The Number of Irreducible Polynomials of Even Degree over $\mathbb{F}_2$ with the First Four Coefficients Given

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

July 22, 2010

Definitions and Background

For $\beta \in \mathbb{F}_{2^n}$ the k^{th} trace is denoted by $T_k(\beta)$, and defined as

$$T_k(\beta) = \sum_{0 \leq i_1 < i_2 < \cdots < i_k \leq n-1} \beta^{i_1} \beta^{i_2} \cdots \beta^{i_k}.$$

$F(n, t_1, \cdots, t_r)$: the number of $\beta \in \mathbb{F}_{2^n}$ where $T_i(\beta) = t_i$, $1 \leq i \leq r$.

Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial of degree n over $\mathbb{F}_2$.

a_{n-i} is the i^{th} trace of f, written as $T_i(f) = a_{n-i}$, for $1 \leq i \leq n$.

$P(n, t_1, \cdots, t_r)$: the set of irreducible polynomials of degree n over $\mathbb{F}_2$, where $a_{n-i} = t_i \in \mathbb{F}_2$. Let $N(n, t_1, \cdots, t_r) = |P(n, t_1, \cdots, t_r)|$.

Previous Results

Let $N(n,q)$ be the number of monic irreducible polynomials of degree n over $\mathbb{F}_q[x]$. Then

$$q^n = \sum_{d|n} dN(n,q).$$

By Möbius inversion formula we have

$$N(n,q) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n}\sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

The number of irreducible polynomials with the first coefficient prescribed is given by Carlitz (1952).

Let n be an even integer, and $a \equiv b \pmod 4$ be shortened to $a \equiv b$.

Then Cattell, Miers, Ruskey, Serra, and Sawada, (2003) proved that

$$
\begin{aligned}
nN(n,1,0) &= \sum_{\substack{d|n \\ d\equiv 1}} \mu(d)F(n/d,1,0) + \sum_{\substack{d|n \\ d\equiv 3}} \mu(d)F(n/d,1,1), \\
nN(n,1,1) &= \sum_{\substack{d|n \\ d\equiv 1}} \mu(d)F(n/d,1,1) + \sum_{\substack{d|n \\ d\equiv 3}} \mu(d)F(n/d,1,0), \\
nN(n,0,0) &= \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d)F(n/d,0,0) - \sum_{\substack{d|n, n/d \text{even} \\ d \text{ odd}}} \mu(d)2^{\frac{n}{2d}-1}, \\
nN(n,0,1) &= \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d)F(n/d,0,1) - \sum_{\substack{d|n, n/d \text{even} \\ d \text{ odd}}} \mu(d)2^{\frac{n}{2d}-1}.
\end{aligned}
$$

Also $F(n, t_1, t_2) = 2^{n-2} + G(n, t_1, t_2)$, and for $n = 2m$ we have

Table: Values of $G(n, t_1, t_2)$

$m \pmod 4$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
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}

The number of irreducible polynomials of even degree n over $\mathbb{F}_2$ with given first three coefficients is considered by Yucas and Mullen (2004) . For odd degree n Fitzgerald and Yucas (2003) consider the same problem.

Generalizing Möbius Inversion Formula

For our study we proved the following generalization of Möbius Inversion.

Theorem

Suppose $a \equiv b \pmod 8$ *be written as* $a \equiv b$. *Let* $A(n)$, $B(n)$, $C(n)$, $D(n)$, $\alpha(n)$, $\beta(n)$, $\gamma(n)$, *and* $\delta(n)$ *be functions defined on* $\mathbb{N}$. *Then*

$$A(n) = \sum_{\substack{d|n \\ d\equiv 1}} \alpha\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 3}} \beta\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 5}} \gamma\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 7}} \delta\left(\frac{n}{d}\right),$$

$$B(n) = \sum_{\substack{d|n \\ d\equiv 1}} \beta\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 3}} \alpha\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 5}} \delta\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 7}} \gamma\left(\frac{n}{d}\right),$$

$$C(n) = \sum_{\substack{d|n \\ d\equiv 1}} \gamma\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 3}} \delta\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 5}} \alpha\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 7}} \beta\left(\frac{n}{d}\right),$$

