Mathematica Aeterna, Vol. 7, 2017, no. 3, 269 - 286

On the Number of Irreducible Polynomials Over GF(2) with some Prescribed Coefficients

Kübra Afşar[1]

Ankara University

Department of Mathematics

06100, Ankara, Turkey

Necmettin Erbakan University

Department of Mathematics and Computer Science

42060, Konya, Turkey

kbayraktar@konya.edu.tr

Zülfükar Saygı[2]

TOBB University of Economics and Technology

Department of Mathematics

06560, Ankara, Turkey

zsaygi@etu.edu.tr

Ernist Tilenbaev[3]

TOBB University of Economics and Technology

Department of Mathematics

06560, Ankara, Turkey

etilenbaev@etu.edu.tr

Erdal Güner[4]

Ankara University

Department of Mathematics

06100, Ankara, Turkey

guner@science.ankara.edu.tr

Abstract

In this paper we evaluate the number of monic irreducible polynomials in $\mathbb{F}_2[x]$ of even degree n whose first four coefficients have prescribed values. This problem first studied in [7] and some approximate results are obtained. Our results extends the results given in [7] in some cases.

Mathematics Subject Classification: 12E05; 12E20

Keywords: Irreducible Polynomials, Finite Fields, Trace Function.

1. Introduction

Let r be a positive integer, p be a prime number and $q = p^r$. Let $\mathbb{F}_q$ be the finite field with q elements. We will denote the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree n by $N_q(n)$ and the number of monic irreducible polynomials in

$\mathbb{F}_q[x]$ of degree n with first l coefficients prescribed to $a_1, a_2, \dots, a_l \in \mathbb{F}_q$ by $N_q(n, a_1, a_2, \dots, a_l)$.

In the literature $N_q(n, a_1)$ was studied by Carlitz [2] and $N_q(n, a_1, a_2)$ was given by Kuzmin [8]. Cattell et al. [3] reconsidered $N_2(n, a_1, a_2)$, which is a special case of Kuzmin [8]. Results for three prescribed coefficients are given by Kuzmin [8], Cattell et al. [3], Yucas and Mullen [16] and Fitzgerald and Yucas [4] for the case $p = 2$. Moisio and Ranto [13] considered some special cases for $p = 2$ and $p = 3$. Lalin and Larocque [10] proved Kuzmin's [8] results using elementary combinatorial methods, together with the theory of quadratic forms over finite fields. Ahmadi et al. [1] computed $N_{2^r}(n, 0,0,0)$ using the number of points on certain supersingular curves over finite fields. Granger [5] considered $N_q(n, a_1, a_2, \dots, a_l)$ for $l \leq 7$ where $q = 5$ or $q = 2$ and n is odd and gave an explicit formula for $l = 3$ where $q = 3$ and also gave an algorithm which gives exact expressions in terms of the number of points of certain algebraic varieties over $\mathbb{F}_q$.

In this paper we obtained some result on $N_2(n, a_1, a_2, a_3, a_4)$. Our results extend the results given in [7]. We have combined some previous results with the properties of the extended trace functions.

2. Preliminaries and Previous Results

In this section we will present some useful notations and previous results. To obtain our desired numbers we will use the properties of the first four traces which we denote by Tr_1, Tr_2, Tr_3 and Tr_4. For any $k \geq 1$ these trace functions are the generalizations of the usual trace function and for any $a \in \mathbb{F}_{q^n}$ they can be expressed as

$$Tr_k(a) = \sum_{0 \leq i_1 < i_2 < \cdots < i_k \leq n} a^{q^{i_1} + q^{i_2} + \cdots + q^{i_k}}.$$

For $a_1 \in \mathbb{F}_q$, $E_q(n, a_1)$ denote the number of elements $a \in \mathbb{F}_{q^n}$ such that $Tr_1(a) = a_1$ and in general $E_q(n, a_1, a_2, \dots, a_l)$ be the number of elements $a \in \mathbb{F}_{q^n}$ for which $Tr_1(a) = a_1$, $Tr_2(a) = a_2$, ... , $Tr_l(a) = a_l$. In literature it is shown that $N_q(n, a_1, a_2, \dots, a_l)$ is directly related with $E_q(n, a_1, a_2, \dots, a_l)$ and this relations can be described using the Möbius inversion formula (see, for example [11]). By using the Möbius inversion formula $N_2(n, a_1, a_2, a_3, a_4)$ is given in terms of $E_2(n, a_1, a_2, a_3, a_4)$ in [7]. For completeness of the paper we present this theorem in appendix.

μ denotes the Möbius function defined as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n \text{ is square} - \text{free and a product of } k \text{ distinct primes}, \\ 0 & \text{otherwise.} \end{cases}$$

$E_2(n, a_1, a_2)$ and $E_2(n, a_1, a_2, a_3)$ is obtained in [16] and respectively. We will use these results in our main theorem. For this reason we will present these numbers in the following theorems.

Teorem 1: [16] Let $n \geq 2$ be an integer and $n = 2m$. Then we have $E_2(n, a_1, a_2) = 2^{n-2} + G_2(n, a_1, a_2)$ where $G_2(n, a_1, a_2)$ is given in Table 1.

