}{n\phi(\rho)}\sum_{\substack{r\in D_n\\ m_r=\rho}}\phi(r),$$

where ϕ denotes Euler's function. In this sum for each $r \in D_n$ the number m_r is fixed as $\rho = \mathrm{ord}(c)$. If both trace γ and a nonzero contant c are prescribed, Carlitz [1] obtained an asymptotic formula, as $n \to \infty$,

$$N_\gamma(n, c, q) = \frac{q^n - 1}{nq(q-1)} + O\left(q^{n/2}\right). \tag{2}$$

Using a bijection $f(x) \mapsto c^{-1}x^n f(\frac{1}{x})$, $N_\gamma(n, c, q)$ equals the number of irreducible polynomials of degree n in the arithmetic progression $\{ax + c + g(x)x^2 \mid g(x) \in \mathbb{F}_q[x]\}$, where $a = -\gamma c^{-1}$. Applying a general asymptotic bound on the number of primes on an arithmetic progression, Moisio [10] pointed out the following improvement of Equation (2), as $n \to \infty$,

$$N_\gamma(n, c, q) = \frac{q^{n-1}}{n(q-1)} + O\left(\frac{q^{n/2}}{n}\right).$$

For the estimation of the error term, Wan [14] established the following effective bound

$$\left| N_\gamma(n, c, q) - \frac{q^{n-1}}{n(q-1)} \right| \le \frac{3}{n} q^{\frac{n}{2}}.$$

Recently, this bound was improved by Moisio [10] by considering two separate cases whether γ is zero or not. He obtained for nonzero γ,

$$\left| N_\gamma(n, c, q) - \frac{q^n - 1}{nq(q-1)} \right| < \frac{2}{q-1} q^{\frac{n}{2}},$$

and for zero trace

$$\left| N_0(n, c, q) - \frac{q^{n-1} - 1}{n(q-1)} \right| < \frac{2}{q-1} q^{\frac{n}{2}}.$$

The focus of this paper is in the study of $N_\gamma(n, c, q)$, where γ and c are given.

2.1. The structure of D_n

For a better understanding of $N_\gamma(n, c, q)$, where $1 \le \gamma \le q-1$, we need to know the structure of the set $D_n = \{r \colon r \mid q^n - 1, r \nmid q^m - 1 \text{ for } m < n\}$. Let us assume that we have the prime factorization $q - 1 = p_1^{g_1} \ldots p_k^{g_k}$, such that $p_1, \ldots, p_k$ are distinct prime factors, and $g_i \ge 1$ for $1 \le i \le k$. Similarly, we let $q^n - 1 = p_1^{e_1} \ldots p_k^{e_k} p_{k+1}^{e_{k+1}} \ldots p_t^{e_t}$, where $e_i \ge g_i \ge 1$, for $1 \le i \le k$, and $e_i \ge 1$, for $k + 1 \le i \le t$. Let $S_1 = \{1, \ldots, k\}$, and $S_2 = \{k + 1, \ldots, t\}$. We have the following lemma.

Lemma 1. *For each $r \mid q^n - 1$ where $r = m_r d_r$, with $d_r = \gcd\left(r, \frac{q^n-1}{q-1}\right)$ and $m_r \mid q-1$ there exists a positive integer R such that $r = \frac{q^n-1}{R}$, and $\gcd(R, q-1) = \frac{q-1}{m_r}$.*

PROOF. Since $r \mid q^n-1$, there exists R such that $r = (q^n-1)/R$. Since $r = m_r d_r$ with $m_r \mid q-1$ and $d_r = \gcd\left(r, \frac{q^n-1}{q-1}\right)$, there exist integers T and V, such that $q-1 = m_r T$, and $\frac{q^n-1}{q-1} = d_r V$. Therefore,

$$\begin{aligned}\gcd(R, q-1) &= \gcd\left(\frac{q^n-1}{m_r d_r}, q-1\right)\\ &= \frac{q-1}{m_r}\gcd\left(\frac{q^n-1}{d_r(q-1)}, m_r\right) = \frac{q-1}{m_r}\gcd(V, m_r).\end{aligned}$$

Moreover $d_r = \gcd\left(r, \frac{q^n-1}{q-1}\right) = \gcd(m_r d_r, d_r V) = d_r \gcd(m_r, V)$. Hence, we get $\gcd(m_r, V) = 1$, and the result follows. ■

In terms of the $\gcd(R, q-1)$ we can consider two cases:

Case 1: If $\gcd(R, q-1) = \frac{q-1}{m_r} = 1$, then $m_r = q-1$, and all the factors of R are from $q^{n-1} + q^{n-2} + \cdots + q + 1$, and not from $q-1$. Then $r = p_1^{e_1} \dots p_k^{e_k} p_{k+1}^{f_{k+1}} \dots p_t^{f_t}$, where $0 \le f_i \le e_i$, for $i \in S_2$.

Case 2: If $\gcd(R, q-1) > 1$, then $m_r < q-1$ and there exist some common primes between R and $q-1$. Then let r be given by $r = p_1^{f_1} p_2^{f_2} \dots p_k^{f_k} p_{k+1}^{f_{k+1}} \dots p_t^{f_t}$ where $f_i \le e_i$ for all $i \in S_1 \cup S_2$, and let us assume that the factorization of $q^m - 1$ is

$$q^m - 1 = p_1^{h_{m,1}} \dots {p_k}^{h_{m,k}} {p_{k+1}}^{h_{m,k+1}} \dots p_t^{h_{m,t}} {p_{t+1}}^{h_{m,t+1}} \dots p_l^{h_{m,l}}, \qquad (3)$$

where $h_{m,i} \ge g_i$, for $i \in S_1$, and $h_{m,i} \ge 0$, for $i \in S_2$. Also for all $i = t+1, \dots, l$, we have $h_{m,i} \ge 1$.