$$D(n) = \sum_{\substack{d|n \\ d\equiv 1}} \delta\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 3}} \gamma\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 5}} \beta\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 7}} \alpha\left(\frac{n}{d}\right),$$

if and only if

Theorem

(Countinued)

$$\alpha(n) = \sum_{\substack{d|n \\ d\equiv 1}} \mu(d) A\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 3}} \mu(d) B\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 5}} \mu(d) C\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 7}} \mu(d) D\left(\frac{n}{d}\right),$$

$$\beta(n) = \sum_{\substack{d|n \\ d\equiv 1}} \mu(d) B\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 3}} \mu(d) A\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 5}} \mu(d) D\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 7}} \mu(d) C\left(\frac{n}{d}\right),$$

$$\gamma(n) = \sum_{\substack{d|n \\ d\equiv 1}} \mu(d) C\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 3}} \mu(d) D\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 5}} \mu(d) A\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 7}} \mu(d) B\left(\frac{n}{d}\right),$$

$$\delta(n) = \sum_{\substack{d|n \\ d\equiv 1}} \mu(d) D\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 3}} \mu(d) C\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 5}} \mu(d) B\left(\frac{n}{d}\right) + \sum_{\substack{d|n \\ d\equiv 7}} \mu(d) A\left(\frac{n}{d}\right).$$

In general, we proved that when modulo is 2^j, where $j > 3$, we have 2^{j-1} functions in terms of some other 2^{j-1} functions. For our case, $j = 3$.

Computing $F(n, t_1, t_2, t_3, t_4)$

Lemma

Let $\beta \in \mathbb{F}_{2^n}$ and $f \in \mathbb{F}_2[x]$ of degree n/d be the minimal polynomial of β. Then the i^{th} trace of β is the coefficient of x^{n-i} in f^d, or $T_i(\beta) = T_i(f^d)$, where $1 \leq i \leq n$.

Lemma

Let $d \geq 1$ be an integer, and $f \in \mathbb{F}_2[x]$. Then

(i) $T_1(f^d) = dT_1(f)$;

(ii) $T_2(f^d) = \binom{d}{2} T_1(f) + dT_2(f)$;

(iii) $T_3(f^d) = \binom{d}{3} T_1(f) + dT_3(f)$;

(iv) $T_4(f^d) = \binom{d}{4} T_1(f) + \binom{d}{2} T_2(f) + dT_4(f)$.

Lemma

Let d be a given integer such that $d \geq 1$. For $0 \leq j \leq 7$ we shorten $d \equiv j \pmod 8$ as $d \equiv j$. If $f \in \mathbb{F}_2[x]$ is a given polynomial, then for $0 \leq j \leq 7$ the coefficients $T_i(f^d)$ where $i = 1, 2, 3, 4$ are given in the following table.

Table: Different coefficients of f^d

$d \equiv i$	$T_1(f^d)$	$T_2(f^d)$	$T_3(f^d)$	$T_4(f^d)$
$d \equiv 0$	0	0	0	0
$d \equiv 1$	$T_1(f)$	$T_2(f)$	$T_3(f)$	$T_4(f)$
$d \equiv 2$	0	$T_1(f)$	0	$T_2(f)$
$d \equiv 3$	$T_1(f)$	$T_1(f) + T_2(f)$	$T_1(f) + T_3(f)$	$T_2(f) + T_4(f)$
$d \equiv 4$	0	0	0	$T_1(f)$
$d \equiv 5$	$T_1(f)$	$T_2(f)$	$T_3(f)$	$T_1(f) + T_4(f)$
$d \equiv 6$	0	$T_1(f)$	0	$T_1(f) + T_2(f)$
$d \equiv 7$	$T_1(f)$	$T_1(f) + T_2(f)$	$T_1(f) + T_3(f)$	$T_1(f) + T_2(f) + T_4(f)$