Table 1 Values of $G_2(n, a_1, a_2)$

m **(mod 4)**	**(0, 0)**	**(0, 1)**	**(1, 0)**	**(1, 1)**
0	-2^{m-1}	2^{m-1}	0	0
1	0	0	-2^{m-1}	2^{m-1}
2	2^{m-1}	-2^{m-1}	0	0
3	0	0	2^{m-1}	-2^{m-1}

Teorem 2: [16] Let $n \geq 2$ be an integer and $n = 2m$. Then we have $E_2(n, a_1, a_2, a_3) = 2^{n-3} + G_2(n, a_1, a_2, a_3)$ where $G_2(n, a_1, a_2, a_3)$ is given in Table 2.

Table 2 Values of $G_2(n, a_1, a_2, a_3)$

m(mod12)	000	001	010	011	100	101	110	111
0	$-2^m - 2^{m-2}$	$2^{m-1} +$	2^{m-2}	2^{m-2}	0	0	0	0
1 or 5	2^{m-2}	-2^{m-2}	2^{m-2}	-2^{m-2}	-2^{m-2}	-2^{m-2}	$2^{m-1} + 2^{m-2}$	-2^{m-2}
2 or 10	0	2^{m-1}	0	-2^{m-1}	2^{m-1}	-2^{m-1}	-2^{m-1}	2^{m-1}
3	2^{m-2}	-2^{m-2}	2^{m-2}	-2^{m-2}	2^{m-1}	0	2^{m-1}	-2^m
4 or 8	-2^{m-1}	0	-2^{m-1}	2^m	0	0	0	0
6	$2^{m-1} + 2^{m-2}$	-2^{m-2}	$-2^{m-1} - 2^{m-2}$	2^{m-2}	2^{m-1}	-2^{m-1}	-2^{m-1}	2^{m-1}
7 or 11	2^{m-2}	-2^{m-2}	2^{m-2}	-2^{m-2}	-2^{m-2}	$2^{m-1} + 2^{m-2}$	-2^{m-2}	-2^{m-2}
9	2^{m-2}	-2^{m-2}	2^{m-2}	-2^{m-2}	-2^m	2^{m-1}	0	2^{m-1}

3. Main Results

In this section we will present our main results that extends the results given in [7]. Throughout the rest of the paper we assume that $n \equiv 4\ (mod\ 8)$. We start by a useful lemma.

Lemma 3: Let $n \equiv 4\ (mod\ 8)$. Then we have $E_2(n, a_1, a_2, a_3, a_4) = E_2(n, a_1, a_1 + a_2, a_1 + a_3, a_4 + a_3 + a_2 + a_1 + 1)$.

Proof: For any $\alpha \in \mathbb{F}_{2^n}$ it is enough to consider the values of $Tr_i(\alpha)$ and $Tr_i(1 + \alpha)$ for all $i = 1,2,3,4$. By definition of the trace function we directly obtain that $Tr_1(1 + \alpha) = Tr_1(\alpha)$ since n is even. For $i = 2$ we have

$$Tr_2(1 + \alpha) = \sum_{0 \leq i < j \leq n-1} (1 + \alpha)^{q^i} (1 + \alpha)^{q^j}$$

$$= \sum_{0 \leq i < j \leq n-1} 1^{q^i} 1^{q^j} + \sum_{0 \leq i < j \leq n-1} 1^{q^i} \alpha^{q^j} + \sum_{0 \leq i < j \leq n-1} \alpha^{q^i} 1^{q^j} + \sum_{0 \leq i < j \leq n-1} \alpha^{q^i} \alpha^{q^j}$$

$$= Tr_2(1) + \sum_{0\le i\le n-1} 1^{q^i} \sum_{0\le j\le n-1} \alpha^{q^j} + Tr_2(\alpha)$$

$$= Tr_2(1) + (n-1)Tr_1(\alpha) + Tr_2(\alpha)$$

$$= Tr_1(\alpha) + Tr_2(\alpha)$$

since $n \equiv 4\ (mod\ 8)$ $n-1 \equiv 1(mod\ 2)$ and $Tr_2(1) = 0$.

For $i = 3$ we have

$$Tr_3(1+\alpha) = \sum_{0\le i<j<k\le n-1} (1+\alpha)^{q^i}(1+\alpha)^{q^j}(1+\alpha)^{q^k}$$

$$= \sum_{0\le i<j<k\le n-1} 1^{q^i}1^{q^j}1^{q^k} + \sum_{0\le i<j<k\le n-1} 1^{q^i}\alpha^{q^j}\alpha^{q^k} + \sum_{0\le i<j<k\le n-1} \alpha^{q^i}\alpha^{q^j}1^{q^k}$$

$$+ \sum_{0\le i<j<k\le n-1} \alpha^{q^i}1^{q^j}\alpha^{q^k} \sum_{0\le i<j<k\le n-1} \alpha^{q^i}1^{q^j}1^{q^k} + \sum_{0\le i<j<k\le n-1} 1^{q^i}\alpha^{q^j}1^{q^k}$$

$$+ \sum_{0\le i<j<k\le n-1} 1^{q^i}1^{q^j}\alpha^{q^k} + \sum_{0\le i<j<k\le n-1} \alpha^{q^i}\alpha^{q^j}\alpha^{q^k}$$