Now let us consider the structure of D_n. For the above r to be in D_n, r must not a divisor of $q^m - 1$ for any $m \le n-1$. To separate the two cases, we represent the elements of D_n by r and r' where $r = \frac{q^n-1}{R}$, with $\gcd(R, q-1) = 1$, and $r' = \frac{q^n-1}{R'}$ such that $\gcd(R', q-1) > 1$ respectively. Let $p_1^{f_1} \dots p_k^{f_k} p_{k+1}^{f_{k+1}} \dots p_t^{f_t}$ be any r or r' from the set D_n. Since r and r' are not divisors of $q^m - 1$, for $m \le n-1$, we have the following conditions

1. $f_i \le e_i$ for all $i \in S_1 \cup S_2$;

2.(a) $f_j = e_j$, for all $j \in S_1$, and $r = p_1^{e_1} \dots p_k^{e_k} p_{k+1}^{f_{k+1}} \dots p_t^{f_t} \nmid q^m - 1$, for $m \le n-1$; or

2.(b) There exist $\delta \in S_1$ such that $f_\delta < e_\delta$. Then since for all $m \le n-1$ we have $p_1^{f_1} \dots p_k^{f_k} p_{k+1}^{f_{k+1}} \dots p_t^{f_t} \nmid q^m - 1$, by considering (3) as the factorization of $q^m - 1$, there exists $j \in S_1 \cup S_2$ such that $f_j > h_{m,j}$.

2.2. Fixed constant term with different traces

Let $c \in \mathbb{F}_q^\times$ be a fixed nonzero constant. We study the number of irreducible polynomials of degree n and constant term c for different values of the trace coefficient.

Lemma 2. *Let γ and δ be two nonzero traces. If c is a constant from $\mathbb{F}_q^{\times}$, then*

$$N_{\gamma}(n,c,q) = N_{\delta}\left(n, c\left(\frac{\delta}{\gamma}\right)^{n}, q\right).$$

PROOF. Suppose γ and δ are two nonzero traces in $\mathbb{F}_q$, and let $P_{\gamma}(n,c,q)$ denote the set of all irreducible polynomials of degree n, trace γ and constant term c over the finite field $\mathbb{F}_q$. We show that there exists a one-to-one correspondence between $P_{\gamma}(n,c,q)$ and $P_{\delta}\left(n, c(\frac{\delta}{\gamma})^{n}, q\right)$. For this we consider the mapping used in Lemma 2.1 of [12]. Namely, let the mapping $\varphi : P_{\gamma}(n,c,q) \to P_{\delta}\left(n, c(\frac{\delta}{\gamma})^{n}, q\right)$ be defined by

$$\varphi(f(x)) = \left(\frac{\delta}{\gamma}\right)^{n} f\left(\frac{\gamma}{\delta}x\right).$$

It is straightforward to verify that ϕ is well-defined and it is a bijection. ∎

Let $\mathbb{F}_q = \{a_0 = 0, a_1 = 1, a_2, \ldots, a_{q-1}\}$. The following table gives the number of irreducible polynomials of degree n with given trace and constant term.

Table 1: Distribution of polynomials of degree n over a finite field $\mathbb{F}_q$.

Tr \ Cons	a_1	$\cdots$	a_j	$\cdots$	a_{q-1}	Row Total
a_0	$y_{0,1}$	$\cdots$	$y_{0,j}$	$\cdots$	$y_{0,q-1}$	$N_0(n,q)$
a_1	$x_{1,1}$	$\cdots$	$x_{1,j}$	$\cdots$	$x_{1,q-1}$	$N_1(n,q)$
$\vdots$	$\vdots$		$\vdots$		$\vdots$	$\vdots$
a_i	$x_{i,1}$	$\cdots$	$x_{i,j}$	$\cdots$	$x_{i,q-1}$	$N_i(n,q)$
$\vdots$	$\vdots$		$\vdots$		$\vdots$	$\vdots$
a_{q-1}	$x_{q-1,1}$	$\cdots$	$x_{q-1,j}$	$\cdots$	$x_{q-1,q-1}$	$N_{q-1}(n,q)$
Column Total	$N(n,1,q)$	$\cdots$	$N(n,j,q)$	$\cdots$	$N(n,q-1,q)$	$N(n,q)$

Abusing notation, if $c = a_j \in \mathbb{F}_q^{\times}$, for some $j \in \{1,2,\ldots,q-1\}$, then we denote $N(n,c,q)$ by $N(n,j,q)$. Also for $\gamma = a_i$, where $i \in \{0,1,\ldots,q-1\}$, we use $N_i(n,q)$ for $N_{\gamma}(n,q)$. Moreover $N_{\gamma}(n,c,q) = N_i(n,j,q)$, where $0 \leq i,j \leq q-1$, and $j \neq 0$. For simplicity, we use notations $x_{i,j}$ for $N_i(n,j,q)$ where $1 \leq i,j \leq q-1$, and $y_{0,j}$ for $N_0(n,j,q)$ where $1 \leq j \leq q-1$.

For any n, we know that $c\left(\frac{\delta}{\gamma}\right)^{n} = c^{'}$ is a constant in $\mathbb{F}_q$. Clearly by Lemma 2, we have $N_{\gamma}(n,c,q) = N_{\delta}(n,c^{'},q)$, which implies that for any nonzero traces $\gamma = a_i$ and $\delta = a_k$ the numbers on the row a_k are a permutation of the numbers on the row a_i, where $1 \leq i,j \leq q-1$. If we consider any column which is related to a constant $c = a_j$ then we have an equation of the form

$$y_{0,j} + \sum_{i=1}^{q-1} x_{i,j} = N(n,j,q). \tag{4}$$

Also in column a_j we know that some entries $x_{i,j}$ could be repeated. Let $R_j = \{1, 2, \ldots, k\}$ be the set of indices i in the column a_j such that no $x_{i,j}$ is repeated. Clearly $R_j \subseteq \{1, 2, \ldots, q-1\}$, and if in the column a_j there is no repeated entry, then $R_j = \{1, 2, \ldots, q-1\}$. Let $A_{i,j}$ represent the number of times $x_{i,j}$ appears in the entries of column a_j. Then by Equation (4), for each column a_j, we have

$$y_{0,j} + \sum_{i \in R_j} A_{i,j} x_{i,j} = N(n, j, q).$$

The last column of Table 1 gives the total number of polynomials in each row, and the last row gives the total number of polynomials in each column. By Equation (1) we have

$$N(n, q) = N_0(n, q) + \sum_{i=1}^{q-1} N_i(n, q) = N_0(n, q) + (q-1)N_1(n, q).$$

Next we study $x_{i,j}$, $y_{0,j}$, and $N(n, j, q)$.