Theorem

Let n be an even positive integer and $t_i \in \mathbb{F}_2$, for $1 \leq i \leq 4$. Also let $a \equiv b \pmod 8$ be shortened as $a \equiv b$. Then the number of elements $\beta \in \mathbb{F}_{2^n}$ with prescribed first four traces $T_i(\beta) = t_i$ can be given by

$$F(n, t_1, t_2, t_3, t_4) = \sum_{i=0}^{7} \bigcup_{\substack{d|n \\ d \equiv i}} \frac{n}{d}. |S_i| ,$$

where the sets $S_0, \ldots, S_7$ are defined as:

$$\begin{aligned} S_0 = &\quad \{f \in P(n/d) : t_i = 0,\ i = 1, 2, 3, 4\}, \\ S_1 = &\quad \{f \in P(n/d) : T_i(f) = t_i,\ i = 1, 2, 3, 4\}, \\ S_2 = &\quad \{f \in P(n/d) : t_1 = t_3 = 0,\ T_1(f) = t_2,\ T_2(f) = t_4\}, \end{aligned}$$

Theorem

(Continued)

$$
\begin{aligned}
S_3 = \; & \{f \in P(n/d) : T_1(f) = t_1,\ T_1(f) + T_i(f) = t_i,\ i = 2, 3, \\
& T_2(f) + T_4(f) = t_4\}, \\
S_4 = \; & \{f \in P(n/d) : t_i = 0,\ i = 1, 2, 3,\ T_1(f) = t_4\}, \\
S_5 = \; & \{f \in P(n/d) : T_i(f) = t_i,\ i = 1, 2, 3,\ T_1(f) + T_4(f) = t_4\}, \\
S_6 = \; & \{f \in P(n/d) : t_1 = t_3 = 0,\ T_1(f) = t_2,\ T_1(f) + T_2(f) = t_4\}, \\
S_7 = \; & \{f \in P(n/d) : T_1(f) = t_1,\ T_1(f) + T_i(f) = t_i,\ i = 2, 3, \\
& T_1(f) + T_2(f) + T_4(f) = t_4\}.
\end{aligned}
$$

We use the last theorem and our generalization of Möbius Inversion formula to find the number $N(n, t_1, t_2, t_3, t_4)$.

The Formula For $N(n, t_1, t_2, t_3, t_4)$

Theorem

For even degree n, different values of $N(n, t_1, t_2, t_3, t_4)$ are given as

$$
\begin{aligned}
(i)\, nN(n,1,1,1,0) &= \sum_{\substack{d|n \\ d\equiv 1}} \mu(d) F(n/d,1,1,1,0) + \sum_{\substack{d|n \\ d\equiv 3}} \mu(d) F(n/d,1,0,0,0) \\
&+ \sum_{\substack{d|n \\ d\equiv 5}} \mu(d) F(n/d,1,1,1,1) + \sum_{\substack{d|n \\ d\equiv 7}} \mu(d) F(n/d,1,0,0,1), \\
nN(n,1,0,0,1) &= \sum_{\substack{d|n \\ d\equiv 1}} \mu(d) F(n/d,1,0,0,1) + \sum_{\substack{d|n \\ d\equiv 3}} \mu(d) F(n/d,1,1,1,0) \\
&+ \sum_{\substack{d|n \\ d\equiv 5}} \mu(d) F(n/d,1,0,0,0) + \sum_{\substack{d|n \\ d\equiv 7}} \mu(d) F(n/d,1,1,1,1), \\
nN(n,1,1,1,1) &= \sum_{\substack{d|n \\ d\equiv 1}} \mu(d) F(n/d,1,1,1,1) + \sum_{\substack{d|n \\ d\equiv 3}} \mu(d) F(n/d,1,0,0,1) \\
&+ \sum_{\substack{d|n \\ d\equiv 5}} \mu(d) F(n/d,1,1,1,0) + \sum_{\substack{d|n \\ d\equiv 7}} \mu(d) F(n/d,1,0,0,0),
\end{aligned}
$$