$$= Tr_3(1) + \sum_{0\le i\le n-1} 1^{q^i} \sum_{0\le j<k\le n-1} \alpha^{q^j}\alpha^{q^k} + \sum_{0\le i\le n-1} \alpha^{q^i} \sum_{0\le j<k\le n-1} 1^{q^j}1^{q^k} + Tr_3(\alpha)$$

$$= Tr_3(1) + (n-2)Tr_2(\alpha) + \binom{n-1}{2} Tr_1(\alpha) + Tr_3(\alpha)$$

$$= Tr_1(\alpha) + Tr_3(\alpha)$$

since $n \equiv 4\ (mod\ 8)$, $n-2 \equiv 0(mod 2)$, $\binom{n-1}{2} \equiv 1\ (mod\ 2)$ and $Tr_3(1) = 0$.

Similarly, for $i = 4$ by expanding

$$Tr_4(1+\alpha) = \sum_{0\le i<j<k<l\le n-1} (1+\alpha)^{q^i}(1+\alpha)^{q^j}(1+\alpha)^{q^k}(1+\alpha)^{q^l}$$

we obtained the desired result $Tr_4(1+\alpha) = Tr_1(\alpha) + Tr_2(\alpha) + Tr_3(\alpha) + Tr_4(\alpha) + 1$ which completes the proof.

Combining Lemma 3 with Theorem 2 we present values of $E_2(n, a_1, a_2, a_3, a_4)$ in some cases in the following corollary.

Corollary 4: Let $n \equiv 4\ (mod 8)$. We have

$$E_2(n,0,0,0,0) = E_2(n,0,0,0,1) = \begin{cases} 2^{n-4} & \frac{n}{2} \equiv 2\ or\ 10\ (mod\ 12) \\ 2^{n-4} + 3 \cdot 2^{n/2-3} & \frac{n}{2} \equiv 6\ (mod\ 12) \end{cases}$$

and

$$E_2(n,0,1,1,0) = E_2(n,0,1,1,1) = \begin{cases} 2^{n-4} - 2^{n/2-2} & \frac{n}{2} \equiv 2\ or\ 10\ (mod\ 12) \\ 2^{n-4} + 2^{n/2-3} & \frac{n}{2} \equiv 6\ (mod\ 12) \end{cases}$$

Proof: From Lemma 3 we know that $E_2(n,0,0,0,0) = E_2(n,0,0,0,1)$ and $E_2(n,0,1,1,0) = E_2(n,0,1,1,1)$. Furthermore we have

$E_2(n,0,0,0,0) + E_2(n,0,0,0,1) = E_2(n,0,0,0)$ and

$E_2(n,0,1,1,0) + E_2(n,0,1,1,1) = E_2(n,0,1,1)$

Therefore using Theorem 3 we get

$$E_2(n,0,0,0,0) = E_2(n,0,0,0,1) = \frac{E_2(n,0,0,0)}{2}$$

$$= \begin{cases} 2^{n-4} & \frac{n}{2} \equiv 2\ or\ 10\ (mod\ 12) \\ 2^{n-4} + 3 \cdot 2^{n/2-3} & \frac{n}{2} \equiv 6(mod\ 12) \end{cases}$$

and

$$E_2(n,0,1,1,0) = E_2(n,0,1,1,1) = \frac{E_2(n,0,1,1)}{2}$$

$$= \begin{cases} 2^{n-4} - 2^{n/2-2} & \frac{n}{2} \equiv 2\ or\ 10\ (mod 12) \\ 2^{n-4} + 2^{n/2-3} & \frac{n}{2} \equiv 6\ (mod 12) \end{cases}$$

Furthermore, by combining Lemma 3 and Theorem 1 with Theorem 7 given in the appendix we directly obtain the following result which extends Theorem 7.

Theorem 5: Let $n \equiv 4\ (mod 8)$. Then we have

$$nN_2(n,1,1,1,0) = \sum_{\substack{d|n \\ d\equiv 1,3\ (mod 8)}} \mu(d)E_2(n/d\,,1,0,0,0) + \sum_{\substack{d|n \\ d\equiv 5,7\ (mod 8)}} \mu(d)E_2(n/d\,,1,0,0,1)$$

$$nN_2(n,1,0,0,1) = \sum_{\substack{d|n \\ d\equiv 1,7\ (mod 8)}} \mu(d)E_2(n/d\,,1,0,0,1) + \sum_{\substack{d|n \\ d\equiv 3,5\ (mod 8)}} \mu(d)E_2(n/d\,,1,0,0,0)$$

$$nN_2(n,1,1,1,1) = \sum_{\substack{d|n \\ d\equiv 1,3\ (mod 8)}} \mu(d)E_2(n/d\,,1,0,0,1) + \sum_{\substack{d|n \\ d\equiv 5,7\ (mod 8)}} \mu(d)E_2(n/d\,,1,0,0,0)$$

$$nN_2(n,1,0,0,0) = \sum_{\substack{d|n \\ d\equiv 1,7\ (mod 8)}} \mu(d)E_2(n/d\,,1,0,0,0) + \sum_{\substack{d|n \\ d\equiv 3,5\ (mod 8)}} \mu(d)E_2(n/d\,,1,0,0,1)$$