3. Our bounds for $N_\gamma(n, c, q)$

Let $\gamma = a_i \in \mathbb{F}_q$, and $c = a_j \in \mathbb{F}_q^\times$ be any given elements, where $0 \le i \le q-1$, and $1 \le j \le q-1$. In Theorem 5.1 of [14], bounds for the number $x_{i,j}$ are given as

$$\left| x_{i,j} - \frac{q^{n-1}}{n(q-1)} \right| \le \frac{3}{n} q^{\frac{n}{2}}. \tag{5}$$

In [10], better bounds for $x_{i,j}$ are given by considering different cases for the trace. If the trace is zero, from Corollary 3.4 of [10], then we have the following bounds for $y_{0,j}$

$$\left| y_{0,j} - \frac{q^{n-1} - 1}{n(q-1)} \right| \le \frac{s-1}{n} q^{\frac{n-2}{2}} + \frac{q^{\frac{n}{2}} - 1}{q-1} < \frac{2}{q-1} q^{\frac{n}{2}}, \tag{6}$$

where $s = \gcd(n, q-1)$. For a nonzero trace $\gamma = a_i$ we have $i > 0$. By Corollary 4.3 of [10], we have the following bounds for $x_{i,j}$

$$\left| x_{i,j} - \frac{q^n - 1}{nq(q-1)} \right| \le q^{\frac{n-2}{2}} + \frac{q^{\frac{n}{2}} - 1}{q(q-1)} + \frac{n}{2} q^{\frac{n-4}{4}} < \frac{2}{q-1} q^{\frac{n}{2}}. \tag{7}$$

Suppose that the constant $c = a_j \in \mathbb{F}_q^\times$, where $1 \le j \le q-1$, is such that $\rho = \mathrm{ord}(c)$. Let $x_{r,j} = \max\{x_{i,j} : i \in R_j\}$. Then we have the following result.

Lemma 3. *If $c = a_j$ is a given constant from $\mathbb{F}_q^\times$, for some $1 \le j \le q-1$, then*

$$\frac{N(n, j, q)}{q-1} - \frac{q^{n-1} - 1}{n(q-1)^2} - \frac{2q^{\frac{n}{2}}}{(q-1)^2} \le x_{r,j} \le \frac{N(n, j, q)}{A_{r,j}} - \frac{q^{n-1} - 1}{n(q-1)A_{r,j}} + \frac{2q^{\frac{n}{2}}}{(q-1)A_{r,j}}.$$

Proof. From Equation (6) we have

$$\frac{q^{n-1}-1}{n(q-1)}-\frac{2q^{\frac{n}{2}}}{q-1}\le y_{0,j}\le \frac{q^{n-1}-1}{n(q-1)}+\frac{2q^{\frac{n}{2}}}{q-1}.$$

By adding $\sum_{i\in R_j} A_{i,j}x_{i,j}$ to each expression in this inequality, we have

$$\frac{q^{n-1}-1}{n(q-1)}-\frac{2q^{\frac{n}{2}}}{q-1}+\sum_{i\in R_j} A_{i,j}x_{i,j}\le N(n,j,q)\le \frac{q^{n-1}-1}{n(q-1)}+\frac{2q^{\frac{n}{2}}}{q-1}+\sum_{i\in R_j} A_{i,j}x_{i,j}.$$

Then applying the lower and upper bounds for $\sum_{i\in R_j} A_{i,j}x_{i,j}$, we have

$$\frac{q^{n-1}-1}{n(q-1)}-\frac{2q^{\frac{n}{2}}}{q-1}+A_{r,j}x_{r,j}\le N(n,j,q)\le \frac{q^{n-1}-1}{n(q-1)}+\frac{2q^{\frac{n}{2}}}{q-1}+(q-1)x_{r,j},$$

which implies the result. ■

Next we provide lower and upper bounds for $x_{r,j}$ in terms of n and $q-1$, instead of $N(n,j,q)$. We need to find lower and upper bounds for $N(n,j,q)$.

Definition 4. *Let q and n be two positive integers, and the prime factorization of q^n-1 be given by $q^n-1=p_1^{e_1}p_2^{e_2}\dots p_t^{e_t}$, where p_t is the largest prime factor of q^n-1. Then, the pair (q,n) is said to be a* lps *(largest prime survives) pair of integers, if $p_t\nmid q^m-1$, for $m<n$.*

Experimental data show that for any q, there exist many n's such that (q,n) is a lps pair. We also found some sporadic pairs (q,n) that are not lps pairs. Let $\upsilon=p_t^{e_t}$, and $m_r\mid q-1$ be fixed, where $1\le m_r\le q-1$. We let $m_r=\rho=\mathrm{ord}(c)$. Then suppose that $D_{\rho,\upsilon}$ is the subset of D_n defined by those r which υ divides them, that is

$$D_{\rho,\upsilon}=\{r\in D_n\colon r=m_rd_r, m_r=\rho,\upsilon\mid r\}.$$

Lemma 5. *Let (q,n) be a lps pair of integers. Suppose that p_t is the largest prime in the prime factorization of q^n-1, and $m_r\mid q-1$ be fixed as $\rho=ord(c)$. Then for all $r\in D_{\rho,\upsilon}$ we have*

$$\frac{1}{n\phi(\rho)}\sum_{r\in D_{\rho,\upsilon}}\phi(r)=\left(1-\frac{1}{p_t}\right)\frac{q^n-1}{n(q-1)}.$$

Proof. Let $m_r=\rho$ be a fixed divisor of $q-1$. Then $m_r={p_1}^{l_1}\dots {p_k}^{l_k}$, where $0\le l_i\le g_i$, for $i\in S_1=\{1,\dots,k\}$. Each $r\in D_{\rho,\upsilon}$ is $r=m_rd_r$, where $m_r=\rho$, and $\upsilon\mid r$. By Lemma 1 such r can be given by $r=\frac{q^n-1}{R}$, where

$$\gcd(R,q-1)=\frac{q-1}{m_r}={p_1}^{g_1-l_1}\dots {p_k}^{g_k-l_k}.$$

Therefore $R={p_1}^{g_1-l_1}\dots {p_k}^{g_k-l_k}{p_{k+1}}^{c_{k+1}}\dots {p_{t-1}}^{c_{t-1}}$, where $0\le c_i\le e_i$, for all $i\in S_2-\{t\}=\{k+1,\dots,t-1\}$. Then each $r\in D_{\rho,\upsilon}$ can be considered as