Theorem

(Continued)

$$
\begin{aligned}
nN(n,1,0,0,0) &= \sum_{\substack{d|n \\ d\equiv 1}} \mu(d)F(n/d,1,0,0,0) + \sum_{\substack{d|n \\ d\equiv 3}} \mu(d)F(n/d,1,1,1,1) \\
&+ \sum_{\substack{d|n \\ d\equiv 5}} \mu(d)F(n/d,1,0,0,1) + \sum_{\substack{d|n \\ d\equiv 7}} \mu(d)F(n/d,1,1,1,0), \\
(ii)\, nN(n,0,0,1,0) &= \sum_{\substack{d|n \\ d \ odd}} \mu(d)F\left(n/d,0,0,1,0\right), \\
(iii)\, nN(n,0,0,1,1) &= \sum_{\substack{d|n \\ d \ odd}} \mu(d)F\left(n/d,0,0,1,1\right), \\
(iv)\, nN(n,1,1,0,0) &= \sum_{\substack{d|n \\ d\equiv 1}} \mu(d)F(n/d,1,1,0,0) + \sum_{\substack{d|n \\ d\equiv 3}} \mu(d)F(n/d,1,0,1,0) \\
&+ \sum_{\substack{d|n \\ d\equiv 5}} \mu(d)F(n/d,1,1,0,1) + \sum_{\substack{d|n \\ d\equiv 7}} \mu(d)F(n/d,1,0,1,1),
\end{aligned}
$$

Theorem

(Continued)

$$
\begin{aligned}
nN(n,1,0,1,1) &= \sum_{\substack{d|n \\ d\equiv 1}} \mu(d)F(n/d,1,0,1,1) + \sum_{\substack{d|n \\ d\equiv 3}} \mu(d)F(n/d,1,1,0,0) \\
&+ \sum_{\substack{d|n \\ d\equiv 5}} \mu(d)F(n/d,1,0,1,0) + \sum_{\substack{d|n \\ d\equiv 7}} \mu(d)F(n/d,1,1,0,1), \\
nN(n,1,1,0,1) &= \sum_{\substack{d|n \\ d\equiv 1}} \mu(d)F(n/d,1,1,0,1) + \sum_{\substack{d|n \\ d\equiv 3}} \mu(d)F(n/d,1,0,1,1) \\
&+ \sum_{\substack{d|n \\ d\equiv 5}} \mu(d)F(n/d,1,1,0,0) + \sum_{\substack{d|n \\ d\equiv 7}} \mu(d)F(n/d,1,0,1,0), \\
nN(n,1,0,1,0) &= \sum_{\substack{d|n \\ d\equiv 1}} \mu(d)F(n/d,1,0,1,0) + \sum_{\substack{d|n \\ d\equiv 3}} \mu(d)F(n/d,1,1,0,1) \\
&+ \sum_{\substack{d|n \\ d\equiv 5}} \mu(d)F(n/d,1,0,1,1) + \sum_{\substack{d|n \\ d\equiv 7}} \mu(d)F(n/d,1,1,0,0).
\end{aligned}
$$

Theorem

(Continued) In the following cases, $a \equiv b$ represents $a \equiv b \pmod 4$.

$$(v)\; nN(n,0,1,1,1) = \sum_{\substack{d|n \\ d\equiv 1}} \mu(d)F(n/d,0,1,1,1) + \sum_{\substack{d|n \\ d\equiv 3}} \mu(d)F(n/d,0,1,1,0),$$

$$nN(n,0,1,1,0) = \sum_{\substack{d|n \\ d\equiv 1}} \mu(d)F(n/d,0,1,1,0) + \sum_{\substack{d|n \\ d\equiv 3}} \mu(d)F(n/d,0,1,1,1),$$

$$(vi)\; nN(n,0,0,0,0) = \sum_{\substack{d|n \\ d\ odd}} \mu(d)F(n/d,0,0,0,0) - \sum_{\substack{d|n,\frac{n}{d}\ even \\ d\ odd}} \mu(d)F(n/2d,0,0),$$

$$(vii)\; nN(n,0,0,0,1) = \sum_{\substack{d|n \\ d\ odd}} \mu(d)F(n/d,0,0,0,1) - \sum_{\substack{d|n,\frac{n}{d}\ even \\ d\ odd}} \mu(d)F(n/2d,0,0),$$