$$nN_2(n,0,0,1,0) = \sum_{\substack{d|n \\ d\ odd}} \mu(d)E_2(n/d\,,0,0,1,0)$$

$$nN_2(n,0,0,1,1) = \sum_{\substack{d|n \\ d\ odd}} \mu(d)E_2(n/d\,,0,0,1,1)$$

$$nN_2(n,1,1,0,0) = \sum_{\substack{d|n \\ d\equiv 1,7\ (mod 8)}} \mu(d)E_2(n/d\,,1,1,0,0) + \sum_{\substack{d|n \\ d\equiv 3,5\ (mod 8)}} \mu(d)E_2(n/d\,,1,1,0,1)$$

$$nN_2(n,1,0,1,1)$$

$$= \sum_{\substack{d|n \\ d\equiv 1,3\ (mod 8)}} \mu(d)E_2(n/d\,,1,1,0,0) + \sum_{\substack{d|n \\ d\equiv 5,7\ (mod 8)}} \mu(d)E_2(n/d\,,1,1,0,1)$$

$$nN_2(n,1,1,0,1)$$

$$= \sum_{\substack{d|n \\ d\equiv 1,7\ (mod 8)}} \mu(d)E_2(n/d\,,1,1,0,1) + \sum_{\substack{d|n \\ d\equiv 3,5\ (mod 8)}} \mu(d)E_2(n/d\,,1,1,0,0)$$

$$nN_2(n,1,0,1,0)$$

$$= \sum_{\substack{d|n \\ d\equiv 1,3\ (mod 8)}} \mu(d)E_2(n/d\,,1,1,0,1) + \sum_{\substack{d|n \\ d\equiv 5,7\ (mod 8)}} \mu(d)E_2(n/d\,,1,1,0,0)$$

$$nN_2(n,0,1,1,1) = nN_2(n,0,1,1,0) = \sum_{\substack{d|n \\ d\ odd}} \mu(d)E_2(n/d\,,0,1,1,1)$$

$$nN_2(n,0,0,0,0) = nN_2(n,0,0,0,1)$$
$$= \sum_{\substack{d|n \\ d\ odd}} \mu(d)E_2(n/d\,,0,0,0,0) - \sum_{\substack{d|n \\ d\ odd}} \mu(d)2^{\frac{n}{2d}-2}$$

$$nN_2(n,0,1,0,0)$$

$$= \left(\sum_{\substack{d|n \\ d\equiv 1(mod 4)}} \mu(d)E_2(n/d\,,0,1,0,0) - \sum_{\substack{d|n \\ d\equiv 1\ (mod 4)}} \mu(d)E_2(n/2d\,,1,0) \right.$$
$$\left. + \sum_{\substack{d|n \\ d\equiv 3\ (mod 4)}} \mu(d)E_2(n/d\,,0,1,0,1) - \sum_{\substack{d|n \\ d\equiv 3\ (mod 4)}} \mu(d)E_2(n/2d\,,1,1) \right)$$

$$nN_2(n,0,1,0,1)$$

$$= \left(\sum_{\substack{d|n \\ d\equiv 1\ (mod 4)}} \mu(d)E_2(n/d\,,0,1,0,1) - \sum_{\substack{d|n \\ d\equiv 1\ (mod 4)}} \mu(d)E_2(n/2d\,,1,1) \right.$$
$$\left. + \sum_{\substack{d|n \\ d\equiv 3\ (mod 4)}} \mu(d)E_2(n/d\,,0,1,0,0) - \sum_{\substack{d|n \\ d\equiv 3\ (mod 4)}} \mu(d)E_2(n/2d\,,1,0) \right)$$

In Theorem 5 we see that the values of $N_2(n, a_1, a_2, a_3, a_4)$ are directly related with the values of $E_2(n, a_1, a_2, a_3, a_4)$ and $E_2(n/d, a_1, a_2, a_3, a_4)$ where d is an odd divisor of n. In this paper we are only dealing with n's of the form $n = 8k + 4$, therefore we need the following useful result.

Proposition 6: Let n be a positive integer satisfying $n \equiv 4 \ (mod\ 8)$ and d be a positive odd divisor of n. Then we have $n/d \equiv 4 \ (mod\ 8)$.

Proof: Assume that $n = 8k + 4 = 4(2k + 1)$ for some positive integer k. Then we have $n/d = 4t$ where $t = (2k + 1)/d$ is an odd integer. Therefore, we have $n/d = 4t \equiv 4 \ (mod\ 8)$.

4. Values of $N_2(n, a_1, a_2, a_3, a_4)$

In this section using Corollary 4, Theorem 5 and Proposition 6 we will present the values of $N_2(n, a_1, a_2, a_3, a_4)$ depending on the coefficients (a_1, a_2, a_3, a_4) and the prime decomposition of n. In some cases we obtained the exact values of $N_2(n, a_1, a_2, a_3, a_4)$.

Assume that $n = 4$. In this case we know that the only monic irreducible polynomials are $x^4 + x + 1$, $x^4 + x^3 + 1$ and $x^4 + x^3 + x^2 + x + 1$; therefore we have $N_2(n, 0,0,1,1) = N_2(n, 1,0,0,1) = N_2(n, 1,1,1,1) = 1$. Furthermore we have $E_2(4,0,0,1,1) = E_2(4,1,0,0,1) = E_2(4,1,1,1,1) = 4$, $E_2(4,0,1,0,1) = 2$, $E_2(4,0,0,0,0) = E_2(4,0,0,0,1) = 1$ and $E_2(4, a_1, a_2, a_3, a_4) = 0$ in all other 10 cases.