$$r={p_1}^{e_1-g_1+l_1}\dots {p_k}^{e_k-g_k+l_k}{p_{k+1}}^{d_{k+1}}\dots {p_{t-1}}^{d_{t-1}}{p_t}^{e_t},$$

such that $d_i = e_i - c_i$, for $i \in S_2 - \{t\}$. Then

$$\begin{aligned}
&\frac{1}{n\phi(\rho)} \sum_{r \in D_{\rho,\upsilon}} \phi(r) \\
= \quad & \frac{\sum_{d_{k+1},\ldots d_{t-1}} \phi\left(\left(\prod_{s=1}^{k} p_s{}^{e_s - g_s + l_s}\right)\left(\prod_{u=k+1}^{t-1} p_u{}^{d_u}\right) p_t^{e_t}\right)}{n\phi(p_1{}^{l_1} \ldots p_k{}^{l_k})} \\
= \quad & \frac{\phi\left(\prod_{s=1}^{k} p_s{}^{e_s - g_s + l_s}\right)}{n\phi(p_1{}^{l_1} \ldots p_k{}^{l_k})} \left(\prod_{u=k+1}^{t-1} \sum_{d_u=0}^{e_u} \phi(p_u{}^{d_u})\right) \phi(p_t^{e_t}) \\
= \quad & \frac{\prod_{s=1}^{k}(p_s - 1) p_s{}^{e_s - g_s + l_s - 1}}{n \prod_{s=1}^{k}(p_s - 1) p_s{}^{l_s - 1}} \left(\prod_{u=k+1}^{t-1} p_u{}^{e_u}\right) p_t^{e_t} \left(1 - \frac{1}{p_t}\right) \\
= \quad & \frac{\left(1 - \frac{1}{p_t}\right)}{n} \left(\prod_{s=1}^{t} p_s{}^{e_s}\right)\left(\prod_{u=1}^{k} p_u{}^{-g_u}\right) = \left(1 - \frac{1}{p_t}\right) \frac{q^n - 1}{n(q-1)}.
\end{aligned}$$

■

We state now our main result about the bounds for $x_{r,j}$.

Theorem 6. *Suppose that (q, n) is a lps pair of integers, and $c = a_j \in \mathbb{F}_q^{\times}$ be such that $\rho = ord(c)$, for some $1 \leq j \leq q-1$. If p_t is the largest prime in the factorization of $q^n - 1$, then*

$$\begin{aligned}
&\frac{\left(1 - \frac{1}{p_t}\right)(q^n - 1) - q^{n-1} - 2nq^{\frac{n}{2}} + 1}{n(q-1)^2} \leq x_{r,j} \\
\leq \quad & \frac{1}{A_{r,j}} \left(\frac{q^n - 1}{n\rho} - \frac{q^{n-1} - 1}{n(q-1)} + \frac{2q^{\frac{n}{2}}}{q-1}\right).
\end{aligned}$$

Proof. For a given $m_r = \rho$, using the definition of $D_{\rho,\upsilon}$ and that (q, n) is a lps pair, we have

$$N(n, j, q) = \frac{1}{n\phi(\rho)} \sum_{\substack{r \in D_n \\ m_r = \rho}} \phi(r) \geq \frac{1}{n\phi(\rho)} \sum_{r \in D_{\rho,\upsilon}} \phi(r).$$

Therefore, using Lemma 5, a lower bound for $N(n, j, q)$ can be given as

$$N(n, j, q) \geq \left(1 - \frac{1}{p_t}\right) \frac{q^n - 1}{n(q-1)}.$$

Using Lemma 3, we obtain the stated lower bound for $x_{r,j}$.

An upper bound for $N(n, j, q)$ can be derived using

$$N(n, j, q) = \frac{1}{n\phi(\rho)} \sum_{\substack{r \in D_n \\ m_r = \rho}} \phi(r) \leq \frac{1}{n\phi(\rho)} \sum_{\substack{r | q^n - 1 \\ m_r = \rho}} \phi(r),$$

where the sum at the right-hand side is simply

$$\frac{1}{n\phi(\rho)} \sum_{\rho d_r | q^n-1} \phi(\rho d_r) = \frac{1}{n} \sum_{d_r | \frac{q^n-1}{\rho}} \phi(d_r) = \frac{q^n-1}{n\rho}.$$

Using Lemma 3, this implies the stated upper bound for $x_{r,j}$. ■

The following table compares our lower bound with other lower bounds. We choose different n and q such that (q,n) is a lps pair of integers, and they are small enough to compute the number in the table. For each entry (a,b,c), a represents the lower bound obtained by Wan, b the one by Moisio, and c ours. To compare our lower bound and Moisio's lower bound in general, we look at

Table 2: Different lower bounds for $x_{r,j}$.

$\mathbb{F}_q$	**Degree n**		
	4	7	11
$\mathbb{F}_4$	(0, 0, 1.74)	(140.19, 142.55, 164.56)	(31216.48, 31030.21, 31257.89)
$\mathbb{F}_5$	(0, 0, 3.94)	(438.2, 476.5, 523.06)	(220040.28, 220107.19, 221072.5)
$\mathbb{F}_7$	(0, 4.14, 8.24)	(2412.24, 2634.88, 2750.06)	(4267800.61, 4272351.16, 4277440.6)
$\mathbb{F}_8$	(0, 7.16, 14.07)	(4729.24, 5126.36, 5272.63)	(13919422.13, 13931249.46, 13940889.49)
$\mathbb{F}_9$	(0, 10.66, 19.62)	(8552.73, 9198.47, 9411.91)	(39574237.19, 39600149.44, 39605439.16)
$\mathbb{F}_{11}$	(0, 19.18, 30.25)	(23416.12, 24845.44, 25219.11)	(235649092.99, 235740989.11, 235783942.58)
$\mathbb{F}_{13}$	(0, 29.7, 40.51)	(54067.13, 56777.94, 57351.98)	(1044017409.66, 1044270464.84, 1044301207.22)

their difference,

$$\frac{\left(1-\frac{1}{p_t}\right)(q^n-1) - q^{n-1} - 2nq^{\frac{n}{2}} + 1}{n(q-1)^2} - \frac{q^n-1}{nq(q-1)} + \frac{2}{q-1}q^{\frac{n}{2}},$$

or,

$$-\frac{(q^n-1)}{n(q-1)^2 p_t} + \frac{2(q-2)}{(q-1)^2}q^{\frac{n}{2}} + \frac{1}{nq(q-1)}.$$

Therefore, if the number p_t is of size $q^{\frac{n}{2}-1}$ or larger, then this difference is positive, and so our bound is better. Checking different q and n, this situation happens very often.