Theorem

(Continued) and finally,

$$
\begin{aligned}
(viii)\, nN(n,0,1,0,0) &= \sum_{\substack{d|n \\ d\equiv 1}} \mu(d)F(n/d,0,1,0,0) - \sum_{\substack{d|n,\, \frac{n}{d}\, even \\ d\equiv 1}} \mu(d)F(n/2d,1,0) \\
&+ \sum_{\substack{d|n \\ d\equiv 3}} \mu(d)F(n/d,0,1,0,1) - \sum_{\substack{d|n,\, \frac{n}{d}\, even \\ d\equiv 3}} \mu(d)F(n/2d,1,1), \\
nN(n,0,1,0,1) &= \sum_{\substack{d|n \\ d\equiv 1}} \mu(d)F(n/d,0,1,0,1) - \sum_{\substack{d|n,\, \frac{n}{d}\, even \\ d\equiv 1}} \mu(d)F(n/2d,1,1) \\
&+ \sum_{\substack{d|n \\ d\equiv 3}} \mu(d)F(n/d,0,1,0,0) - \sum_{\substack{d|n,\, \frac{n}{d}\, even \\ d\equiv 3}} \mu(d)F(n/2d,1,0).
\end{aligned}
$$

Theorem

(Continued) and finally,

$$
\begin{aligned}
(viii)\, nN(n,0,1,0,0) &= \sum_{\substack{d|n \\ d\equiv 1}} \mu(d)F(n/d,0,1,0,0) - \sum_{\substack{d|n,\, \frac{n}{d}\, even \\ d\equiv 1}} \mu(d)F(n/2d,1,0) \\
&+ \sum_{\substack{d|n \\ d\equiv 3}} \mu(d)F(n/d,0,1,0,1) - \sum_{\substack{d|n,\, \frac{n}{d}\, even \\ d\equiv 3}} \mu(d)F(n/2d,1,1), \\
nN(n,0,1,0,1) &= \sum_{\substack{d|n \\ d\equiv 1}} \mu(d)F(n/d,0,1,0,1) - \sum_{\substack{d|n,\, \frac{n}{d}\, even \\ d\equiv 1}} \mu(d)F(n/2d,1,1) \\
&+ \sum_{\substack{d|n \\ d\equiv 3}} \mu(d)F(n/d,0,1,0,0) - \sum_{\substack{d|n,\, \frac{n}{d}\, even \\ d\equiv 3}} \mu(d)F(n/2d,1,0).
\end{aligned}
$$

Cosets of $\mathbb{F}_{2^l}$ in $\mathbb{F}_{2^n}$

Let $n = 4l$. For a given $\alpha \in \mathbb{F}_{2^l}$ the linear functional $L_\alpha : \mathbb{F}_{2^l} \longrightarrow \mathbb{F}_2$ is defined as $L_\alpha(\beta) = T_{2^l}(\alpha\beta)$, for all $\beta \in \mathbb{F}_{2^l}$. We define

$$W_0 = \mathrm{Ker}(T_{2^l}) = \{\beta \in \mathbb{F}_{2^l} \mid T_{2^l}(\beta) = 0\},$$

and $W_i(\gamma) = \{\beta \in \mathbb{F}_{2^l} \mid T_i(\beta + \gamma) = T_i(\beta) + T_i(\gamma)\}$, for $i = 1, \ldots, 4$.

For $\gamma \in \mathbb{F}_{2^n}$ there exist three possibilities for $W_i(\gamma)$, where $i = 2, 3, 4$.

Either $W_i(\gamma) = \mathbb{F}_{2^l}$, or $W_i(\gamma) = W_0$, or $W_i(\gamma)$ is a hyperplane different that W_0. In total there exist 27 different cases. We proved that some of these cases are possible. We divide them into three groups, based on W_2.