Now assume that $n = 4p^k$ for some odd prime p and positive integer k. In this case note that the only positive odd divisors of n are p^i where $0 \leq i \leq k$. But note that by definition $\mu(1) = 1$, $\mu(p) = -1$ and $\mu(p^i) = 0$ for $i \in \{2, \dots, k\}$.

In the following four cases we have the exact values of $N_2(n, a_1, a_2, a_3, a_4)$

$$N_2(n,0,1,1,1) = N_2(n,0,1,1,0) = \frac{1}{n}(E_2(n,0,1,1,1) - E_2(n/p,0,1,1,1))$$

$$= \begin{cases} \frac{1}{n}\left(2^{n-4} - 2^{n/2-2} - 2^{n/p-4} + 2^{n/(2p)-2}\right) & if\ p \neq 3 \\ \frac{1}{n}\left(2^{n-4} + 2^{n/2-3} - 2^{n/p-4} - 2^{n/(2p)-3}\right) & if\ p = 3 \end{cases}$$

and

$$N_2(n,0,0,0,0) = N_2(n,0,0,0,1)$$

$$= \frac{1}{n}\left(E_2(n,0,0,0,0) - E_2(n/p,0,0,0,0) - 2^{n/2-2} + 2^{n/(2p)-2}\right)$$

$$= \begin{cases} \frac{1}{n}\left(2^{n-4} - 2^{n/p-4} - 2^{n/2-2} + 2^{n/(2p)-2}\right) & if\ p \neq 3 \\ \frac{1}{n}\left(2^{n-4} + 3\cdot 2^{n/2-3} - 2^{\frac{n}{p}-4} - 3\cdot 2^{n/(2p)-3} - 2^{n/2-2} + 2^{n/(2p)-2}\right) & if\ p = 3 \end{cases}$$

Now assume that $n = 4{p_1}^{k_1}{p_2}^{k_2}$ for some odd primes p_1, p_2 (W.L.O.G assume that $p_1 < p_2$) and positive integers k_1, k_2 . In this case note that the only positive odd divisors of n are ${p_1}^i, {p_2}^j$ and ${p_1}^i{p_2}^j$ where $0 \le i \le k_1$ and $0 \le j \le k_2$. But note that by definition $\mu(1) = 1, \mu(p_1) = \mu(p_2) = -1, \mu(p_1p_2) = 1$, $\mu({p_1}^i) = \mu({p_2}^j) = 0$ for $i \in \{2,\dots,k_1\},\ j \in \{2,\dots,k_2\}$, $\mu({p_1}^i{p_2}^j) = 0$ for $i \in \{1,2,\dots,k_1\},\ j \in \{2,\dots,k_2\}$ and $\mu({p_1}^i{p_2}^j) = 0$ for $i \in \{2,\dots,k_1\},\ j \in \{1,2,\dots,k_2\}$.

In the following four cases we have the exact values of $N_2(n,a_1,a_2,a_3,a_4)$

$$N_2(n,0,1,1,1) = N_2(n,0,1,1,0)$$

$$= \frac{1}{n}\left(E_2(n,0,1,1,1) - E_2\left(\frac{n}{p_1},0,1,1,1\right) - E_2\left(\frac{n}{p_2},0,1,1,1\right) + E_2\left(\frac{n}{p_1p_2},0,1,1,1\right)\right) =$$

$$\begin{cases} \frac{1}{n}\left(2^{n-4} + 2^{n/2-3} - 2^{\frac{n}{p_1}-4} + 2^{n/(2p_1)-2} - 2^{\frac{n}{p_2}-4} - 2^{n/(2p_2)-3} + 2^{\frac{n}{p_1p_2}-4} - 2^{n/(2p_1p_2)-2}\right) & if\ p_1 = 3\ and\ k_1 = 1 \\ \frac{1}{n}\left(2^{n-4} + 2^{n/2-3} - 2^{\frac{n}{p_1}-4} - 2^{n/(2p_1)-3} - 2^{\frac{n}{p_2}-4} - 2^{n/(2p_2)-3} + 2^{\frac{n}{p_1p_2}-4} + 2^{n/(2p_1p_2)-3}\right) & if\ p_1 = 3\ and\ k_1 > 1 \\ \frac{1}{n}\left(2^{n-4} - 2^{n/2-2} - 2^{\frac{n}{p_1}-4} + 2^{n/(2p_1)-2} - 2^{\frac{n}{p_2}-4} + 2^{n/(2p_2)-2} + 2^{\frac{n}{p_1p_2}-4} - 2^{n/(2p_1p_2)-2}\right) & if\ p_1 \neq 3 \end{cases}$$

and

$$N_2(n,0,0,0,0) = N_2(n,0,0,0,1)$$
$$= \frac{1}{n}\begin{pmatrix} E_2(n,0,0,0,0) - E_2\left(\frac{n}{p_1},0,0,0,0\right) - E_2\left(\frac{n}{p_2},0,0,0,0\right) + E_2\left(\frac{n}{p_1p_2},0,0,0,0\right) \\ -2^{n/2-2} + 2^{n/(2p_1)-2} + 2^{n/(2p_2)-2} - 2^{n/(2p_1p_2)-2} \end{pmatrix}$$