Remark. If $A_{r,j} = \rho = q-1$, our upper bound is better than Moisio's upper bound. In the next section we show that this is the case if n is a multiple of $q-1$. Examples are given in the next section.

4. The special case n being a multiple of $q-1$

Suppose that the degree of the polynomials is fixed as $n = a(q-1)$, for some positive integer a. Then we have the following results.

Lemma 7. *Let $1 \le m \le n-1$, $q-1 \nmid m$, and $n = a(q-1)$, for some positive integer a. Then $(q-1)^2 \mid q^n - 1$ and $(q-1)^2 \nmid q^m - 1$. In particular, $n^2 \mid a^2(q^n-1)$, and $n^2 \nmid a^2(q^m-1)$.*

Proof. From $q^i \equiv 1 \pmod{q-1}$ for any positive integer i, we have $q^{m-1} + q^{m-2} + \cdots + q + 1 \equiv m \not\equiv 0 \pmod{q-1}$ and $q^{n-1} + q^{n-2} + \cdots + q + 1 \equiv n \equiv 0 \pmod{q-1}$. Hence, multiplying by $q-1$, we have the conclusion. ■

Lemma 8. *Suppose that $n = a(q-1)$, for some integer a. Let $r = \frac{q^n-1}{R}$ such that $R \mid q^n - 1$, and $\gcd(R, q-1) = 1$, that is $m_r = q-1$. Then $r \nmid (q^m - 1)$, for all $m = 1, 2, \ldots, n-1$, and m is not a multiple of $q-1$.*

Proof. Since $q-1 = p_1^{g_1} \ldots p_k^{g_k}$, $q^n - 1 = p_1^{e_1} \ldots p_k^{e_k} p_{k+1}^{e_{k+1}} \ldots p_t^{e_t}$ and $\gcd(R, q-1) = 1$, r has the form $r = (q^n-1)/R = p_1^{e_1} \ldots p_k^{e_k} p_{k+1}^{f_{k+1}} \ldots p_t^{f_t}$, where $0 \leq f_i \leq e_i$, for $i \in S_2$. It is clear that $(q-1)^2 \mid r$ since $e_i \geq 2g_i$ for $i = 1, \ldots, k$. Now we show that $r \nmid q^m - 1$, for $m = 1, 2, \ldots, n-1$ and $q-1 \nmid m$. Suppose $r \mid q^m - 1$. Since $n^2 = a^2(q-1)^2 \mid a^2 r$, we have $n^2 \mid a^2(q^m - 1)$, which contricts to Lemma 7. ∎

Let $c \in \mathbb{F}_q^\times$ be such that $\rho = \mathrm{ord}(c)$. The constant c can be a primitive, or nonprimitive constant. For different r, in the relation

$$N(n, c, q) = \frac{1}{n\phi(\rho)} \sum_{\substack{r \in D_n \\ m_r = \rho}} \phi(r), \tag{8}$$

the value of m_r is fixed as $m_r = \rho$. Let $c \in \mathbb{F}_q^\times$ represent any primitive element. Then obviously $\rho = q-1$, and let $r \in D_n$ be such that $m_r = \rho = q-1$.

Theorem 9. *Let $n = a(q-1)$, for some integer a, and $c \in \mathbb{F}_q^\times$ be primitive. Then*

$$N(n, c, q) \leq \frac{q^n - 1}{a(q-1)^2}.$$

In addition, if q and n are such that $p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k} \nmid q^m - 1$, for m multiple of $q-1$ and $m < n$, where $q^n - 1 = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k} p_{k+1}^{e_{k+1}} \ldots p_t^{e_t}$, then $N(n, c, q) = \frac{q^n-1}{a(q-1)^2}$.

Proof. Let $q - 1 = p_1^{g_1} p_2^{g_2} \ldots p_k^{g_k}$ be the prime factorization of $q-1$, where $g_i \geq 1$, for $i \in S_1$. Similarly, $q^n - 1 = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k} p_{k+1}^{e_{k+1}} \ldots p_t^{e_t}$, such that $e_i \geq g_i \geq 1$, when $i \in S_1$, and $e_i \geq 1$, when $i \in S_2$. Since $c \in \mathbb{F}_q^\times$ is primitive, so $\rho = q-1$. Let $n = a(q-1)$, then by Equation (8) we have

$$N(n, c, q) = \frac{1}{a(q-1)\phi(q-1)} \sum_{\substack{r \in D_n \\ m_r = q-1}} \phi(r).$$

For any $r = (q^n - 1)/R$, where $\gcd(R, q-1) = (q-1)/m_r = 1$ and $R = {p_{k+1}}^{c_{k+1}} \ldots {p_t}^{c_t}$ with $0 \leq c_i \leq e_i$ for $i \in S_2$, we can write $r = (q^n-1)/R = p_1^{e_1} \ldots p_k^{e_k} p_{k+1}^{f_{k+1}} \ldots p_t^{f_t}$, where $f_i = e_i - c_i$, for $i \in S_2$. By Lemma 8, $r \nmid q^m - 1$, for all m not multiple of $q-1$, and $m < n$. Since $p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k} \nmid q^m - 1$ for all m multiple of $q-1$ and $m < n$, we conclude that any r of this form is in D_n. Hence, the number $N(n, c, q)$ can be given by

$$N(n, c, q) \quad = \quad \frac{1}{a\left(p_1^{g_1} \ldots p_k^{g_k}\right) \phi\left(p_1^{g_1} \ldots p_k^{g_k}\right)} \sum_{f_{k+1}, \ldots, f_t} \phi(p_1^{e_1} \ldots p_k^{e_k} p_{k+1}^{f_{k+1}} \ldots p_t^{f_t})$$

$$\begin{aligned}
&= \frac{\phi\left(p_1^{e_1}\dots p_k^{e_k}\right)}{a\left(p_1^{g_1}\dots p_k^{g_k}\right)\phi\left(p_1^{g_1}\dots p_k^{g_k}\right)}\sum_{f_{k+1},\dots,f_t}\phi\left(p_{k+1}^{f_{k+1}}\dots p_t^{f_t}\right)\\
&= \frac{\left(p_1^{e_1-g_1}\dots p_k^{e_k-g_k}\right)}{a\left(p_1^{g_1}\dots p_k^{g_k}\right)}\prod_{s=k+1}^{t}\sum_{f_s=0}^{e_s}\phi({p_s}^{f_s})\\
&= \frac{p_1^{e_1}\dots p_k^{e_k}}{a\left(p_1^{2g_1}\dots p_k^{2g_k}\right)}\prod_{s=k+1}^{t}{p_s}^{e_s} = \frac{q^n-1}{a(q-1)^2}.
\end{aligned}$$