Table: Group one, $W_2(\gamma) = \mathbb{F}_{2^l}$

W_4 \ W_3	$\mathbb{F}_{2^l}$	W_0	$W_3 \neq W_0, \mathbb{F}_{2^l}$
$\mathbb{F}_{2^l}$	Cat A	N/A	N/A
W_0	Cat A_1	N/A	N/A
$W_4 \neq W_0, \mathbb{F}_{2^l}$	Cat A_2	N/A	N/A

Table: Group two, $W_2(\gamma) = W_0$

W_4 \ W_3	$\mathbb{F}_{2^l}$	W_0	$W_3 \neq W_0, \mathbb{F}_{2^l}$
$\mathbb{F}_{2^l}$	N/A	N/A	N/A
W_0	Cat B_1	Cat C_1	N/A
$W_4 \neq W_0, \mathbb{F}_{2^l}$	Cat B_2	Cat C_2	N/A

Table: Group three, $W_2(\gamma) \neq W_0, \mathbb{F}_{2^l}$

W_4 \ W_3	$\mathbb{F}_{2^l}$	W_0	$W_3 \neq W_0, \mathbb{F}_{2^l}$
$\mathbb{F}_{2^l}$	N/A	N/A	N/A
W_0	Cat F_1	Cat D_1	Cat E_1
$W_4 \neq W_0, \mathbb{F}_{2^l}$	Cat F_2	Cat D_2	Cat E_2

For each category we have some conditions on $\gamma \in \mathbb{F}_{2^n}$. For example, a coset $\gamma + \mathbb{F}_{2^l}$ is in D_1 iff $\hat{\gamma} = \gamma + \gamma^{2^l} + \gamma^{2^{2l}} + \gamma^{2^{3l}} \neq 1$ and either

(i) $T_{2^l}(\hat{\gamma}) = 0$ and $\hat{\gamma}^4 = \hat{\gamma} + 1$, or

(ii) $T_{2^l}(\hat{\gamma}) = 1$ and $\hat{\gamma}^4 = \hat{\gamma}^2 + \hat{\gamma} + 1$.

For $\gamma \in \mathbb{F}_{2^n}$ the coset $\gamma + \mathbb{F}_{2^l}$ is in one of the 13 categories. Then we can compute different traces of an element $\gamma + \beta$ from the coset $\gamma + \mathbb{F}_{2^l}$, where $\beta \in \mathbb{F}_{2^l}$. For example if the coset $\gamma + \mathbb{F}_{2^l}$ is in category D_1, the traces of an element $\gamma + \beta$ are given in the following table.

Table: Traces in Category D_1

$\beta \in \mathbb{F}_{2^l}$ \ $T_i(\beta+\gamma)$	$T_1(\beta+\gamma)$	$T_2(\beta+\gamma)$	$T_3(\beta+\gamma)$	$T_4(\beta+\gamma)$
$\beta \in W_2 \cap W_0$	$T_1(\gamma)$	$T_2(\gamma)$	$T_3(\gamma)$	$T_4(\gamma)$
$\beta \in W_2 \setminus (W_2 \cap W_0)$	$T_1(\gamma)$	$T_2(\gamma)$	$T_3(\gamma)+1$	$T_4(\gamma)$
$\beta \in W_0 \setminus (W_2 \cap W_0)$	$T_1(\gamma)$	$T_2(\gamma)+1$	$T_3(\gamma)$	$T_4(\gamma)$
$\beta \in \mathbb{F}_{2^l} \setminus (W_2 \cup W_0)$	$T_1(\gamma)$	$T_2(\gamma)+1$	$T_3(\gamma)+1$	$T_4(\gamma)$

In different categories $T_i(\gamma+\beta)$, $1 \leq i \leq 4$, is in terms of $T_i(\gamma)$, which is either zero or one. To complete the study, we need to know in each category for how many of the elements γ we have $T_i(\gamma) = 0$, and $T_i(\gamma) = 1$. We expect that $T_i(\gamma)$ depends on m, or l, where $n = 2m = 4l$. Once the conditions are obtained one is able to compute the the exact value of $N(n, t_1, t_2, t_3, t_4)$, where $n = 4l$. Similar results to these studies are then needed for the case $n = 4l + 2$.