$$= \begin{cases} \frac{1}{n}\begin{pmatrix} 2^{n-4} + 3\cdot 2^{n/2-3} - 2^{\frac{n}{p_1}-4} - 2^{\frac{n}{p_2}-4} - 3.2^{n/2p_2-3} + 2^{\frac{n}{p_1p_2}-4} \\ -2^{n/2-2} + 2^{n/(2p_1)-2} + 2^{n/(2p_2)-2} - 2^{n/(2p_1p_2)-2} \end{pmatrix} & if\ p_1 = 3\ and\ k_1 = 1 \\ \frac{1}{n}\begin{pmatrix} 2^{n-4} + 3\cdot 2^{n/2-3} - 2^{\frac{n}{p_1}-4} - 3\cdot 2^{n/(2p_1)-3} - 2^{\frac{n}{p_2}-4} - 3.2^{n/2p_2-3} \\ +2^{\frac{n}{p_1p_2}-4} + 3.2^{n/2p_1p_2-3} - 2^{n/2-2} + 2^{n/(2p_1)-2} + 2^{n/(2p_2)-2} - 2^{n/(2p_1p_2)-2} \end{pmatrix} & if\ p_1 = 3\ and\ k_1 > 1 \\ \frac{1}{n}\begin{pmatrix} 2^{n-4} - 2^{n/p_1-4} - 2^{n/p_2-4} + 2^{n/p_1p_2-4} \\ -2^{n/2-2} + 2^{n/(2p_1)-2} + 2^{n/(2p_2)-2} - 2^{n/(2p_1p_2)-2} \end{pmatrix} & if\ p_1 \neq 3 \end{cases}$$

For the general case assume that $n = 4{p_1}^{k_1}{p_2}^{k_2}\cdots{p_s}^{k_s}$ where $p_1, p_2, \ldots, p_s$ are relatively prime odd primes and $k_1, k_2, \ldots, k_s$ are positive integers. Then by the above argument using Corollary 4 and Theorem 5 we can easily evalute the values of $N_2(n,0,0,0,0)$ $\left(= N_2(n,0,0,0,1)\right)$ and $N_2(n,0,1,1,1)$ $(= N_2(n,0,1,1,0))$.

For the other 12 cases as we don't know the values of $E_2(n,a_1,a_2,a_3,a_4)$ we can use the same approximation argument given in [7]. Note that using Theorem 5 one can observe some further equalities depending on the prime factorization of n.

As an example we evaluate the values of $N_2(20,a_1,a_2,a_3,a_4)$ and presented them in Table 3. The bold entries in Table 3 are the exact values of $N_2(20,a_1,a_2,a_3,a_4)$ that are obtained using our results.

Table 3 Values of $N_2(20,a_1,a_2,a_3,a_4)$

a_1,a_2,a_3,a_4	Koma's estimate	Our estimate	Exact Value
0, 0, 0, 0	3264	**3264**	3264
0, 0, 0, 1	3264	**3264**	3264
0, 0, 1, 0	3276.75	3276.75	3264
0, 0, 1, 1	3276.75	3276.75	3315
0, 1, 0, 0	3264.75	3264.75	3280
0, 1, 0, 1	3263.25	3263.25	3248
0, 1, 1, 0	3276.75	**3264**	3264
0, 1, 1, 1	3276.75	**3264**	3264

1, 0, 0, 0	3276.75	3276.75	3275
1, 0, 0, 1	3276.75	3276.75	3304
1, 0, 1, 0	3276.75	3276.75	3264
1, 0, 1, 1	3276.75	3276.75	3264
1, 1, 0, 0	3276.75	3276.75	3264
1, 1, 0, 1	3276.75	3276.75	3264
1, 1, 1, 0	3276.75	3276.75	3275
1, 1, 1, 1	3276.75	3276.75	3304

References

[1] Ahmadi, O., Göloğlu, F., Granger, R., McGuire, G. and Yılmaz, E. S., Fibre products of supersingular curves and the enumeration of irreducible polynomials with prescribed coefficients, Finite Fields and Their Applications, 2016, 42, 128-164.

[2] Carlitz, L., A theorem of dickson on irreducible polynomials. Proceedings of the American Mathematical Society, 1952, 3 (5), 693-700.

[3] Cattell, K., Miers, C. R., Ruskey, F., Serra, M. and Sawada, J., The number of irreducible polynomials over GF(2) with given trace and subtrace. Journal of Combinatorial Mathematics and Combinatorial Computing, 2003, 47 (November), 31-64.

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

[5] Granger, R., On the enumeration of irreducible polynomials over GF(q) with prescribed coefficients, https://arxiv.org/pdf/1610.06878.pdf, 2016.

[6] Koma, B. O., Panario, D. and Wang, Q., The number of irreducible polynomials of degree n over Fq with given trace and constant terms, Discrete Mathematics, 2010, 310, 1282-1292.

[7] Koma, O., The number of irreducible polynomials over a finite field with prescribed coefficients, PhD thesis, 2010.