Finally, we observe that if $p_1^{e_1}p_2^{e_2}\dots p_k^{e_k} \mid q^m-1$, for some m multiple of $q-1$ and $m<n$, then we can only conclude that $N(n,c,q) < \frac{q^n-1}{a(q-1)^2}$. ■

Suppose that $c^{'} \in \mathbb{F}_q^{\times}$ is any nonprimitive constant, which is related to $r^{'} \in D_n$, where $r^{'} = m_{r'}d_{r'}$ and $m_{r'} = \rho^{'} = \mathrm{ord}(c^{'}) < q-1$, we have $r^{'} \in D_n$, such that $r^{'} = \frac{q^n-1}{R^{'}}$, and $\gcd(q-1, R^{'}) = \frac{q-1}{m_{r^{'}}} > 1$. Moreover $r^{'} \nmid q^m-1$, for $1 \le m \le n-1$. Let us remove the last condition and define $\widehat{r}^{'} = \frac{q^n-1}{\widehat{R}^{'}}$, such that $\widehat{R}^{'} \mid q^n-1$, and $\gcd(q-1, \widehat{R}^{'}) = \frac{q-1}{m_{r^{'}}} > 1$.

Lemma 10. *Let $c^{'} \in \mathbb{F}_q^{\times}$ be nonprimitive, where $\rho^{'} = ord(c^{'}) = m_{r'} < q-1$. Then*

$$\frac{1}{n\phi(\rho^{'})}\sum_{\widehat{r}^{'}}\phi(\widehat{r}^{'}) = \frac{q^n-1}{a(q-1)^2},$$

where the sum runs over all $\widehat{r}^{'}$, defined as $\widehat{r}^{'} = \frac{q^n-1}{\widehat{R}^{'}}$, with $\gcd(q-1, \widehat{R}^{'}) = \frac{q-1}{m_{r^{'}}} = \frac{q-1}{\rho^{'}}$.

Proof. Suppose $c^{'} \in \mathbb{F}_q^{\times}$ be such that $\rho^{'} = \mathrm{ord}(c^{'}) = m_{r^{'}} = {p_1}^{l_1}\dots {p_k}^{l_k} \mid q-1$, where $0 \le l_i \le g_i$, for $i \in S_1$. Let $\widehat{r}^{'} = \frac{q^n-1}{\widehat{R}^{'}}$, where $\gcd(q-1, \widehat{R}^{'}) = \frac{q-1}{m_{r^{'}}} = p_1^{g_1-l_1}\dots p_k^{g_k-l_k}$. This implies that $\widehat{R}^{'} = p_1^{g_1-l_1}\dots p_k^{g_k-l_k}{p_{k+1}}^{c_{k+1}}\dots {p_t}^{c_t}$, with $0 \le c_i \le e_i$, for $i \in S_2$. Therefore, for $d_i = e_i - c_i$ and $i \in S_2$, $\widehat{r}^{'}$ can be considered as $\widehat{r}^{'} = p_1^{e_1-g_1+l_1}\dots p_k^{e_k-g_k+l_k}p_{k+1}^{d_k+1}$. Then

$$\begin{aligned}
&\frac{1}{n\phi(\rho^{'})}\sum_{\widehat{r}^{'}}\phi(\widehat{r}^{'})\\
&= \frac{1}{a(p_1^{g_1}\dots p_k^{g_k})\phi(p_1^{l_1}\dots p_k^{l_k})}\sum_{d_{k+1},\dots d_t}\phi\left(\left(\prod_{s=1}^{k}{p_s}^{e_s-g_s+l_s}\right)\prod_{u=k+1}^{t}{p_u}^{d_u}\right)\\
&= \frac{\phi\left(\prod_{s=1}^{k}{p_s}^{e_s-g_s+l_s}\right)}{a(p_1^{g_1}\dots p_k^{g_k})\phi({p_1}^{l_1}\dots {p_k}^{l_k})}\left(\prod_{u=k+1}^{t}\sum_{d_u=0}^{e_u}\phi({p_u}^{d_u})\right)
\end{aligned}$$

$$
\begin{aligned}
&= \frac{\prod_{s=1}^{k}(p_s-1){p_s}^{e_s-g_s+l_s-1}}{a\prod_{s=1}^{k}(p_s-1){p_s}^{g_s+l_s-1}}\left(\prod_{u=k+1}^{t}{p_u}^{e_u}\right) \\
&= \left(\frac{1}{a}\prod_{s=1}^{k}{p_s}^{e_s-2g_s}\right)\left(\prod_{u=k+1}^{t}{p_u}^{e_u}\right) = \frac{q^n-1}{a(q-1)^2}.
\end{aligned}
$$

■

Theorem 11. *If $n = a(q-1)$, for some integer a. Then for any nonprimitive constant $c^{'} \in \mathbb{F}_q^{\times}$, we have $N(n, c^{'}, q) \leq \frac{q^n-1}{a(q-1)^2}$.*

Proof. For the nonprimitive $c^{'} \in \mathbb{F}_q^{\times}$, let $\rho^{'} = \mathrm{ord}(c^{'})$. Then by Lemma 10,

$$
\frac{q^n-1}{a(q-1)^2} = \frac{1}{n\phi(\rho^{'})}\sum_{\widehat{r}^{'}}\phi(\widehat{r}^{'}) \geq \frac{1}{n\phi(\rho^{'})}\sum_{\substack{r^{'}\in D_n \\ m_{r^{'}}=\rho^{'}}}\phi(r^{'}) = N(n, c^{'}, q).
$$

■

If $n = a(q-1)$, then we have the following restatement of Lemma 2.