An Approximation of $N(n, t_1, t_2, t_3, t_4)$

We have 16 cases for (t_1, t_2, t_3, t_4). In our main theorem these 16 cases are divided to 8 groups, and each group has some of the cases of (t_1, t_2, t_3, t_4) that are connected to each other. Then for different groups the formulas for the number $N(n, t_1, t_2, t_3, t_4)$ are given in terms of $F(n/d, t_1', t_2', t_3', t_4')$'s where $d \mid n$, and (t_1', t_2', t_3', t_4') is from the same group as (t_1, t_2, t_3, t_4). Assume that

$$F(n/d, t_1', t_2', t_3', t_4') = \begin{cases} 2^{\frac{n}{d}-4} & \text{if } \frac{n}{d} \geq 4\ , \\ 0 & \text{otherwise.} \end{cases}$$

We let $n = 2^{k_0} {p_1}^{k_1} \cdots {p_s}^{k_s}$, where $k_0, \ldots, k_s \geq 1$, and $p_1, \ldots, p_s$ are odd prime divisors of n. Assume that $S_1 = \{p_1, \ldots, p_s\}$, and for $2 \leq q \leq s$ let

$S_q = \{d : d \mid n, d \text{ is the product of exactly } q \text{ distinct odd primes } p_i \in S_1\}$

For the first 12 cases of (t_1, t_2, t_3, t_4) which are in groups (i) to (v), the number $N(n, t_1, t_2, t_3, t_4)$ can be given as

$$N(n, t_1, t_2, t_3, t_4) = \frac{1}{n} \left(2^{n-4} + \sum_{q=1}^{s} \sum_{d \in S_q} [n/d \geq 4](-1)^q 2^{n/d-4} \right).$$

For (t_1, t_2, t_3, t_4) from groups (vi) we have $(t_1, t_2, t_3, t_4) = (0, 0, 0, 0)$ and

$$\begin{aligned} N(n,0,0,0,0) &= \frac{1}{n}\left(2^{n-4} + \sum_{q=1}^{s}\sum_{d\in S_q}[n/d \geq 4](-1)^q 2^{n/d-4}\right) \\ &- \frac{1}{n}\left((F(n/d,0,0) + \sum_{q=1}^{s}\sum_{d\in S_q}(-1)^q F(n/2d,0,0)\right). \end{aligned}$$

In group (vii) we have $(t_1, t_2, t_3, t_4) = (0, 0, 0, 1)$ and

$$\begin{aligned} N(n,0,0,0,1) &= \frac{1}{n}\left(2^{n-4} + \sum_{q=1}^{s}\sum_{d\in S_q}[n/d \geq 4](-1)^q 2^{n/d-4}\right) \\ &- \frac{1}{n}\left((F(n/d,0,1) + \sum_{q=1}^{s}\sum_{d\in S_q}(-1)^q F(n/2d,0,1)\right). \end{aligned}$$

Finally in group (*viii*), if $(t_1, t_2, t_3, t_4) = (0, 1, 0, 0)$ then the estimate for $N(n, t_1, t_2, t_3, t_4)$ can be given as

$$\frac{1}{n}\left(2^{n-4} + \sum_{q=1}^{s}\sum_{d\in S_q}(-1)^q[n/d \geq 4]2^{n/d-4} - F(n/2, 1, 0)\right)$$
$$- \frac{1}{n}\left(\sum_{q=1}^{s}\sum_{d\in S_q}(-1)^q([d \equiv 1]F(n/2d, 1, 0) + [d \equiv 3]F(n/2d, 1, 1))\right),$$

and if $(t_1, t_2, t_3, t_4) = (0, 1, 0, 1)$ the estimate for $N(n, t_1, t_2, t_3, t_4)$ is

$$\frac{1}{n}\left(2^{n-4} + \sum_{q=1}^{s}\sum_{d\in S_q}(-1)^q[n/d \geq 4]2^{n/d-4} - F(n/2, 1, 1)\right)$$
$$- \frac{1}{n}\left(\sum_{q=1}^{s}\sum_{d\in S_q}(-1)^q([d \equiv 1]F(n/2d, 1, 1) + [d \equiv 3]F(n/2d, 1, 0))\right).$$

Table: Different values of $N(16, t_1, t_2, t_3, t_4)$, where $t_i = 0, 1$.