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

[9] Kuz'min, E. N., Irreducible polynomials over a finite field and an analogue of Gauss sums over a field of characteristic 2, Siberian Mathematical Journal, 1991, 32(6), 982-989.

[10] Lalin, M. and Larocque, O. The number of irreducible polynomials with first two prescribed coefficients over a finite field, Rocky Mountain Journal of Mathematics, 2016, 46 (5), 1587-1618.

[11] Lidl, R. and Niedderreiter, H., Finite fields, Cambridge University Press, 2008, 755, New York.

[12] Moisio, M., Kloosterman sums, elliptic curves and irreducible polynomials with prescribed trace and norm, Acta Arithmetica, 2008, 132, 329-350.

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

[14] Ri, W. H., Myong, G. C., Kim, R. And Rim, C. I., The number of irreducible polyomials over finite fields of characteristic 2 with given trace and subtrace, Finite Fields and Their Applications, 2014, 29, 118-131.

[15] Ruskey, F., Miers, C.R. and Sawada, J., The number of Lyndon words and irreducible polynomials of given trace, SIAM Journal Discrete Mathematics, 2001, 14(2), 240-245.

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

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

Received: September 18, 2017

Appendix

Theorem 7 [7] Let n be even. Then we have

$$N_2(n,1,1,1,0)$$
$$=\frac{1}{n}\left(\begin{array}{l}\sum\limits_{\substack{d|n\\ d\equiv 1\ (mod 8)}}\mu(d)E_2(n/d\,,1,1,1,0)+\sum\limits_{\substack{d|n\\ d\equiv 3\ (mod 8)}}\mu(d)E_2(n/d\,,1,0,0,0)\\ +\sum\limits_{\substack{d|n\\ d\equiv 5\ (mod 8)}}\mu(d)E_2(n/d\,,1,1,1,1)+\sum\limits_{\substack{d|n\\ d\equiv 7\ (mod 8)}}\mu(d)E_2(n/d\,,1,0,0,1)\end{array}\right)$$

$$N_2(n,1,0,0,1)$$
$$=\frac{1}{n}\left(\begin{array}{l}\sum\limits_{\substack{d|n\\ d\equiv 1\ (mod 8)}}\mu(d)E_2(n/d\,,1,0,0,1)+\sum\limits_{\substack{d|n\\ d\equiv 3 (mod 8)}}\mu(d)E_2(n/d\,,1,1,1,0)\\ +\sum\limits_{\substack{d|n\\ d\equiv 5(mod 8)}}\mu(d)E_2(n/d\,,1,0,0,0)+\sum\limits_{\substack{d|n\\ d\equiv 7\ (mod 8)}}\mu(d)E_2(n/d\,,1,1,1,1)\end{array}\right)$$

$$N_2(n,1,1,1,1)$$
$$=\frac{1}{n}\left(\begin{array}{l}\sum\limits_{\substack{d|n\\ d\equiv 1\ (mod 8)}}\mu(d)E_2(n/d\,,1,1,1,1)+\sum\limits_{\substack{d|n\\ d\equiv 3\ (mod 8)}}\mu(d)E_2(n/d\,,1,0,0,1)\\ +\sum\limits_{\substack{d|n\\ d\equiv 5\ (mod 8)}}\mu(d)E_2(n/d\,,1,1,1,0)+\sum\limits_{\substack{d|n\\ d\equiv 7\ (mod 8)}}\mu(d)E_2(n/d\,,1,0,0,0)\end{array}\right)$$

$$N_2(n,1,0,0,0)$$
$$=\frac{1}{n}\left(\begin{array}{l}\sum\limits_{\substack{d|n\\ d\equiv 1\ (mod 8)}}\mu(d)E_2(n/d\,,1,0,0,0)+\sum\limits_{\substack{d|n\\ d\equiv 3\ (mod 8)}}\mu(d)E_2(n/d\,,1,1,1,1)\\ +\sum\limits_{\substack{d|n\\ d\equiv 5\ (mod 8)}}\mu(d)E_2(n/d\,,1,0,0,1)+\sum\limits_{\substack{d|n\\ d\equiv 7\ (mod 8)}}\mu(d)E_2(n/d\,,1,1,1,0)\end{array}\right)$$

$$N_2(n,0,0,1,0) = \frac{1}{n}\left(\sum_{\substack{d|n \\ d\ odd}} \mu(d)E_2(n/d\,,0,0,1,0)\right)$$

$$N_2(n,0,0,1,1) = \frac{1}{n}\left(\sum_{\substack{d|n \\ d\ odd}} \mu(d)E_2(n/d\,,0,0,1,1)\right)$$

$$N_2(n,1,1,0,0)$$

$$= \frac{1}{n}\left(\begin{array}{c} \sum\limits_{\substack{d|n \\ d\equiv 1\ (mod 8)}} \mu(d)E_2(n/d\,,1,1,0,0) \\ + \sum\limits_{\substack{d|n \\ d\equiv 3\ (mod 8)}} \mu(d)E_2(n/d\,,1,0,1,0) + \sum\limits_{\substack{d|n \\ d\equiv 5 (mod 8)}} \mu(d)E_2(n/d\,,1,1,0,1) \\ + \sum\limits_{\substack{d|n \\ d\equiv 7\ (mod 8)}} \mu(d)E_2(n/d\,,1,0,1,1) \end{array}\right)$$