Lemma 12. *Let $n = a(q-1)$ for some integer a, and $c \in \mathbb{F}_q^{\times}$ be any constant. Then for any two nonzero traces γ and δ, we have $N_\gamma(n, c, q) = N_\delta(n, c, q)$.*

This means that, when $n = a(q-1)$, for any $i, l \in \{1, 2, \ldots, q-1\}$, and $j \in \{0, 1, \ldots, q-1\}$, we have $x_{i,j} = x_{l,j}$. So we let x_j represent $x_{i,j}$. Moreover, for $\gamma \in \mathbb{F}_q^{\times}$, let $N_\gamma(n, a_j, q) = x_j$, and $N_0(n, a_j, q) = y_j$, where $j \in \{1, 2, \ldots, q-1\}$; see Table 3. In Table 3, we have the same rows for different $\gamma \in \mathbb{F}_q^{\times}$. In this case,

Table 3: Distribution of polynomials of degree $n = a(q-1)$ over a finite field $\mathbb{F}_q$.

Cons / Tr	a_1	$\cdots$	a_j	$\cdots$	a_{q-1}	Total
a_0	y_1	$\cdots$	y_j	$\cdots$	y_{q-1}	$N_0(n,q)$
a_1	x_1	$\cdots$	x_j	$\cdots$	x_{q-1}	$N_1(n,q)$
$\vdots$	$\vdots$		$\vdots$		$\vdots$	$\vdots$
a_{q-1}	x_1	$\cdots$	x_j	$\cdots$	x_{q-1}	$N_{q-1}(n,q)$
Total	$N(n,1,q)$	$\cdots$	$N(n,j,q)$	$\cdots$	$N(n,q-1,q)$	$N(n,q)$

let A_j be the number of repeated entries of the column a_j, where $1 \leq j \leq q-1$. Clearly $A_j = q-1$. Thus for a given nonzero constant c (or $c^{'}$), Equation (4) changes to

$$
y_c + (q-1)x_c = N(n, c, q). \tag{9}
$$

Then using Equation (9), and Theorem 9, we have the following bounds for x_c.

Theorem 13. *Let $n = a(q-1)$, such that $q-1 = p_1^{g_1}p_2^{g_2}\dots p_k^{g_k}$, $q^n - 1 = p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}p_{k+1}^{e_{k+1}}\dots p_t^{e_t}$ satisfies $p_1^{e_1}p_2^{e_2}\dots p_k^{e_k} \nmid q^m - 1$, for m multiple of $q-1$, and $m < n$. Then for any primitive constant $c \in \mathbb{F}_q^{\times}$ we have*

$$\left| x_c - \frac{q^n - q^{n-1}}{a(q-1)^3} \right| \leq \frac{2}{(q-1)^2} q^{\frac{n}{2}}.$$

PROOF. Let $n = a(q-1)$, for some integer a, and $c = a_j$ be a primitive constant from $\mathbb{F}_q^{\times}$, for some $1 \leq j \leq q-1$. Then $A_j = q-1$, and $\rho = \mathrm{ord}(c) = q-1$. Suppose that q and n are such that $p_1^{e_1}p_2^{e_2}\dots p_k^{e_k} \nmid q^m - 1$, for m multiple of $q-1$, and $m < n$. Then by Theorem 9, the lower and upper bounds for x_c given in Lemma 3 change to

$$\frac{q^n - q^{n-1}}{a(q-1)^3} - \frac{2q^{\frac{n}{2}}}{(q-1)^2} \leq x_c \leq \frac{q^n - q^{n-1}}{a(q-1)^3} + \frac{2q^{\frac{n}{2}}}{(q-1)^2}.$$

We note that the upper bound does not require the condition $p_1^{e_1}p_2^{e_2}\dots p_k^{e_k} \nmid q^m - 1$, for m multiple of $q-1$, and $m < n$. ■

The difference between our lower bound and Moisio's lower bound is

$$\frac{q^n - q^{n-1}}{a(q-1)^3} - \frac{2}{(q-1)^2} q^{\frac{n}{2}} - \frac{q^n - 1}{aq(q-1)^2} + \frac{2}{q-1} q^{\frac{n}{2}} = \frac{1}{(q-1)^2}\left(2q^{\frac{n}{2}}(q-2) + \frac{1}{aq}\right),$$

which is always positive. This shows that our lower bound is better.

The difference between our upper bound and Moisio's upper bound is

$$\frac{q^n - q^{n-1}}{a(q-1)^3} + \frac{2}{(q-1)^2} q^{\frac{n}{2}} - \frac{q^n - 1}{aq(q-1)^2} - \frac{2}{q-1} q^{\frac{n}{2}} = \frac{1}{(q-1)^2}\left(2q^{\frac{n}{2}}(2-q) + \frac{1}{aq}\right),$$

which is always negative if $q \geq 3$. This shows that our upper bound is better.

Table 4 compares our lower and upper bounds with Wan bounds given in (5), and Moisio bounds given in (7) for different finite fields $\mathbb{F}_q$, and degree $n = q-1$. In each column, the entry $[x, y]$ of the table, represents the corresponding [lower bound, upper bound].

Table 4: Bounds for x_c, for different finite fields $\mathbb{F}_q$, when $n = q-1$.

q	Wan [14]	Moisio [10]	Our Bounds	Min/Max
4	[0, 9.78]	[0, 5.39]	[0, 4.407]	1
5	[0, 26.56]	[0, 16]	[3.109, 12.484]	[7, 8]
7	[295.36, 638.36]	[401.78, 531.94]	[438.273, 495.439]	[466, 471]
8	[4729.24, 5970.52]	[5126.36, 5573.38]	[5261.212, 5438.537]	5344
9	[72273.52, 74938.92]	[73877.78, 75590]	[74426.342, 75041.436]	74691
11	[23,531,161, 23,627,792]	[23,563,189, 23,595,764]	[23,574,645, 23,584,308]	[23,578,887, 23,580,368]

Now let $c' \in \mathbb{F}_q^{\times}$ be a nonprimitive constant with $\rho' = \mathrm{ord}(c')$. Using Theorem 6 and Theorem 11, we have the following bounds for $x_{c'}$.

