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

B. Omidi Koma
School of Mathematics and Statistics, Carleton University
bomidi@math.carleton.ca

Joint work with
D. Panario and Q. Wang

Fq9, July 2009

Definitions

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial of degree n over $\mathbb{F}_q$, where $q = p^\omega$ with p a prime number. We define:

$N(n,q)$: the number of irreducible polynomials of degree n over $\mathbb{F}_q$.

$N(n,c,q)$: the number of irreducible polynomials of degree n with given constant term $a_0 = c$.

$N_\gamma(n,q)$: the number of irreducible polynomials of degree n and trace $a_{n-1} = \gamma$.

$N_\gamma(n,c,q)$: the number of irreducible polynomials of degree n, trace $a_{n-1} = \gamma$, and constant term $a_0 = c$.

Previous results

Carlitz (1952) and Kuz′min (1990) give the number of irreducible polynomials with the first coefficient prescribed and the first two coefficients prescribed (over $\mathbb{F}_{p^3}$), respectively.

Fitzgerald and Yucas (2003) consider the number of irreducible polynomials of odd degree n over $\mathbb{F}_2$ with the first three coefficients prescribed.

The number of irreducible polynomials of even degree n over $\mathbb{F}_2$ with the first three coefficients prescribed is considered by Yucas and Mullen (2004).

Let $n = p^\kappa \psi$ where $p \nmid \psi$. For $\gamma \neq 0$, Yucas (2006) shows that

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

For the case $\gamma = 0$, Yucas (2006) proves that

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

where $\varepsilon = 0$ if $\kappa = 0$, and $\varepsilon = 1$ if $\kappa > 0$.

Moreover Yucas (2006) gives the number $N(n,c,q)$.

There is no general formula for the number $N_\gamma(n,c,q)$ but there are some proven bounds.

Wan (1997) gives the bound

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

For a nonzero trace, Moisio (2008) provides

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

Also for zero trace, Moisio (2008) gives

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

In this work we improve these bounds on $N_\gamma(n,c,q)$ for some particular cases. We show with concrete examples.

Relation between different nonzero traces

Lemma

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. Use the bijection $\varphi : P_\gamma(n, c, q) \rightarrow P_\delta\left(n, c(\frac{\delta}{\gamma})^n, q\right)$. ☐

Let $\mathbb{F}_q = \{a_0 = 0, a_1 = 1, a_2, \ldots, a_{q-1}\}$, and $c = a_j \in \mathbb{F}_q^\times$, for some j in $\{1, 2, \ldots, q-1\}$. Also $\gamma = a_i$, where $0 \leq i \leq q-1$.

Table: 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	$N(n,1,q)$	$\cdots$	$N(n,j,q)$	$\cdots$	$N(n,q-1,q)$	$N(n,q)$

If we add all the entries of any column $c = a_j$, then

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

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. Then $R_j \subseteq \{1, 2, \ldots, q-1\}$, and

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

where $A_{i,j}$ is the number of times $x_{i,j}$ appears in the entries of column a_j.

Let $x_{r,j} = \max\{x_{i,j} : i \in R_j\}$. Then we have the following bounds.

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

Lemma

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

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

Definition

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

Theorem

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

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

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

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

$\mathbb{F}_q$	**Degree** n	
	4	11
$\mathbb{F}_4$	$(0, 0, 1.74)$	$(31216.48, 31030.21, 31257.89)$
$\mathbb{F}_5$	$(0, 0, 3.94)$	$(220040.28, 220107.19, 221072.5)$
$\mathbb{F}_7$	$(0, 4.14, 8.24)$	$(4267800.61, 4272351.16, 4277440.6)$
$\mathbb{F}_8$	$(0, 7.16, 14.07)$	$(13919422.13, 13931249.46, 13940889.49)$
$\mathbb{F}_9$	$(0, 10.66, 19.62)$	$(39574237.19, 39600149.44, 39605439.16)$
$\mathbb{F}_{11}$	$(0, 19.18, 30.25)$	$(235649092.99, 235740989.11, 235783942.58)$
$\mathbb{F}_{13}$	$(0, 29.7, 40.51)$	$(1044017409.66, 1044270464.84, 1044301207.22)$

In each entry (a, b, c), a represents the lower bound obtained by Wan, b by Moisio, and c ours.

Remarks

(1) Our lower bound is always better than Moisio's lower bound for all good pair of integers (n, q).

(2) Our upper bound is better than Moisio's upper bound, if $A_{r,j} = m = q-1$. We show that this is the case if n is a multiple of $q-1$.

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

In some special cases, Moisio (2008) has found $N_\gamma(n,c,q)$.

If $\gcd(p,n,q-1)=1$ then

$$N_0(n,c,q)=\frac{1}{n(q-1)}\sum_{d|n}\mu\left(\frac{n}{d}\right)(q^{d-1}-1),$$

and if $n=p^k$, for some integer k, then

$$N_0(n,c,q)=\frac{1}{n(q-1)}\left(q^{n-1}-q^{\frac{n}{p}}\right).$$

We consider now the special case when n is a multiple of $q-1$.

Theorem

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

Moreover, for any nonprimitive constant $c' \in \mathbb{F}_q^\times$, we have $N(n,c',q) \leq \frac{q^n-1}{a(q-1)^2}$.

Therefore when $n = a(q-1)$ the maximum value of $N(n,j,q)$ occurs, when $c = a_j \in \mathbb{F}_q^\times$ is primitive.

Theorem

Let γ and δ be two nonzero traces. If $n = a(q-1)$, and c is a constant from $\mathbb{F}_q^\times$, then

$$N_\gamma(n,c,q) = N_\delta(n,c,q).$$

When $n = a(q-1)$ and the constant term is fixed, we have the same number of irreducible polynomials for any different nonzero traces.

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

Tr \ Const	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_i	x_1	$\cdots$	x_j	$\cdots$	x_{q-1}	$N_i(n,q)$
$\vdots$	$\vdots$		$\vdots$		$\vdots$	$\vdots$
a_{q-1}	x_1	$\cdots$	x_j	$\cdots$	x_{q-1}	$N_{q-1}(n,q)$
Total	$N(n,1,q)$	$\cdots$	$N(n,j,q)$	$\cdots$	$N(n,q-1,q)$	$N(n,q)$

In the table, we have the same rows for different nonzero $\gamma \in \mathbb{F}_q^\times$. Let A_j be the number of repeated entries of the column a_j, where $1 \le j \le q-1$.

Therefore $A_j = q-1$.

For each column related to constant c, we have

$$y_c + (q-1)x_c = N(n,c,q),$$

and we have the following bounds for x_c.

Theorem

If $n = a(q-1)$ and $c \in \mathbb{F}_q^\times$ is a primitive constant, then we have

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

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

q	Wan	Moisio	Our Bounds	Max/Min
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]

Each entry $[x, y]$ of the table, represents the corresponding [lower bound, upper bound].

Theorem

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*

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

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

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

q	Wan	Moisio	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]

Conclusions and future work

The overall goal of this project is to find the exact value of $N_\gamma(n,c,q)$, for any trace γ, constant c, and degree n. This seems to be a hard problem.

Bounds on $N_\gamma(n,c,q)$ have been given and we improve those bounds for some special cases. Moisio uses Kloosterman sums to find $N_\gamma(n,c,q)$ in some special cases different than ours (for example, for $n=p^k>2$, and $\gamma c\neq 0$).

For the future, we plan to study $N_\gamma(n,c,q)$ for other special cases of n, c and γ.