Case No.	(t_1, t_2, t_3, t_4)	our estimate	$N(16, t_1, t_2, t_3, t_4)$
1	$(1, 1, 1, 0)$	256	260
2	$(1, 0, 0, 1)$	256	260
3	$(1, 1, 1, 1)$	256	252
4	$(1, 0, 0, 0)$	256	252
5	$(0, 0, 1, 0)$	256	256
6	$(0, 0, 1, 1)$	256	256
7	$(1, 1, 0, 0)$	256	256
8	$(1, 0, 1, 1)$	256	256
9	$(1, 1, 0, 1)$	256	256
10	$(1, 0, 1, 0)$	256	256
11	$(0, 1, 1, 1)$	256	264
12	$(0, 1, 1, 0)$	256	264
13	$(0, 0, 0, 0)$	252.5	240
14	$(0, 0, 0, 1)$	251.5	256
15	$(0, 1, 0, 0)$	252	248
16	$(0, 1, 0, 1)$	252	248
Total		4080	4080

Table: Different values of $N(18, t_1, t_2, t_3, t_4)$, where $t_i = 0, 1$.

Case No.	(t_1, t_2, t_3, t_4)	our estimate	$N(18, t_1, t_2, t_3, t_4)$
1	$(1, 1, 1, 0)$	910	917
2	$(1, 0, 0, 1)$	910	896
3	$(1, 1, 1, 1)$	910	917
4	$(1, 0, 0, 0)$	910	896
5	$(0, 0, 1, 0)$	910	921
6	$(0, 0, 1, 1)$	910	892
7	$(1, 1, 0, 0)$	910	927
8	$(1, 0, 1, 1)$	910	917
9	$(1, 1, 0, 1)$	910	893
10	$(1, 0, 1, 0)$	910	917
11	$(0, 1, 1, 1)$	910	921
12	$(0, 1, 1, 0)$	910	892
13	$(0, 0, 0, 0)$	906.89	913
14	$(0, 0, 0, 1)$	903.5	900
15	$(0, 1, 0, 0)$	906.44	913
16	$(0, 1, 0, 1)$	906.44	900
Total		14543.27	14532

Future Directions

(1) A natural way to extend this problem is completing the counting argument to find $N(n, t_1, t_2, t_3, t_4)$.

(2) Studying the number $N(n, t_1, t_2, t_3, t_4)$, where n is an odd number.

(3) Change the finite field to a general field $\mathbb{F}_q$

(4) Studying the number $N(n, t_1, \ldots, t_k)$, where $4 \leq k \leq n$.

Thank You

References

- L. Carlitz, A theorem of Dickson on irreducible polynomials, *Proc. Amer. Math. Soc.*, **3** (1952), 693-700.
- 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.
- S. D. Cohen, Explicit theorems on generator polynomials, *Finite Fields and Their Applications*, **11** (2005), 337-357.
- S. D. Cohen, M. Presern, Primitive polynomials with prescribed second coefficient, *Glasgow Mathematical Journal Trust*, **48** (2006), 281-307.
- S. D. Cohen, Primitive elements and polynomials with arbitrary trace, *Journal of American Mathematics Society*, **83** (1990), 1???7.

- 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.
- E. N. Kuz???min, 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.)
- R. Lidl and H. Niederreiter, "Finite Fields", Cambridge Univ. Press, Cambridge, second edition, 1994.
- M. Moisio, Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm. Acta Artith., to appear
- 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.

- J.L. Yucas, Irreducible polynomials over finite fields with prescribed trace/prescribed constant term. Finite Fields and Their Applications, **12** (2006), 211-221.
- J. L. Yucas and G. L. Mullen, Irreducible polynomials over GF(2) with prescribed coefficients, *Discrete Mathematics*, **274** (2004), 265-279.
- D. Wan, Generators and irreducible polynomials over finite fields. Math. Comp., **219** (1997), 1195-1212.