Theorem 14. *Suppose (q, n) is a* lps pair, *and $n = a(q-1)$, for some integer a. Let $c' \in \mathbb{F}_q^{\times}$ be a nonprimitive constant. If p_t is the largest prime in the factorization of $q^n - 1$, then we have*

$$\frac{\left(1 - \frac{1}{p_t}\right)(q^n - 1) - q^{n-1} - 2a(q-1)q^{\frac{n}{2}} + 1}{a(q-1)^3} \leq x_{c'} \leq \frac{q^n - q^{n-1} + 2a(q-1)q^{\frac{n}{2}}}{a(q-1)^3}.$$

Proof. Let $n = a(q-1)$, for some integer a. For any nonprimitive constant $c^{'} \in \mathbb{F}_q^{\times}$ we have $y_{c'} + (q-1)x_{c'} = N(n, c^{'}, q)$. By Equation (6) we have

$$\frac{q^{n-1}-1}{a(q-1)^2} - \frac{2}{q-1} q^{\frac{n}{2}} \leq y_{c'} \leq \frac{q^{n-1}-1}{a(q-1)^2} + \frac{2}{q-1} q^{\frac{n}{2}}.$$

If we add $(q-1)x_{c'}$ to this inequality, then

$$\frac{q^{n-1}-1}{a(q-1)^2} - \frac{2q^{\frac{n}{2}}}{q-1} + (q-1)x_{c'} \leq N(n, c^{'}, q) \leq \frac{q^{n-1}-1}{a(q-1)^2} + \frac{2q^{\frac{n}{2}}}{q-1} + (q-1)x_{c'},$$

therefore, we obtain

$$\frac{N(n, c^{'}, q)}{q-1} - \frac{q^{n-1}-1}{a(q-1)^3} - \frac{2q^{\frac{n}{2}}}{(q-1)^2} \leq x_{c'} \leq \frac{N(n, c^{'}, q)}{q-1} - \frac{q^{n-1}-1}{a(q-1)^3} + \frac{2q^{\frac{n}{2}}}{(q-1)^2}.$$

Since $n = a(q-1)$ then by Theorem 11 we have $N(n, c^{'}, q) \leq \frac{q^n - 1}{a(q-1)^2}$, which simplifies the upper bound for $x_{c'}$ to

$$\frac{q^n - q^{n-1} + 2a(q-1)q^{\frac{n}{2}}}{a(q-1)^3}.$$

An argument similar to Theorem 6 gives the lower bound for $x_{c'}$. ■

For the same reason as above, our upper bound is better than Moisio's result as long as $q \geq 3$ and our lower bound is better if p_t is of size $q^{\frac{n}{2}-1}$ or larger.

In Table 4 we compare our bounds for $x_{c'}$ with Wan and Moisio bounds, when $n = q-1$ and for different finite fields $\mathbb{F}_q$.

Table 5: Bounds for $x_{c'}$, for different finite fields $\mathbb{F}_q$, with $n = q-1$.

q	Wan[13]	Moisio[9]	Our Bounds	Min/Max
4	[0, 9.78]	[0, 5.39]	[0, 3.56]	2
5	[0, 26.56]	[0, 16]	[3.94, 10.94]	[7, 8]
7	[295.36, 638.36]	[401.78, 531.94]	[435.139, 485.917]	[458, 471]
8	[4729.24, 5970.52]	[5126.36, 5573.38]	[5272.626, 5408.986]	[5337, 5360]
9	[72273.52, 74938.92]	[73877.78, 75590]	[74093.32, 74938.922]	[74700, 74754]
11	[23,531,161, 23,627,792]	[23,563,189, 23,595,764]	[23,574,323, 23,582,697]	[23,578,378, 23,579,568]

Remark. For any given finite field $\mathbb{F}_q$ and given degree n such that $q-1 \nmid n$, we know that $A_{r,j} < q-1$. Indeed, let γ and δ be two nonzero elements in $\mathbb{F}_q$. Thus, $\left(\frac{\gamma}{\delta}\right)^n \neq 1$, and by Lemma 2 we have $N_\gamma(n, c, q) = N_\delta\left(n, c\left(\frac{\delta}{\gamma}\right)^n, q\right) \neq N_\delta(n, c, q)$. However, we do not know whether we can still improve upper bounds in this case.

References

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

[2] K. Cattell, C. R. Miers, F. Ruskey, M. Serra and J. Sawada, The number of irreducible polynomials over GF(2) with given trace and subtrace, *J. Combin. Math. Combin. Comput.*, **47** (2003), 31-64.

[3] S. D. Cohen, Primitive elements and polynomials with arbitrary trace, *Journal of the American Mathematical Society*, **83** (1990), 1-7.

[4] S. D. Cohen, Explicit theorems on generator polynomials, *Finite Fields and Their Applications*, **11** (2005), 337-357.

[5] S. D. Cohen and M. Presern, Primitive polynomials with prescribed second coefficient, *Glasgow Mathematical Journal*, **48** (2006), 281-307.

[6] R. W. Fitzgerald and J. L. Yucas, Irreducible polynomials over GF(2) with three prescribed coefficients, *Finite Fields and Their Applications*, **9** (2003), 286-299.

[7] K. Kononen, M. Moisio, M. Rinta-aho and K. Väänänen, *JP Journal of Algebra, Number Theory and Applications*, **11** (2008), 223-248.

[8] E. N. Kuzmin, On a class of irreducible polynomials over a finite field, *Dokl. Akad. Nauk SSSr* **313 (3)** (1990), 552-555. (Russian: English translation in *Soviet Math. Dokl.* **42(1)** (1991), 45-48.)

[9] R. Lidl and H. Niederreiter, "Finite Fields", Cambridge Univ. Press, Cambridge, second edition, 1994.

[10] M. Moisio, Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm, *Acta Artith*, **132** (2008), 329-350.

[11] M. Moisio and K. Ranto, Elliptic curves and explicit enumeration of irreducible polynomials with two coefficients prescribed, *Finite Fields and Their Applications*, **14** (2008), 798-815.

[12] J. L. Yucas, Irreducible polynomials over finite fields with prescribed trace/prescribed constant term, *Finite Fields and Their Applications*, **12** (2006), 211-221.

[13] J. L. Yucas and G. L. Mullen, Irreducible polynomials over GF(2) with prescribed coefficients, *Discrete Mathematics*, **274** (2004), 265-279.

[14] D. Wan, Generators and irreducible polynomials over finite fields, *Math. Comp.*, **66** (1997), 1195-1212.