$$N_2(n,1,0,1,1)$$

$$= \frac{1}{n}\left(\begin{array}{l} \sum\limits_{\substack{d|n \\ d\equiv 1\ (mod 8)}} \mu(d)E_2(n/d\,,1,0,1,1) + \sum\limits_{\substack{d|n \\ d\equiv 3\ (mod 8)}} \mu(d)E_2(n/d\,,1,1,0,0) \\ + \sum\limits_{\substack{d|n \\ d\equiv 5\ (mod 8)}} \mu(d)E_2(n/d\,,1,0,1,0) + \sum\limits_{\substack{d|n \\ d\equiv 7\ (mod 8)}} \mu(d)E_2(n/d\,,1,1,0,1) \end{array}\right)$$

$$N_2(n,1,1,0,1)$$

$$= \frac{1}{n}\left(\begin{array}{l} \sum\limits_{\substack{d|n \\ d\equiv 1\ (mod 8)}} \mu(d)E_2(n/d\,,1,1,0,1) + \sum\limits_{\substack{d|n \\ d\equiv 3\ (mod 8)}} \mu(d)E_2(n/d\,,1,0,1,1) \\ + \sum\limits_{\substack{d|n \\ d\equiv 5\ (mod 8)}} \mu(d)E_2(n/d\,,1,1,0,0) + \sum\limits_{\substack{d|n \\ d\equiv 7\ (mod 8)}} \mu(d)E_2(n/d\,,1,0,1,0) \end{array}\right)$$

$$N_2(n,1,0,1,0)$$

$$= \frac{1}{n}\left(\sum_{\substack{d|n \\ d\equiv 1\,(mod 8)}} \mu(d)E_2(n/d\,,1,0,1,0) + \sum_{\substack{d|n \\ d\equiv 3\,(mod 8)}} \mu(d)E_2(n/d\,,1,1,0,1) + \sum_{\substack{d|n \\ d\equiv 5\,(mod 8)}} \mu(d)E_2(n/d\,,1,0,1,1) + \sum_{\substack{d|n \\ d\equiv 7\,(mod 8)}} \mu(d)E_2(n/d\,,1,1,0,0) \right)$$

$$N_2(n,0,1,1,1) = \frac{1}{n}\left(\sum_{\substack{d|n \\ d\equiv 1\,(mod 4)}} \mu(d)E_2(n/d\,,0,1,1,1) + \sum_{\substack{d|n \\ d\equiv 3\,(mod 4)}} \mu(d)E_2(n/d\,,0,1,1,0) \right)$$

$$N_2(n,0,1,1,0) = \frac{1}{n}\left(\sum_{\substack{d|n \\ d\equiv 1\,(mod 4)}} \mu(d)E_2(n/d\,,0,1,1,0) + \sum_{\substack{d|n \\ d\equiv 3\,(mod 4)}} \mu(d)E_2(n/d\,,0,1,1,1) \right)$$

$$N_2(n,0,0,0,0) = \frac{1}{n}\left(\sum_{\substack{d|n \\ d\ odd}} \mu(d)E_2(n/d\,,0,0,0,0) - \sum_{\substack{d|n,n/d\ even \\ d\ odd}} \mu(d)E_2(n/2d\,,0,0) \right)$$

$$N_2(n,0,0,0,1) = \frac{1}{n}\left(\sum_{\substack{d|n \\ d\ odd}} \mu(d)E_2(n/d\,,0,0,0,1) - \sum_{\substack{d|n,n/d\ even \\ d\ odd}} \mu(d)E_2(n/2d\,,0,1) \right)$$

$$N_2(n,0,1,0,0)$$

$$= \frac{1}{n}\left(\begin{array}{l} \sum\limits_{\substack{d|n \\ d\equiv 1\ (mod 4)}} \mu(d)E_2(n/d\,,0,1,0,0) - \sum\limits_{\substack{d|n,n/d\ even \\ d\equiv 1\ (mod 4)}} \mu(d)E_2(n/2d\,,1,0) \\ + \sum\limits_{\substack{d|n \\ d\equiv 3\ (mod 4)}} \mu(d)E_2(n/d\,,0,1,0,1) - \sum\limits_{\substack{d|n,n/d\ even \\ d\equiv 3\ (mod 4)}} \mu(d)E_2(n/2d\,,1,1) \end{array} \right)$$

$$N_2(n,0,1,0,1)$$

$$= \frac{1}{n}\left(\begin{array}{c} \sum\limits_{\substack{d|n \\ d\equiv 1\ (mod 4)}} \mu(d)E_2(n/d\,,0,1,0,1) \\ - \sum\limits_{\substack{d|n,n/d\ even \\ d\equiv 1\ (mod 4)}} \mu(d)E_2(n/2d\,,1,1) + \sum\limits_{\substack{d|n \\ d\equiv 3\ (mod 4)}} \mu(d)E_2(n/d\,,0,1,0,0) \\ - \sum\limits_{\substack{d|n,n/d\ even \\ d\equiv 3\ (mod 4)}} \mu(d)E_2(n/2d\,,1,0) \end{array} \right)$$